ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ: ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

Υπεύθυνος Καθηγητής : Τσιαντής Λεωνίδας

Υπεύθυνος Εργασίας : Κυραγιάννης Γιώργος

ΑΡΤΑ 2005

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

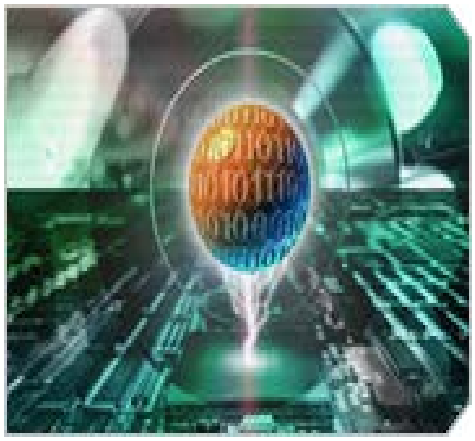
Οι φορητοί υπολογιστές αποτελούν έναν από τους γρηγορότερα εξελισσόμενους τομείς της βιομηχανίας των υπολογιστών. Παραδείγματα αποτελούν τα notebooks, τα laptops και οι προσωπικοί ψηφιακοί βοηθοί *(Personal Digital Assistants - PDAs)*. Πολλοί από τους κατόχους ασύρματων υπολογιστών έχουν παράλληλα και προσωπικούς υπολογιστές γραφείου συνδεδεμένους σε κάποιο τοπικό δίκτυο, το οποίο μπορεί να βρίσκεται είτε στο σπίτι τους, είτε στο χώρο εργασίας τους. Αποτελεί πολύ συνηθισμένη περίπτωση αυτοί οι χρήστες να θέλουν να βρίσκονται συνδεδεμένοι με το δίκτυο αυτό, είτε όταν βρίσκονται σε κάποια άλλη τοποθεσία, είτε καθοδόν. Από τη στιγμή που δεν είναι καθόλου πρακτική η χρήση καλωδίων σε αεροπλάνα, πλοία, ή τραίνα, η έννοια της ασύρματης δικτύωσης αποτελεί μια πολύ ευέλικτη και πρακτική λύση.

Οι χρήσεις των ασύρματων δικτύων είναι πολλές. Η πιο κοινή είναι εκείνη του *φορητού γραφείου*. Οι χρήστες που βρίσκονται στη μέση ενός ταξιδιού πολύ συχνά θέλουν να χρησιμοποιούν τους φορητούς τους υπολογιστές, για να στέλνουν και να λαμβάνουν μηνύματα, τηλεφωνήματα, fax, να συνδέονται με το δίκτυο της εταιρείας τους, κλπ και θέλουν να μπορούν να το κάνουν αυτό, είτε όταν βρίσκονται στην ξηρά, είτε στη θάλασσα, είτε στον αέρα.

Ένα από τα μεγαλύτερα πλεονεκτήματα των ασύρματων τοπικών δικτύων είναι η εύκολη εγκατάσταση. Η τοπική δικτύωση τον υπολογιστών με τη χρήση κεραιών είναι πολύ φθηνότερη και πρακτικότερη από την εισαγωγή ενός συστήματος καλωδίωσης, το οποίο περιλαμβάνει την εισαγωγή καλωδίων μέσα από τοίχους, ταβάνια, κάτω από πατώματα κλπ.

Παρόλο που τα ασύρματα τοπικά δίκτυα έχουν το πολύ ισχυρό πλεονέκτημα της εύκολης εγκατάστασης, έχουν και πολύ σοβαρά μειονεκτήματα. Καταρχήν, χαρακτηρίζονται από πολύ χαμηλότερες χωρητικότητες μεταφοράς δεδομένων από τα αντίστοιχα τοπικά δίκτυα καλωδίου. Δηλαδή, ενώ σε ένα τυπικό δίκτυο Ethernet η ταχύτητα μεταφοράς δεδομένων μπορεί να φθάσει και μέχρι τα 100 Mbps, σε ένα ασύρματο τοπικό δίκτυο η χωρητικότητα δε ξεπερνά τα 1 - 2 Mbps. Ακόμη, η συχνότητα λαθών είναι υψηλότερη και οι παρεμβολές από τις μεταδόσεις γειτονικών σταθμών πολλές.

Η εργασία αυτή αποτελεί μια γνωριμία με τα ασύρματα τοπικά δίκτυα. Χωρίζονται σε τέσσερις ενότητες. Στην πρώτη περιγράφονται τα ασύρματα τοπικά δίκτυα και η ιστορία τους.Στην δεύτερη οι εφαρμογές των ασύρματων τοπικών δικτύων. Η τρίτη ενότητα αναφέρεται στα οπτικά ασύρματα δίκτυα και τέλος η τέταρτη και τελευταία ενότητα αναφέρεται στα πρότυπα των ασύρματων δικτύων (IEEE 802.11 και Bluetooth).



Εικόνα 1

ΚΕΦΑΛΑΙΟ 1

ΟΙ ΔΥΝΑΤΟΤΗΤΕΣ ΑΠΟ ΑΣΥΡΜΑΤΟ ΔΙΚΤΥΟ LANs

1.1 ΓΕΝΙΚΑ

Οι άνθρωποι κινούνται. Τα δίκτυα όχι.

Περισσότερο από τίποτ' άλλο, αυτές οι δύο δηλώσεις μπορούν να εξηγήσουν την έκρηξη του ασύρματου υλικού του τοπικού LAN. Ακριβώς σε μερικά έτη, τα μελλοντικά εισοδήματα από τα ασύρματα προϊόντα του τοπικού LAN θα είναι στα δισεκατομμύρια των δολαρίων. Η τιμή του ασύρματου εργαλείου του τοπικού LAN έχει πέσει κατακόρυφα και συνεχίζει να πέφτει εντυπωσιακά. Ασύρματα LANs είναι τώρα ένα προσάρτημα στο τοπίο δικτύωσης, το οποίο σημαίνει ότι πρέπει να μάθετε να τους εξετάζετε. Τα ασύρματα δίκτυα προσφέρουν διάφορα πλεονεκτήματα πέρα από τα σταθερά (ή "συνδεμένα με καλώδιο") δίκτυα:

- ***Κινητικότητα***

Οι χρήστες κινούνται, αλλά τα δεδομένα αποθηκεύονται συνήθως κεντρικά. Η διευκόλυνση των χρηστών για να έχουν πρόσβαση στα δεδομένα, ενώ είναι σε κίνηση μπορεί να οδηγήσει σε μεγάλα κέρδη παραγωγικότητας.

- ***Ευκολία και ταχύτητα επέκτασης***

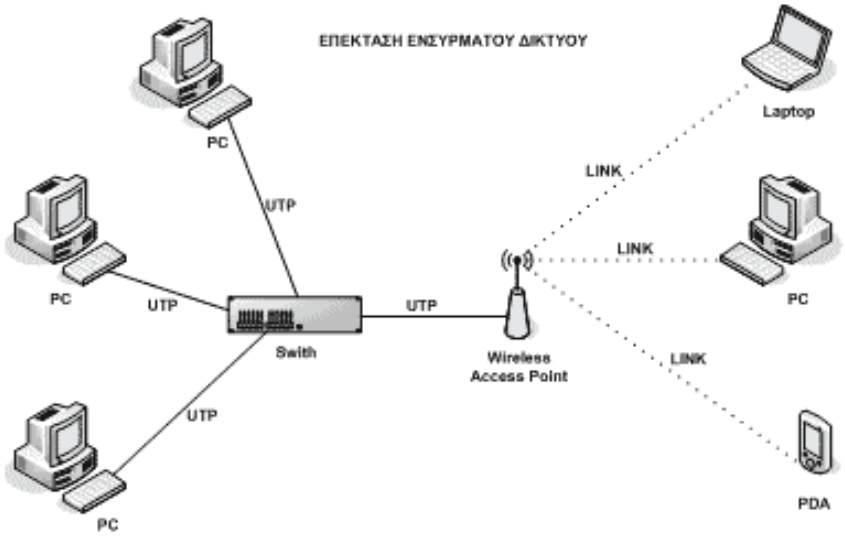
Σε πολλές περιοχές είναι δύσκολο να κατασκευαστούν παραδοσιακά, δηλαδή διασυνδεδεμένα με καλώδιο, LANs. Ιδιαίτερα σε παλαιά κτήρια, όπου ακόμα και τα σχεδιαγράμματα μπορεί να έχουν χαθεί. Αλλά ακόμη και στις σύγχρονες εγκαταστάσεις η διαδικασία της καλωδίωσης είναι ακριβή και χρονοβόρα. Οι περιορισμοί αυτοί υπερβαίνονται από τις τεχνολογίες των ασυρματων δικτύων.

- ***Ευελιξία***

Η έλλειψη καλωδίων δίνει στον χρήστη ευκολία μετακίνησης και παροχή υπηρεσιών δικτύου ακόμα και σε περιοχές όπου δεν υπάρχει η απαραίτητη υποδομή.

- **Κόστος**

Σε μερικές περιπτώσεις, οι δαπάνες μπορούν να μειωθούν με τη χρησιμοποίηση της ασύρματης τεχνολογίας. Ο εξοπλισμός 802.11 μπορεί να χρησιμοποιηθεί για να δημιουργήσει μια ασύρματη γέφυρα μεταξύ δύο κτηρίων. Η σύσταση μιας ασύρματης γέφυρας απαιτεί κάποιο κόστος αρχικού κεφαλαίου από την άποψη του υπαίθριου εξοπλισμού, των σημείων πρόσβασης, και των ασύρματων διεπαφών. Μετά από τις αρχικές κύριες δαπάνες, εντούτοις, η βασισμένη σε δίκτυο 802.11 οπτική επαφή θα έχει μόνο μια αμελητέα επαναλαμβανόμενη μηνιαία λειτουργική δαπάνη. Κατά τη διάρκεια του χρόνου, οι από σημείο σε σημείο ασύρματες συνδέσεις είναι πολύ φτηνότερες από τις ενσύρματες που προσφέρουν οι τηλεφωνικές εταιρείες.



Εικόνα 2 - Μετατροπή και επέκταση ενσύρματου τοπικού δικτύου σε ασύρματο τοπικό δίκτυο

1.2 ΙΣΤΟΡΙΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ο χώρος της ασύρματης επικοινωνίας και των προτύπων, τα οποία θα την καθορίζουν, όμως, βρίσκεται ακόμη στα σπάργανα. Οι μεγαλύτερες εταιρίες έχουν χωριστεί σε ομάδες και αναπτύσσουν ανταγωνιστικές τεχνολογίες με σκοπό την κυριαρχία σε μια αγορά που αναμένεται μέσα στα επόμενα δύο χρόνια να εκτοξευτεί σε μερικά δισεκατομμύρια δολάρια. Ασύρματα δίκτυα υπάρχουν εδώ και αρκετά χρόνια από διάφορους κατασκευαστές, αλλά η ταχύτητα που προσέφεραν (1,5Mbps) ήταν μικρή και δεν υπήρχε συμβατότητα μεταξύ τους. Τα τελευταία χρόνια ο χώρος της ασύρματης επικοινωνίας βρίσκεται σε αναβρασμό: Αναλυτές υποστηρίζουν πότε τη μία και πότε την άλλη τεχνολογία, κάποιες εταιρίες αλλάζουν στρατόπεδα ενώ άλλες εταιρίες παίζουν σε δύο ταμπλό. Η κατάσταση μόλις τώρα δείχνει να σταθεροποιείται κάπως και τα πράγματα αποσαφηνίζονται.

Τα ασύρματα δίκτυα επιτρέπουν σε ηλεκτρονικές συσκευές (από υπολογιστές μέχρι video) να επικοινωνούν μεταξύ τους και να ανταλλάσσουν δεδομένα χωρίς την ύπαρξη καλωδίων. Σε όλα τα νέα πρότυπα ασύρματων δικτύων, εκτός από το πρότυπο IrDA (Infrared Data Association, Σύνδεσμος για τα Υπέρυθρα Δεδομένα), το οποίο ούτως ή άλλως δεν αφορά ασύρματα δίκτυα αλλά ασύρματη επικοινωνία, δεν απαιτείται οπτική επαφή. Σε κάθε ασύρματο δίκτυο υπάρχουν δύο μέρη: η ασύρματη κάρτα δικτύου (wireless LAN adapter), η οποία επικοινωνεί είτε με άλλες συσκευές που έχουν ασύρματη κάρτα δικτύου, είτε με τον πομποδέκτη-κόμβο (Access Point) που λειτουργεί και ως γέφυρα με το ενσύρματο δίκτυο. Η κάρτα δικτύου μοιάζει με μια τυπική κάρτα δικτύου (είτε σε ISA ή PCI για σταθερούς υπολογιστές, είτε σε PC Card για φορητούς) με μια μικρή κεραία, ενώ ο πομποδέκτης έχει τις διαστάσεις ενός βιβλίου και, εκτός από την κεραία, έχει και τα κατάλληλα βύσματα για σύνδεση με σταθερό δίκτυο. Οσον αφορά την ασφάλεια, τα πιο πολλά ασύρματα δίκτυα χρησιμοποιούν επίσης μεθόδους εξουσιοδότησης των συνδεόμενων και κρυπτογράφησης των δεδομένων. Αρκετά πρότυπα χρησιμοποιούν την τεχνική εναλλαγής συχνότητας (frequency hopping) σύμφωνα με την οποία ο κάθε πομποδέκτης αλλάζει συχνότητα μετά την αποστολή/λήψη ενός πακέτου δεδομένων αποφεύγοντας έτσι τα παράσιτα.

Εικόνα 3 - Access Point της Compaq

Το πρότυπο Bluetooth που δημιουργήθηκε από τις Ericsson, IBM, Toshiba, Intel, Nokia και Motorola και υποστηρίζεται από άλλες 1900 εταιρίες, είναι το de facto πρότυπο για μικρών επιδόσεων ασύρματη δικτύωση ηλεκτρονικών συσκευών (κινητά, PDA, PC, εκτυπωτές, fax, modem, πληκτρολόγια κ.τ.λ.) με χαμηλή κατανάλωση (0,01W) και χαμηλό κόστος. Τα δίκτυα αυτά ονομάζονται PAN (Personal Area Networks, Δίκτυα Προσωπικού Χώρου) γιατί σε αντίθεση με τα LAN, ο χώρος ο οποίος καλύπτεται είναι πολύ λίγα μέτρα. Τα PAN έχουν ουσιαστικά σχεδιαστεί με σκοπό την κατάργηση των καλωδίων. Η ταχύτητα μεταφοράς δεδομένων είναι μέχρι 1Mbps ενώ είναι δυνατή και η ταυτόχρονη μεταφορά ήχου. Η συχνότητα που εκπέμπονται τα δεδομένα είναι τα 2,4GHz ενώ χρησιμοποιείται η τεχνική εναλλαγής συχνότητας. Το Bluetooth υποστηρίζει τόσο άμεση επικοινωνία ανάμεσα σε δύο συσκευές (point to point) όσο και επικοινωνία πολλών συσκευών με ένα access point (point to multipoint). Η χωρητικότητά του είναι 8 συσκευές ανά δίκτυο αλλά η μέθοδος εναλλαγής συχνοτήτων (1600 εναλλαγές ανά δευτερόλεπτο σε 79 κανάλια) επιτρέπει σε περισσότερα από 1 δίκτυα να συνυπάρχουν στον ίδιο χώρο. Η ελάχιστη απόσταση ανάμεσα στον πομπό και το δέκτη είναι 10 εκατοστά και η μέγιστη 10 μέτρα. Από πλευράς ασφάλειας, αν και το Bluetooth δεν παρέχει ιδιαίτερα υψηλό επίπεδο, η μικρή του εμβέλεια περιορίζει τον κίνδυνο.

Η κυκλοφορία των συσκευών που υποστηρίζουν το Bluetooth έχει ήδη αρχίσει με τη μορφή κινητών τηλεφώνων και καρτών δικτύου για υπολογιστές. Δεδομένου ότι το κόστος υλοποίησης του Bluetooth είναι πολύ μικρό, μέχρι το τέλος του 2004 το 90% των κινητών τηλεφώνων θα το ενσωματώνει και η επικράτησή του θεωρείται δεδομένη. Εταιρείες όπως η Palm και η Microsoft έχουν ήδη ανακοινώσει υποστήριξη του Bluetooth στα μελλοντικά προϊόντα τους.

Αν το Bluetooth στοχεύει στο να καταργήσει τα καλώδια που συνδέουν τα διάφορα gadgets και περιφερειακά μεταξύ τους και με τον υπολογιστή, το πρωτόκολλο IEEE 802.11b στοχεύει στο να καταργήσει τα καλώδια ανάμεσα στους υπολογιστές. Το 802.11 είναι το όνομα του project της ομάδας εργασίας του IEEE (Institute of Electrical and Electronics Engineers, Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών) για τα ασύρματα δίκτυα. Το IEEE 802.11, το οποίο δημιουργήθηκε τον Ιούνιο του 1997, έχει ταχύτητα 2Mbps και είναι το πρότυπο που ακολουθούσαν μέχρι τώρα τα ασύρματα δίκτυα Ethernet. Η έκδοση IEEE 802.11b (γνωστή και ως IEEE 802.11 High Rate ή Wi-Fi) δημιουργήθηκε τον Ιούλιο του 1998 και έχει ταχύτητα 11Mbps ενώ η έκδοση IEEE 802.11a, που βρίσκεται ακόμη στο στάδιο της ανάπτυξης, προβλέπει ταχύτητες μέχρι 54Mbps. Το IEEE802.11b είναι, ουσιαστικά, το στάνταρ στα ασύρματα δίκτυα Ethernet και υποστηρίζει τόσο επικοινωνία point to point (η οποία ονομάζεται ad hoc) όσο και επικοινωνία point to multipoint. Οι υπολογιστές που βρίσκονται στον ίδιο χώρο, π.χ., μπορούν να οριστούν σε κατάσταση ad hoc και να επικοινωνήσουν άμεσα μεταξύ τους. Η ανάγκη για access point προκύπτει όταν χρειάζεται επικοινωνία με ενσύρματα δίκτυα και/ή περιφερειακά ή στην περίπτωση του roaming (π.χ. όταν ο χρήστης ενός φορητού υπολογιστή πρέπει να κινείται μέσα σ' ένα κτίριο). Μέρος επίσης του 802.11b αποτελεί και το WEP (Wired Equivalent Privacy, μυστικότητα αντίστοιχη με τα καλωδιωμένα δίκτυα) το οποίο χρησιμοποιεί τον αλγόριθμο RC4 και προσφέρει τη δυνατότητα εξουσιοδότησης του κάθε κόμβου και κρυπτογράφησης των δεδομένων. Οπως και το Bluetooth, λειτουργεί και αυτό στα 2,4GHz και χρησιμοποιείται και εδώ η τεχνική εναλλαγής συχνότητας. Η συχνότητα αυτή, η ίδια που χρησιμοποιείται και από τους φούρνους μικροκυμάτων, επιλέχθηκε διότι είναι ελεύθερη και δεν απαιτείται έκδοση αδείας για τις συσκευές που τη χρησιμοποιούν. Η χρήση, όμως, κοινής συχνότητας και από τα δύο πρότυπα μπορεί να δημιουργήσει προβλήματα στην συνύπαρξή τους. Οι παρεμβολές μπορεί να προκύψουν εάν τα δύο δίκτυα βρίσκονται πολύ κοντά και προσπαθούν να λειτουργήσουν ταυτόχρονα. Οι παρεμβολές θα οδηγήσουν σε λάθος μεταφορά των δεδομένων και αυτόματα θα επαναληφθεί η μεταφορά του χαμένου πακέτου σε άλλη συχνότητα. Το Bluetooth, όμως, μεταφέρει μικρότερα πακέτα και δοκιμάζει εναλλακτικές συχνότητες 600 φορές ταχύτερα από το IEEE802.11b, με αποτέλεσμα, ουσιαστικά, το πρώτο να μπλοκάρει το δεύτερο μειώνοντας δραματικά την

ταχύτητά του. Ηδη έχει σχηματιστεί η ομάδα IEEE802.15 η οποία έχει ως σκοπό την ελαχιστοποίηση των παρεμβολών ανάμεσα στα δύο αυτά πρότυπα και την ομαλή τους συνύπαρξη.

Εικόνα 4 - Ασύρματη Κάρτα Δικτύου της Compaq

Μια τρίτη εναλλακτική πρόταση είναι το πρότυπο HomeRF , το οποίο προωθείται από την Proxim (μετοχές της οποίας έχουν η Intel και η Motorola) και για το οποίο έχουν δηλώσει υποστήριξη εταιρίες όπως η Hewlett Packard. Το HomeRF στηρίζεται στην τεχνολογία SWAP (Shared Wireless Access Protocol, μοιραζόμενο ασύρματο πρωτόκολλο πρόσβασης). Το SWAP συνδυάζει στοιχεία από το IEEE802.11 μαζί με ιδέες από το ευρωπαϊκό σύστημα ψηφιακής ασύρματης τηλεφωνίας DECT (Digital Enhanced Cordless Telephone) φτιάχνοντας έτσι ένα φθηνό πρότυπο για μεταφορά ήχου και δεδομένων με ταχύτητα μέχρι 2Mbps. Αν και το HomeRF υποστηρίζει ταυτόχρονη μεταφορά ήχου και δεδομένων, η χαμηλή ταχύτητα που προσφέρει σε συνδυασμό με το κόστος υλοποίησής του, που είναι παρόμοιο με αυτό του IEEE802.11b, δεν του δίνει ιδιαίτερες προοπτικές επιτυχίας. Τα υπόλοιπα τεχνικά χαρακτηριστικά του HomeRF είναι ίδια με αυτά του IEEE802.11 έχοντας τα ίδια προβλήματα παρεμβολών με το Bluetooth.

Η τελευταία εναλλακτική πρόταση είναι το πρότυπο HiperLAN το οποίο αναπτύσσεται από το ETSI (European Telecommunications Standardization Institute, Ευρωπαϊκό Ινστιτούτο Τυποποίησης Τηλεπικοινωνιών) και υποστηρίζεται από διάφορες εταιρίες του χώρου. Μέχρι στιγμής προϊόντα που να στηρίζονται στο πρότυπο HiperLAN έχουν αναγγελθεί από μία μόνο εταιρία, αλλά έντονο ενδιαφέρον για την υλοποίησή του έχουν εκδηλώσει πολλές ακόμη εταιρίες. Το HiperLAN υπάρχει σε δύο εκδόσεις, τη HiperLAN

Type 1 που τυποποιήθηκε το 1996 και υποστηρίζει ταχύτητες μέχρι 24Mbps και τη HiperLAN Type 2, η ανάπτυξη της οποίας δεν έχει ακόμη ολοκληρωθεί και που θα υποστηρίζει ταχύτητες μέχρι 54Mbps. Αμφότερες οι εκδόσεις του HiperLAN χρησιμοποιούν τη συχνότητα των 5GHz, η οποία στην Αμερική και στην Ιαπωνία είναι ελεύθερη και στην Ευρώπη έχει επισήμως παραχωρηθεί για χρήση από τα ασύρματα δίκτυα, με αποτέλεσμα αφενός μεν να μη δημιουργούνται προβλήματα με τα δίκτυα που τρέχουν στα 2,4GHz και αφετέρου οι συσκευές HiperLAN να μπορούν να χρησιμοποιηθούν σε οποιοδήποτε μέρος του κόσμου χωρίς τροποποιήσεις. Μια άλλη ιδιαιτερότητα του HiperLAN είναι επίσης το ad hoc roaming, η δυνατότητα δηλαδή της αυτόματης προώθησης των δεδομένων από access point σε access point σε περίπτωση που ο παραλήπτης δεν βρίσκεται στο βεληνεκές του αποστολέα. Εκτός από αυτό, η υπεροχή στην ταχύτητα και η δυνατότητα QoS (Quality Of Service, Ποιότητα Υπηρεσιών) που μόνο το HiperLAN έχει από τα πρότυπα ασύρματης δικτύωσης. Με το QoS μπορούν τα πακέτα δεδομένων να κατηγοριοποιούνται και να αποκτούν διαφορετική σειρά προτεραιότητας ανάλογα με το είδος τους. Ετσι, τα πακέτα που αφορούν ένα video π.χ., μπορεί να έχουν μεγαλύτερη προτεραιότητα κατά τη μεταφορά, με αποτέλεσμα την πιο ομαλή εμφάνισή του. Το HiperLAN2, σε αντίθεση με όλα τα υπόλοιπα πρότυπα, είναι συμβατό με μια τεράστια ποικιλία δικτύων γιατί, εκτός από το να συνδέεται με δίκτυα Ethernet, έχει τη δυνατότητα και για μεταφορά πακέτων IP, Firewire, ATM, UMTS κ.ά.

Απ' όλες τις παραπάνω εναλλακτικές, το Bluetooth είναι αυτό που αναμένεται να έχει την πιο άμεση επικράτηση, κυρίως λόγω του χαμηλού του κόστους και της ευκολίας που προσφέρει. Οι υπόλοιπες από τις παραπάνω λύσεις δεν έχουν ως σκοπό την άμεση αντικατάσταση του πατροπαράδοτου καλωδιωμένου Ethernet, λόγω της δυσανάλογης σχέσης κόστους/ταχύτητας που έχουν αυτή τη στιγμή, αλλά και των χαμηλών επιδόσεων. Πολύ σύντομα όμως η ασύρματη δικτύωση θα μπει στη ζωή μας και θα την αλλάξει ριζικά. Η εξάλειψη των καλωδίων θα δώσει τη δυνατότητα στους κατασκευαστές να αλλάξουν (επιτέλους) την κλασική εικόνα του υπολογιστή.

Θα μπορούμε πλέον κάθε φορά να τοποθετούμε τον εκτυπωτή στο βολικότερο για μας σημείο, βγάζοντάς τον από την πρίζα, πηγαίνοντάς τον στην άλλη άκρη του δωματίου,

ενώ θα έχουμε τη δυνατότητα να τοποθετούμε ελεύθερα τον υπολογιστή σε απόσταση από τη θέση που καθόμαστε. Ετσι, σιγά-σιγά, το PC θα μπορέσει να αφομοιωθεί από τον περιβάλλοντα χώρο.

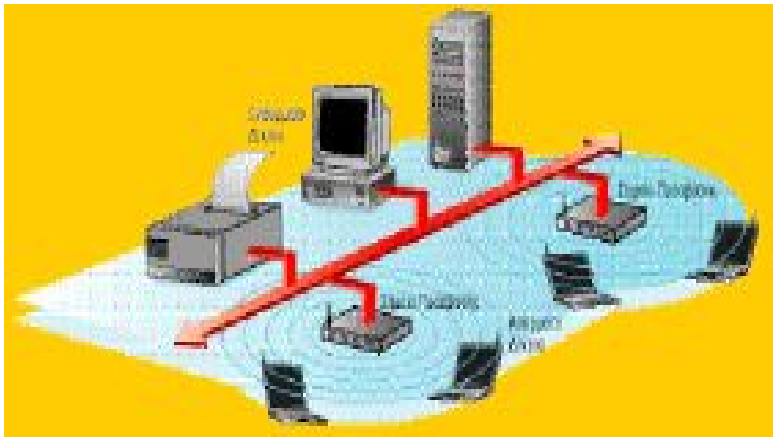
	Bluetooth	**HomeRF**	**802.11**	**802.11b**	**802.11a**	**HiperLAN1**	**HiperLAN2**
Ταχύτητα	1Mbps	2Mbps	2Mbps	11Mbps	54Mbps	24Mbps	54Mbps
Εμβέλεια	10μ	50μ	100μ	100μ	100μ	50μ	30-150μ
Συχνότητα	2,4GHz	2,4GHz	2,4GHz	2,4GHz	5GHz	5GHz	5GHz
Διασύνδεση	Καμία	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet, ATM, IP, UMTS, Firewire, PPP
Κατάσταση	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο		Διαθέσιμο	
Υποστηρικτές	Ericsson, IBM, Toshiba, Intel, Nokia, Motorola	Proxim, Intel, HP, 3COM, Motorola		Cisco, Lucent, 3Com, Apple, Compaq, Zoom, Dell, Nokia		ETSI, Proxim, HP, Xircom, IBM, Nokia	ETSI, HP, Xircom, IBM, TI, Dell, Ericsson, Nokia, Proxim

Πίνακας 1 - Πρότυπα Ασύρματης δικτύωσης

1.3 ΤΟΠΙΚΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Μέχρι πρόσφατα, τα ασύρματα τοπικά δίκτυα δεν είχαν μεγάλη ζήτηση. Μερικές από τις αιτίες ήταν το υψηλό κόστος, η χαμηλή χωρητικότητα μεταφοράς δεδομένων, η απαίτηση κατοχής ειδικής άδειας για τη μετάδοση σε συγκεκριμένες περιοχές συχνοτήτων, κλπ. Με την αντιμετώπιση όμως όλων αυτών των προβλημάτων η δημοτικότητα της ασύρματης τοπικής δικτύωσης αυξήθηκε σημαντικά.

Στο τμήμα αυτό θα μιλήσουμε για πολλά από τα θέματα που αφορούν τα ασύρματα τοπικά δίκτυα υπολογιστών. Θα κινηθούμε από την αναφορά των χρήσεων που μπορεί να έχει ένα ασύρματο τοπικό δίκτυο, μέχρι την περιγραφή διαφόρων τεχνολογιών, όπως τα οπτικά ασύρματα δίκτυα (IR LANs) και τα ασύρματα δίκτυα και τα προτυπά τους (802.11 & Bluetooth)



Εικόνα 5: Τοπικό Ασύρματο δίκτυο.

ΚΕΦΑΛΑΙΟ 2

ΕΦΑΡΜΟΓΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

2.1 ΓΕΝΙΚΑ

Τέσσερις περιοχές εφαρμογής των ασύρματων τοπικών δικτύων είναι:

- Η χρήση τους ως η επέκταση ενός τοπικού δικτύου
- Η χρήση τους στη διασύνδεση τοπικών δικτύων που βρίσκονται σε διαφορετικά κτίρια
- Η νομαδική πρόσβαση και
- Η δικτύωση Ad Hoc

ΕΦΑΡΜΟΓΕΣ ΤΗΣ WLAN ΤΕΧΝΟΛΟΓΙΑΣ

Υπάρχουν ποικίλες εφαρμογές για WLANs. Αυτά τα προϊόντα καλύπτουν τις ίδιες ανάγκες πελατών με τα καλωδιωμένα LANs (εκτός από την χαμηλότερη μέγιστη ταχύτητα μεταφοράς δεδομένων) και λύνουν τα ίδια επιχειρησιακά προβλήματα. Εντούτοις, η κινητικότητα και η ευελιξία, τα οποία είναι έμφυτα σε WLANs, επιτρέπουν την υποστήριξη πρόσθετων εφαρμογών.
Οι πρόσφατες εξελίξεις στην αγορά έχουν επεκτείνει την ανάγκη χρήσης ασύρματου LAN σε νέους τύπους πελατών όπως τα πανεπιστήμια και τα σπίτια. Εκτός από τις ιδιωτικές εγκαταστάσεις WLAN, διάφοροι ISPs παρέχουν πρόσβαση WLAN σε δημόσιες περιοχές, π.χ., τους αερολιμένες, τα εστιατόρια και τα ξενοδοχεία, επιτρέποντας την πρόσβαση στο Διαδίκτυο.

Ο αριθμός των εφαρμογών ενός ασύρματου δικτύου περιορίζεται μόνο από την φαντασία. Έτσι ασύρματα δίκτυα μπορούμε να έχουμε σε:

- **Νοσοκομεία**: Το προσωπικό αποκτά πρόσβαση σε ζωτικές πληροφορίες για τον ασθενή, σε πραγματικό χρόνο από οπουδήποτε.

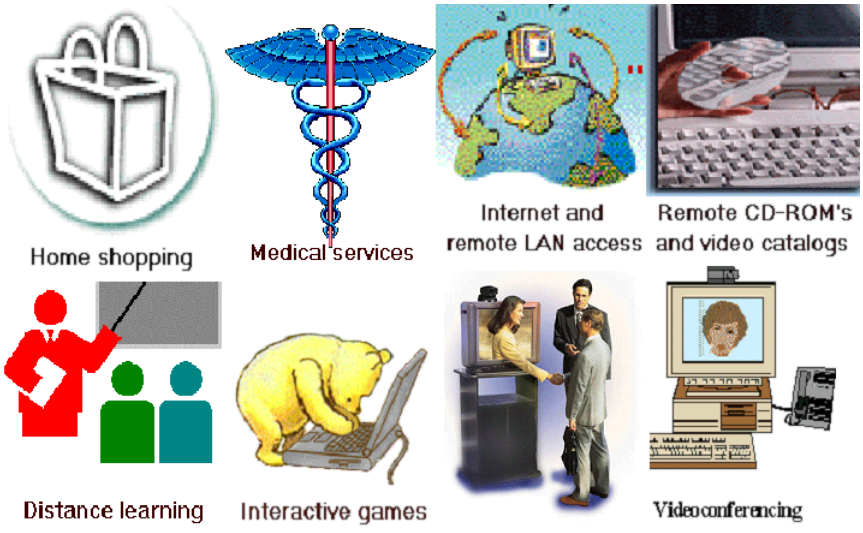
- **Εργοστασιακό περιβάλλον**: Επικοινωνία πραγματικού χρόνου ανάμεσα σε προσωπικό – μηχανές για έλεγχο, διάγνωση, συντήρηση.

- **Εμπόριο**: Τιμολόγηση προϊόντων. Προβολή διαφημιστικών – πληροφοριακών μηνυμάτων σε εμπορικά κέντρα.

- **Εκπαίδευση**: Σε πανεπιστήμια, σχολεία, πρόσβαση μαθητών σε βιβλιοθήκες, εκπαιδευτικό υλικό, βάσεις δεδομένων.

- **Εργασία**: Ευέλικτη, χαμηλού κόστους δικτύωση σε περιπτώσεις όπου οι εναλλακτικές λύσεις είναι δύσκολα υλοποιήσιμες ή και αδύνατες. Ευελιξία στην πρόσβαση στην πληροφορία, ευκολία λήψης αποφάσεων, αυξημένη παραγωγικότητα.

- **Πρόσβαση**: Σε σημεία υψηλής κίνησης (Hot Spots), όπως αεροδρόμια, εμπορικά καταστήματα, συνεδριακά κέντρα, σημεία ψυχαγωγίας, προσφέρει ενημέρωση, διαφήμιση, ψυχαγωγία.



Εικόνα 5 - Παραδείγματα εφαρμογών της WLAN τεχνολογίας

ΟΦΕΛΗ, ΠΛΕΟΝΕΚΤΗΜΑΤΑ & ΠΡΟΒΛΗΜΑΤΑ

Σε μια πρόσφατη μελέτη της InfoTech, τα περισσότερο συχνά αναφερόμενα οφέλη από τη χρήση WLANs συνοψίζονται στα εξής:

1. Ένας χρήστης είναι συνδεδεμένος συνεχώς με το δίκτυο, χωρίς καλώδια και σε πλήρη κινητικότητα, απολαμβάνοντας την δυνατότητα κάλυψης και τη λειτουργία Ethernet, αποφεύγοντας μάλιστα το χάος που μπορεί να δημιουργηθεί από την ύπαρξη καλωδίων.

2. Οι χρήστες είναι σε θέση να κάνουν οτιδήποτε θα μπορούσαν να κάνουν με ένα σταθερό δίκτυο: αποστολή και λήψη ηλεκτρονικού ταχυδρομείου, ανάκτηση και αποστολή εγγράφων, πρόσβαση σε τοπικές βάσεις δεδομένων.

3. Οι χρήστες μπορούν να περιπλανηθούν χωρίς διακοπή της σύνδεσής τους μέσα σε μια περιοχή, καθώς και να περιπλανηθούν από περιοχή σε περιοχή

4. Τα WLANs ανοίγουν νέους ορίζοντες στον τρόπο εργασίας μέσα στις ομάδες.

5. Οι οργανώσεις επίσης χρησιμοποιούν WLANs για να ενισχύσουν τα λειτουργικά περιβάλλοντα εργασίας, που παρέχουν στους χρήστες τη δυνατότητα να εργαστούν οπουδήποτε στην περιοχή ή την πανεπιστημιούπολη, μέσα και έξω από τα κτίρια, παρέχοντας μέγιστη ευελιξία.

2.2 ΕΠΕΚΤΑΣΗ ΤΟΠΙΚΟΥ ΔΙΚΤΥΟΥ

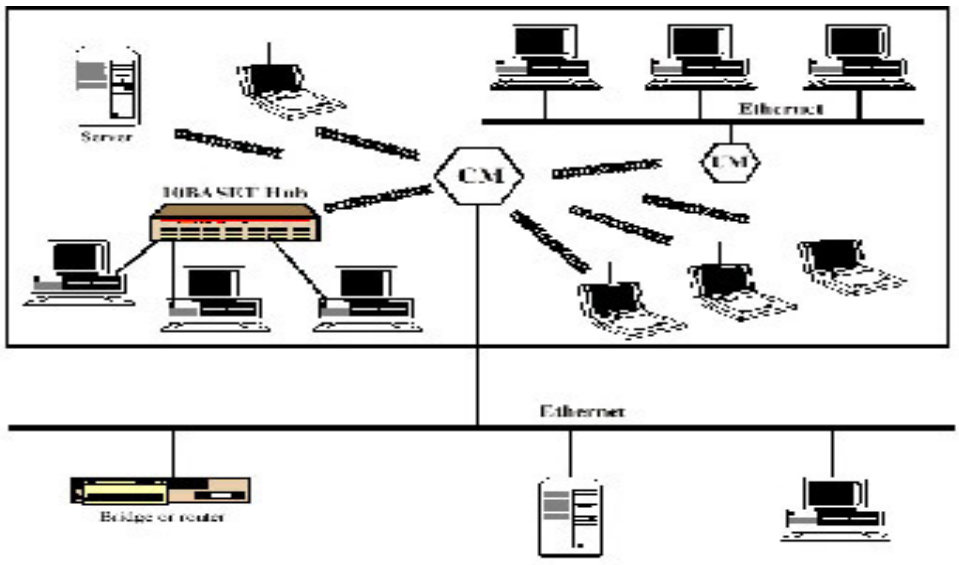
Παλαιότερα, τα ασύρματα τοπικά δίκτυα θεωρούνταν ως ένα *υποκατάστατο* των τοπικών δικτύων με καλώδιο. Με ένα ασύρματο τοπικό δίκτυο αποφεύγονται τα διάφορα έξοδα που σχετίζονται με την εγκατάσταση της καλωδίωσης και παράλληλα διευκολύνονται οι λειτουργίες της αναδιάρθρωσης - ανακατάταξης της δικτυακής υποδομής (όταν βέβαια αυτή χρειάζεται να λάβει χώρα).

Ωστόσο, αυτό το πολύ σημαντικό κίνητρο για τη χρήση των ασύρματων τοπικών δικτύων επικαλύφθηκε από μια σειρά άλλων γεγονότων. Καταρχήν, καθώς η ανάγκη για τοπική δικτύωση γινόταν ολοένα και μεγαλύτερη, τα νέα κτίρια σχεδιάζονταν με τέτοιο τρόπο ώστε να μπορούν να συμπεριλάβουν επιπλέον καλωδίωση για εφαρμογές δεδομένων. Επίσης, με την εξέλιξη της τεχνολογίας στη μετάδοση των δεδομένων, άρχισε να υπάρχει μια αυξανόμενη εμπιστοσύνη στην καλωδίωση σύστροφου ζεύγους (twisted pair). Κατά συνέπεια, η χρήση των ασύρματων τοπικών δικτύων ως οι αντικαταστάτες των τοπικών δικτύων με καλώδιο δε γνώρισε μεγάλη αποδοχή.

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

- Περιβάλλοντα μεγάλων εκτάσεων, όπως οι χώροι παραγωγής ενός εργοστασίου ή μιας αποθήκης.
- Πολύ παλιά κτίρια, στα οποία είτε το άνοιγμα τρυπών στους τοίχους απαγορεύεται, είτε η καλωδίωση είναι ανεπαρκής ή ανύπαρκτη
- Μικρά γραφεία, όπου η εγκατάσταση και η συντήρηση ενός δικτύου με καλώδιο είναι αντιοικονομική

Σε όλες αυτές τις περιπτώσεις, ένα ασύρματο δίκτυο αποτελεί μια αποδοτική και ελκυστική εναλλακτική λύση. Στις περισσότερες από αυτές τις περιπτώσεις, θα υπάρχει επίσης και ένα δίκτυο με καλώδιο το οποίο θα πρέπει να διασυνδεθεί με ένα ασύρματο δίκτυο. Για παράδειγμα, είναι πολύ συνηθισμένο μια εργοστασιακή επιχείρηση να αποτελείται από ένα χώρο γραφείων, ο οποίος βρίσκεται ξεχωριστά από το χώρο παραγωγής, αλλά πρέπει να είναι συνδεδεμένος με αυτόν, έτσι ώστε να παρέχονται δικτυακές υπηρεσίες στο προσωπικό (π.χ. παρακολούθηση των χώρων λειτουργίας από τον επόπτη, ηλεκτρονική διαχείριση της αποθήκης κλπ). Μια τυπική λύση στην περίπτωση αυτή είναι η σύνδεση ενός ενσύρματου με ένα ασύρματο τοπικό δίκτυο, με το πρώτο να βρίσκεται στο χώρο των γραφείων και το δεύτερο στο χώρο της παραγωγής. Ο τύπος αυτός της εφαρμογής των ασύρματων τοπικών δικτύων αναφέρεται ως *επέκταση τοπικού δικτύου*. Στο παρακάτω σχήμα δίδεται ένα παράδειγμα.



Εικόνα 6 - Χρήση ενός ασύρματου δικτύου ως επέκταση ενός παραδοσιακού (ενσύρματου) τοπικού δικτύου

Στο παραπάνω σχήμα βλέπουμε μια εγκατάσταση ενός ασύρματου δικτύου. Υπάρχει μια «ραχοκοκαλιά» (backbone) ενός παραδοσιακού τοπικού δικτύου (με καλωδίωση δηλαδή, όπως Ethernet), στην οποία βρίσκονται συνδεδεμένοι οι διακομιστές, μερικοί σταθμοί εργασίας και οπωσδήποτε μερικές συσκευές διασύνδεσης τοπικών δικτύων, όπως γέφυρες και δρομολογητές. Επιπρόσθετα, υπάρχουν και δύο *υπομονάδες:* η *υπομονάδα ελέγχου (Control Module - CM)* και η *υπομονάδα χρήστη (User Module - UM).* Η CM εκτελεί τις λειτουργίες είτε μιας γέφυρας, είτε ενός δρομολογητή, δια-συνδέοντας το ασύρματο δίκτυο με τη ραχοκοκαλιά και η UM αποτελεί μια οποιαδήποτε *συσκευή χρήστη,* η οποία μπορεί να χρησιμοποιηθεί για τη δια-σύνδεση ενός τοπικού δικτύου με ένα άλλο (όπως ένα hub, ένας δρομολογητής, μια γέφυρα, κλπ).

2.2 ΔΙΑ-ΚΤΙΡΙΑΚΗ ΔΙΑΣΥΝΔΕΣΗ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Μία άλλη χρήση των ασύρματων τοπικών δικτύων βρίσκεται στη σύνδεση τοπικών δικτύων (ασύρματων ή μη) που βρίσκονται σε διπλανά κτίρια. Στην περίπτωση αυτή,

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

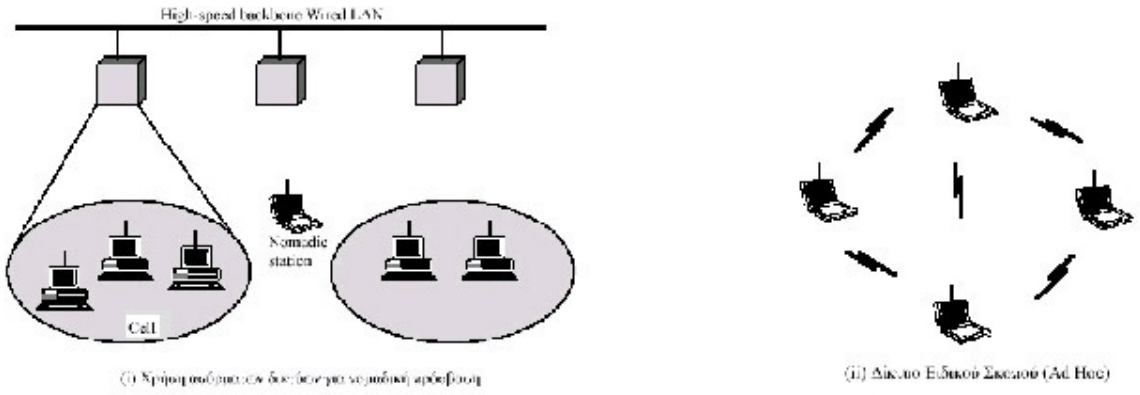
2.3 ΝΟΜΑΔΙΚΗ ΠΡΟΣΒΑΣΗ

Η νομαδική πρόσβαση παρέχει μία ασύρματη σύνδεση μεταξύ ενός τοπικού δικτύου και ενός φορητού υπολογιστή, ο οποίος είναι εξοπλισμένος με μια κεραία, όπως είναι ένα laptop ή ένα notepad. Ένα παράδειγμα χρήσης μιας τέτοιου είδους σύνδεσης είναι να μπορεί ένας υπάλληλος που γυρίζει από ένα ταξίδι να μεταφέρει πληροφορίες από τον προσωπικό του υπολογιστή στον υπολογιστή στο γραφείο του. Η νομαδική πρόσβαση είναι επίσης χρήσιμη και σε χώρους όπως μια επιχείρηση, ή μια πανεπιστημιούπολη, στους οποίους τα κτίρια βρίσκονται συγκεντρωμένα ανά ομάδες. Στις περιπτώσεις αυτές, οι χρήστες μπορούν να μετακινούνται μέσα στο χώρο της επιχείρησης ή του πανεπιστημίου και με τους φορητούς υπολογιστές τους να προσπελαύνουν αρχεία των servers και των υπολογιστών που βρίσκονται συνδεδεμένοι σε κάποιο τοπικό δίκτυο.

2.4 ΔΙΚΤΥΩΣΗ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ

Μία ακόμη χρήση των ασύρματων δικτύων είναι εκείνη της δικτύωσης ειδικού σκοπού ή αλλιώς της Ad Hoc Networking. Στην περίπτωση αυτή δεν υπάρχει κάποιος κεντρικός υπολογιστής που να διαχειρίζεται το δίκτυο, αλλά απλά οι υπολογιστές είναι συνδεδεμένοι ο ένας με τον άλλο. Δίκτυα τέτοιου είδους συνήθως εγκαθίστανται προσωρινά και έχουν ως σκοπό την εξυπηρέτηση μιας άμεσης ανάγκης. Για παράδειγμα, μπορούμε να σκεφτούμε την περίπτωση όπου μια ομάδα υπαλλήλων συνδέουν τους φορητούς υπολογιστές τους, ώστε να εξυπηρετηθούν οι ανάγκες μιας on-line σύσκεψης ή παρουσίασης, όπου σε έναν υπολογιστή θα γίνεται η παρουσίαση και οι υπόλοιποι θα μπορούν να την παρακολουθούν από τους προσωπικούς τους υπολογιστές.

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



Εικόνα 7 - Σύγκριση δύο εφαρμογών ασύρματων δικτύων

2.5 ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ – ΑΝΑΓΚΑΙΕΣ ΠΡΟΥΠΟΘΕΣΕΙΣ

Ένα ασύρματο δίκτυο θα πρέπει να πληροί ορισμένες προϋποθέσεις, όπως της υψηλής χωρητικότητας, της ικανότητας κάλυψης μικρών αποστάσεων, της πλήρους συνδεσιμότητας και της δυνατότητας εκπομπής (broadcasting). Επιπρόσθετα, υπάρχουν και μερικές άλλες προϋποθέσεις, που θα πρέπει να πληρούνται αποκλειστικά από τα ασύρματα τοπικά δίκτυα. Παρακάτω παραθέτουμε τις περισσότερο σημαντικές:

- **Αποδοτική χρήση του μέσου μετάδοσης:** Το πρωτόκολλο ελέγχου πρόσβασης στο μέσο, θα πρέπει να κάνει όσο το δυνατόν αποδοτικότερη χρήση του ασύρματου μέσου μετάδοσης, έτσι ώστε να μεγιστοποιείται η χωρητικότητα.
- **Αριθμός Κόμβων:** Τα ασύρματα δίκτυα θα πρέπει να μπορούν να υποστηρίζουν συνδέσεις σε τοπικό δίκτυο μέχρι και εκατοντάδων κόμβων διαμέσου πολλών κελιών.

- **Σύνδεση σε ραχοκοκαλιά τοπικού δικτύου:** Στις περισσότερες περιπτώσεις είναι απαραίτητο το ασύρματο δίκτυο να μπορεί να διασυνδεθεί με σταθμούς εργασίας που βρίσκονται σε κάποιο τοπικό δίκτυο «ραχοκοκαλιάς». Για δομημένα ασύρματα δίκτυα αυτό μπορεί εύκολα να επιτευχθεί με τη χρήση υπομονάδων ελέγχου, οι οποίες συνδέονται και στους δύο τύπους τοπικών δικτύων. Είναι επίσης πιθανό να πρέπει να προβλεφθεί και η περίπτωση εξυπηρέτησης «κινητών» χρηστών καθώς επίσης και περιπτώσεις Ad Hoc δικτύωσης.

- **Περιοχή Εξυπηρέτησης (Service area):** Ένα συνηθισμένο ασύρματο τοπικό δίκτυο θα πρέπει να μπορεί να εξυπηρετήσει χρήστες, που βρίσκονται σε διάμετρο από 100 μέχρι 300 μέτρα από τους κεντρικούς υπολογιστές.

- **Οικονομική κατανάλωση ενέργειας μπαταρίας:** Οι «κινητοί» χρήστες χρησιμοποιούν φορητούς υπολογιστές οι οποίοι χρειάζεται να έχουν μια αρκετά μεγάλη διάρκεια ζωής μπαταρίας. Αυτό υπονοεί ότι ένα πρωτόκολλο ελέγχου πρόσβασης στο διαμοιραζόμενο μέσο (MAC protocol), δε θα απαιτεί από τους κινητούς κόμβους να εποπτεύουν συνεχώς τα σημεία πρόσβασης στο μέσο, όπως συμβαίνει στα κλασσικά πρωτόκολλα MAC, έτσι ώστε να εξοικονομείται όσο το δυνατόν περισσότερη ενέργεια για περισσότερο ουσιαστικές λειτουργίες.

2.6 ΤΕΧΝΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Τα ασύρματα δίκτυα μπορούν να κατηγοριοποιηθούν ανάλογα με την τεχνική μετάδοσης δεδομένων που χρησιμοποιούν. Τα προϊόντα ασύρματης δικτύωσης που κυκλοφορούν στην αγορά σήμερα ανήκουν σε μια από τις παρακάτω κατηγορίες:

- **Ασύρματα δίκτυα υπέρυθρων ακτινών (InfraRed - IR LANs).** Τοπικά δίκτυα αυτού του τύπου περιορίζονται σε ένα δωμάτιο ή γενικότερα σε έναν κλειστό χώρο, μιας και οι υπέρυθρες ακτίνες δε μπορούν να διαπεράσουν τοίχους. Η περιοχή συχνοτήτων για αυτού του τύπου τα δίκτυα είναι από 10^{12} - 6 x 10^{14} Hz.

- **Ασύρματα δίκτυα διασποράς φάσματος (Spread Spectrum LANs).** Ασύρματα τοπικά δίκτυα αυτού του τύπου κάνουν χρήση της τεχνολογίας *διασποράς φάσματος* ή αλλιώς της τεχνολογίας Spread Spectrum. Στις περισσότερες των περιπτώσεων, τα δίκτυα αυτά δε χρειάζονται ειδική άδεια λειτουργίας, μιας και λειτουργούν στις *Βιομηχανικές, Επιστημονικές και Ιατρικές (Industrial, Scientific and Medical - ISM)* περιοχές συχνοτήτων, όπου δεν απαιτείται ειδική άδεια λειτουργίας. Οι περιοχές αυτές αριθμούνται σε τρεις και κυμαίνονται από 902 - 928 MHz, από 2,4 - 2,4835 GHz και από 5,725 - 5,85 GHz.
- **Ασύρματα δίκτυα μικροκυμάτων στενής ζώνης (Narrowband Microwave).** Αυτού του τύπου τα δίκτυα λειτουργούν σε συχνότητες μικροκυμάτων (υψηλές - της τάξεως των 3 - 100 GHz). Αναφορικά με τη λειτουργία τους, δε χρησιμοποιούν την τεχνολογία διασποράς φάσματος και επίσης χρειάζονται ειδική άδεια λειτουργίας, αν εκπέμπουν σε συχνότητες εκτός της Βιομηχανικής, Επιστημονικής και Ιατρικής περιοχής συχνοτήτων.

Περιγραφή	Συχνότητα	Μήκος Κύματος
HF	3 - 30MHz	100 - 10m
VHF	30 - 300MHz	10 - 1m
UHF	300 -3000MHz	1m - 10cm
Μικροκύματα	3×10^9 - 10^{12} Hz	10cm - 3mm
Millimeter Waves	$10^{11} - 10^{12}$Hz	3mm - 0.3mm
Υπέρυθρες Ακτίνες	10^{12} 6×10^{14}Hz	0.3mm 0.5μm
Ορατό Φως	6×10^{14} 8×10^{14}Hz	0.5 μm 0.4μm
Ultra - Violet	$8 \times 10^{14} - 10^{17}$Hz	0.4μm - 10^{-9}m
Ακτίνες X	$10^{17} - 10^{19}$Hz	10^{-9}m - 10^{-11}m
Ακτίνες Γάμμα	$> 10^{19}$Hz	$< 10^{-11}$m

Πίνακας 2 - Οι συχνότητες και τα μήκη κύματος των διαφόρων περιοχών συχνοτήτων

ΚΕΦΑΛΑΙΟ 3

ΟΠΤΙΚΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ(InfraRed - IR LANs)

3.1 ΓΕΝΙΚΑ

Η οπτική ασύρματη τεχνολογία κατέχει ορισμένα χαρακτηριστικά που ταιριάζουν απόλυτα σε ασύρματα δίκτυα εσωτερικών χώρων. Οι οπτικοί πομποί και δέκτες μπορούν να κατασκευαστούν με σχετικά χαμηλό κόστος, έχουν σχετικά μικρό μέγεθος και χαμηλές απαιτήσεις κατανάλωσης ενέργειας. Η χαμηλή κατανάλωση ενέργειας είναι ένας ιδιαίτερα σημαντικός παράγοντας σε περιβάλλοντα όπου η λειτουργία των εξαρτημάτων γίνεται με μπαταρίες. Ακόμη, οι οπτικοί διαμορφωτές / αποδιαμορφωτές (optical modems) είναι πολύ φθηνότεροι στην κατασκευή απ' ότι ο RF εξοπλισμός, με κόστος κοντά στο κόστος κατασκευής των modems καλωδίου. Επιπλέον, οι υπέρυθρες μεταδόσεις δεν παρεμβάλλονται από μεταδόσεις συστημάτων RF (όπως π.χ. με τη ραδιοφωνική λήψη) και οι περιοχές συχνοτήτων στις οποίες λειτουργούν δεν υπόκεινται στις ρυθμίσεις της FCC, οπότε και δίκτυα αυτού του τύπου μπορούν να λειτουργήσουν χωρίς ειδική άδεια.

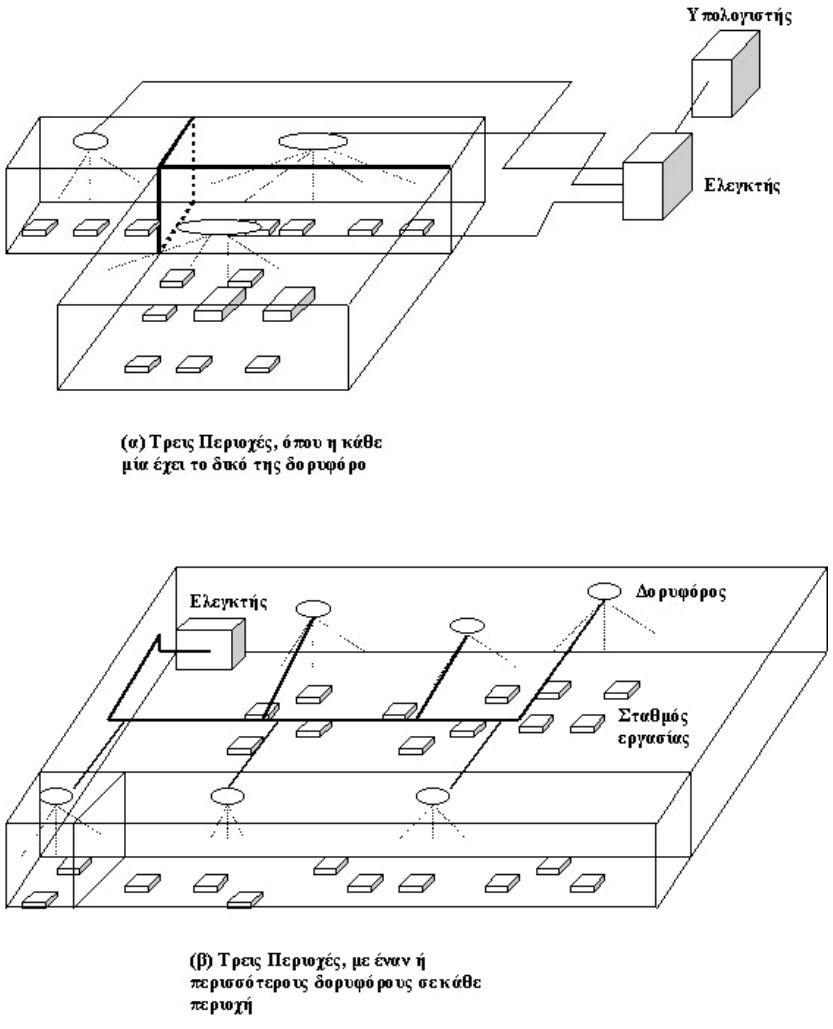
Επειδή τα υπέρυθρα σήματα δε μπορούν να διαπεράσουν τους τοίχους ενός δωματίου, τα οπτικά συστήματα παρέχουν έναν υψηλό βαθμό μυστικότητας και ασφάλειας από υποκλοπές, απλά και μόνο επειδή περιορίζουν τις μεταδόσεις σε ένα συγκεκριμένο χώρο, όπως είναι ένα δωμάτιο ή ένα μικρό γραφείο. Ο μόνος τρόπος με τον οποίο είναι δυνατός ο εντοπισμός των IR σημάτων έξω από την περιοχή εγκατάστασης είναι μέσω των παραθύρων, εμπόδιο που μπορεί όμως να ξεπεραστεί σχετικά εύκολα αν χρησιμοποιηθούν κουρτίνες ή ρολά. Ένα άλλο πλεονέκτημα της χρήσης οπτικών ασύρματων δικτύων είναι ότι πανομοιότυπα συστήματα (σε συχνότητα μετάδοσης, κλπ) μπορούν να βρίσκονται εγκατεστημένα σε γειτονικά δωμάτια, χωρίς οι μεταδόσεις του ενός να παρεμβάλλονται με του άλλου.

Σε ένα ασύρματο σύστημα υπέρυθρων ακτινών, οι σταθμοί εργασίας ενός κελιού επικοινωνούν με υπέρυθρες ακτίνες με έναν *κόμβο ή «δορυφόρο»*, ο οποίος βρίσκεται εγκατεστημένος στο ταβάνι και επικοινωνεί με το υπόλοιπο δίκτυο μέσω ενσύρματων (ομοαξονικό καλώδιο, σύστροφο ζεύγος, οπτική ίνα) ή ασύρματων συνδέσεων. Το κάθε κελί μπορεί να είναι είτε ένα μικρό γραφείο, είτε ένα τμήμα ενός μεγαλύτερου γραφείου, ανάλογα με την αρχιτεκτονική του κτιρίου.

Στο παρακάτω σχήμα φαίνονται δύο συνήθεις εγκαταστάσεις οπτικών ασύρματων δικτύων. Σύμφωνα με την πρώτη εγκατάσταση, ολόκληρος ο όροφος χωρίζεται σε μικρότερες περιοχές, όπου η καθεμιά έχει το δικό της δορυφόρο. Οι δορυφόροι με τη σειρά τους είναι συνδεδεμένοι, μέσω καλωδίων, με ένα σταθμό - ελεγκτή, ο οποίος εκτελεί χρέη ελέγχου πρόσβασης στο μέσο. Στη δεύτερη εγκατάσταση, ο όροφος χωρίζεται σε τρεις περιοχές όπου στην καθεμία μπορούν να υπάρχουν περισσότεροι από ένας δορυφόροι. Και σε αυτή την περίπτωση, όλοι οι κόμβοι συνδέονται σε μια ραχοκοκαλιά που οδηγεί σε έναν κεντρικό σταθμό ελέγχου.

Τα κυριότερα μειονεκτήματα της υπέρυθρης επικοινωνίας είναι:

- Ο μικρός ρυθμός μετάδοσης δεδομένων
- Οι εκτεταμένες διακυμάνσεις στην ισχύ των σημάτων
- Η ευαισθησία στις παρεμβολές από το φως του περιβάλλοντος



Εικόνα 8 - Δύο εγκαταστάσεις οπτικών Ασύρματων δικτύων

3.2 ΘΕΜΑΤΑ ΥΛΟΠΟΙΗΣΗΣ

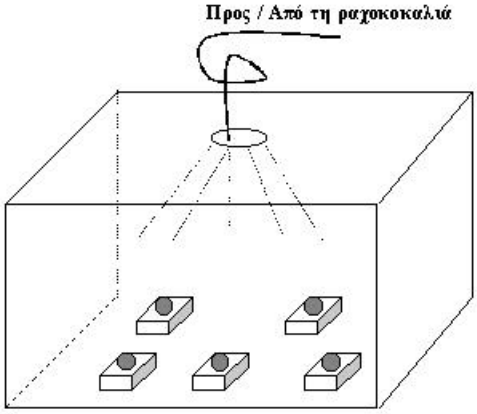
Η τεχνολογία η οποία χρησιμοποιούνταν περισσότερο παλαιότερα στα οπτικά ασύρματα δίκτυα, στηρίζεται στην *υπέρυθρη ακτινοβολία με διάχυση (Diffused Infrared - DFIR technology)*. Στο παρακάτω σχήμα φαίνεται μια τυπική εγκατάσταση DFIR. Ένα από τα

κυριότερα πλεονεκτήματα αυτής της μεθόδου είναι ότι δεν απαιτεί την άμεση οπτική επαφή μεταξύ του πομπού και του δέκτη. Αντ' αυτού, ο δέκτης «συλλέγει» και στη συνέχεια ανακατασκευάζει το σήμα που μεταδίδεται από το δορυφόρο, μέσω των αντανακλάσεών του στους τοίχους, στα ταβάνια και στα άλλα αντικείμενα που υπάρχουν στο γύρω χώρο.

Αυτή η μέθοδος είναι κατάλληλη για εφαρμογές που απαιτούν φορητότητα, όπως είναι τα ασύρματα τηλέφωνα, οι laptop ή palmtop computers και οι ασύρματοι ψηφιακοί βοηθοί (Personal Digital Assistants - PDAs).

Μερικά από τα μειονεκτήματα αυτής της μεθόδου είναι:

- Η υψηλή κατανάλωση ισχύος που απαιτείται για την κάλυψη ολόκληρου του χώρου εργασίας.
- Λόγω της ανακλάσεως των μεταδιδόμενων σημάτων εμφανίζεται το φαινόμενο του multipath fading, μιας και το σήμα μπορεί να φθάσει στον δέκτη από πολλά διαφορετικά μονοπάτια και με διαφορετική φάση. Αυτό με τη σειρά του έχει ως αποτέλεσμα τον περιορισμό του ρυθμού μετάδοσης δεδομένων.
- Η διάχυση αυξάνει τον κίνδυνο της έκθεσης των ματιών σε υπέρυθρη ακτινοβολία.
- Σε περιβάλλοντα αμφίδρομης επικοινωνίας, ο κάθε πομπός συλλέγει και το σήμα που μεταδίδει ο ίδιος, το οποίο είναι προφανώς ισχυρότερο από το σήμα που έρχεται από την άλλη πλευρά, με αποτέλεσμα να αυξάνονται οι παρεμβολές.



Εικόνα 9 - Τεχνολογία DFIR

Μια εναλλακτική τεχνολογία που μπορεί να χρησιμοποιηθεί είναι αυτή της *κατευθυνόμενης ακτίνας (Directed beam IR - DBIR)*. Στο παρακάτω σχήμα φαίνεται μια απλή εγκατάσταση ενός δικτύου DBIR. Οι πομποί και δέκτες του δικτύου βρίσκονται σε **άμεση οπτική επαφή**. Τα κύρια πλεονεκτήματα αυτής της μεθόδου είναι:

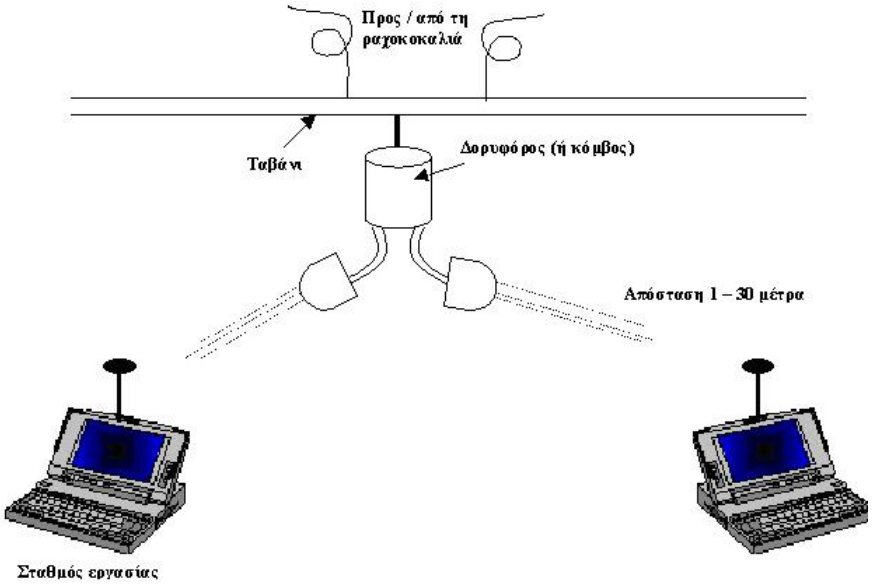
- Απαιτεί χαμηλότερη κατανάλωση ισχύος απ' ότι η DFIR τεχνολογία, καλύπτοντας εργασιακούς χώρους με μεγαλύτερη έκταση.
- Δεν παρουσιάζει το πρόβλημα του multipath fading υποστηρίζοντας μεγαλύτερους ρυθμούς μετάδοσης δεδομένων.
- Μπορεί να χειριστεί την αμφίδρομη επικοινωνία πολύ καλύτερα απ' ότι η τεχνολογία με διάχυση.

Μερικά από τα μειονεκτήματα της μεθόδου αυτής είναι:

- Η ανάγκη της ευθυγράμμισης του πομπού και του δέκτη
- Το σήμα παρουσιάζει διακοπές σε σκιερά σημεία (π.χ. σε σκοτεινές γωνίες).

Η μέθοδος DBIR χρησιμοποιείται σε περιβάλλοντα όπου οι τερματικοί σταθμοί βρίσκονται σε σταθερές τοποθεσίες. Στη συνήθη περίπτωση, οι σταθμοί τοποθετούνται σε υψηλά σημεία, έτσι ώστε να αποφεύγονται φαινόμενα φωτοσκίασης. Σε

εγκαταστάσεις DBIR είναι απαραίτητη η λήψη μέριμνας για την ελαχιστοποίηση του κινδύνου της έκθεσης των ματιών στις υπέρυθρες ακτίνες.



Εικόνα 10 - Παράδειγμα τεχνολογίας DBIR

Στα οπτικά ασύρματα δίκτυα, τα στοιχεία που χρησιμοποιούνται για τη μετάδοση των δεδομένων είναι είτε *δίοδοι laser (Laser Diodes - LDs)*, είτε *δίοδοι εκπομπής φωτός (Light Emitting Diodes - LEDs).* Η δίοδος laser εκπέμπει μια **στενή οπτική ακτίνα** και αν χρησιμοποιείται η μέθοδος DFIR, τότε θα πρέπει να χρησιμοποιηθεί κάποιος φακός διάχυσης (diffusing lens) ή κάποιο άλλο οπτικό μέσο για να αυξηθεί η περιοχή κάλυψης. Οι πιο ακριβές δίοδοι laser έχουν περισσότερο γραμμική απόκριση στην μετατροπή από ηλεκτρική - σε - οπτική ισχύ και παρέχουν υψηλότερη εκπομπή ισχύος. Οι δίοδοι εκπομπής φωτός, είναι φθηνότερες από τις διόδους laser και παρουσιάζουν χαμηλότερη ποιότητα στο εκπεμπόμενο φως.

Ένα άλλο θέμα που θα πρέπει να εξετασθεί κατά την υλοποίηση ενός οπτικού ασύρματου δικτύου είναι η επιλογή του μήκους κύματος που θα χρησιμοποιηθεί. Η χρήση μεγαλύτερων μηκών κύματος μειώνει τον κίνδυνο βλάβης των ματιών από τις

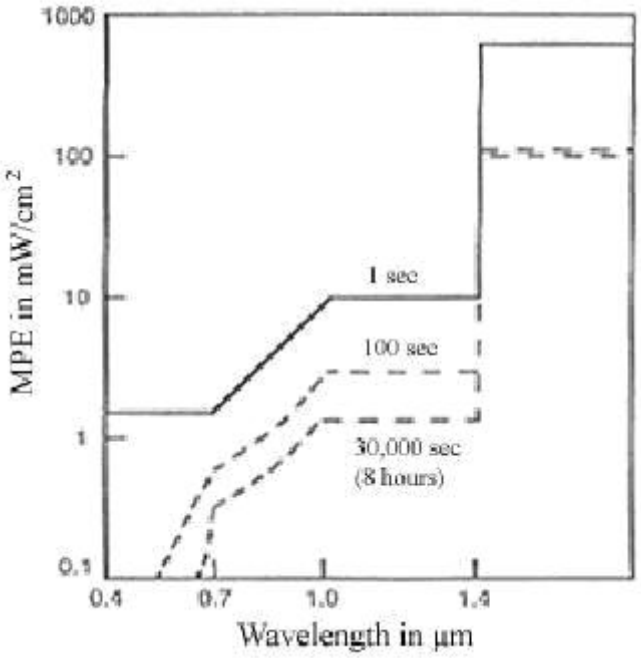
υπέρυθρες ακτίνες και επιτρέπει τη μετάδοση μεγαλύτερης ισχύος, η οποία με τη σειρά της επιτρέπει την αύξηση του ρυθμού μετάδοσης δεδομένων. Μερικά από τα μειονεκτήματα της χρήσης ακτινών μεγάλου μήκους κύματος είναι ότι οι συσκευές που λειτουργούν σε αυτές τις συχνότητες είναι πιο ακριβές και περισσότερο «θορυβώδεις» (ευαίσθητες στον εξωτερικό θόρυβο). Η σύγχρονη τεχνολογία υπέρυθρης μετάδοσης χρησιμοποιεί μήκη κύματος της τάξεως των 900 nm, ενώ σε εξέλιξη βρίσκονται και προϊόντα που λειτουργούν σε μήκη κύματος της τάξεως των 1,5 μm (1500 nm).

3.3 ΤΑ ΜΑΤΙΑ ΚΑΙ Η ΥΠΕΡΥΘΡΗ ΑΚΤΙΝΟΒΟΛΙΑ

Στο σημείο αυτό θα μιλήσουμε λίγο για το θέμα της ασφάλειας των ανθρώπινων ματιών στις υπέρυθρες ακτίνες. Το ανθρώπινο μάτι δρα παρόμοια με μια κάμερα, συγκεντρώνοντας την ενεργειακή πυκνότητα του φωτός επάνω στον αμφιβληστροειδή χιτώνα κατά 100.000 φορές ή περισσότερο. Το εξωτερικό επίπεδο του ματιού, ο κερατοειδής χιτώνας, δρα σαν ένα φίλτρο διέλευσης συγκεκριμένης ζώνης συχνοτήτων (band-pass filter), αφήνοντας να περάσουν μήκη κύματος περίπου από 0,4 μm έως 1,4 μm. Ενέργεια που βρίσκεται έξω από αυτό το διάστημα απορροφάται από τον κερατοειδή και δεν φτάνει στον αμφιβληστροειδή χιτώνα. Λόγω αυτού του φαινομένου, μήκη κύματος ίσα ή μεγαλύτερα του 1,5μm θεωρούνται σχετικά ασφαλή για το ανθρώπινο μάτι

Το χαμηλό κόστος των συσκευών που λειτουργούν σε μήκη κύματος 0,85μm τις κάνει αρκετά δημοφιλείς, αλλά θα πρέπει να ληφθεί η απαραίτητη μέριμνα, ώστε τα συστήματα που τις χρησιμοποιούν να μην υπερβαίνουν τα **επιτρεπτά επίπεδα ασφαλείας**, ή αλλιώς τα *επίπεδα MPE* (Maximum Permissible Exposure limits). Τα επίπεδα MPE, προσδιορίζουν το μέγιστο δυνατό επίπεδο υπέρυθρης ακτινοβολίας στην οποία μπορεί να εκτεθεί ένα άτομο, χωρίς να προκληθούν ζημιές στην όρασή του ή βιολογικές αλλαγές στα μάτια του. Τα επίπεδα MPE εκφράζονται συνήθως είτε σε όρους *έκθεσης στην ακτινοβολία (radiant exposure)* και μετριούνται σε J/cm^2 , είτε σε όρους *ακτινοβολίας (irradiance)* και μετριούνται σε W/cm^2 για **δεδομένο μήκος κύματος και**

απαιτούμενο χρόνο έκθεσης στην ακτινοβολία. Η έκθεση σε υπέρυθρη ακτινοβολία πάνω από τα επίπεδα αυτά είναι επικίνδυνη και θα πρέπει να αποφεύγεται. Γενικά, όσο μεγαλύτερο είναι το μήκος κύματος, τόσο μεγαλύτερο είναι το MPE, ενώ όσο μεγαλύτερος είναι ο απαιτούμενος χρόνος έκθεσης, τόσο μικρότερο είναι το MPE. Παρακάτω παρατίθεται ένα γράφημα που δείχνει τα επίπεδα MPE εκφρασμένα σε mW/cm^2 ως συνάρτηση του χρόνου έκθεσης και του χρησιμοποιούμενου μήκους κύματος. Παρατηρούμε ότι όσο μεγαλώνει το μήκος κύματος, το MPE αυξάνει, ενώ όσο μεγαλώνει ο απαιτούμενος χρόνος έκθεσης στην ακτινοβολία, το MPE μειώνεται.



Εικόνα 11 - Γράφημα επιπέδων MPE

ΚΕΦΑΛΑΙΟ 4

ΠΡΟΤΥΠΑ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

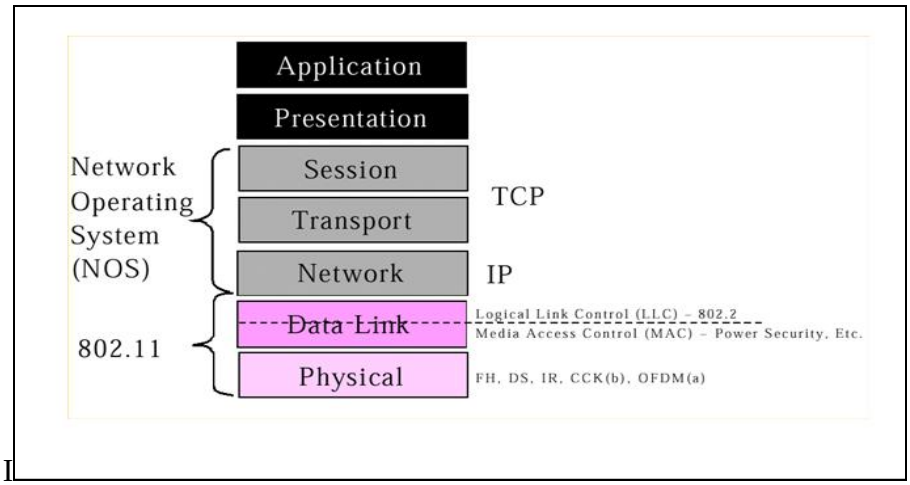
4. 1 ΤΟ ΠΡΟΤΥΠΟ 802.11 ΤΗΣ IEEE ΓΙΑ ΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Καθώς τα προϊόντα ασύρματης δικτύωσης κατακλύζουν όλο και περισσότερο την αγορά και καθώς ο αριθμός των υλοποιήσεων ασύρματων δικτύων μεγαλώνει συνεχώς, είναι απαραίτητη η ύπαρξη ενός ή περισσοτέρων αποδεκτών μηχανισμών και προτύπων (standards), τα οποία θα προσδιορίζουν λύσεις με τις οποίες θα αντιμετωπίζονται τα διάφορα προβλήματα που διέπουν τα ασύρματα δίκτυα. Σε αυτά περιλαμβάνονται ο καθορισμός της τοπολογίας ενός ασύρματου τοπικού δικτύου, πρωτόκολλα διαμοιρασμού ενός κοινού μέσου μετάδοσης (Medium Access Control - MAC issues), θέματα ελέγχου και ασφάλειας των χρηστών, κ.α.

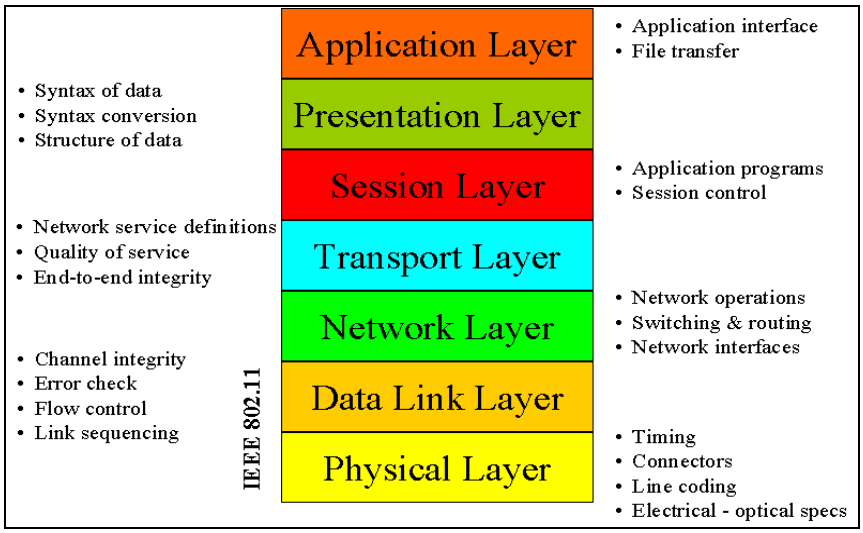
Το πρότυπο 802.11 της IEEE για τα ασύρματα δίκτυα αποτελεί ένα τέτοιο μηχανισμό. Το τμήμα αυτό εισάγει τον αναγνώστη στις βασικές έννοιες και αρχές λειτουργίας του προτύπου 802.11.

Το πρότυπο 802.11 περιορίζεται στα δύο πρώτα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, ήτοι, στο φυσικό επίπεδο (ΦΕ) και στο επίπεδο σύνδεσης δεδομένων (ΕΣΔ). Για την ακρίβεια, δεν καλύπτει ολόκληρο το ΕΣΔ, αλλά το *πρώτο μισό* του, δηλαδή το *υπο-επίπεδο πρόσβασης στο μέσο* (MAC Layer).

Προτού προχωρήσουμε στην ανάλυση βασικών όρων των ασυρμάτων τοπικών δικτύων παρουσιάζονται τα παρακάτω σχήματα που περιγράφουν τη σχέση της WLAN τεχνολογίας με το μοντέλο OSI.



Εικόνα 12 - 802.11 και Μοντέλο OSI (1)



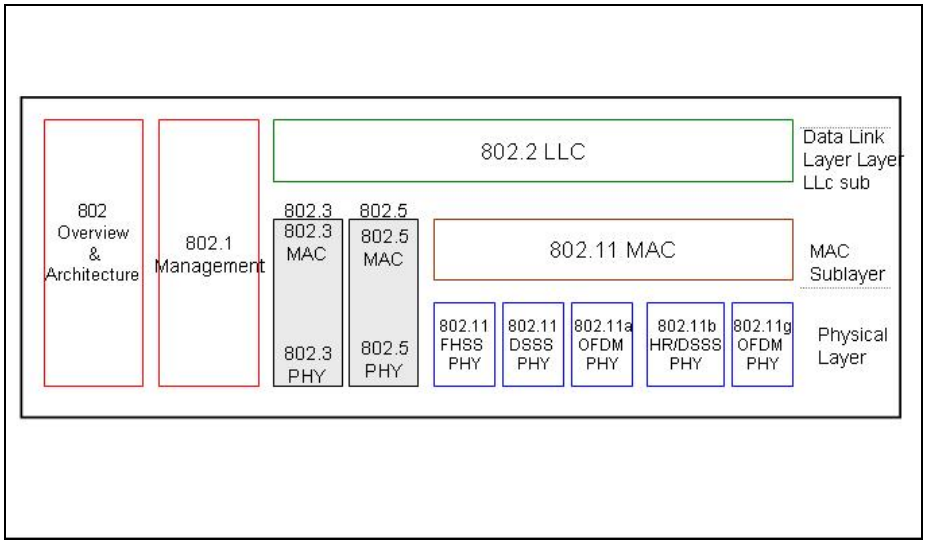
Εικόνα 13 - 802.11 και Μοντέλο OSI (2)

Όπως όλα τα δίκτυα, έτσι και τα ασύρματα δίκτυα μεταδίδουν τα δεδομένα μέσω ενός μέσου μεταφοράς το οποίο είναι κάποιου τύπου ηλεκτρομαγνητικά κύματα. Τα ασύρματα τοπικά δίκτυα τύπου 802.11 λειτουργούν στο φάσμα συχνοτήτων 2.4GHz έως 2.5GHz, που ονομάζεται ISM(Industrial Scientific Medicine) band και είναι ελεύθερο για χρήση από οποιονδήποτε, δίχως να χρειάζεται ειδική άδεια.

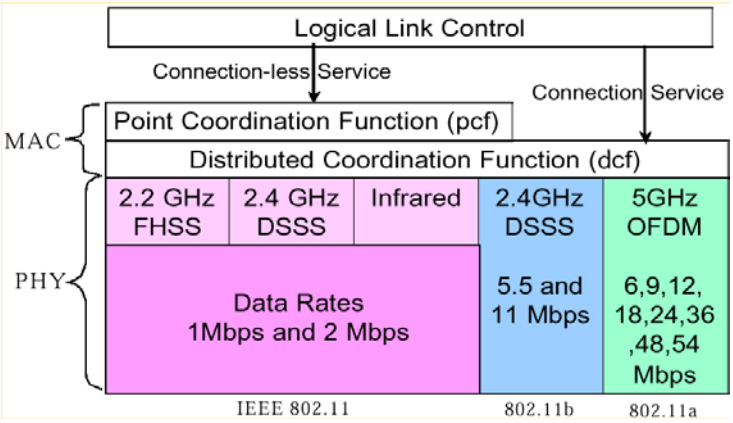
Το μειονέκτημα είναι ότι η παραπάνω συχνότητα χρησιμοποιείται από κάποιες ηλεκτρικές συσκευές, με συνέπεια να δημιουργούνται παρεμβολές.

Πρότυπο IEEE	Μέγιστος Ρυθμός Μετάδοσης	Φάσμα Συχνοτήτων
802.11	1,2 Mbps	2.4 GHz
802.11a	έως 54 Mbps	5 GHz
802.11b	5.5 Mbps 11 Mbps	2.4 GHz
802.11g	108 Mbps	2.4 GHz

Πίνακας 3 - 802.11 Πρότυπα



Εικόνα 14 - 802.11 και Μοντέλο OSI (3)



Εικόνα 15

Τα βασικά δομικά στοιχεία ενός δικτύου IEEE 802.11 είναι:

Station (STA)

Ένας προσωπικός υπολογιστής ή μια συσκευή με ασύρματη σύνδεση.

Access Point (AP)

Η γέφυρα μεταξύ του ασύρματου και του ενσύρματου LAN

Basic Service Set (BSS):

Σύνολο από STAs τα οποία επικοινωνούν μέσω του ίδιου καναλιού στην ίδια περιοχή.

Extended Service Set (ESS)

Ένα σύνολο από BSSs και ενσύρματα LANs.

DS(Distribution System)

Το σύστημα κατανομής είναι το συστατικό του 802.11 που χρησιμοποιείται ώστε να μεταφέρονται πακέτα μεταξύ των APs .

Τα πρότυπα της ομάδος IEEE 802 :

IEEE 802.1™ : Bridging & Management

IEEE 802.2™: Logical Link Control

IEEE 802.3™: CSMA/CD Access Method

IEEE 802.4™: Token-Passing Bus Access Method

IEEE 802.5™: Token Ring Access Method

IEEE 802.6™: DQDB Access Method

IEEE 802.7™: Broadband LAN

IEEE 802.10™: Security

IEEE 802.11™: Wireless

IEEE 802.12™: Demand Priority Access

IEEE 802.15™: Wireless Personal Area Networks

IEEE 802.16™: Broadband Wireless Metropolitan Area Networks

Τα υποπρότυπα του IEEE 802.11 είναι :

IEEE 802.11a

Χρησιμοποιεί τη ζώνη των 5GHz και OFDM (Ταχύτητα:<54Mbps)

IEEE 802.11b (Χρησιμοποιείται στην Ελλάδα)

Χρησιμοποιεί τη ζώνη των 2.4GHz και DSSS (Ταχύτητα:<11Mbps)

IEEE 802.11c

MAC Bridges (802.1d supp)

IEEE 802.11d

International Roaming

IEEE 802.11e

Παρέχει εγγυήσεις για ποιότητα υπηρεσίας

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 υψηλότερες από 11Mbps

IEEE 802.11h

Transmit Power Control / Dynamic Freq. Selection

IEEE 802.11i

Πρότυπο το οποίο μελετά θέματα ασφάλειας στα WLANs

IEEE 802.11j

HiperLAN interworking

IEEE 802.11n

Προσπάθεια για μεταφορά της (ονομαστικής) ρυθμαπόδοσης στα 100 Mbps

IEEE 802.11r

Fast hand-off, roaming που αφορά real-time εφαρμογές

IEEE 802.11s

Προτυποποίηση για self-healing/self-configuring mesh networks

Στο κοντινό μέλλον αναμένεται να υπάρξουν οι παρακάτω ομάδες εργασίας :

802.11p (Wi-Fi in moving vehicles, TGp)

802.11t (perfomane predicition in testing, TGt)

ΤΟ ΦΥΣΙΚΟ ΕΠΙΠΕΔΟ

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

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

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

Εικόνα 15 - Επίπεδα που καλύπτονται από το πρότυπο 802.11

Οι δύο διαφορετικές τεχνολογίες ΦΕ ραδιοσυχνότητας που απεικονίζονται στο παραπάνω σχήμα, ανήκουν στην κατηγορία των τεχνικών *διασποράς φάσματος (spread spectrum techniques)* οι οποίες όμως δεν καλύπτονται εδώ. Αναφορικά μόνο, οι τεχνολογίες διασποράς φάσματος που προσδιορίζει το 802.11 για τα δύο ΦΕ ραδιοσυχνότητας είναι η *τεχνική διασποράς φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum - DSSS)* [2],[13] και η *τεχνική διασποράς φάσματος αναπήδησης συχνότητας (Frequency Hopping Spread Spectrum - FHSS)* [1],[2]

Το μικρό εύρος κάλυψης που έχει το υπέρυθρο ΦΕ το καθιστά κατάλληλο μόνο για εφαρμογές κλειστού χώρου, όπως ένα μικρό γραφείο, ένα δωμάτιο, κλπ. Αντίθετα, οι άλλοι δύο τύποι ΦΕ μπορούν να χρησιμοποιηθούν σε εφαρμογές όπου υπάρχει η ανάγκη

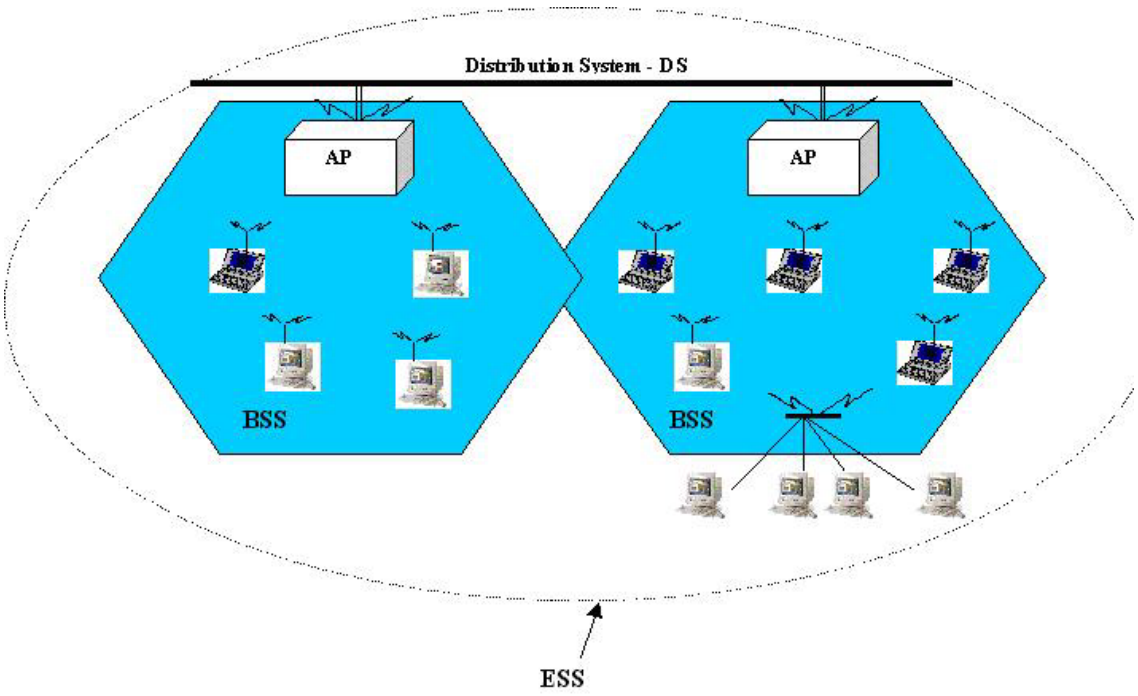
κάλυψης μεγάλων περιοχών (ανοικτών ή κλειστών), όπως είναι μια πανεπιστημιούπολη, τα κτίρια μιας επιχείρησης, κλπ.

Τέλος, το 802.11 προσδιορίζει ρυθμούς μετάδοσης δεδομένων της τάξεως των 1 και 2 Mbps για όλα τα ΦΕ (οπτικά και ραδιοσυχνότητας).

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ΠΡΟΤΥΠΟΥ IEEE 802.11

Ένα ασύρματο δίκτυο 802.11 βασίζεται σε μια κυψελοειδή αρχιτεκτονική, σύμφωνα με την οποία, ολόκληρο το σύστημα διαιρείται σε περιοχές ή *κελιά* με το κάθε κελί να ελέγχεται από ένα *Σταθμό - Βάσης (Base Station)*. Στην ορολογία του 802.11 ένα κελί ονομάζεται *Βασικό Σύνολο Υπηρεσιών (Basic Service Set - BSS)* και ο σταθμός βάσης, *Σημείο Πρόσβασης (Access Point - AP).* Παρόλο που ένα δίκτυο μπορεί να αποτελείται από ένα μόνο κελί, οι περισσότερες δικτυακές εγκαταστάσεις 802.11 συνήθως αποτελούνται από πολλά κελιά με τα σημεία πρόσβασης να βρίσκονται συνδεδεμένα σε μια ραχοκοκαλιά, η οποία ονομάζεται *Σύστημα Διανομής (Distribution System - DS)* και η οποία μπορεί να είναι είτε ένα ενσύρματο (π.χ.Ethernet), είτε ένα ασύρματο δίκτυο.

Το σύνολο όλων των δια-συνδεδεμένων ασύρματων δικτύων, μαζί με τα σημεία πρόσβασης και το σύστημα διανομής, ονομάζεται *Εκτεταμένο Σύνολο Υπηρεσιών (Extended Service Set - ESS)* και όσον αφορά τα ανώτερα επίπεδα του δικτυακού μοντέλου αναφοράς OSI, σύμφωνα με το πρότυπο, θα πρέπει να θεωρείται ως ένα **ενιαίο** τοπικό δίκτυο κατηγορίας 802. Στο παρακάτω σχήμα απεικονίζεται η αρχιτεκτονική ενός δικτύου 802.11.



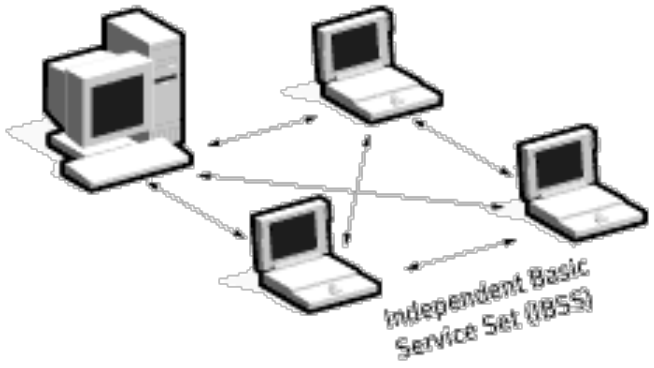
Εικόνα 16 - Αρχιτεκτονική δικτύου κατά το πρότυπο 802.11 της IEEE

Το πρότυπο ορίζει επίσης και την έννοια της *πύλης (Portal).* Η *πύλη* είναι μια συσκευή που χρησιμοποιείται για τη δια-σύνδεση ενός δικτύου 802.11 με ένα άλλο δίκτυο κατηγορίας 802. Η λειτουργία της μπορεί να παρομοιαστεί με τη λειτουργία ενός *δρομολογητή (router),* ο οποίος είναι ικανός να δια-συνδέει διαφορετικά δίκτυα. Η λειτουργικότητα μιας *πύλης* μπορεί να βρίσκεται είτε σε ξεχωριστή συσκευή, είτε να είναι ενσωματωμένη με το σημείο πρόσβασης.

Η διάρθρωση ενός ασύρματου IEEE 802.11 δικτύου μπορεί να είναι πολύ απλή ως και αρκετά σύνθετη, παρουσιάζοντας εξαιρετική δυνατότητα κλιμάκωσης. Ορίζονται δύο διαφορετικοί τρόποι διάρθρωσης δικτύου, ad-hoc και infrastructure.

Ad-hoc ή peer to peer

Η πιο απλή διάρθρωση στην οποία οι ασύρματοι σταθμοί που μετέχουν είναι ισότιμοι και επικοινωνούν μεταξύ τους κατευθείαν. Πλεονέκτημα είναι η γρήγορη και εύκολη εγκατάσταση. Παράδειγμα εφαρμογής η σύνδεση μεταξύ φορητών υπολογιστών σε μία αίθουσα συσκέψεων. Βασικός περιορισμός είναι ότι για την επικοινωνία μεταξύ δύο σταθμών πρέπει ο ένας να είναι εντός της εμβέλειας του άλλου. Έτσι στο παρακάτω σχήμα ο AH1 δεν μπορεί να επικοινωνήσει με τον AH4, διότι είναι εκτός εμβέλειας ο ένας με τον άλλον. Λέμε ότι οι σταθμοί που σχηματίζουν ένα τέτοιο δίκτυο αποτελούν ένα IBSS (Independent Basic Service Set)



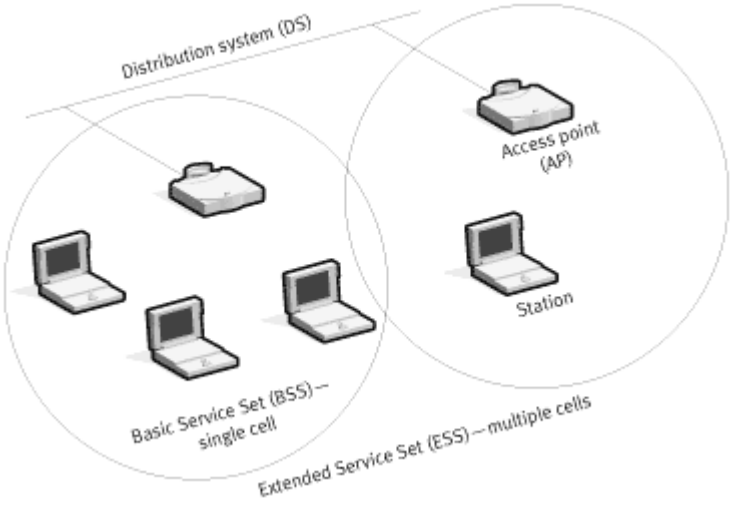
Εικόνα 18

Infrastructure WLAN

Ακολουθεί μια κυψελοειδή αρχιτεκτονική, όπου το δίκτυο χωρίζεται σε κυψέλες με κάθε κυψέλη να ονομάζεται BSS (Basic Service Set). Κάθε κυψέλη περιλαμβάνει ένα σταθμό βάσης AP (Access Point) και ένα αριθμό από ασύρματους σταθμούς. Το AP παρέχει τη λειτουργία της μεταγωγής στο BSS. Έτσι όλοι οι σταθμοί επικοινωνούν κατευθείαν μόνο με το AP και αυτό μετάγει τα πακέτα από τον ένα σταθμό στον άλλον.

Τα AP συνδέονται μεταξύ τους ή/και με άλλα δίκτυα μέσω ενός δικτύου μετάδοσης το οποίο ονομάζεται DS (Distribution System). Η IEEE δεν προδιαγράφει την υλοποίηση αυτού του δικτύου. Έτσι αυτό μπορεί να είναι Ethernet ενσύρματο, ασύρματο, ή και

κάποια άλλη τεχνολογία. Το δίκτυο αυτό έχει τη μορφή ενός δικτύου κορμού (backbone). Έτσι τα AP παρέχουν την υπηρεσία της τοπικής πρόσβασης στους ασύρματους σταθμούς (πελάτες), καλύπτοντας εκατοντάδες μέτρα. Στην συνέχεια το δίκτυο κορμού μεταφέρει την πληροφορία από το ένα AP στο άλλο. Όλη αυτή η δομή δικτύου ονομάζεται ESS (Extended Service Set).



Εικόνα 19

ΤΟ ΕΠΙΠΕΔΟ ΣΥΝΔΕΣΗΣ ΔΕΔΟΜΕΝΩΝ

Σε ένα δίκτυο 802.11, το υπο-επίπεδο προσπέλασης μέσου (MAC layer), είναι υπεύθυνο για την εκτέλεση των παρακάτω λειτουργιών.

- Για τον έλεγχο της πρόσβασης των σταθμών στο κοινό μέσο μετάδοσης
- Για τη λειτουργία του *κατακερματισμού και της επανασυναρμολόγησης (fragmentation and reassembly)*
- Για τη λειτουργία της *αναμετάδοσης πακέτου (packet retransmission)*
- Για τη λειτουργία της *επιβεβαίωσης λήψης (acknowledges).*

ΤΟ ΕΠΙΠΕΔΟ MAC

Ορίζονται δύο τρόποι πρόσβασης στο MAC μέσο.

DCF (Distribution Coordination Function)

Αποτελείται βασικά από ένα μηχανισμό CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Σύμφωνα με αυτόν ένας σταθμός που επιθυμεί να εκπέμψει ανιχνεύει τον ασύρματο δίαυλο. Αν ο δίαυλος είναι ελεύθερος για ένα χρονικό διάστημα ο σταθμός εκπέμπει μετά από ένα τυχαίο χρονικό διάστημα. Αυτός ο τρόπος είναι ένας καλός συμβιβασμός ανάμεσα στην καθυστέρηση μετάδοσης και στην πιθανότητα συγκρούσεων των πακέτων. Ο δέκτης θα ελέγξει το λαμβανόμενο πακέτο και θα στείλει ένα μήνυμα επιβεβαίωσης ACK. Αν ο αποστολέας δεν δεχτεί το μήνυμα ACK θα υποθέσει ότι μία σύγκρουση πακέτων έγινε και θα γίνει επανεκπομπή του από το MAC επίπεδο.
Επειδή σε μία κυψέλη μπορεί ένας σταθμός να μην μπορεί να ακούσει τους υπόλοιπους, αλλά μόνο το AP, ορίζεται ένας μηχανισμός ανίχνευσης ιδεατής φέρουσας (virtual carrier sense). Σύμφωνα με αυτόν ο σταθμός που επιθυμεί να εκπέμψει στέλνει ένα μήνυμα RTS (Request To Send) στο AP και αυτό του απαντά με ένα μήνυμα CTS (Clear To Send) αν ο ασύρματος δίαυλος είναι κενός. Με αυτόν τον τρόπο έχουμε μία κράτηση του διαύλου για τον συγκεκριμένο σταθμό.

PCF (Point Coordination Function)

Προαιρετικός τρόπος πρόσβασης, χρησιμοποιείται για εφαρμογές πραγματικού χρόνου, όπου απαιτείται προνομιακή μεταχείριση έναντι της απλής μετάδοσης δεδομένων. Σε αυτό το AP ερωτά κάθε ένα σταθμό ξεχωριστά εάν έχει δεδομένα προς μετάδοση. Με αυτόν τον τρόπο ένας σταθμός μπορεί να αποκτήσει μεγαλύτερης προτεραιότητας πρόσβαση. Το AP μοιράζει τον χρόνο του ανάμεσα στους δύο τρόπους πρόσβασης

Ένα *802.11 MAC* πλαίσιο έχει την ακόλουθη μορφή:

MAC Header(30)							**Data (0-2312)**		**CRC(4)**	
FC	ID	Add1	Add2	Add3	SC	Add4	Data		CRC	
2	2	6	6	6	2	6	0-2312		4	
Protocol Version	Type	Sub Type	ToDS	FromDS	More Frag	Retry	Power Management	More Data	WEP	Order
2	2	4	1	1	1	1	1	1	1	1

Πίνακας 4 - MAC Header

FC: Πεδίο που περιέχει πληροφορία ελέγχου

Duration/ID: Διάρκεια πλαισίου

Address: MAC διευθύνσεις αποστολέα και παραλήπτη

Sequence: Αύξων αριθμός πλαισίου και τμήματος

Data: Δεδομένα προς μετάδοση

CRC: Κώδικας ανίχνευσης λαθών

Επειδή ο ραδιοφορέας είναι μη αξιόπιστο μέσο μετάδοσης και εισάγει μεγάλο αριθμό λαθών το MAC επίπεδο κατατμεί τα πλαίσια σε μικρότερου μεγέθους τμήματα (fragments). Έτσι η πιθανότητα να έχουμε λανθασμένο τμήμα είναι μικρότερη, ενώ στην περίπτωση που αυτό έχει λάθη, το πλαίσιο που θα χρειαστεί να εκπέμψουμε θα είναι μικρότερο.

ΕΛΕΓΧΟΣ ΤΗΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΚΟΙΝΟ ΜΕΣΟ

Η τεχνική που χρησιμοποιείται από το ΕΣΔ στο 802.11 είναι **παρόμοια** με μια από τις βασικότερες μεθόδους ελέγχου πρόσβασης στο μέσο, την *Μέθοδο πολλαπλής πρόσβασης*

με ανίχνευση φέροντος σήματος και αποφυγή συγκρούσεων (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA) [12].

Σύμφωνα με τη μέθοδο αυτή, ένας σταθμός ο οποίος θέλει να μεταδώσει «αφουγκράζεται» πρώτα το μέσο μετάδοσης, για να διαπιστώσει εάν είναι κατειλημμένο. Εάν είναι, τότε δε μεταδίδει, περιμένει ένα τυχαίο χρονικό διάστημα και προσπαθεί ξανά. Εάν είναι ελεύθερο, τότε στέλνει **πρώτα** ένα ειδικό σήμα για να προειδοποιήσει ότι **πρόκειται** να μεταδώσει και στη συνέχεια, αν δε συμβεί καμιά σύγκρουση, στέλνει τα δεδομένα του. Με τον τρόπο αυτό οι υπολογιστές αντιλαμβάνονται πότε υπάρχει πιθανότητα σύγκρουσης, κάτι που τους επιτρέπει να **αποφεύγουν** τις συγκρούσεις μετάδοσης. Ωστόσο, η αποστολή του ειδικού σήματος μετάδοσης, αυξάνει την κίνηση στο καλώδιο, υποβαθμίζοντας την επίδοση ολόκληρου του δικτύου.

Παρόλο που αυτοί οι μηχανισμοί είναι αρκετά αποδοτικοί στα παραδοσιακά ενσύρματα δίκτυα, αυτό δε θα μπορούσαμε να πούμε ότι ισχύει και στα ασύρματα δίκτυα, για τους παρακάτω λόγους:

- Η υλοποίηση ενός μηχανισμού ανίχνευσης συγκρούσεων θα απαιτούσε την υλοποίηση ενός *αμφίδρομου πομποδέκτη*, που θα μπορούσε να στέλνει και να λαμβάνει δεδομένα ταυτόχρονα, κάτι που θα αύξανε κατά πολύ το κόστος υλοποίησης.
- Σε ένα ασύρματο δίκτυο δε θα ήταν σωστό να υποθέσουμε ότι **όλοι** οι σταθμοί μπορούν να «ακούσουν» όλους τους υπόλοιπους, μια πολύ βασική υπόθεση στις μεθόδους πρόσβασης με ανίχνευση φέροντος. Ακόμη και αν κάποιος σταθμός που επιθυμεί να μεταδώσει ανιχνεύσει το κανάλι ελεύθερο, αυτό δε σημαίνει απαραίτητα ότι αυτό είναι ελεύθερο γύρω από την περιοχή του δέκτη (αυτό το επιχείρημα αναλύεται αναλυτικότερα παρακάτω, στο τμήμα *Δέσμευση του καναλιού*).

Λόγω των παραπάνω προβλημάτων, το πρότυπο 802.11 χρησιμοποιεί μια μέθοδο αποφυγής συγκρούσεων (Collision Avoidance mechanism), παράλληλα με ένα σύστημα *θετικής επιβεβαίωσης λήψης (Positive Acknowledgement Scheme)*, που περιγράφεται παρακάτω.

Ανίχνευση των Συγκρούσεων (collision detection)

Ένας σταθμός ο οποίος επιθυμεί να μεταδώσει, ελέγχει αρχικά το μέσο (τον αέρα στην περίπτωσή μας). Αν είναι κατειλημμένο, τότε αναβάλει τη μετάδοση για αργότερα. Αν είναι ελεύθερο, τότε περιμένει να δει αν θα **παραμείνει** ελεύθερο για ένα συγκεκριμένο χρονικό διάστημα, το οποίο ονομάζεται **DIFS (Distributed Inter Frame Space - βλέπε παρακάτω)** και στη συνέχεια μεταδίδει το πακέτο που περιέχει τα δεδομένα. Ο δέκτης από την άλλη, λαμβάνοντας το πακέτο ελέγχει να δει εάν αυτό περιέχει τυχόν λάθη και αν όχι τότε στέλνει πίσω στον πομπό μια επιβεβαίωση λήψης (Acknowledgement - ACK). Παραλαβή της επιβεβαίωσης λήψης από τον πομπό σημαίνει ότι το πακέτο παραδόθηκε στον προορισμό του χωρίς να συγκρουστεί με κάποιο άλλο. Αν ο αποστολέας δεν παραλάβει μια επιβεβαίωση, τότε θεωρεί ότι συνέβη μια σύγκρουση και επαναλαμβάνει τη μετάδοση του πακέτου, μέχρις ότου είτε λάβει την επιβεβαίωση, είτε ακυρώσει τη μετάδοση μετά από έναν αριθμό προσπαθειών.

Δέσμευση του καναλιού

Μέχρις αυτό το σημείο δε μιλήσαμε ακόμη για τον τρόπο με τον οποίο μπορεί ένας σταθμός να σιγουρευτεί ότι **όντως** το μέσο μετάδοσης είναι ελεύθερο προτού μεταδώσει. Το πρότυπο 802.11 προσδιορίζει ένα μηχανισμό *εικονικής ανίχνευσης φέροντος (virtual carrier sense mechanism)*, με τον οποίο εξασφαλίζεται ότι **όλοι** οι σταθμοί που μοιράζονται το ίδιο μέσο θα γνωρίζουν ότι κάποιος σταθμός μεταδίδει ακόμη και αν αυτοί είναι «κρυμμένοι».

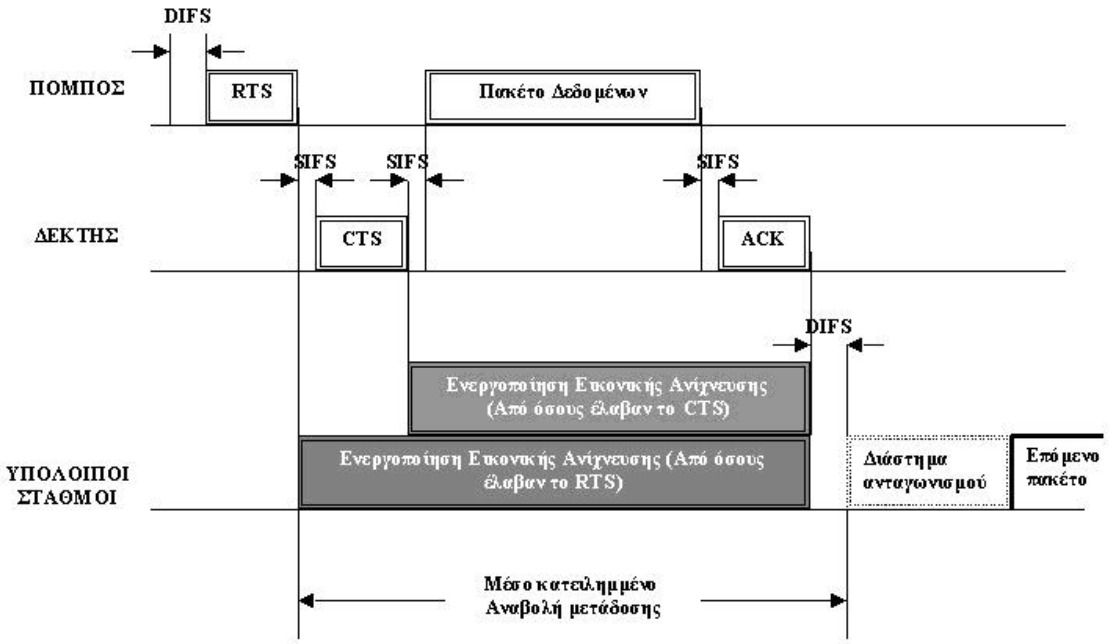
Για να κατανοήσουμε καλύτερα την παραπάνω έννοια, ας φανταστούμε την ακόλουθη περίπτωση. Θεωρείστε ότι έχουμε ένα ασύρματο δίκτυο που έχει μια αρχιτεκτονική παρόμοια με αυτή του σχήματος 8. Έστω ότι υπάρχουν τρεις σταθμοί στο κάθε κελί, ο Α, ο Β και ο Γ. Ο Α και ο Β έστω ότι αποτελούν απλούς σταθμούς, ενώ ο Γ αποτελεί ένα *σημείο πρόσβασης (AP).* Φανταστείτε το ακόλουθο σενάριο: ο Α μπορεί να επικοινωνήσει με τον Γ, ο Β μπορεί να επικοινωνήσει με τον Γ, αλλά ο Α δε μπορεί να επικοινωνήσει απευθείας με τον Β, γιατί απέχουν τέτοια απόσταση ο ένας από τον άλλο που δεν είναι δυνατή η άμεση επικοινωνία (το σήμα δε μπορεί να διαδοθεί από τον Α στον Β). Οπότε, αν σε μια δεδομένη χρονική στιγμή και ο Α και ο Β θέλουν να μεταδώσουν, θα ανιχνεύσουν και οι δύο το μέσο ελεύθερο, αφού ο ένας δε μπορεί να

«ακούσει» τον άλλο. Στη συγκεκριμένη περίπτωση θα υπάρξει σύγκρουση στην *περιοχή του δέκτη,* γιατί μπορεί ο Α να μη μπορεί να επικοινωνήσει με τον Β, αλλά και οι δύο είναι σε θέση να επικοινωνήσουν με το σημείο πρόσβασης, το Γ. Στην περίπτωση αυτή λέμε ότι ο σταθμός Β είναι «κρυμμένος» από το σταθμό Α και αντίστροφα.

Ο μηχανισμός εικονικής ανίχνευσης φέροντος λειτουργεί ως εξής: ένας σταθμός που επιθυμεί να μεταδώσει και έχει ανιχνεύσει το μέσο ελεύθερο (τουλάχιστον στην περιοχή γύρω από αυτόν), στέλνει πρώτα ένα μικρό πακέτο που ονομάζεται **RTS (Request To Send - Αίτηση για αποστολή)** και το οποίο περιέχει τη **διεύθυνση αποστολής**, τη **διεύθυνση προορισμού** και το **χρονικό διάστημα της όλης διαδικασίας** (το χρόνο δηλαδή που απαιτείται για την αποστολή του πακέτου δεδομένων και της λήψης της επιβεβαίωσης από το δέκτη). Στη συνέχεια, ο δέκτης ελέγχει εάν το μέσο είναι **όντως** ελεύθερο (και στη δική του περιοχή δηλαδή) και αν είναι, τότε αποστέλλει ένα άλλο πακέτο μικρού μεγέθους που ονομάζεται **CTS (Clear To Send - Αποστολή Δεκτή)** το οποίο περιέχει τις ίδιες πληροφορίες με το πακέτο RTS. Σε αντίθετη περίπτωση δεν αποστέλλει τίποτε.

Όλοι οι σταθμοί που λαμβάνουν το RTS ή / και το CTS, ενεργοποιούν έναν ειδικό δείκτη που ονομάζεται *δείκτης εικονικής ανίχνευσης (virtual sense indicator),* ο οποίος καλείται **NAV - από το Network Allocation Vector.** Η ενεργοποίηση διαρκεί για το χρονικό διάστημα που αναφέρεται στο CTS (ή το RTS) και χρησιμοποιείται παράλληλα με την *φυσική ανίχνευση φέροντος* από τους σταθμούς όταν αυτοί ανιχνεύουν το καλώδιο.

Η μέθοδος αυτή μειώνει κατά πολύ την πιθανότητα συγκρούσεων στην περιοχή του δέκτη, γιατί ακόμη και οι «κρυμμένοι» από τον πομπό σταθμοί (που δε μπορούν να λάβουν το RTS δηλαδή) θα λάβουν σίγουρα το πακέτο CTS και θα θεωρήσουν το μέσο κατειλημμένο για το χρονικό διάστημα που αναφέρεται σ' αυτό. Επίσης, η αποστολή του πακέτου RTS προφυλάσσει τον **δέκτη** από συγκρούσεις στην **περιοχή του πομπού** κατά τη διάρκεια αποστολής της επιβεβαίωσης λήψης (ACK), γιατί το RTS θα ληφθεί σίγουρα από όλους τους σταθμούς που είναι «κρυμμένοι» από το δέκτη. Στο παρακάτω σχήμα δίδεται ένα χρονοδιάγραμμα των ενεργειών που λαμβάνουν χώρα κατά τη διάρκεια της επικοινωνίας μεταξύ δύο σταθμών.



Εικόνα 17 - Χρονοδιάγραμμα των ενεργειών που λαμβάνουν χώρα κατά τη διάρκεια της επικοινωνίας δυο σταθμών

Στο παραπάνω σχήμα μπορούμε να διακρίνουμε και τα διάφορα χρονικά διαστήματα που μεσολαβούν πριν και μετά τις μεταδόσεις των πλαισίων. Οι χρόνοι αυτοί, κατά λέξη, ονομάζονται *δια-πλαισιακά διαστήματα (Inter-Frame Spaces - IFS)* και ανήκουν σε διάφορες κατηγορίες:

- **Short IFS - SIFS (Δια-πλαισιακό διάστημα μικρής διάρκειας):** Ο χρόνος αυτός χρησιμοποιείται για το διαχωρισμό των μεταδόσεων που ανήκουν σε ένα διάλογο μεταξύ δύο σταθμών (π.χ. πακέτο δεδομένων και ACK) και αποτελεί το μικρότερο από τους δια-πλαισιακούς χρόνους. Έχει σταθερή τιμή, η οποία διαφέρει ανά ΦΕ, και υπολογίζεται με τέτοιον τρόπο, ώστε ο πομπός να έχει αρκετό χρόνο να μεταβεί σε κατάσταση λήψης, για να μπορέσει να λάβει και να αποκωδικοποιήσει το εισερχόμενο πακέτο (π.χ. ACK ή CTS) από το δέκτη. Για παράδειγμα, για τα ΦΕ τεχνολογίας διασποράς φάσματος αναπήδησης συχνότητας, ο χρόνος αυτός ορίζεται στα 28 μsec.

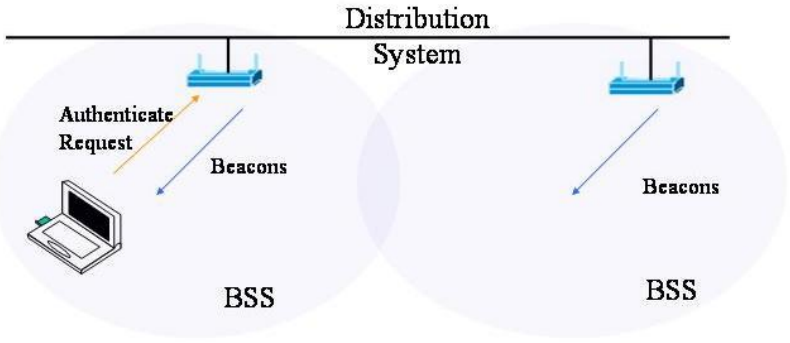
- **Point Coordination IFS - PIFS (Δια-πλαισιακό διάστημα συντονισμού σημείου):** Ο χρόνος αυτός χρησιμοποιείται από τα σημεία πρόσβασης (που εδώ ονομάζονται *συντονιστές σημείου*), όταν θέλουν να προσπελάσουν το μέσο μετάδοσης **πριν** από τους άλλους σταθμούς. Η τιμή του είναι λίγο μεγαλύτερη από του SIFS, δηλαδή 78 μsec.
- **Distributed IFS - DIFS (Κατανεμημένο δια-πλαισιακό διάστημα):** Ο χρόνος αυτός είναι το **επιπλέον** χρονικό διάστημα που μεσολαβεί προτού ένας σταθμός - που έχει ανιχνεύσει το μέσο ως ελεύθερο - προβεί σε οποιαδήποτε αποστολή πακέτου. Η τιμή του ορίζεται λίγο μεγαλύτερη από του PIFS, ήτοι 128 μsec.
- **Extended IFS - EIFS (Εκτεταμένο δια-πλαισιακό διάστημα):** Το χρονικό αυτό διάστημα είναι το μεγαλύτερο από όλα και χρησιμοποιείται από ένα σταθμό ο οποίος έχει λάβει ένα πακέτο το οποίο δε μπόρεσε να αποκωδικοποιήσει, π.χ. λόγω της ύπαρξης λαθών. Ο χρόνος αυτός είναι απαραίτητος, για να εμποδίσει ένα σταθμό, ο οποίος δε μπόρεσε να αποκωδικοποιήσει π.χ. ένα πακέτο RTS ή CTS, να συγκρουστεί με πακέτα ενός διαλόγου που βρίσκεται σε εξέλιξη.

ΜΕΤΑΓΩΓΗ

Το STA θα πρέπει να ανιχνεύσει τα διαθέσιμα AP's που μπορούν να τα εξυπηρετήσουν και να επιλέξει αυτό που του ταιριάζει και να επιχειρήσει να συνδεθεί(association).
Υπάρχουν δύο τρόποι ανίχνευσης ενός AP,ο παθητικός και ο ενεργητικός, ενώ σε περίπτωση ύπαρξης περισσοτέρων του ενός σημείων πρόσβασης(AP) το STA θα επιλέξει εκείνο που έχει το πιο ισχυρό σήμα ή αυτό που έχει το καλύτερο λόγο σήματος προς θόρυβο.

Παθητική Ανίχνευση

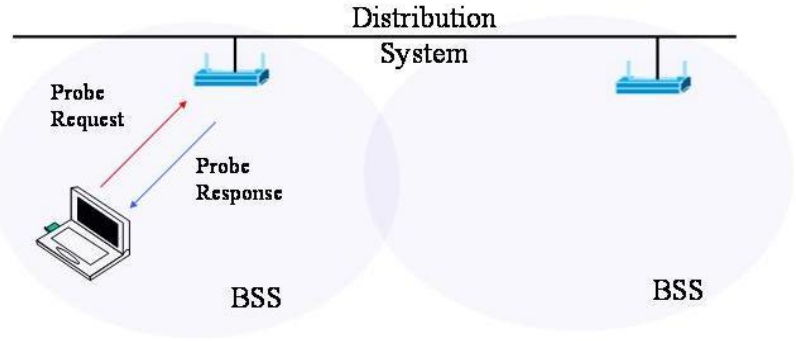
Το κάθε AP στέλνει ανά τακτά χρονικά διαστήματα συγκεκριμένα πακέτα, γνωστά ως Beacons, τα οποία περιέχουν το BSSID και το ESSID του AP. Το STA ακούει όλα τα Beacons και επιλέγει το AP στο οποίο θέλει να συνδεθεί και αποστέλλει Authenticate Request στο AP.



Εικόνα 18 - Παθητική Ανίχνευση

Ενεργητική Ανίχνευση

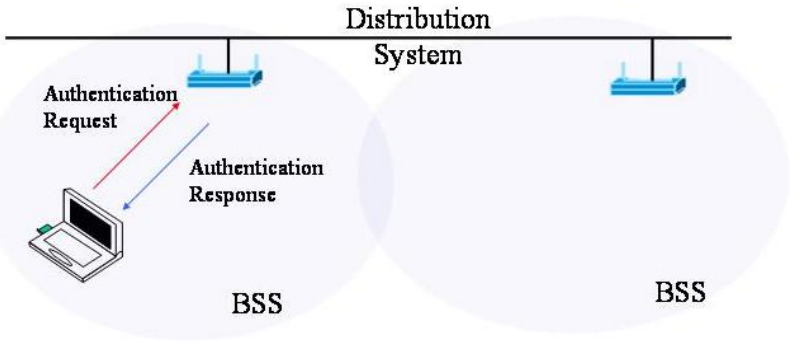
Σε αυτή τη περίπτωση το AP δε δηλώνει την ταυτότητά του συνεχώς όπως στη παθητική, παρά μόνο όταν βρεθεί STA που επιθυμεί να συνδεθεί σε αυτό.
Ένας STA αναζητά AP στέλνοντας Probe Request Frame όπου γνωστοποιεί το ESSID του και τα APs λαμβάνουν το Probe Request Frame απαντούν με Probe Response Frame όπου υπάρχουν πληροφορίες παρόμοιες με το Beacon.



Εικόνα 19 - Ενεργητική Ανίχνευση

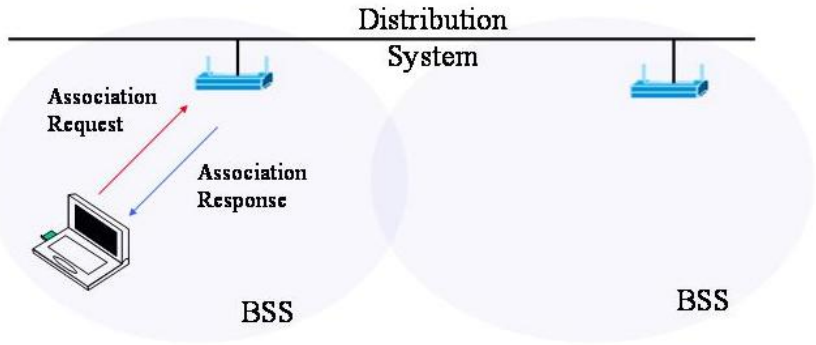
Αφού μια κινητή συσκευή εντοπίσει ένα σημείο πρόσβασης είτε παθητικά είτε ενεργητικά, το επόμενο βήμα είναι να δημιουργηθεί η σύνδεση και σε αρκετές

περιπτώσεις να υπάρξει αυθεντικοποίηση(authentication),δηλαδή έλεγχος της ταυτότητας τόσο του χρήστη(STA) όσο και του AP.



Εικόνα 20 - Authentication Process

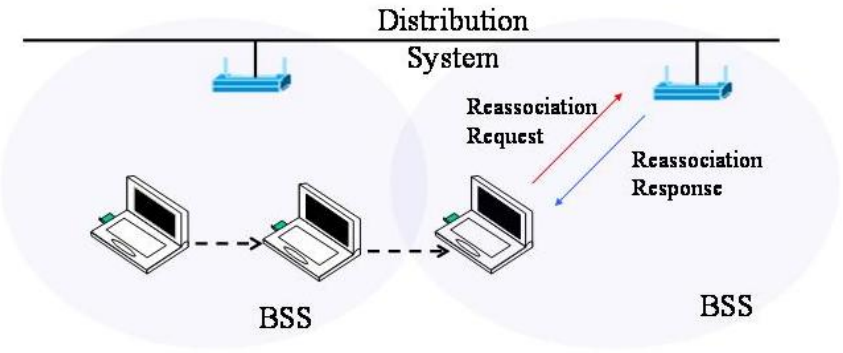
Η φάση του association περιγράφει τη προσπάθεια σύνδεσης ενός STA σε συγκεκριμένο AP για πρώτη φορά ,το STA αποστέλλει στο AP ένα πακέτο Association Request και το AP απαντά με Association Response. Εάν υπάρχει αποδοχή της σύνδεσης από το AP, το STA είναι μέλος του AP και κατ'επέκταση του ESS και μπορεί πλέον να δεχτεί και να στείλει πληροφορία στο δίκτυο.



Εικόνα 21 - Association Process

Αφού το STA εισέλθει στο ESS υπάρχει το ενδεχόμενο αλλαγής AP, σε αυτή περίπτωση το STA αποστέλλει στο νέο AP πακέτο Reassociation Request ενώ το AP απαντά με Reassociation Response.

Το νέο AP θα πρέπει να ενημερώσει το DS για το νέο association και τη νέα θέση του STA,ώστε να υπάρξει προώθηση μηνυμάτων στο νέο AP για τη νέα σύνδεση του STA.



Εικόνα 22

Λόγοι που μπορούν να οδηγήσουν έναν σταθμό σε διαδικασία επανασύνδεσης είναι :

I. Το αρχικό AP έχει τεθεί εκτός λειτουργίας
II. Το σήμα του δευτέρου AP είναι πιο ισχυρό είτε λόγω της μετακίνησης του χρήστη είτε λόγω φυσικών φαινομένων που έχουν μειώσει το λόγο σήματος προς θόρυβο.

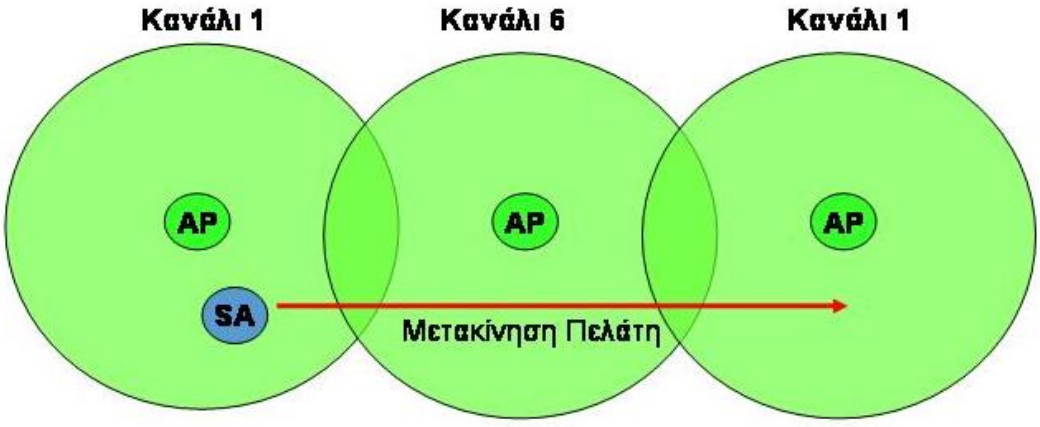
Το IEEE 802.11b πρότυπο που μέχρι στιγμής έχει επικρατήσει στα τοπικά ασύρματα δίκτυα(WAN) δεν αναφέρει τίποτα για το roaming τόσο εντός του ίδιου υποδικτύου (subnet) όσο και σε διαφορετικά subnets(όπου προφανώς το STA θα πρέπει να αλλάξει και IP).Μέχρι πρότινος οι λύσεις για roaming ήταν κυρίως εταιρικές και κάθε εταιρεία δημιουργεί το δικός της πρωτόκολλο, δίχως να υπάρχει συμβατότητα, όσο αφορά το roaming,σε APs διαφορετικών εταιρειών.

Ένα νέο πρότυπο που προτάθηκε από την IEEE το 802.11f καλείται να δώσει μια ενιαία αντιμετώπιση του roaming και κυρίως να προσδιορίσει τις διαδικασίες επικοινωνίας μεταξύ των APs διαμέσου του DS για intra-network handover(ενδοδικτυακή μεταγωγή)

Υπάρχουν δύο είδη μεταγωγής(Handover) :

- Ενδοδικτυακή Μεταγωγή(Intra-network Handover)
- Διαδικτυακή Μεταγωγή (Inter-network Handover)

Η *ενδοδικτυακή μεταγωγή*(Intra-network) σχετίζεται με την μετακίνηση ενός κινητού χρήστη από ένα ασύρματο σημείο σύνδεσης σε έναν άλλο εντός του ίδιου IP δικτύου.
Αντίθετα, η διαδικτυακή μεταγωγή (Inter-network) αφορά τη μετακίνηση κατά την οποία ο χρήστης αλλάζει IP δίκτυο.
Σε ένα IEEE 802.11 WLAN, κατά τη μετακίνηση ενός STA από ένα BSS σε ένα άλλο, εντός του ιδίου ESS, ο σταθμός πραγματοποιεί Intra-network Handover. Κατά τη μετακίνηση αυτή, η προηγούμενη φυσική σύνδεση (Layer 2) του σταθμού χάνεται, και ο σταθμός παραμένει προσωρινά αποκομμένος, ωσότου συνδεθεί σε ένα νέο AP.
Κατά τη διάρκεια της περιόδου όπου ένας σταθμός παραμένει ασύνδετος (handover period), οι προηγούμενες IP συνδέσεις του παύουν να υφίστανται. Το intra-network handover των 802.11 ασύρματων σταθμών υποστηρίζεται από το IEEE 802.11f Inter Access Point Protocol (IAPP).



Εικόνα 23 - Παράδειγμα Περιαγωγής (roaming)

ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΣ ΚΑΙ ΕΠΑΝΑΣΥΝΑΡΜΟΛΟΓΗΣΗ

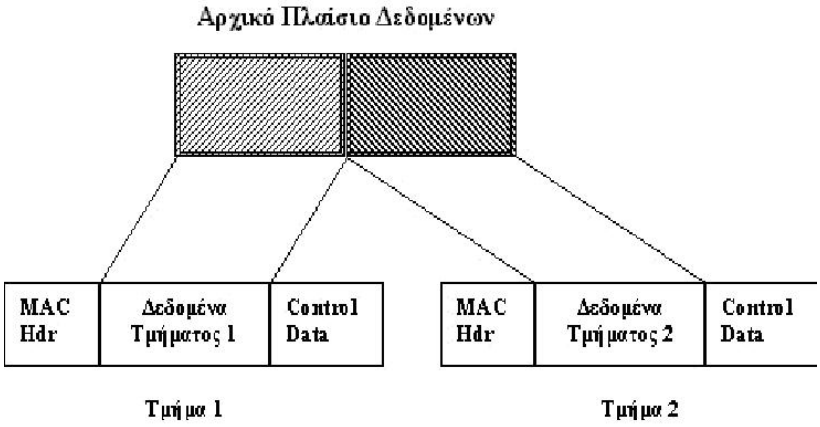
Στα τοπικά δίκτυα με καλώδιο (π.χ.Ethernet) τα πακέτα έχουν μέγεθος μερικών εκατοντάδων bytes. Στο Ethernet για παράδειγμα, το μέγιστο μέγεθος πακέτου φτάνει περίπου τα 1500 bytes. Ωστόσο, σε ένα ασύρματο δίκτυο, τα μεγάλα πακέτα δεν αποτελούν πλεονέκτημα για τους εξής λόγους:

- Λόγω του υψηλότερου ρυθμού λαθών στα ασύρματα περιβάλλοντα (bit-error rate), η πιθανότητα ένα πακέτο να περιέχει λάθη αυξάνεται σύμφωνα με το μέγεθός του.
- Στην περίπτωση όπου ένα πακέτο καταστραφεί, είτε λόγω μιας σύγκρουσης, είτε λόγω εξωτερικών παρεμβολών, όσο μικρότερο είναι το μέγεθός του, τόσο μικρότερη είναι και η επιβάρυνση που απαιτείται για την αναμετάδοσή του.
- Στα συστήματα αναπήδησης συχνότητας, η συχνότητα μετάδοσης αλλάζει συνεχώς. Κατά συνέπεια, όσο μικρότερο είναι το μέγεθος ενός πακέτου, τόσο μικρότερη είναι και η πιθανότητα ότι η μετάδοσή του θα αναβληθεί για μετά την αναπήδηση.

Από την άλλη, όμως, δεν είναι λογικό να δημιουργηθεί ένα πρωτόκολλο το οποίο δε θα μπορεί να χειριστεί πακέτα μεγάλου μεγέθους (π.χ. πακέτα μεγέθους Ethernet - 1500 bytes), γιατί τότε δε θα μπορούσε να υπάρξει δια-σύνδεση των δικτύων 802.11 με τα άλλα δίκτυα της κατηγορίας 802.

Η λύση που προτείνει το 802.11 είναι ένας *μηχανισμός κατακερματισμού και επανασυναρμολόγησης*, όπου τα πακέτα που είναι μεγαλύτερα σε μέγεθος από αυτό που μπορεί να δεχθεί το δίκτυο *κατακερματίζονται* σε μικρότερου - επιτρεπτού μεγέθους **τμήματα (fragments).** Ο μηχανισμός αυτός βασίζεται σε ένα μηχανισμό *μετάδοσης - και - αναμονής (Send - and - wait),* όπου ένας σταθμός αφού μεταδώσει ένα τμήμα δεν επιτρέπεται να προβεί στη μετάδοση ενός νέου τμήματος προτού, είτε λάβει την επιβεβαίωση από το δέκτη, είτε εγκαταλείψει τη μετάδοση του τμήματος μετά από έναν αριθμό προσπαθειών και ακυρώσει τη μετάδοση ολόκληρου του πλαισίου.

Στο παρακάτω σχήμα απεικονίζεται ένα πλαίσιο το οποίο έχει κατακερματιστεί σε δύο μικρότερα για να μπορέσει να μεταδοθεί σε ένα δίκτυο 802.11. Ο πομπός θα πρέπει να περιμένει να λάβει συνολικά δύο επιβεβαιώσεις, μία για το καθένα τμήμα.



Εικόνα 24 - Η λειτουργεία του κατακερματισμού σε ένα δίκτυο 802.11

ΕΙΣΑΓΩΓΗ ΕΝΟΣ ΣΤΑΘΜΟΥ ΣΤΟ ΔΙΚΤΥΟ

Όταν ένας σταθμός θέλει να αποκτήσει πρόσβαση σε ένα BSS (είτε λόγω εκκίνησής του, είτε επειδή εισέρχεται στην περιοχή που καλύπτεται από το κελί, κλπ) το πρώτο μέλημά του είναι να συγχρονιστεί με το σημείο πρόσβασης του κελιού. Υπάρχουν δύο τρόποι να το επιτύχει αυτό.

- *Παθητική Σάρωση (passive scanning):* Στην περίπτωση αυτή ο σταθμός απλά περιμένει να λάβει ένα *πλαίσιο - φάρο (beacon frame)*, από το σημείο πρόσβασης. Το πλαίσιο - φάρος, είναι ένα πλαίσιο που μεταδίδεται περιοδικά από το σημείο πρόσβασης και περιέχει πληροφορίες συγχρονισμού. Οι σταθμοί που επιθυμούν να συγχρονιστούν με το BSS χρησιμοποιούν τις πληροφορίες που υπάρχουν στο πλαίσιο αυτό.
- *Ενεργητική σάρωση (active scanning):* Στην περίπτωση αυτή ο σταθμός προσπαθεί μόνος του να εντοπίσει ένα σημείο πρόσβασης μεταδίδοντας *πλαίσια*

αίτησης εξερεύνησης (probe request frames) και περιμένοντας να λάβει *πλαίσια απάντησης εξερεύνησης (probe response frames)* από κάποιο σημείο πρόσβασης.

Επικύρωση χρήστη (authentication process)

Άπαξ και ένας σταθμός εντοπίσει και συγχρονιστεί με το σημείο πρόσβασης, προχωρά στη διαδικασία επικύρωσης, η οποία αφορά την επικοινωνία μεταξύ του σταθμού και του σημείου πρόσβασης, ώστε να διαπιστωθεί η γνώση ενός μυστικού κωδικού πρόσβασης.

Συσχέτιση χρήστη (association process)

Μετά την επικύρωση του, ο σταθμός εισέρχεται στη διαδικασία συσχέτισης, με την οποία ανταλλάσσονται πληροφορίες σχετικά με τους σταθμούς και τις δυνατότητες του BSS, και με την οποία το *σύστημα διανομής* (distribution system - DS) μπορεί να ενημερώνεται για την τρέχουσα θέση του σταθμού. Μόνο αφού ολοκληρωθεί και αυτή η διαδικασία μπορεί ο σταθμός να μεταδώσει και να λάβει πλαίσια στο δίκτυο.

ΠΕΡΙΑΓΩΓΗ

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. Η περιαγωγή στα δίκτυα 802.11 είναι παρόμοια με τη *διαδικασία μετάβασης (handover)* στις κινητές τηλεπικοινωνίες με δύο διαφορές:

- Σε ένα τοπικό δίκτυο 802.11, το οποίο βασίζεται στη μετάδοση πακέτων, η μετάβαση από κελί σε κελί μπορεί να πραγματοποιηθεί **μεταξύ** μεταδόσεων, καθιστώντας τη διαδικασία της περιαγωγής ευκολότερη απ' ότι σε ένα δίκτυο κινητής τηλεφωνίας, όπου η μετάβαση μπορεί να γίνει και κατά τη διάρκεια μιας τηλεφωνικής συνδιάλεξης.
- Σε ένα δίκτυο κινητής τηλεφωνίας, μια προσωρινή διακοπή της σύνδεσης δεν επηρεάζει σημαντικά την επικοινωνία, ενώ σε ένα τοπικό δίκτυο πακέτου η διακοπή της μετάδοσης ενός πλαισίου λόγω της μετάβασης σε ένα άλλο κελί, σημαίνει ότι η αναμετάδοσή του θα πρέπει να γίνει από τα ανώτερα επίπεδα, γεγονός που υποβαθμίζει σημαντικά την απόδοση του δικτύου.

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 ενεργητική / παθητική σάρωση και μια διαδικασία ανασυσχέτισης, με την οποία ένας σταθμός ο οποίος μεταβαίνει από ένα κελί σε ένα άλλο θα μπορεί να συσχετιστεί με το καινούργιο κελί.

ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ

Ένα από τα πρώτα θέματα που θα πρέπει να αντιμετωπίζεται από όσους υλοποιούν ένα ασύρματο δίκτυο είναι το θέμα της ασφάλειας (security). Οι μεγαλύτερες ανησυχίες που απασχολούν τους διαχειριστές ενός ασύρματου δικτύου σχετικά με τη δράση ενός εισβολέα είναι δύο: (α) η πρόσβαση στους πόρους του τοπικού δικτύου με τη χρήση παρόμοιου ασύρματου εξοπλισμού και (β) η υποκλοπή της κυκλοφορίας του δικτύου.

Η αντιμετώπιση της παράνομης πρόσβασης στο δίκτυο γίνεται, όπως έχει ήδη αναφερθεί, με τη χρήση ενός μηχανισμού επικύρωσης, όπου ο ασύρματος σταθμός για να αποκτήσει πρόσβαση στο δίκτυο θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει ένα μυστικό κωδικό.

Η αντιμετώπιση της υποκλοπής της κυκλοφορίας γίνεται με τη χρήση του αλγορίθμου WEP (Wired Equivalent Privacy), ο οποίος εκτελείται σε όλους τους σταθμούς και δεν είναι τίποτε άλλο από μία γεννήτρια ψευδοτυχαίων αριθμών (Pseudo Random Number Generator), η οποία αρχικοποιείται από ένα διαμοιραζόμενο μυστικό κλειδί. Για κάθε πακέτο που μεταδίδεται από ένα σταθμό, η γεννήτρια παράγει μια ψευδοτυχαία ακολουθία bit, της οποίας το μήκος είναι ίσο με το μεγαλύτερο δυνατό μέγεθος πακέτου και η οποία χρησιμοποιείται για την κρυπτογράφηση των bits του μηνύματος. Ο δέκτης από την πλευρά του θα πρέπει να γνωρίζει το μυστικό κλειδί αρχικοποίησης, έτσι ώστε για κάθε εισερχόμενο πακέτο να μπορεί να παράγει τη σωστή ψευδοτυχαία ακολουθία για την αποκρυπτογράφησή του.

ΤΥΠΟΙ ΠΛΑΙΣΙΩΝ

Το πρότυπο 802.11 υποστηρίζει τρεις διαφορετικούς τύπους πλαισίων:

Πλαίσια Δεδομένων: Χρησιμοποιούνται για τη μετάδοση δεδομένων

Πλαίσια Ελέγχου: Χρησιμοποιούνται για τον έλεγχο της πρόσβασης στο μέσο (πακέτα, RTS, CTS, ACK).

Πλαίσια Διαχείρισης: Χρησιμοποιούνται για τη μετάδοση πληροφοριών διαχείρισης μεταξύ των σταθμών και είναι παρόμοια με τα πλαίσια δεδομένων με τη μόνη διαφορά ότι δεν προωθούνται στα ανώτερα επίπεδα.

Η κάθε μία από τις κατηγορίες αυτές χωρίζεται σε υπο-κατηγορίες, ανάλογα με τη συγκεκριμένη λειτουργία που εκτελεί.

ΔΟΜΗ ΠΛΑΙΣΙΩΝ

Όλα τα πλαίσια του προτύπου 802.11 έχουν την παρακάτω γενική μορφή.

Preamble	PLCP header	MAC data	CRC

Εικόνα 25 - Η γενική μορφή ενός πλαισίου 802.11

Τα πεδία *Preamble* και *PLCP header*, είναι δύο πεδία ελέγχου τα οποία δε θα μας απασχολήσουν εδώ. Εμείς θα ασχοληθούμε με τα πεδία *MAC data* και *CRC*. Ειδικότερα,

<u>*MAC Data:*</u> Το πεδίο αυτό περιέχει τις πληροφορίες που αποθηκεύονται σε ένα πλαίσιο MAC. Η γενική του μορφή φαίνεται παρακάτω.

2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	8 bytes	6 bytes	0 - 2312 bytes	4 bytes
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	CRC Check

Εικόνα 26 - Η γενική μορφή ενός πλαισίου MAC στο 802.11

Από τα πεδία αυτά, τα πρώτα 7 αποτελούν την *επικεφαλίδα* του πλαισίου (MAC Header), τα οποία επεξηγούνται παρακάτω. Εδώ να σημειώσουμε ότι δεν περιέχονται όλα τα πεδία σε όλα τα πλαίσια. Ο τύπος και ο αριθμός των πεδίων που περιέχονται σε κάθε πλαίσιο είναι ανάλογο του τύπου του.

Frame Control (Έλεγχος Πλαισίου): Το πεδίο αυτό έχει μήκος 16 bits και χωρίζεται στα παρακάτω υπο-πεδία:

2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgt	More Data	WEP	Order

Εικόνα 27 - Η μορφή πεδίου Frame Control

Protocol Version: Έχει μέγεθος 2 bits και χρησιμοποιείται για τον προσδιορισμό της έκδοσης του πρωτοκόλλου 802.11 (π.χ. 802.11, 802.11a, 802.11b, 802.11g, κλπ).

Type & Subtype: Τα δύο αυτά πεδία χρησιμοποιούνται για τον προσδιορισμό του *κύριου* και του *δευτερεύοντος τύπου* του πλαισίου. Για παράδειγμα, στο 802.11, η τιμή 00 στο πεδίο **Type** και η τιμή 1011 στο πεδίο **Subtype**, ορίζουν ότι το πλαίσιο αυτό είναι πλαίσιο *διαχείρισης (Type: management)* και ειδικότερα περιέχει πληροφορίες που σχετίζονται με την *επικύρωση* του σταθμού *(subtype: authentication).*

ToDS: Το πεδίο αυτό έχει τιμή 1, όταν αποστέλλεται στο Σημείο Πρόσβασης με σκοπό την **προώθησή** του στο Σύστημα Διανομής (συμπεριλαμβάνεται και η περίπτωση όπου ο σταθμός προορισμού βρίσκεται μέσα στο ίδιο BSS και το AP χρησιμοποιείται απλά ως αναμεταδότης).

FromDS: Προσδιορίζει αν το πλαίσιο αυτό προήλθε από το σύστημα διανομής (1), ή όχι (0).

More Fragments: Το πεδίο αυτό χρησιμοποιείται στην περίπτωση όπου ένα πλαίσιο (frame) έχει κατακερματιστεί σε μικρότερα τμήματα (fragments). Έχει την τιμή 1, όταν ακολουθούν και άλλα τμήματα που ανήκουν στο συγκεκριμένο πλαίσιο και την τιμή 0 όταν πρόκειται για το τελευταίο τμήμα ενός πλαισίου.

Retry: Το πεδίο αυτό χρησιμοποιείται για να σηματοδοτήσει αν το πλαίσιο αυτό (ή τμήμα του) αποτελεί την **αναμετάδοση** ενός πλαισίου (ή τμήματος). Χρησιμοποιείται από το δέκτη για να μπορεί να ξεχωρίζει τα πακέτα που λαμβάνει δύο φορές (duplicates) σε περίπτωση όπου έχει χαθεί η επιβεβαίωση λήψης.

Power Management: Το πεδίο αυτό χρησιμοποιείται για τον προσδιορισμό της κατάστασης κατανάλωσης ενέργειας στην οποία θα εισέλθει ο σταθμός μετά τη μετάδοση του τρέχοντος πλαισίου (π.χ. σε κατάσταση *χαμηλής κατανάλωσης, ή αποθήκευσης ενέργειας (power saving mode),* κλπ). Αυτό το πεδίο είναι χρήσιμο, μιας και οι σταθμοί ως ασύρματοι μπορεί να λειτουργούν με μπαταρίες.

More Data: Το πεδίο αυτό έχει σχέση με τη διαχείριση της κατανάλωσης ισχύος του σταθμού (power management) και χρησιμοποιείται από το σημείο πρόσβασης.

WEP: Το πεδίο αυτό χρησιμοποιείται, για να σηματοδοτήσει ότι το κυρίως σώμα του πλαισίου έχει κρυπτογραφηθεί χρησιμοποιώντας τον αλγόριθμο Wired Equivalent Privacy.

Order: Αυτό είναι ένα εξειδικευμένο πεδίο και χρησιμοποιείται μόνο από το πρωτόκολλο της Digital Equipment Corporation, LAT.

Duration / ID: Το πεδίο αυτό έχει παραπάνω από μία έννοιες, ανάλογα με τον **τύπο** του πλαισίου (ο οποίος προσδιορίζεται από τα πεδία Type & Subtype που είδαμε παραπάνω). Στη πιο συνηθισμένη περίπτωση, η τιμή που περιέχει χρησιμοποιείται για τον υπολογισμό του NAV (Network Allocation Vector).

Πεδία Διευθύνσεων (Address 1,2,3,4): Τα πεδία αυτά χρησιμοποιούνται για τη διευθυνσιοδότηση των πλαισίων. Η χρήση τους ποικίλει ανάλογα με την τιμή που έχουν τα πεδία **ToDS** και **FromDS**.

Sequence Control (Έλεγχος Ακολουθίας): Χρησιμοποιείται για τον έλεγχο της σειράς των τμημάτων (fragments) που ανήκουν στο ίδιο πλαίσιο (frame). Αποτελείται από δύο υπο-πεδία:

a) **Frame Number:** Προσδιορίζει τον αριθμό του πλαισίου.

b) **Sequence Number:** Προσδιορίζει τον αριθμό του **τμήματος** του πλαισίου.

CRC Check: Αυτό το πεδίο περιέχει τον CRC - 32 έλεγχο λαθών για ολόκληρο το πλαίσιο (ή τμήμα).

ΔΙΚΤΥΑ ΕΙΔΙΚΟΥ ΣΚΟΠΟΥ ΜΕ ΤΟ 802.11 (Ad hoc networks)

Σε μερικές περιπτώσεις μπορεί να χρειάζεται να υλοποιηθεί ένα ασύρματο δίκτυο που να ακολουθεί το πρότυπο 802.11, αλλά του οποίου η δομή να μην είναι απαραίτητο να είναι κυψελοειδής, ή καλύτερα να μην περιέχει *Σημεία Πρόσβασης*. Παραδείγματα αυτού του τύπου περιλαμβάνουν την ασύρματη διασύνδεση δύο φορητών υπολογιστών (laptops).

Το πρότυπο 802.11, αντιμετωπίζει αυτήν την ανάγκη, προσδιορίζοντας τον *Ad-Hoc τρόπο λειτουργίας (Ad-Hoc mode)*. Ένα ασύρματο δίκτυο που βρίσκεται σε Ad-Hoc τρόπο λειτουργίας, δεν περιέχει σημεία πρόσβασης και ένα τμήμα των λειτουργιών του εκτελείται από τους ίδιους τους σταθμούς, όπως είναι ο συγχρονισμός, η εκπομπή πλαισίων - φάρων, κλπ. Επίσης, κάποιες άλλες λειτουργίες δεν υποστηρίζονται, όπως η αναμετάδοση πλαισίων μεταξύ σταθμών του δικτύου που δεν έχουν τη δυνατότητα άμεσης επικοινωνίας, μιας και αυτή η λειτουργία κανονικά εκτελείται από το σημείο πρόσβασης. Αυτό σημαίνει ότι όλοι οι σταθμοί σε ένα ad-hoc δίκτυο θα πρέπει να μπορούν να επικοινωνήσουν με όλους τους υπόλοιπους.

ΤΑ ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΥΠΟΠΡΟΤΥΠΑ ΤΟΥ 802.11

- **IEEE 802.11a**

Η IEEE επικύρωσε το πρότυπο 802.11a το 1999 αναγνωρίζοντας ότι οι τηλεοπτικές, όπως και οι ‘βαριές’ εφαρμογές πολυμέσων θα απαιτούσαν ταχύτητες υψηλότερες από 11 Mb/s. Το πρότυπο 802.11a είναι βελτιστοποιημένο για υψηλή απόδοση στα εσωτερικά περιβάλλοντα. Προσδιορίζει τις μεθόδους που χρησιμοποιούνται για τη μετάδοση δεδομένων μέχρι 54 Mb/s. Ένας κατασκευαστής μάλιστα έχει δηλώσει ότι είναι σε θέση να προχωρήσει το πρότυπο ώστε να υποστηρίζει ταχύτητες μέχρι 108 Mb/s, με κάποιος μικρές αλλαγές.

Το IEEE 802.11b χρησιμοποιεί το πλήρες εύρος ζώνης συχνοτήτων κάθε υποκαναλιού για να διαμορφώσει τα σήματά του. Το IEEE 802.11a χρησιμοποιεί μια διαφορετική προσέγγιση η οποία καλείται Coded Orthogonal Frequency Division Multiplexing (CODFM). Τα χαμηλότερα 200 MHz υποδιαιρούνται σε οκτώ κανάλια των 20 MHz το κάθε ένα. (Τα πρόσθετα 40 MHz είναι για το χωρισμό καναλιών.) Κάθε κανάλι υποδιαιρείται σε 52 υποκανάλια, το κάθε ένα περίπου της τάξης των 300 KHz. Αυτά τα στενότερα κανάλια βελτιώνουν τη μεταφορά δεδομένων επειδή είναι λιγότερο ευαίσθητα στη διασπορά χρόνου και συχνότητας. Από τα 52 κανάλια, τα 48 χρησιμοποιούνται για δεδομένα και τα υπόλοιπα τέσσερα χρησιμοποιούνται για την ανίχνευση σφάλματος.
Κάθε κανάλι χρησιμοποιεί διαμόρφωση μετατόπισης φάσης (PSK). Το πρότυπο απαιτεί τα συμβατά συστήματα να υποστηρίζουν διαμόρφωση φάσης 90 μοιρών 2,4 και 16 επιπέδων για κάθε κανάλι. Αυτά αντιστοιχούν σε ταχύτητες 6,12, και 24 Mb/s αντίστοιχα. Το 802.11a επίσης προσδιορίζει και υψηλότερους ρυθμούς μεταφοράς που αντιστοιχούν σε ταχύτητες 36, 48 και 54 Mb/s.
Οι τεχνολογίες 802.11a και 802.11b πρέπει να είναι σε θέση να λειτουργήσουν παράλληλα στο τοπικό LAN δεδομένου ότι χρησιμοποιούν την ίδια MAC και λειτουργούν σε διαφορετικές περιοχές συχνότητας. Εντούτοις, οι διαφορές στη διάδοση μπορούν να κάνουν απαραίτητο τον επαναπροσδιορισμό των περιοχών κάλυψης τους.

- **IEEE 802.11g**

  Βλέποντας την ανάγκη για ακόμα μεγαλύτερους ρυθμούς η IEEE ολοκλήρωσε πρόσφατα την επέκταση 802.11g, η οποία υποστηρίζει ρυθμούς μέχρι 54Mbps και παράλληλα είναι συμβατό προς τα πίσω με το 802.11b. Αναπτύσσει μια επέκταση υψηλότερης-ταχύτητας του PHY επιπέδου στο 802.11b πρότυπο, διατηρώντας την προς τα πίσω συμβατότητα με τις υπάρχουσες 802.11b συσκευές. Ο ρυθμός μετάδοσης που έχει ως στόχο το πρόγραμμα είναι τουλάχιστον 20 Mbps.

- **IEEE 802.11b**

Το έτος 2000, το 802.11b έγινε η πρότυπη ασύρματη τεχνολογία δικτύωσης Ethernet. Ο οργανισμός WiFI δημιουργήθηκε για να εξασφαλίσει διαλειτουργικότητα μεταξύ των

προϊόντων που ακολουθούν το 802.11b. Με μια ρεαλιστική ρυθμοαπόδοση 2.5- 4Mbps, είναι αρκετά γρήγορο για τις περισσότερες εφαρμογές δικτύων και ανεκτό για τις μεταφορές μεγάλων αρχείων.

Ένας ασύρματος προσαρμογέας δικτύων (network adapter) 802.11b μπορεί να λειτουργήσει σε δύο τρόπους: Στον ειδικό (ad-hoc) και υποδομής (infrastructure). Στον τρόπο υποδομής, όλη η κυκλοφορία περνά μέσω ενός ασύρματου σημείου πρόσβασης (access point) το οποίο συνδέει τις ασύρματες συσκευές μεταξύ τους και με το ενσύρματο δίκτυο Ethernet. Στον ειδικό τρόπο οι υπολογιστές μιλούν άμεσα ο ένας στον άλλο και δεν χρειάζονται κάποιο σημείο πρόσβασης.Τα σημεία πρόσβασης χωρίζονται σε τρία είδη – γέφυρες (bridges), δρομολογητής NAT και δρομολογητής NAT με γέφυρα.Ο τύπος γέφυρας συνδέει ένα ασύρματο δίκτυο με ένα ενσύρματο δίκτυο διαφανώς.Η επικοινωνία είναι δυνατή μεταξύ των δύο δικτύων και προς τις δύο κατευθύνσεις.Ο τύπος δρομολογητή NAT δρομολογεί την κυκλοφορία από το ασύρματο δίκτυο σε ένα ενσύρματο Ethernet δίκτυο, αλλά όχι προς την αντίθετη κατεύθυνση. Αυτός ο τύπος μπορεί να χρησιμοποιηθεί για να μοιραστεί μια σύνδεση με το Διαδίκτυο.

Τέλος, υπάρχουν οι υβριδικές συσκευές που είναι ταυτόχρονα δρομολογητές NAT και γέφυρες, οι οποίες γεφυρώνουν τα ενσύρματα με τα ασύρματα δίκτυά, και τα δρομολογούν και τα δύο στο Διαδίκτυο χρησιμοποιώντας μια ενιαία διεύθυνση IP. Αυτό είναι καλό για το μοίρασμα μιας σύνδεσης με το Διαδίκτυο όταν συνυπάρχουν και οι δύο τύποι δικτύων.

Οι προσαρμογείς δικτύου 802.11b βγαίνουν σε δύο σημαντικούς τύπους. Κάρτες PCMCIA για τα laptop και USB για τους υπολογιστές γραφείου. Επιπλέον, υπάρχουν προσαρμογείς PCI που επιτρέπουν τη σύνδεση μιας κάρτας PCMCIA με μια υποδοχή PCI.Οποιοσδήποτε προσαρμογέας δικτύου που θα βρεθεί μέσα στην εμβέλεια ενός άλλου προσαρμογέα δικτύου 802.11b ή ενός σημείου πρόσβασης, μπορεί αμέσως να συνδεθεί με το δίκτυο εκτός αν το ασύρματο πρωτόκολλο κρυπτογράφησης (WEP – Wireless Encryption Protocol) είναι ενεργοποιημένο. Το WEP είναι αρκετά ασφαλές για τις περισσότερες οικιακές εφαρμογές και επιχειρήσεις αλλά αυτό δεν σημαίνει ότι δεν μπορεί να παραβιαστεί. Υπάρχουν αρκετά ελαττώματα στο WEP καθιστώντας το ακατάλληλο προς χρήση για υψηλές εφαρμογές ασφάλειας.

Η χρήση WEP επιβραδύνει ένα ασύρματο δίκτυο σε ποσοστό 20-50% της ταχύτητας ανάλογα με το προϊόν. Το ζήτημα ταχύτητας είναι συχνά το αποτέλεσμα ενός σημείου πρόσβασης χωρίς αρκετή δύναμη επεξεργασίας.

Υπάρχουν δύο τύποι κρυπτογράφησης: 64μπιτες και 128μπιτες. Όλοι οι κόμβοι πρέπει να είναι στο ίδιο επίπεδο κρυπτογράφησης με το ίδιο κλειδί για να λειτουργήσουν. Η 40μπιτη και η 64μπιτη κρυπτογράφηση είναι ταυτόσημες, είναι μόνο θέμα του πώς ο κατασκευαστής αποφάσισε να ονομάσει το προϊόν. Συχνά οι 128μπιτες κάρτες μπορούν να τεθούν σε ρυθμό 40/64 μπιτ.

Ένα σήμα 802.11b πλήρους ισχύος μπορεί να δώσει πραγματικό ρυθμό μεταφοράς δεδομένων 3.5 - 4.5 Mbps χωρίς την ενεργοποίηση του WEP. Με το WEP ενεργοποιημένο ο ρυθμός περιορίζεται στα 2.5 - 3.5 Mbps. Καθώς προστίθενται τοίχοι και απόσταση μεταξύ του ασύρματου προσαρμογέα και του σημείου πρόσβασής, η ταχύτητά μειώνεται παραπάνω.

Το 802.11b είναι ένα πρωτόκολλο Half Duplex - μπορεί να στείλει ή να λάβει δεδομένα, αλλά όχι και οι δύο συγχρόνως. Επιπλέον χρησιμοποιεί την ίδια ζώνη συχνοτήτων στα 2.4 GHz με πολλά ασύρματα τηλέφωνα έτσι υπάρχουν αρκετές πιθανότητες παρεμβολών όταν τα παραπάνω συνυπάρχουν στον ίδιο χώρο.

Ορισμοί και ομάδες εργασίας προτύπων ασύρματης δικτύωσης 802.11

Το 1997 η IEEE υιοθέτησε το πρώτο πρότυπο ασύρματων τοπικών δικτύων (WLAN), το IEEE 802.11, Το πρότυπο αυτό καθορίζει τον έλεγχο πρόσβασης μέσου (MAC) και τα φυσικά στρώματα (PHY) για ένα LAN με ασύρματη σύνδεση. Το πρότυπο αυτό εξετάζει την τοπική δικτύωση όπου οι συνδεδεμένες συσκευές επικοινωνούν μέσω του αέρα με άλλες συσκευές που βρίσκονται κοντά η μια στην άλλη.

Από την αρχική καθιέρωση της ομάδας εργασίας 802.11, αυτή έχει επεκταθεί σε πολυάριθμες στοιχειώδεις ομάδες, που καθορίζονται από τα γράμματα a μέχρι το i. Οι ομάδες a, b, και c έχουν ολοκληρώσει την εργασία τους, και τα αποτελέσματα προστέθηκαν στα αρχικά πρότυπα. Οι λεπτομέρειες κάθε στοιχειώδους ομάδας εργασίας παρατίθενται κατωτέρω.

Το 802.11b είναι ιδιαίτερα επιτυχημένο, και υπάρχουν πολλά προϊόντα διαθέσιμα σήμερα στην αγορά που χρησιμοποιούν αυτό το πρότυπο. Προϊόντα βασισμένα σε 802.11a είναι στην ανάπτυξη από πολλές εταιρίες επίσης. Επειδή τα πρότυπα αυτά χρησιμοποιούν διαφορετικά τμήματα του φάσματος, τα 802.11a και 802.11b δεν είναι συμβατά μεταξύ τους. Συνεπώς, μια νέα στοιχειώδης ομάδα εργασίας, η 802.11g, ελπίζει να παρέχει το υψηλό ρυθμό μεταφοράς δεδομένων του 802.11a, διατηρώντας την προς τα πίσω συμβατότητα με τα 802.11b προϊόντα.

802.11c – Παρέχει τεκμηρίωση για συγκεκριμένες διαδικασίες επιπέδου MAC του 802.11στο ISO/ IEC (Διεθνής Οργανισμός για την Τυποποίηση / Διεθνής Ηλεκτροτεχνική Επιτροπή) 10038 πρότυπο (IEEE 802.1D). Η εργασία του ολοκληρώθηκε.

802.11d – Δημοσιεύει ορισμούς και απαιτήσεις για να επιτρέψει στο πρότυπο 802.11 να λειτουργήσει στις χώρες που δεν εξυπηρετούνται αυτήν την περίοδο από το πρότυπο. Σε εξέλιξη.

802.11e - Προσπαθεί να εμπλουτίσει το MAC επίπεδο του 802.11 για να αυξήσει την ποιότητα της παρεχόμενης υπηρεσίας. Η βελτίωση στις ικανότητες και την αποδοτικότητα σχεδιάζονται έτσι ώστε να επιτρέψουν σε εφαρμογές όπως η φωνή, το βίντεο, ή η μεταφορά ήχου πάνω από 802.11 ασύρματα δίκτυα. Σε εξέλιξη.

802.11f - Αναπτύσσει τις συνιστώμενες πρακτικές για την εφαρμογή ορισμών του 802.11 για τα σημεία πρόσβασης και τα συστήματα διανομής. Ο σκοπός είναι να αυξηθεί η συμβατότητα μεταξύ των συσκευών σημείου πρόσβασης διαφορετικών προμηθευτών. Σε εξέλιξη.

802.11h - Ενισχύει τα επίπεδα MAC του 802.11 και PHY του 802.11a για να παρέχει τις επεκτάσεις διαχείρισης και ελέγχου δικτύων, για τη διαχείριση του φάσματος και της ισχύος μετάδοσης στη ζώνη 5 GHz. Αυτό θα επιτρέψει τη ρυθμιστική αποδοχή των προτύπων σε μερικές ευρωπαϊκές χώρες. Σε εξέλιξη.

802.11i - Ενισχύει τους μηχανισμούς ασφάλειας και πιστοποίησης ταυτότητας του προτύπου 802.11. Σε εξέλιξη. Ύστερα από 3.5 χρόνια έρευνας η ομάδα εργασίας IEEE 802.11i ολοκλήρωσε την προτυποποίηση του 802.11i που έρχεται να συμπληρώσει τα κενά ασφάλειας των ασύρματων τοπικών δικτύων (802.11). Στις βελτιώσεις συμπεριλαμβάνονται η ισχυρότερη κρυπτογράφηση, η αυθεντικοποίηση και οι στρατηγικές διαχείρισης κλειδιών (key management strategies). Όλα αυτά προσφέρουν ένα αρκετά καλό επίπεδο ασφάλειας των δεδομένων αλλά και του συνόλου του συστήματος.

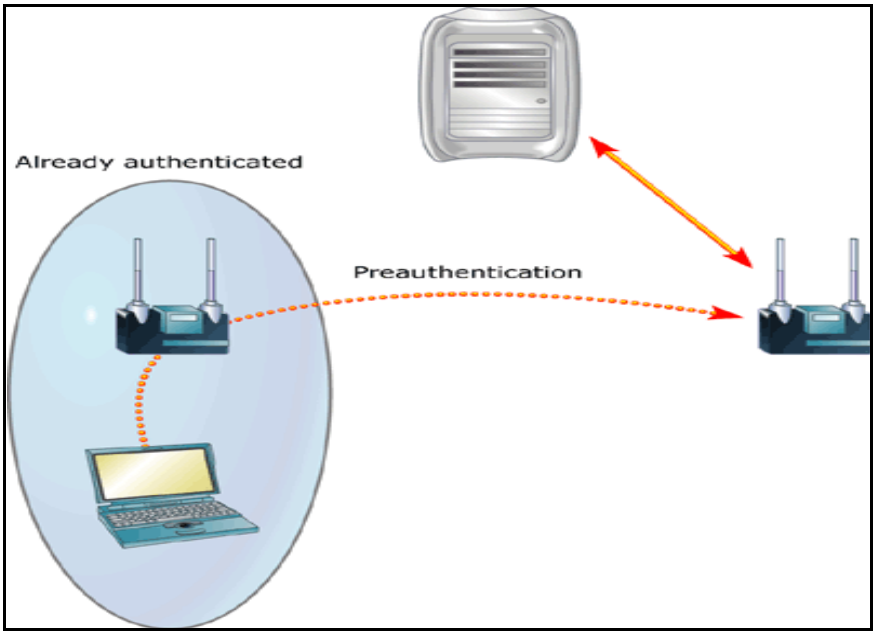
Εν αναμονή του 802.11i, το 2002 η συνεργασία των εταιρειών σχετικών με το χώρο των ασυρμάτων δικτύων (Wi-Fi Alliance) προχώρησε στην έκδοση του WPA(WiFi Protected Access), το οποίο θεωρείται ως προάγγελος και υποσύνολο του 802.11i. Παρείχε καλύτερη κρυπτογράφηση με TKIP (Temporal Key Integrity Protocol), ευκολότερη εγκατάσταση (pre-shared key) και δυνατότητα συνεργασίας με RADIUS Server για 802.1X αυθεντικοποίηση.
Πρόσφατα ολοκληρώθηκε η προτυποποίηση του 802.11i (Ιούνιος 2004) το οποίο περιλαμβάνει τα στοιχεία του WAP, προσφέροντας επιπλέον την δυνατότητα κωδικοποίησης με χρήση του αλγορίθμου AES (Advanced Encryption Standard). Πρόκειται για έναν αρκετά ισχυρό συμμετρικό αλγόριθμο κρυπτογράφησης, τύπου block cipher, το οποίο επιτελεί τις λειτουργίες του σε blocks δεδομένων και όχι άμεσα στο σύνολο αυτών. Τα κλειδιά του AES είναι δυνατόν να έχουν μήκος 128, 192, 256 bits αλλά για την απλούστερη και ταχύτερη διαδικασία προτιμάται το μήκος να είναι 128 bits. Το αντίτιμο στην ισχυρή κρυπτογράφηση που προσφέρει ο AES είναι ότι χάνουμε σε επιδόσεις, διότι οι απαιτήσεις για κρυπτογράφηση και αποκρυπτογράφηση έχουν κάποιο κόστος στη CPU και κατ' επέκταση σε ενέργεια εδικά πρόκειται για φορητές συσκευές. Στα επιπλέον χαρακτηριστικά του 802.11i είναι :

Key-Caching

Αποθήκευση πληροφοριών της συσκευής μας στο «δίκτυο» έτσι ώστε όταν αποσυνδεθούμε από το Access Point και προσπαθήσουμε να συνδεθούμε ξανά να μην χρειαστεί να εισάγουμε όλες τις πληροφορίες και όλα αυτά με διαφάνεια προς το χρήστη.

Pre-authentication

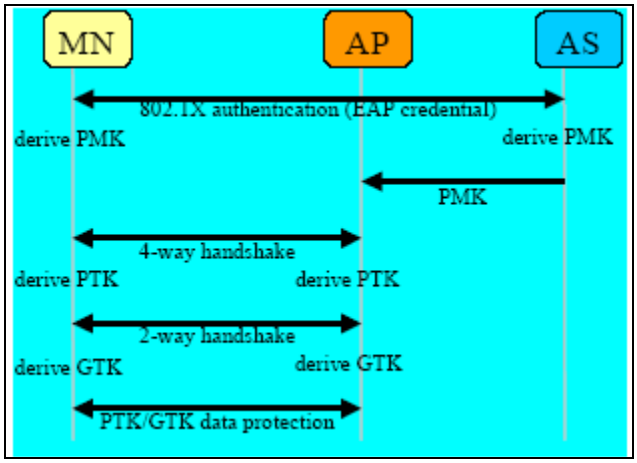
Επιτρέπει στο χρήστη να αυθεντικοποιηθεί σε κάποιο Access Point δίχως να έχει συνδεθεί μαζί του, και αυτό επιτυγχάνεται με το να αποσταλεί πακέτο αυθεντικοποίησης του κινούμενου σταθμού από το Access Point που βρίσκεται τη δεδομένη στιγμή στα υπόλοιπα κοντινά Access Points. Στοιχείο ιδιαίτερα σημαντικό για την γρήγορη περιαγωγή των κινούμενων σταθμών.



Εικόνα 28 - pre - authenticated MN

Από την φύση τους όπως έχουμε παρατηρήσει τα ασύρματα δίκτυα έχουν πολλές απειλές. Κάποιος τρίτος μπορεί να εισέλθει σε μια επικοινωνία και να κρυφακούσει ή τροποποιήσει δεδομένα. Γι' αυτό άλλωστε επιζητούμε την αυθεντικοποίηση κυρίως της κινούμενης συσκευής αλλά και του χρήστη. Για να το πετύχει αυτό το 802.11i βασίζεται στο μηχανισμό EAP/801.1X. Κατά την φάση αυθεντικοποίησης του MN στον AS

παράγεται το Pairwise Master Key (PMK), η συνάρτηση παραγωγής PMK καθορίζεται από την EAP μέθοδο που χρησιμοποιείται κάθε φορά (EAP-MD5, EPA-TLS, EAP-TTLS). Η μέθοδος είναι επίσης που καθορίζει εάν θα αυθεντικοποιηθεί μόνο ο MN(EAP-MD5) ή θα υπάρξει αμοιβαία αυθεντικοποίηση MN και τουAS (π.χ. EAP-TLS). Όταν δημιουργηθεί το PMK στη συνέχεια μεταβιβάζεται στο Access Point μέσω RADIUS μηνύματος όπου και αποτελεί την αποδοχή(access-accept) και αυθεντικοποίηση του MN.



Εικόνα 29 - Φάσεις Λειτουργίας IEEE 802.11i

Από το PMK μέσω τετραπλής χειραψίας(4-way handshake) μεταξύ MN και AP παράγεται το Pairwise Transient Key(PTK) για την ασφαλή επικοινωνία MN και AP και την επιβεβαίωση ότι δεν υπάρχει ο κίνδυνος κάποιος τρίτος ενδιάμεσος στην επικοινωνία να κρυφακούει (Man in the middle). Επίσης, για την αποστολή ασφαλών broadcast ή multicast μηνυμάτων στα APs δημιουργείται και το GTK(Group Transient Key) το οποίο προκύπτει από το PTK.

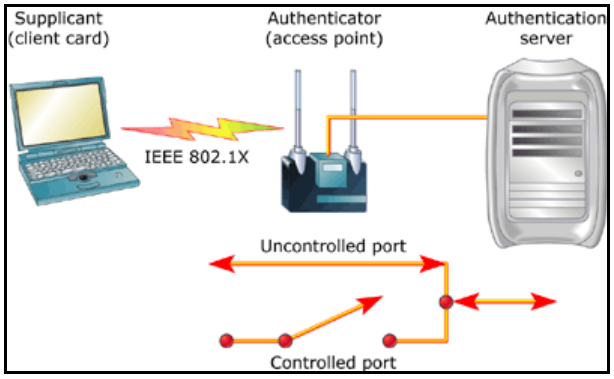
Για την προστασία της μεταδιδόμενης πληροφορίας και τη διατήρηση της ακεραιότητάς της, χρησιμοποιείται από το 802.11i τόσο το TKIP όσο και το CCMP

	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key-size	40 ή 104	128	128
Key-life	24 bit IV	48 bit IV	48 bit IV
Integrity Data	CRC-32	Michael	CCM
Header	-	Michael	CCM
Replay	-	Χρήση IV	Χρήση IV
Key Management	-	Βασισμένο στο EAP	Βασισμένο στο EAP

Πίνακας 5 - Προστασία Δεδομένων στο 802.11i

802.1X - παρέχει ένα πλαίσιο (πρότυπο) αυθεντικοποίησης και εξουσιοδότησης μιας συσκευής σε ένα δίκτυο. Αποτρέπει την είσοδο μιας συσκευής σε ένα δίκτυο μέχρι να αυθεντικοποιηθεί και παρέχει ένα μηχανισμό μετάδοσης/μεταφοράς κλειδιών μεταξύ authenticator and supplicant.

Το IEEE 802.1X αποτελείται από τρία δομικά στοιχεία όπως φαίνεται και στη παρακάτω εικόνα.



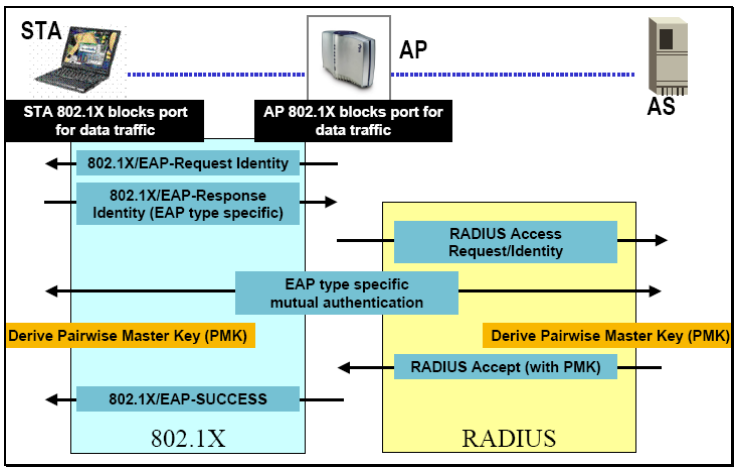
Εικόνα 30 - IEEE 802.1X

- Supplicant : Mobile Node
- Authenticator : Access Point συμβατό με IEEE 802.1X
- Authentication server : RADIUS SERVER π.χ. Free Radius Server

Το πρότυπο 802.1X για τον έλεγχο πρόσβασης σε ένα δίκτυο, στηρίζεται στο πρωτόκολλο EAP (Extensible Application Protocol) και το οποίο παρέχει μεθόδους αυθεντικοποίησης χρηστών. Το EAP έχει προταθεί από την IETF και έχει αποτελέσει την βάση για πολλά διαφορετικά πρωτόκολλα.

Τα στάδια της EAP διαδικασίας είναι :

1. Ο client αποστέλλει ένα **EAP-Start** μήνυμα
2. Το access Point στέλνει στον client ένα **EAP-request identity** μήνυμα
3. Ο πελάτης(supplicant) αποστέλλει ένα EAP-response πακέτο με τα αναγνωριστικά του(identity) και το οποίο μεταβιβάζεται στον εξυπηρετητή αυθεντικοποίησης
4. Ο εξυπηρετητής αυθεντικοποίησης προσκαλεί τον πελάτη να δείξουν ο ένας στον άλλον τα διαπιστευτήρια τους (αποστέλλει και τα δικά του, εάν πρόκειται για αμοιβαία αυθεντικοποίηση – mutual authentication)
5. Ο πελάτης αποστέλλει τα διαπιστευτήριά του στον εξυπηρετητή αυθεντικοποίησης.
6. Ο εξυπηρετητής αυθεντικοποίησης αποδέχεται ή απορρίπτει την αίτηση **(Access-Reject, Access-Accept)** για πρόσβαση στο δίκτυο από τον πελάτη
7. Το Access Point αλλάζει το port του πελάτη σε εξουσιοδοτημένη κατάσταση (authorized state) σε περίπτωση που ο εξυπηρετητής αυθεντικοποίησης έκανε αποδεκτό τον πελάτη (supplicant). Και τελικά αποκτά πρόσβαση προς το δίκτυο
8. Με την αποσύνδεση το port του (εξουσιοδοτημένου) πελάτη (the client port) μεταφέρεται στην μη εξουσιοδοτημένη κατάσταση(unauthorized state) περιμένοντας να ανατεθεί σε κάποιον άλλον.



Εικόνα 31

Μέχρι στιγμής έχουν προταθεί πολλές προεκτάσεις του EAP που έχουν εφαρμογή τόσο στα ενσύρματα όσο και στα ασύρματα δίκτυα. Οι πιο γνωστές είναι :

ΤΥΠΟΣ EAP	Dynamic Rekeying	Mutual Authentication	User ID& Password	Attack Methods	Σχόλια
EAP-MD5	OXI	OXI	NAI	Dictionary attack Man in the middle Session hijack	- Ανασφαλές - Εύκολα υλοποιήσιμο - Υποστηρίζεται από πολλούς εξυπηρετητές
EAP-TLS	NAI	NAI	OXI		- Πιστοποιητικά στους clients - Αυξάνει ασφάλεια και σταθερότητα
EAP-LEAP	NAI	NAI	NAI	Dictionary attack	- Προτεινόμενο από την εταιρεία Cisco
EAP-TTLS	NAI	NAI	NAI		-Δημιουργία ασφαλών συνδέσεων(TLS) - Κρυπτογράφηση ταυτότητας χρήστη
EAP-PEAP	NAI	NAI	OXI		- Παρόμοια με το EAP-TTLS - Κρυπτογράφηση ταυτότητας χρήστη
EAP-SIM	NAI	NAI	OXI		-Βασισμένο στα GSM δίκτυα -Αμοιβαία αυθεντικοποίηση (μόνο στο UMTS)
EAP-AKA	NAI	NAI	OXI		-Βασισμένο στα GSM δίκτυα -Αμοιβαία αυθεντικοποίηση (μόνο στο UMTS)

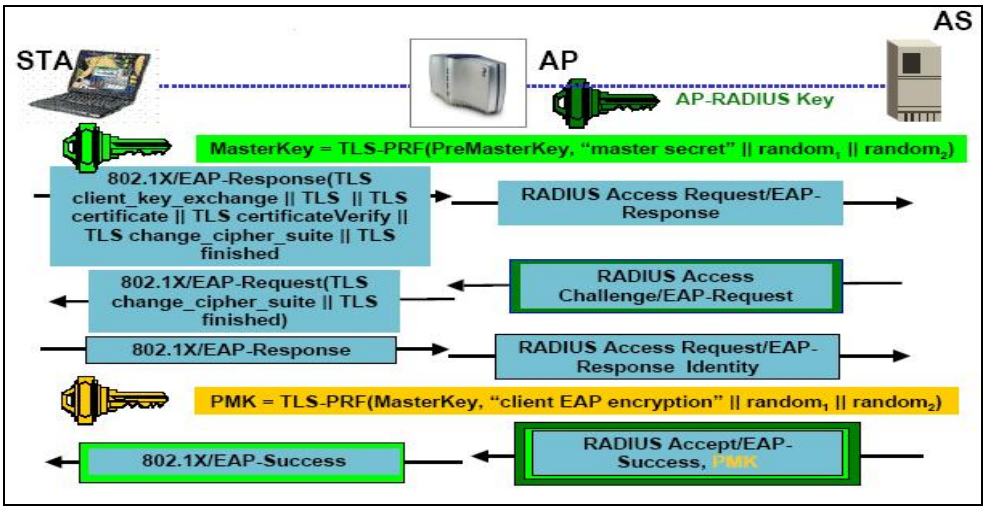
Πίνακας 6 - EAP πρωτόκολλο

EAP-TLS

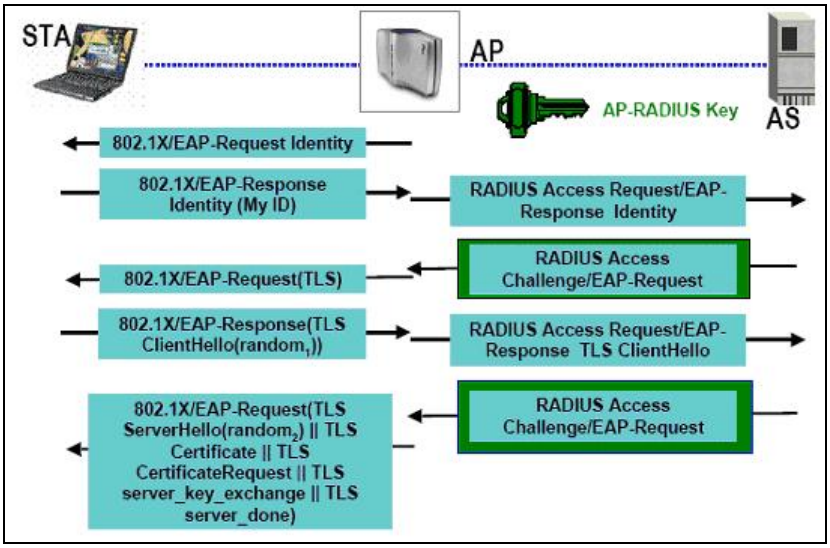
EAP-TLS = TLS Handshake over EAP

- EAP-TLS προσδιορίζεται από το RFC 2716
- TLS προσδιορίζεται από το RFC 2246

Στην αρχική του μορφή το EAP δεν σχεδιάστηκε με σκοπό να προστατέψει από υποκλοπές δεδομένων (eavesdropping). Κάτι που είναι φυσιολογικό εάν σκεφτούμε ότι αρχικά το EAP προοριζόταν για χρήση με το PPP με ενσύρματες συνδέσεις, οπότε και ο κίνδυνο υποκλοπής είναι περιορισμένος. Στα ασύρματα τοπικά δίκτυα κάτι τέτοιο μπορεί να προκαλέσει σημαντικά προβλήματα. Το TLS είναι ο απόγονος του ευρέως αποδεκτού SSL, και η διαδικασία αυθεντικοποίησεις κληρονομεί πολλά από τα θετικά στοιχεία του SSL, όπως η αμοιβαία αυθεντικοποίηση. Περιλαμβάνει αμοιβαία αυθεντικοποίηση τόσο του κινούμενου χρήστη, όσο και του εξυπηρετητή αυθεντικοποίησης(Authentication Server) προς τον MN. Επίσης, το EAP-TLS παρέχει και μέθοδο για ανταλλαγή κλειδιού συνόδου (session key) μεταξύ του πελάτη και του authenticator.Το EAP-TLS είναι το περισσότερο μέχρι στιγμής αποδεκτό στο χώρο των ασύρματων δικτύων.



Εικόνα 32 - EAP-TLS ανταλλαγή πακέτων (1)



Εικόνα 33 - EAP-TLS ανταλλαγή πακέτων (2)

ΑΣΦΑΛΕΙΑ ΤΟΥ ΠΡΟΤΥΠΟΥ 802.11

Ένα από τους σημαντικότερους τομείς στο πεδίο των ασυρμάτων δικτύων είναι αυτός της ασφάλειας. Είναι προφανές ότι σε ένα ασύρματο δίκτυο οι απειλές(threats) είναι περισσότερες από ένα ενσύρματο και αυτό λόγω του ότι το μέσο μετάδοσης των ραδιοκυμάτων είναι ο αέρας και όχι κάποιο προστατευόμενο ενσύρματο μέσο, χωρίς αυτό να σημαίνει ότι οι απαιτήσεις ασφάλειας των ασυρμάτων τεχνολογιών διαφέρουν ριζικά από τις απαιτήσεις ασφάλειας των υπολογιστών και των ενσύρματων δικτύων.

Για να θεωρηθεί ότι παρέχεται ένα ικανοποιητικό επίπεδο ασφάλειας στην επικοινωνία ενός κινητού σταθμού με το Access Point θα πρέπει να διατηρείται η εμπιστευτικότητα της επικοινωνίας, η ακεραιότητα των μεταδιδόμενων δεδομένων(*encryption*), να αυθεντικοποιούνται οι χρήστες προτού γίνει η σύνδεση (*authentication*) και σε αρκετές περιπτώσεις να διατηρούνται στατιστικά-λογιστικά (*accounting*) στοιχεία για το συνδεδεμένο σταθμό. Επιπλέον, να διατηρείται συνεχώς η διαθεσιμότητα της υπηρεσίας και γενικότερα να περιοριστούν οι απειλές κάποιος να κρυφακούσει ην επικοινωνία των ασύρματων σταθμών και η ακόμη χειρότερη να τις τροποποιήσει.

Η αυθεντικοποίηση επιτυγχάνεται με έναν ή περισσότερους από τους παρακάτω τρόπους :

1. Με κάτι που ξέρουμε (π.χ. username και password)
2. Με κάτι που είμαστε (π.χ. βιομετρικές μεθόδους, δακτυλικό αποτύπωμα)
3. Με κάτι που κατέχουμε (π.χ. smart cards, security tokens, certificates)

Ο πιο διαδεδομένος μέχρι στιγμής είναι ο πρώτος σε συνδυασμό με τον τρίτο.

Σε ό,τι αφορά την αυθεντικοποίηση, το 802.11 ορίζει δύο μεθόδους ελέγχου πρόσβασης μιας οντότητας στο ασύρματο δίκτυο :

a. Αυθεντικοποίηση ανοικτού συστήματος (Open-system Authentication)
b. Αυθεντικοποίηση κοινού κλειδιού (Shared-key Authentication)

Στην *αυθεντικοποίηση ανοικτού συστήματος* μια οντότητα αυθεντικοποιείται μόνο αν έχει συμπληρώσει κατάλληλα κάποια πεδία των μηνυμάτων που ανταλλάσσει με το σημείο πρόσβασης. Η μορφή αυτή είναι ευπαθής σε επιθέσεις μη εξουσιοδοτημένης πρόσβασης, εκτός και αν γίνει χρήση κρυπτογραφικών τεχνικών. Η *αυθεντικοποίηση κοινού κλειδιού* βασίζεται στη διαδικασία πρόκλησης-απόκρισης (challenge-response) με χρήση κρυπτογραφικών τεχνικών. Κατά την αίτηση αυθεντικοποίησης μιας συσκευής, το δεύτερο σημείο παράγει ένα τυχαίο αριθμό (challenge) ο οποίος αποστέλλεται στη συσκευή, κρυπτογραφείται με χρήση ενός κοινού μυστικού κλειδιού και αποστέλλεται πίσω στο σημείο πρόσβασης . Αν κατά την αποκρυπτογράφηση, που γίνεται με χρήση του ίδιου κλειδιού, ο αριθμός είναι ο ίδιος, τότε η διαδικασία αυθεντικοποίησης ολοκληρώνεται με επιτυχία.

Ο πιο σημαντικός μηχανισμός ασφάλειας σε ένα ασύρματο δίκτυο είναι η κρυπτογράφηση. Η πρώτη προσπάθεια για κρυπτογράφηση της μεταδιδόμενης πληροφορίας στο 802.11 έγινε με το WEP (Wired Equivalent Privacy) αλλά είναι γνωστό ότι πρόκειται για μια εντελώς αναξιόπιστη λύση και έναν πολύ αδύναμο μηχανισμό κρυπτογράφησης,ενώ πάντα παραμένουν αξιόπιστες λύσεις που χρησιμοποιούνται και στα ενσύρματα δίκτυα όπως το VPN (Virtual Private Network). Για να θεωρηθεί μια κρυπτογράφηση ισχυρή θα πρέπει να βασίζεται σε έναν ισχυρό αλγόριθμο που δύσκολα «σπάει» και το κλειδί κρυπτογράφησης να είναι μήκους τουλάχιστον 128 bit.

Οι τελευταίες λύσεις βασίζονται στο 802.1X (EAP) πρωτόκολλο με αρκετές προεκτάσεις EAP-MD5, EAP-LEAP, EPA-TLS, EAP-TTLS κ.λ.π. με διαφορετικά πλεονεκτήματα και μειονεκτήματα η κάθε μία (βλ. Πίνακα 4).
Μέχρι στιγμής έχουν προταθεί πολλές λύσεις, οι οποίες περισσότερο μπερδεύουν την κατάσταση παρά προσφέρουν ένα ενιαίο πλαίσιο ασφάλειας. Δεδομένης της ασάφειας αλλά και της ιδιαιτερότητας των ασυρμάτων δικτύων η IEEE προχώρησε στην έκδοση του προτύπου 802.11i, το οποίο έχει ως στόχο να προσφέρει μια ολοκληρωμένη λύση ασφαλείας.

4.2 BLUETOOTH - ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ ΜΙΚΡΩΝ ΑΠΟΣΤΑΣΕΩΝ

Το 1994 η εταιρεία Ericsson έδειξε ενδιαφέρον για τη σύνδεση των κινητών της τηλεφώνων σε άλλες συσκευές (όπως συσκευές PDA) χωρίς καλώδια. Μαζί με άλλες τέσσερις εταιρίες (IBM, Intel, Nokia και Toshiba), σχημάτισε μια Ομάδα Ειδικών Ενδιαφερόντων ή SIG (Special Interest Group, δηλαδή 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 αυτό ονομάστηκε Bluetooth.Αν και η αρχική ιδέα ήταν να απαλλαγούμε από τα καλώδια μεταξύ συσκευών, το έργο σύντομα άρχισε να επεκτείνεται και να εισβάλλει στον τομέα των ασύρματων LAN.Αν και αυτή η κίνηση κάνει το πρότυπο πιο χρήσιμο, δημιουργεί επίσης κάποιον ανταγωνισμό με το 802.11 . Για να χειροτερέψουν τα πράγματα , τα δύο συστήματα περιβάλλονται ηλεκτρικά μεταξύ τους.Αξίζει επίσης να επισημάνουμε ότι η Hewlett-Packard παρουσίασε πρίν από μερικά χρόνια ένα υπέρυθρο δίκτυο για τη διασύνδεση των περιφερειακών των ηλεκτρονικών υπολογιστών χωρίς καλώδια, το οποίο όμως δεν γνώρισε ποτέ σημαντική επιτυχία.

Χωρίς να αποθαρρυνθεί από όλα αυτά, η επιτροπή του Bluetooth εξέδωσε τον Ιούλιο του 1999 μια προδιαγραφή 1500 σελίδων για την έκδοση 1.0 του συστήματος.Λίγο αργότερα η ομάδα προτύπων του IEEE που μελετούσε τα ασύρματα δίκτυα προσωπικής περιοχής,

η 802.15, υιοθέτησε ως βάση το έγγραφο του Bluetooth και άρχισε να το τροποποιεί.Αν και μπορεί να φαίνεται περίεργη η τυποποιήση 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 ανοιχτού προτύπου το οποίο το διαχειρίζεται μια ουδέτερη αρχή όπως το IEEE συχνά προάγει τη χρήση μιας τεχνολογίας.

Το Bluetooth αποτελεί ένα πρότυπο για τις ασύρματες επικοινωνίες, για μικρά, φθηνά και μικρού εύρους κάλυψης δίκτυα. Η τεχνολογία Bluetooth υπόσχεται την εξαφάνιση όλων εκείνων των συστατικών που περιπλέκουν την επικοινωνία μεταξύ των υπολογιστών, όπως είναι τα πολλά καλώδια, οι συζευκτήρες και τα πολλά είδη επικοινωνιακών πρωτοκόλλων. Με το Bluetooth, οι ασύρματες συσκευές όπως είναι τα κινητά τηλέφωνα, οι τηλε-ειδοποιητές (pagers), οι ψηφιακές κάμερες, οι ψηφιακοί βοηθοί (PDAs), κ.α. αποκτούν μια κοινή επικοινωνιακή δομή.

Το Bluetooth αποτελεί ένα εύρωστο, χαμηλών απαιτήσεων, φθηνό και ασφαλές πρότυπο, κατάλληλο για την υλοποίηση ασύρματων δικτύων υπολογιστών μικρού εύρους κάλυψης. Υποστηρίζει τη ταυτόχρονη μετάδοση φωνής και δεδομένων, την multipoint επικοινωνία και είναι εύκολο στη χρήση. Το εύρος κάλυψης που υποστηρίζει είναι περίπου 10 μέτρα, το οποίο όμως μπορεί να αυξηθεί με τη χρήση ενισχυτών.

Εικόνα 34

4.2.1 ΕΦΑΡΜΟΓΕΣ ΤΟΥ Bluetooth

Τα περισσότερα πρωτόκολλα δικτύου απλώς παρέχουν κανάλια ανάμεσα σε οντότητες που επικοινωνούν, αφήνοντας τους σχεδιαστές των εφαρμογών να αποφασίσουν για ποιό σκοπό θέλουν να χρησιμοποιήσουν τα κανάλια αυτά.Για παράδειγμα, το 802.11 δεν προσδιορίζει κατά πόσον οι χρήστες θα πρέπει να χρησιμοποιούν τους φορητούς υπολογιστές τους για να διαβάζουν ηλεκτρονικό ταχυδρομείο, να περιηγούνται στον Ιστό, ή να κάνουν κάτι άλλο.Αντιθέτως, οι προδιαγραφές της έκδοσης 1.1 του Bluetooth κατανομάζουν 13 συγκεκριμένες εφαρμογές οι οποίες θα υποστηρίζονται, και παρέχουν διαφορετικές στοίβες πρωτοκόλλων για κάθε μία.Δυστυχώς, η προσέγγιση αυτή οδηγεί σε πολύ μεγάλη πολυπλοκότητα, την οποία θα παραλείψουμε εδώ.Οι 13 εφαρμογές, που ονομάζονται προφίλ (profiles), φαίνονται στην παρακάτω εικόνα.Εξετάζοντας σε συντομία αυτές τις εφαρμογές, μπορούμε να δούμε πιο καθαρά τι προσπαθεί να πετύχει το Bluetooth και οι εμπνευστές του.

Εικόνα 35 - D-Link Bluetooth USB Adapter

ΟΝΟΜΑ	**ΠΕΡΙΓΡΑΦΗ**
Γενική πρόσβαση	Διαδικασίες διαχείρισης του συνδέσμου
Ανακάλυψη υπηρεσιών	Πρωτόκολλο για την ανακάλυψη των προσφερόμενων υπηρεσιών.
Σειριακή θύρα	Αντικατάσταση ενός καλωδίου σειριακής θύρας .
Γενική ανταλλαγή αντικειμένων	Καθορίζει τη σχέση πελάτη- διακομιστή για τη μετακίνηση αντικειμένων.
Πρόσβαση σε LAN	Πρωτόκολλο ανάμεσα σε έναν κινητό υπολογιστή και ένα τηλέφωνο.
Τηλεφωνική δικτύωση	Επιτρέπει σε ένα κινητό Η/Υ να καλεί μέσω κινητού τηλεφώνου.
Fax	Επιτρέπει σε μία κινητή μηχανή Fax να μιλάει σε ένα κινητό τηλέφωνο.
Ασύρματη τηλεφωνία	Συνδέει ένα ακουστικό κεφαλής με τον τοπικό του σταθμό βάσης.
Ενδοσυνεννόηση	Ψηφιακή ενδοσυνεννόηση
Ακουστικό κεφαλής	Επιτρέπει τη φωνητική επικοινωνία χωρίς χέρια.
Ώθηση αντικειμένων	Παρέχει μια μέθοδο ανταλλαγής απλών αντικειμένων.
Μεταφορά αρχείων	Παρέχει μια πιο γενική βοηθητική λειτουργία μεταφοράς αρχείων.
Συγχρονισμός	Επιτρέπει σε μια συσκευή PDA να συγχρονίζεται με έναν άλλον Η/Υ.

Πίνακας 7 - Το προφίλ του Bluetooth

Το προφίλ της γενικής πρόσβασης δεν είναι μια πραγματική εφαρμογή, αλλά είναι η βάση πάνω στην οποία χτίζονται οι πραγματικές εφαρμογές. Η βασική δουλειά του είναι να παρέχει μια μέθοδο εγκαθίδρυσεις και διατήρησης ασφαλών συνδέσμων – καναλιών ανάμεσα στον master και τους slaves του.Γενικής χρήσης είναι και το προφίλ ανακάλυψης υπηρεσιών, το οποίο χρησιμοποιείται από τις συσκευές για να ανακαλύψουν ποιές υπηρεσίες προσφέρουν οι άλλες συσκευές. Όλες οι συσκευές Bluetooth αναμένεται ότι θα υλοποιούν αυτά τα δύο προφίλ.Τα υπόλοιπα προφίλ είναι προαιρετικά.

Το προφίλ σειριακής θύρας είναι ένα πρωτόκολλο μεταφοράς που χρησιμοποιείται από τα περισσότερα από τα άλλα προφίλ.Εξομοιώνει μια σειριακή γραμμή και είναι ιδιαίτερα χρήσιμο για παλαιότερες εφαρμογές οι οποίες αναμένουν την παρουσία μιας σειριακής γραμμής.

Το προφίλ γενικής ανταλλαγής αντικειμένων προδιαγράφει μια σχέση πελάτη και διακομιστή για την μεταφορά δεδομένων.Οι λειτουργίες ξεκινούν από τους πελάτες (master), αλλά ο υπηρέτης (slave) μπορεί να είναι είτε πελάτης είτε διακομιστής.Όπως και το προφίλ σειριακής θύρας, το προφίλ αυτό αποτελεί δομικό στοιχείο για τα προφίλ.

Η ομάδα των επόμενων τριών προφίλ χρησιμοποιείται για δικτύωση. Το προφίλ πρόσβασης σε LAN επιτρέπει σε μια συσκευή Bluetooth να συνδέται σε ενα σταθερό δίκτυο.Αυτό το προφίλ είναι άμεσος ανταγωνιστής του 802.11.Το προφίλ τηλεφωνικής δικτύωσης ήταν το αρχικό κίνητρο για όλο το έργο.Επιτρέπει σε ένα φορητό υπολογιστή να συνδέεται χωρίς καλώδια σε ένα κινητό τηλέφωνο που περιέχει ενσωματωμένο μόντεμ.Το προφίλ φαξ είναι παρόμοιο με το προφίλ τηλεφωνικής δικτύωσης,με τη διαφόρα ότι επιτρέπει σε ασύρματες μηχανές φαξ να στέλνουν και να λαμβάνουν φαξ χρησιμοποιώντας κινητά τηλέφωνα ,χωρίς να υπάρχει καλώδιο μεταξύ τους.Τα τρία επόμενα προφίλ χρησιμοποιούνται για τηλεφωνία.Το προφίλ ασύρματης τηλεφωνίας παρέχει έναν τρόπο σύνδεσης του ακουστικού ενός ασύρματου τηλεφώνου στο σταθμό βάσης.Αυτή τη στιγμή τα περισσότερα ασύρματα τηλέφωνα και τα κινητά τηλέφωνα μπορεί να συγχωνευθούν.Το προφίλ ενδοσυνεννόησης.Τέλος,το προφίλ ακουστικού κεφαλήςυπορτηρίζει επικοινωνία φωνής χωρίς χέρια(hands-free)ανάμεσα στο ακουστικό κεφαλής(headset) και το σταθμό βάσης-έτσι ώστε,για παράδειγμα,να τηλεφωνούμε χωρίς

χέρια ενώ οδηγούμε αυτοκίνητο.Τα τρία τελευταία προφίλ χρησιμοποιούνται για την πραγματική ανταλλαγή αντικειμένων ανάμεσα σε δύο ασύρματες συσκευές.Τα αντικείμενα μπορεί να είναι επαγγελματικές κάρτες,εικόνες,ή αρχεία δεδομένων.Συγκεκριμένα,το προφίλ συγχρονισμού προορίζεται για τη φόρτωση δεδομένων σε μια συσκευή PDA ή σε ένα φορητό υπολογιστή όταν η συσκευή φεύγει από το σπίτι και τη συλλογή δεδομένων από αυτήν όταν η συσκευή επιστρέφει.Ήταν πραγματικά απαραίτητο να προδιαγραφούν λεπτομερώς όλες αυτές οι εφαρμογές και να παρέχονται διαφορετικές στοίβες πρωτοκόλλων για την κάθε μία;Πιθανότατα όχι,υπήρχαν όμως πολλές διαφορετικές ομάδες εργασίες οι οποίες επινόησαν διαφορετικά μέρη του προτύπου,και η κάθε μία εστιάστηκε απλώς στο δικό της πρόβλημα παράγοντας το δικό της προφίλ.Είναι άλλη μια περίπτωση του νόμου του Conway.(Στο τεύχος Απριλίου 1968 του περιοδικού Datamation, ο Melvin Conway παρατήρησε ότι αν βάλεις n άτομα να γράψουν ένα μεταγλωττιστή n διελεύσεων,και ότι γενικότερα η δομή του λογισμικού αντικατοπτρίζει τη δομή της ομάδας που το δημιούργησε.)Θα ήταν μάλλον εφικτό να τα καταφέρουμε με δύο μόνο στοίβες πρωτοκόλλων,αντί για 13 –μία για μεταφορά αρχείων και μία για επικοινωνία ροής δεδομένων πραγματικού χρόνου.

ΛΕΙΤΟΥΡΓΙΚΑ ΤΜΗΜΑΤΑ

Ένα σύστημα που βασίζεται στο πρότυπο Bluetooth, απαρτίζεται από τέσσερα λειτουργικά μέρη:

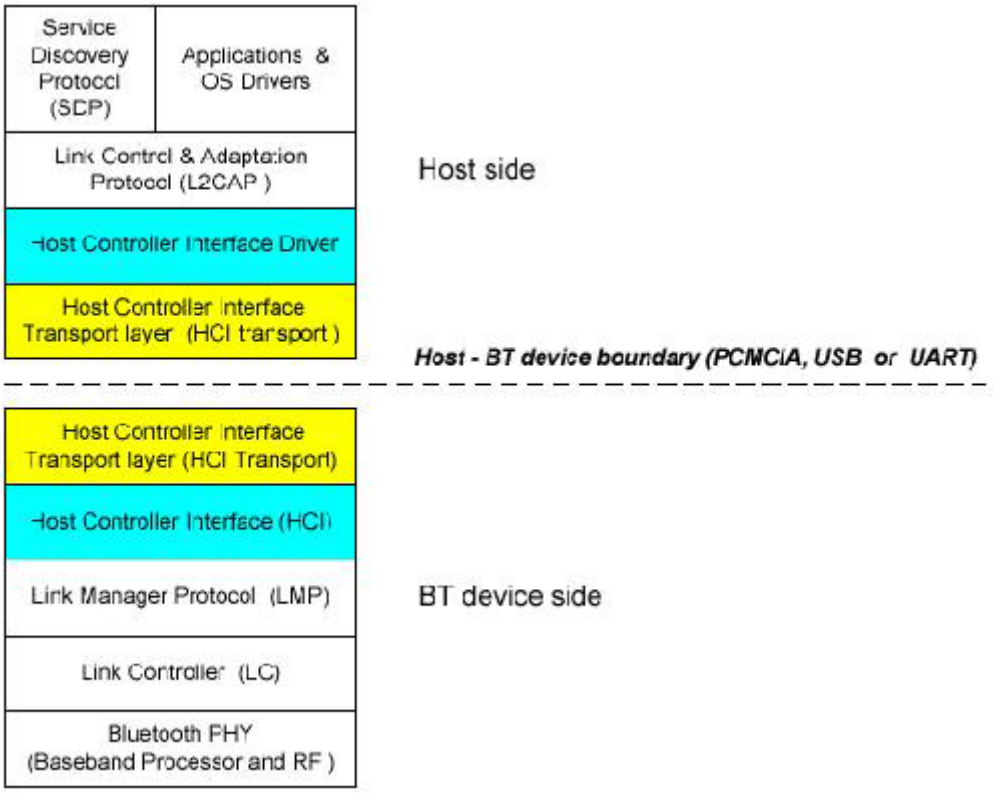
a) **Έναν ραδιοπομποδέκτη** (radio transceiver), ικανό να μεταδίδει και να λαμβάνει φωνή και δεδομένα. Ο ραδιοπομποδέκτης, αποτελεί μια συσκευή με μικρό εύρος κάλυψης και με χαμηλές απαιτήσεις σε κατανάλωση ισχύος, η οποία λειτουργεί στην περιοχή συχνοτήτων 2,4 GHz της ISM. Θεωρώντας ως σημείο αναφοράς μια εικονική κεραία, η οποία έχει ισχύ μετάδοσης 0 dBm (1 mW), τότε το εύρος κάλυψης είναι 10 μέτρα. Το εύρος αυτό μπορεί να αυξηθεί στα 100 μέτρα αυξάνοντας την ισχύ στα 20 dBm (100 mW). Ο μέγιστος ρυθμός μετάδοσης των δεδομένων είναι 1 Mbps, όμως οι επιβαρύνσεις που εισάγονται από τα επικοινωνιακά πρωτόκολλα περιορίζουν το ρυθμό αυτό περίπου στα 725 kbps.

b) **Μια μονάδα βασικής ζώνης ή ελέγχου καναλιού (baseband ή link control unit)**, η οποία είναι ικανή να επεξεργάζεται τα δεδομένα που λαμβάνονται και μεταδίδονται από τον ραδιοπομποδέκτη. Η μονάδα βασικής ζώνης (ή ελέγχου του καναλιού), είναι εκείνο το τμήμα υλικού το οποίο χρησιμοποιείται για το μετασχηματισμό των εισερχόμενων ραδιοκυμάτων σε ψηφιακή μορφή (bits), για να μπορούν να τα επεξεργαστούν οι εφαρμογές. Επίσης μετασχηματίζει τα ψηφιακά και τα φωνητικά δεδομένα σε μορφή κατάλληλη για μετάδοση από την κεραία. Επιπρόσθετα, η μονάδα βασικής ζώνης είναι υπεύθυνη για το μετασχηματισμό της μορφής των δεδομένων (π.χ. μετασχηματισμό της φωνής από αναλογική σε ψηφιακή μορφή), για τη συμπίεσή τους, για την τοποθέτησή τους στα εξερχόμενα και για την εξαγωγή τους από τα εισερχόμενα πακέτα και για τον έλεγχο λαθών.

c) **Λογισμικό διαχείρισης του επικοινωνιακού καναλιού**, το οποίο διαχειρίζεται τις μεταδόσεις. Το Λογισμικό Διαχείρισης του Επικοινωνιακού Καναλιού (Link Manager Software), εκτελείται σε χωριστό μικροεπεξεργαστή και είναι υπεύθυνο για τη διαχείριση της επικοινωνίας μεταξύ των συσκευών Bluetooth. Το κάθε υπολογιστικό σύστημα Bluetooth έχει το δικό του διαχειριστή καναλιού, ο οποίος είναι υπεύθυνος για τον εντοπισμό των άλλων διαχειριστών του τοπικού δικτύου, την εγκατάσταση και τον τερματισμό των συνδέσεων μεταξύ των σταθμών, την κρυπτογράφηση και την αποκρυπτογράφηση (αν λαμβάνει χώρα) των δεδομένων, την προσαρμογή του ρυθμού μετάδοσης δεδομένων δυναμικά και τη διαπραγμάτευση των επικοινωνιακών επιλογών μεταξύ των σταθμών.

d) **Λογισμικό εφαρμογών (Application Software)**, το οποίο αποτελείται από όλες εκείνες τις εφαρμογές που χρησιμοποιούν τη στοίβα πρωτοκόλλων του Bluetooth και βρίσκονται εγκατεστημένες σε κάθε ασύρματη συσκευή τεχνολογίας Bluetooth. Οι εφαρμογές αυτές επιτρέπουν σε όλες τις συσκευές ενός δικτύου Bluetooth να εκτελούν τις εργασίες τους (π.χ. επικοινωνία, μεταφορά αρχείων, κλπ). Στο παρακάτω σχήμα φαίνεται η στοίβα πρωτοκόλλων του Bluetooth. Βλέπουμε πως στο ανώτερο επίπεδο

υπάρχουν οι εφαρμογές των χρηστών οι οποίες χρησιμοποιούν τη στοίβα πρωτοκόλλων και η οποία θα πρέπει να είναι η ίδια σε κάθε συσκευή, έτσι ώστε να καθίσταται δυνατή η επικοινωνία.



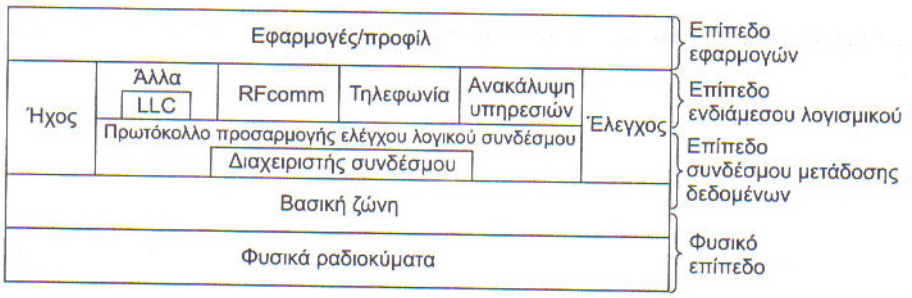
Εικόνα 36 - Η στοίβα πρωτοκόλλων του προτύπου Bluetooth

Η στοίβα πρωτοκόλλων του Bluetooth

Το πρότυπο του Bluetooth περιέχει πολλά πρωτόκολλα που ομαδοποιούνται χαλαρά σε επίπεδα.Η δομή των επιπέδων δεν ακολουθεί το μοντέλο OSI,το μοντέλο TCP\IP,το μοντέλο 802,ή κάποιο άλλο γνωστό μοντέλο.Παρόλα αυτά, το IEEE προσπαθεί να τροποποιήσει το Bluetooth όπως τροποποιήθηκε από την επιτροπή 802 φαίνεται στην παραπάνω εικόνα. Το χαμηλότερο επίπεδο είναι το φυσικό επίπεδο των ραδιοκυμάτων,το οποίο αντιστοιχίζεται αρκετά καλά στο φυσικό επίπεδο των μοντέλων OSI και

802.Ασχολείται με τη μετάδοση των ραδιοκυμάτων και τη διαμόρφωση.Πολλά από τα ζητήματα του επιπέδου αυτού σχετίζονται με το στόχο να είναι το σύστημα φτηνό,έτσι ώστε να μπορεί να γίνει μαζικό προ'ι'όν.Το επίπεδο βασικής ζώνης(baseband)είναι κάπως ανάλογο με το υποεπίπεδο MAC,περιέχει όμως και στοιχεία του φυσικού επιπέδου.Καθορίζει πώς θα ελέγχει ο κύριος τις χρονικές υποδοχές και οι υποδοχές αυτές θα ομαδοποιούνται σε πλαίσια.Στη συνέχεια έχουμε ένα επίπεδο με μια ομάδα κάπως σχετιζομένων πρωτοκόλλων.Ο διαχειριστής συνδέσμου(link manager)χειρίζεται την εγκαθίδρυση λογικών λαναλιών ανάμεσα στις συσκευές,όπου συμπεριλαμβάνεται και η διαχείριση ισχύος,η πιστοποίηση ταυτότητας,και η ποιότητα υπηρεσιών.Το πρωτόκολλο προσαρμογής ελέγχου λογικού συνδέσμου(logical link control adaptation protocol,συχνά αποκαλείται L2CAP)αποκρύπτει από τα ανώτερα επίπεδα τις λεπτομέρειες της μετάδοσης.Είναι ανάλογο με το τυπικό υποεπίπεδο LLC του 802,αλλά διαφέρει από τεχνική άποψη.Όπως υποδηλώνουν τα ονόματά τους ,τα πρωτόκολλα ήχου(audio)και ελέγχου(control)ασχολούνται με τον ήχο και τον έλεγχο,αντίστοιχα.Οι εφαρμογές μπορούν να φτάσουν απευθείας σε αυτά ,χωρίς να χρειαστεί να περάσουν πρώτα από το πρωτόκολλο L2CAP. Το επόμενο επίπεδο προς τα επάνω είναι το επίπεδο ενδιάμεσου λογισμικού(middleware),το οποίο περιέχει ένα μίγμα διαφορετικών πρωτοκόλλων.Το πρωτόκολλο LLC του 802 εισήχθηκε εδώ από το IEEE για συμβατότητα με τα άλλα δίκτυα 802. Τα πρωτόκολλα RFComm, τηλεφωνίας(telephony) και ανακάλυψης υπηρεσιών (service discovery0είναι εγγενή πρωτόκολλα Bluetooth. Το RFComm (επικοινωνία ραδιοκυμάτων συχνοτήτων,Radio Frequency Communication) είναι το πρωτόκολλο που εξομοιώνει την τυπική σειριακή θύρα που υπάρχει στους περισσότερους προσωπικούς υπολογιστές για τη σύνδεση πληκτρολογίων,ποντικιών,μόντεμ,και άλλων συσκευών.Έχει σχεδιαστεί για να επιτρέπει την εύκολη χρήση του από παλαιότερες συσκευές.Το πρωτόκολλο τηλεφωνίας είναι ένα πρωτόκολλο πραγματικού χρόνου που χρησιμοποιείται για τα τρία προφίλ τα οποία είναι προσανατολισμένα στην ομιλία.Διαχειρίζεται επίσης την εγκαθίδρυση και τον τερματισμό των κλήσεων.Τέλος,το πρωτόκολλο ανακάλυψης υπηρεσιών χρησιμοποιείται για τον εντοπισμό υπηρεσιών μέσα στο δίκτυο.Τουψηλότερο επίπεδο είναι αυτό στο οποίο βρίσκονται οι εφαρμογές και τα προφίλ.Οι εφαρμογές χρησιμοποιούν τα πρωτόκολλα των χαμηλότερων επιπέδων για να κάνουν τη δουλειά τους.Κάθε εφαρμογή

έχει το δικό της αποκλειστικό υποσύνολο πρωτοκόλλων.Οι συγκεκριμένες συσκευές,όπως ένα ακουστικό κεφαλής,περιέχουν συνήθως μόνο τα πρωτόκολλα που χρειάζονται για την αντίστοιχη εφαρμογή και τίποτα άλλο.Στις ακόλουθες ενότητες θα εξετάσουμε τα τρία χαμηλότερα επίπεδα της στοίβας πρωτοκόλλων του Bluetooth,επειδή αυτά αντιστοιχούν χονδρικά στο φυσικό επίπεδο και το υποεπίπεδο MAC.



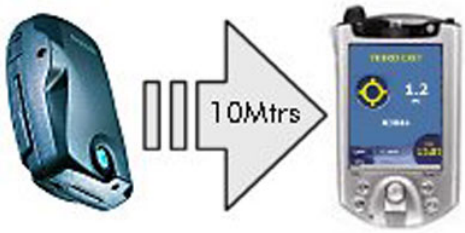
Εικόνα 37 - Παραλλαγή του 802.15 για την αρχιτεκτονική πρωτοκόλλων του Bluetooth

Το επίπεδο ραδιοκυμμάτων του Bluetooth.

Το επίπεδο ραδιοκυμάτων μεταφέρει τα bit από τον κύριο στον υπηρέτη,ή αντίστροφα.Είναι ένα σύστημα χαμηλής ισχύος με εμβέλεια 10 μέτρα που λειτουργεί στη ζώνη ISN των 2,4GHz.Η ζώνη διαιρείται σε 79 κανάλια του 1 MHz το καθένα.Η διαμόρφωση είναι η κωδικοποίηση μετατόπισης συχνότητας,με 1 bit ανά Hz,δίνοντας μικτό ρυθμό μετάδοσης δεδομένων ίσο με 1 Mbps-με μεγάλο μέρος από αυτό το φάσμα,όμως, να καταναλώνεται από τις επιβαρύνσεις.Για να κατανέμονται δίκαια τα κανάλια χρησιμοποιείται εξάπλωση φάσματος με συνεχή αλλαγή συχνότητας,με 1600 αλλαγές\sec και χρόνο παραμονής ίσο με 625 μsec.ι οι κόμβοι του μικροσκοπικού δικτύου αλλάζουν συχνότητα ταυτόχρονα,με τον κύριο να επιβάλλει την ακολουθία των συχνοτήτων.Επειδή τόσο το 802.11 όσο και το Bluetooth λειτουργούν στην ζώνη ISM των 2,4 GHz στα ίδια 79 κανάλια, παρεμβάλονται μεταξύ τους.Αφού το Bluetooth αλλάζει συχνότητες πολύ πιο γρήγορα από το πρότυπο 802.11 , είναι πολύ πιθανό μια συσκευή Bluetooth να καταστρέψει τις μεταδόσεις του 802.11 , παρά το αντίστροφο.

Το επίπεδο βασικής ζώνης του Bluetooth.

Το επίπεδο βασικής ζώνης είναι το πλησιέστερο πράγμα που έχει το Bluetooth ως πρός το υποεπίπεδο MAC.Μετατρέπει την ανεπεξέργαστη ροή bit σε πλαίσια και ορίζει κάποιες βασικές μορφές πλαισίων.Στην απλούστερη περίπτωση , ο κύριος (Master) κάθε δικτύου καθορίζει την ακολουθία χρονικών υποδοχών των 625 μsec , με τις μεταδόσεις του Master να ξεκινούν στις άρτιες υποδοχές και τις μεταδόσεις των Slaves να ξεκινούν στις περιττές υποδοχές.Η μέθοδος αυτή είναι κλασική πολύπλεξη με διαίρεση χρόνου , με τον κύριο (master) να παίρνει τις μισές υποδοχές και τους υπηρέτες (slaves) να μοιράζονται τις άλλες μισές. Τα πλαίσια μπορεί να έχουν μήκος 1, 3 , ή και 5 υποδοχές.
Κάθε πλαίσιο μεταδίδεται μέσω ενός λογικού καναλιού, που ονομάζεται σύνδεσμος (link), ανάμεσα στον Master και τον Slave.Υπάρχουν δύο είδη συνδέσμων, ο Ασύγχρονος Ασυνδεσμικός σύνδεσμος (ACL – Asynchronous Connection Less) και ο Σύγχρονος Συνδεσμοστραφής σύνδεσμος (SCO – Synchronous Connection Oriented).
Ο πρώτος σύνδεσμος χρησιμοποιείται για τα δεδομένα μεταγωγής πακέτων τα οποία παράγονται σε ακανόνιστα χρονικά διαστήματα.Τα δεδομένα αυτά προέρχονται από το επίπεδο L2CAP στο άκρο του αποστολέα και παραδίδονται στο επίπεδο L2CAP στο άκρο του παραλήπτη.Η κίνηση ACL παραδίδεται με βάση τη βέλτιστη προσπάθεια. Δεν παρέχονται εγγυήσεις.Τα πλαίσια μπορεί να χαθούν και μπορεί να χρειαστεί να ξαναμεταδοθούν.Ένας υπηρέτης (Slave) μπορεί να έχει μόνο ένα σύνδεσμο ACL με τον κύριο του (Master).



Εικόνα 38

Το άλλο είδος (ο Σύγχρονος Συνδεσμοστραφής σύνδεσμος) χρησιμοποιείται για δεδομένα πραγματικού χρόνου , όπως τηλεφωνικές συνδέσεις.Σε αυτόν τον τύπο καναλιού εκχωρείται μια σταθερή υποδοχή σε κάθε κατεύθυνση.Λόγω της φύσης των συνδέσμων SCO (παρέχουν δεδομένα που είναι κρίσιμαως προς το χρόνο),τα πλαίσια που στέλνονται μέσω αυτών δεν αναμεταδίδονται ποτέ.Αντιθέτως, μπορεί να χρησιμοποιηθεί ευθεία διόρθωση σφαλμάτων για την παροχή υψηλής αξιοπιστίας.Κάθε σύνδεσμος SCO μπορεί να μεταδίδει ένα κανάλι ήχου PCM στα 64.000 bps.

Το επίπεδο L2CAP του Bluetooth

Το επίπεδο L2CAP έχει τρείς κύριες λειτουργίες.Πρώτον δέχεται πακέτα μέχρι 64 KB από τα ανώτερα επίπεδα και τα τεμαχίζει σε πλαίσια για μετάδοση.Στο άλλο άκρο, τα πλαίσια συναρμολογούνται ξανά σε πακέτα.

Δεύτερον, διαχειρίζεται την πολυπλεξία και αποπολύπλεξη πολλαπλών πηγών πακέτων.

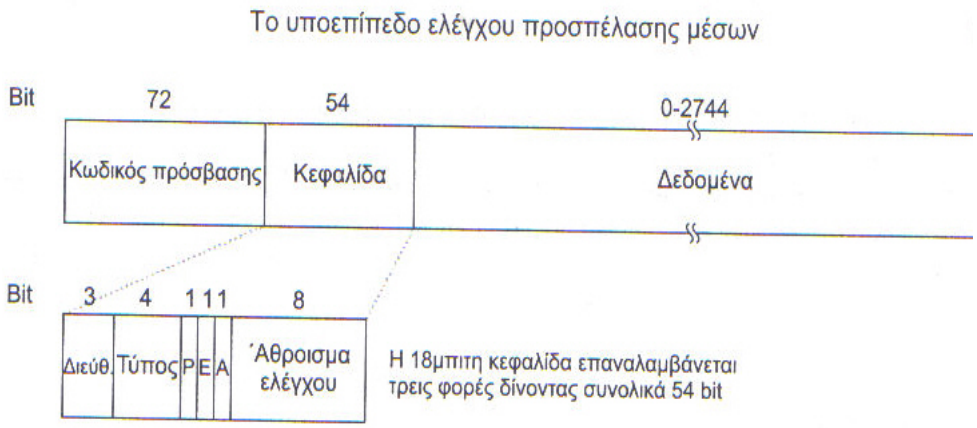
Όταν συναρμολογηθεί ξανά ένα πακέτο, το επίπεδο L2CAP προσδιορίζει σε ποιό πρωτόκολλο υψηλότερου επιπέδου πρέπει να το παραδώσει – για παράδειγμα, στο RFcomm ή το πρωτόκολλο τηλεφωνίας.

Τρίτον το L2CAP χειρίζεται τις απαιτήσεις για ποιότητα υπηρεσιών, τόσο κατά την εγκαθίδρυση των συνδέσμων όσο και κατά την κοινονική λειτουργία. Ένα άλλο αντικείμενο διαπραγμάτευσης κατά την εγκαθίδρυση της σύνδεσης είναι το μέγιστο επιτρεπτό μέγεθος του ωφέλιμου φορτίου, έτσι ώστε να μην μπορεί μια συσκευή με μεγάλα πακέτα να κατακλύσει μια συσκευή μικρών πακέτων. Αυτό το χαρακτηριστικό απαιτείται επειδή δεν μπορούν όλες οι συσκευές να χειριστούν πακέτα με χωρητικότητα 64 KB.

Η δομή πλαισίων του Bluetooth

Υπάρχουν πολλές μορφές πλαισίων, με την πιο σημαντική από αυτές να φαίνεται στην παρακάτω εικόνα.Η μορφή αυτή ξεκινά με έναν κωδικό πρόσβασης που συνήθως

προσδιορίζει τον κύριο, έτσι ώστε οι υπηρέτες που βρίσκονται εντός της εμβέλειας δύο κυριών να μπορούν να αποφασίσουν ποιά κίνηση προορίζεται για αυτούς.Στη συνέχεια έχουμε μια κεφαλίδα 54 bit που περιέχει τα τυπικά πεδία του υποεπιπέδου MAC.Μετά έχουμε το πεδίο δεδομένων, μήκους μέχρι 2744 bit (για μεταδόσεις πέντε υποδοχών). Στην περίπτωση μιας μόνο χρονικής υποδοχής, η μορφή είναι η ίδια με τη διαφορά ότι το πεδίο δεδομένων έχει μέγεθος 240 bit.



Εικόνα 39 - Ένα τυπικό πλαίσιο δεδομένων του Bluetooth

Ας ρίξουμε μια ματιά στην κεφαλίδα του παραπάνω σχήματος.Το πεδίο **Διεύθυνση** προσδιορίζει για ποιά από τις οκτώ ενεργές συσκευές προσδιορίζεται το πλαίσιο.

Το πεδίο **Τύπος** προσδιορίζει τον τύπο του πλαισίου (ACL, SCO, περιόδευση, ή κενό), τον τύπο διόρθωσης σφαλμάτων που χρησιμοποιείται στο πεδίο δεδομένων , και το πλήθος των υποδοχών που περιέχονται στο πλαίσιο.

Το bit **Ροή** (P) ενεργοποιείται από έναν υπηρέτη όταν γεμίσει η περιοχή προσωρινής ποθήκευσης του και δεν μπορεί να δεχτεί άλλα δεδομένα.Πρόκειται λοιπόν για μια στοιχειώδει μορφή ελέγχου ροής.Το bit **Επιβεβαίωση** (E) χρησιμοποιείται για να τοποθετηθεί μια επιβεβαίωση εμβόλιμα μέσα σε ένα πλαίσιο.Το bit **Ακολουθία** (A) χρησιμοποιείται για την αρίθμηση πλαισίων, ώστε να εντοπίζονται οι αναμεταδόσεις.

Το πρωτόκολλο χρησιμοποιεί παύση και αναμονή, οπότε αρκεί 1 bit.Μετά έχουμε το 8μπιτο **Άθροισμα ελέγχου** της κεφαλίδας.Ολόκληρη η 18μπιτη κεφαλίδα

επαναλαμβάνεται τρείς φορές, για να σχηματίσει την κεφαλίδα των 54 bit που φαίνεται στην παραπάνω εικόνα.Στην πλευρά του παραλήπτη, ένα απλό κύκλωμα εξετάζει και τα τρία αντίγραφα κάθε bit.Αν και τα τρία είναι ίδια, το bit γίνεται αποδεκτό.Διαφορετικά, χρησιμοποιείται η τιμή της πλειοψηφίας.Άρα χρησιμοποιούνται 54 bit από την χωρητικότητα μετάδοσης για να σταλούν 10 bit κεφαλίδας.Ο λόγος είναι ότι, όταν θέλουμε να στείλουμε αξιόπιστα τα δεδομένα σε ένα θορυβώδες περιβάλλον χρησιμοποιώντας φτηνές συσκευές χαμηλής ισχύος (2,5 mW) με λίγη υπολογιστική ισχύ,απαιτείται μεγάλος βαθμός πλεονασμού στα δεδομένα.

Για το πεδίο δεδομένων των πλαισίων ACL χρησιμοποιούνται διάφορες μορφές.Τα πλαίσια SCO είναι, όμως απλούστερα : το πεδίο δεδομένων έχει πάντα μέγεθος 240 bit.Έχουν οριστεί τρείς παραλλαγές, οι οποίες επιτρέπουν 80, 160, ή 240 bit πραγματικού ωφέλιμου φορτίου, με τα υπόλοιπα bit να χρησιμοποιούνται για διόρθωση σφαλμάτων.Στην πιο αξιόπιστη έκδοση (ωφέλιμο φορτίο 80 bit), τα περιεχόμενα απλώς επαναλαμβάνονται τρείς φορές, όπως ακριβώς και στη κεφαλίδα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Tanenbaum, Andrew S., "*Computer Networks, 3rd Edition*": Prentice Hall International Inc. (1996)

[2] Stallings William, "*Data and Computer Communications - 5th Edition*": Prentice-Hall International, Inc. (1997)

[3] Pahlavan K., Levesque A., "*Wireless Information Networks*": John Wiley & Sons, Inc. (1995)

[4] Atmel Corp., "*Bluetooth General Information White Paper*": Atmel Corp. (2000).

[5] Cisco Systems Inc., "*GPRS White Paper*": Cisco Systems Inc. (2000).

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

[7] Sempere J. G., "*An overview of the GSM System*", στην ιστοσελίδα http://www.comms.eee.strath.ac.uk/~gozalvez/gsm/gsm.html, University of Glasgow, England.

[8] Buckingham S., "*An Introduction to the General Packet Radio Service*", στην ιστοσελίδα http://www.gsmworld.com/technology/yes2gprs.html: Mobile Lifestreams Limited, (January 2000)

[9] Trimble Navigation Ltd., "*All About GPS*", στην ιστοσελίδα http://www.trimble.com/gps/index.html: Trimble Navigation Ltd. (2002)

[10] Scourias J., "*Overview of the Global System for Mobile Communications*", στην ιστοσελίδα http://www.mdi-ng.org/es53061/overview.htm: John Scourias, University of Waterloo, (1997)

[11] T.S. Chu, M.J. Gans, "*High Speed Infrared Local Wireless Communication*", στο IEEE Communications Magazine, 25, No. 8, 4-10 (1987).

[12] MCSE Training Kit, "*Networking Essential Plus 3rd Edition*": Microsoft Press (2000)

[13] Held G., "*The ABCs of IEEE 802.11*", στο IEEE IT Professional Magazine, Vol. 3, No. 6 (November/December 2001)

[14] IEEE: www.ieee.org

[15]Wireless Ethernet: www.wirelessethernet.com

[16]Wireless Lan Alliance: www.wlana.com

[17]Wi-Fi Allience: www.weca.net/OpenSection/index.asp

[18]Mathew S.Gast ,"The Definitue Guide.",802.11 Wireless Networks(19982)

[19] Tanenbaum, Andrew S., "*Computer Networks, 4rd American Edition*": Prentice Hall International Inc. (2003)

[20] Δικτυακός τόπος της Intracom A.C. :
www.intrasoft.gr/gr/products/command_control/wispr_wlan.htm

[21] Alexander , “ 802.11 Wireless Network Site Surveying A ” : Cisco Press (2000)

[22] David A. Stamper , “ Τοπικά Δίκτυα Περιοχής “ : Παπασωτηρίου (2002)