Τ.Ε.Ι. ΗΠΕΙΡΟΥ
T.E.I. OF EPIRUS

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ & ΟΙΚΟΝΟΜΙΑΣ (Σ.Δ.Ο)
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ & ΔΙΟΙΚΗΣΗΣ

SCHOOL OF MANAGEMENT AND ECONOMICS
DEPARTMENT OF COMMUNICATIONS, INFORMATICS AND MANAGEMENT

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

WLAN HOTSPOTS

« Σημεία Ασύρματης Ευρυζωνικής Πρόσβασης »

Επιβλέπων – Εισηγητής : **Σακκάς Λάμπρος**

Σπουδαστής : **Τρέντσιος Νικόλαος**
Α.Μ. : **5738**

ΑΡΤΑ
ΙΟΥΛΙΟΣ 2008

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω καταρχήν τον επιβλέποντα καθηγητή της εργασίας μου κ. Σακκά Λάμπρο, για την εμπιστοσύνη που μου έδειξε αναθέτοντάς μου αυτή την εργασία, για την καθοδήγησή του καθ' όλη τη διάρκειά της και κυρίως για την ευκαιρία που μου έδωσε να ασχοληθώ με ένα ενδιαφέρον αντικείμενο.

Επίσης, θέλω να ευχαριστήσω ιδιαίτερα τους γονείς μου για όλη τους την προσπάθεια όλα αυτά τα χρόνια που μου στάθηκαν σε οποιοδήποτε πρόβλημα παρουσιάστηκε. Χάρη στη δική τους προσπάθεια βρίσκομαι στην ευχάριστη αυτή στιγμή περάτωσης των σπουδών μου και θέλω να τους ευχαριστήσω για αυτό πάρα πολύ.

Άρτα, Ιούλιος 2008
Τρέντσιος Νικόλαος

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΚΕΦΑΛΑΙΟ 1 :

ΕΙΣΑΓΩΓΗ

Καθώς ζούμε σε μια εποχή που χαρακτηρίζεται από τη διακίνηση μεγάλων όγκων πληροφορίας και την ανάπτυξη της τεχνολογίας, η υλοποίηση ασύρματων δικτύων συμβάλλει δραματικά στην απλούστευση του τρόπου επικοινωνίας και σύνδεσης των οντοτήτων του δικτύου και στην ταχύτερη μετάδοση των πληροφοριών.

Η ασύρματη επικοινωνία αποκτά ιδιαίτερη αξία σε μια χώρα όπως η Ελλάδα, που η μορφολογία του εδάφους της δεν επιτρέπει πολλές φορές τη χρήση εναλλακτικών μέσων μετάδοσης όπως για παράδειγμα οι οπτικές ίνες.

Τα ασύρματα δίκτυα υπάρχουν εδώ και μια δεκαετία, αλλά μόλις τα τελευταία χρόνια πραγματοποιήθηκε μια έκρηξη στη χρήση τους, εξαιτίας κυρίως της τεχνολογικής εξέλιξης στις ασύρματες δικτυακές φορητές συσκευές (φορητοί υπολογιστές, PDA, κλπ.) καθώς και της πτώσης της τιμής των τελευταίων. Τα ασύρματα δίκτυα μπορούν να αναπτυχθούν και να παρέχουν δικτυακές υπηρεσίες σε πολλούς διαφορετικούς χώρους και περιβάλλοντα. Τα ιδιαίτερα χαρακτηριστικά του κάθε χώρου καθώς και οι ανάγκες των χρηστών υποδεικνύουν μια σειρά από λειτουργικές απαιτήσεις οι οποίες πρέπει να ληφθούν υπόψη κατά το σχεδιασμό του ασύρματου δικτύου.

Με την δημιουργία των πρώτων δικτύων ηλεκτρονικών υπολογιστών, παράλληλα με τις μεθόδους που αναπτύχθηκαν για ενσύρματη σύνδεση των κόμβων, είχαμε και την προσπάθεια δημιουργίας ασύρματων τοπικών δικτύων που θα αποδέσμευε την επικοινωνία από τα ενσύρματα μέσα. Σήμερα τα ασύρματα τοπικά δίκτυα υπολογιστών, υλοποιούνται βασισμένα στις προδιαγραφές που ορίζει η οικογένεια πρωτοκόλλων του IEEE 802.11 και που στην ουσία είναι τον πρότυπο ethernet και το csma/ca, δηλαδή το πρωτόκολλο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων.

Ενδεικτικά αναφέρουμε το 802.11b που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 11Mbps και το 802.11g που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 54Mbps. Η κάρτα δικτύου που χρησιμοποιείται στην υλοποίηση, κάνοντας χρήση της ασύρματης τεχνολογίας επιτυγχάνει την ίδια δικτύωση με μια κλασσική κάρτα δικτύου, αλλά χωρίς καλώδια. **Μια ειδική περίπτωση που μας ενδιαφέρει ιδιαίτερα, είναι το Hotspot, το οποίο είναι το ασύρματο δίκτυο στο οποίο ο χρήστης μπορεί να έχει πρόσβαση στο Internet με πολύ χαμηλό κόστος και κάποιες φορές ακόμα και δωρεάν.**

Παρότι οι λύσεις ενσύρματης δικτύωσης παρείχαν ικανές επιδόσεις, ήταν ανεπαρκείς σε αρκετές περιπτώσεις εφαρμογών. Η ευελιξία που παρέχουν οι ασύρματες τεχνολογίες φάνηκε από νωρίς πως θα άνοιγε ένα τεράστιο πεδίο νέων εφαρμογών. Παράλληλα, η τεχνολογική εξέλιξη, έκανε δυνατή την παραγωγή συσκευών με πολύ μικρό κόστος και σε μεγάλες ποσότητες. Το αποτέλεσμα όλων αυτών είναι ότι την τελευταία δεκαετία βιώνουμε την όλο και πιο έντονη παρουσία των ασύρματων τεχνολογιών.

Οι εφαρμογές των ασύρματων δικτύων είναι ολοένα αυξανόμενες προσφέροντας υπηρεσίες σε πολλούς τομείς όπως ενδεικτικά αναφέρονται παρακάτω.

- Πρόσβαση: Σε σημεία υψηλής κίνησης (**HotSpots**), όπως αεροδρόμια, εμπορικά καταστήματα, σημεία ψυχαγωγίας, προσφέρει ενημέρωση, διαφήμιση, ψυχαγωγία.
- 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.
- Νοσοκομεία: Το προσωπικό αποκτά πρόσβαση σε ζωτικές πληροφορίες για τον ασθενή, σε πραγματικό χρόνο από οπουδήποτε.

Τα **WLAN Hotspots** προσφέρουν ταχύτατη σύνδεση στο Ίντερνετ χωρίς καλώδια και με κόστος κατά πολύ χαμηλότερο σε σχέση με την κινητή τηλεφωνία. Μάλιστα, έπειτα από αρκετή καθυστέρηση σε σχέση με ό,τι συμβαίνει σε χώρες του εξωτερικού, φτάνουν και στη χώρα μας. Πρόκειται για χώρους όπου όποιος διαθέτει έναν φορητό υπολογιστή ή κάποιο PDA με δυνατότητες ασύρματης σύνδεσης σε δίκτυο, μπορεί να αποκτήσει πρόσβαση στο Ίντερνετ σε εξαιρετικά υψηλές ταχύτητες, που ξεπερνούν το 1MBps, 20 φορές δηλαδή παραπάνω από μια απλή τηλεφωνική γραμμή.

ΚΕΦΑΛΑΙΟ 2 :

ΔΙΚΤΥΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

2.1. ΕΙΣΑΓΩΓΗ

Σε κάθε ένα από τους τρεις τελευταίους αιώνες επικράτησε μία μοναδική τεχνολογία. Ο 18ος αιώνας ήταν η εποχή των μεγάλων μηχανικών συστημάτων που συνόδευσαν τη βιομηχανική επανάσταση. Ο 19ος αιώνας ήταν η εποχή της ατμομηχανής. Στον 20ο αιώνα η τεχνολογία-κλειδί είναι η συλλογή, επεξεργασία και διανομή της πληροφορίας. Έχουμε δει την εγκατάσταση τηλεφωνικών δικτύων σε όλη την υδρόγειο, την εφεύρεση του ραδιοφώνου και της τηλεόρασης, τη γέννηση και χωρίς προηγούμενο ανάπτυξη της βιομηχανίας υπολογιστών και την εκτόξευση επικοινωνιακών δορυφόρων.

Αν και η βιομηχανία των υπολογιστών είναι νέα σε σύγκριση με άλλες βιομηχανίες (αυτοκινητοβιομηχανία, αερομεταφορές) οι υπολογιστές έχουν εξελιχθεί θεαματικά σε σύντομο διάστημα. Κατά την διάρκεια των πρώτων δεκαετιών της ύπαρξής τους, τα υπολογιστικά συστήματα ήταν συγκεντρωμένα σε μια μεγάλη αίθουσα.

Η ιδέα ότι μέσα σε 20 χρόνια θα παράγονταν μαζικά σε εκατομμύρια εξίσου ισχυροί υπολογιστές (μικρότεροι και από γραμματόσημο) ήταν καθαρά επιστημονική φαντασία. Εξαιτίας της ραγδαίας τεχνολογικής προόδου οι περιοχές της συλλογής, μεταφοράς, αποθήκευσης και επεξεργασίας της πληροφορίας συγκλίνουν ταχύτατα και οι διαφορές τους εξαφανίζονται. Καθώς αναπτύσσεται η ικανότητά μας να συλλέγουμε, να επεξεργαζόμαστε και να διανέμουμε πληροφορίες η ανάγκη για περισσότερη προηγμένη επεξεργασία της πληροφορίας αναπτύσσεται ακόμα ταχύτερα. Η σύγκλιση των δυο ανεξάρτητων-πριν από λίγα χρόνια- τεχνολογιών της πληροφορικής (των υπολογιστών) και των

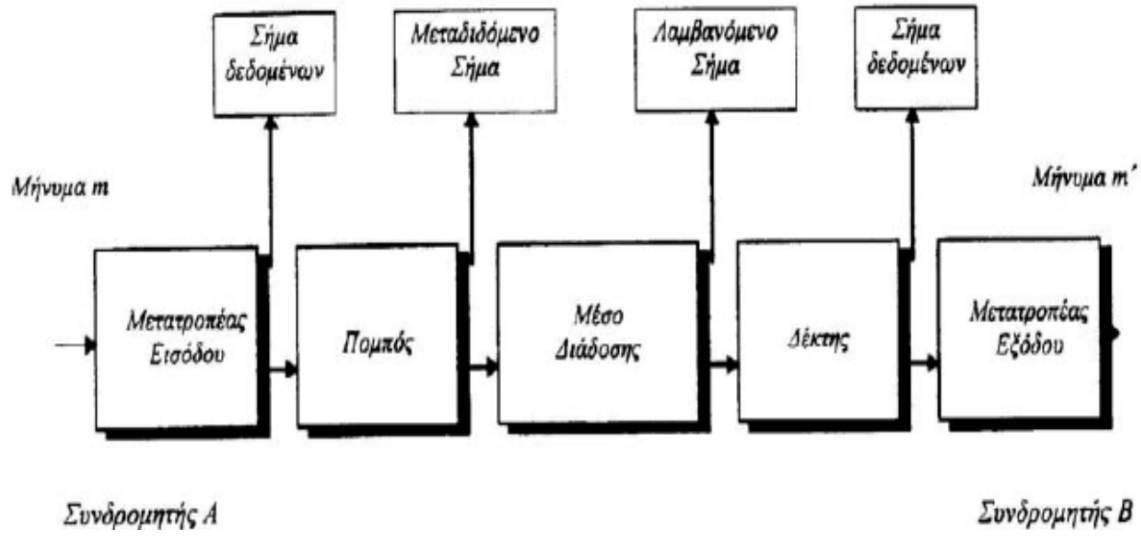
τηλεπικοινωνιών είχε σημαντική επίδραση στον τρόπο με τον οποίο οργανώνονται τα υπολογιστικά συστήματα.

Η ιδέα του "υπολογιστικού κέντρου" με ένα μεγάλο υπολογιστή, όπου οι χρήστες φέρνουν την δουλειά τους για επεξεργασία είναι πλέον ξεπερασμένη. ***Σήμερα ένας μεγάλος αριθμός ξεχωριστών αλλά διασυνδεδεμένων υπολογιστών κάνουν την δουλειά.*** ***Τα συστήματα αυτά αποκαλούνται δίκτυα υπολογιστών.***

Οι αλλαγές που λαμβάνουν χώρα έχουν δραματική επίδραση στον τρόπο με τον οποίο επικοινωνούν άτομα και οργανισμοί. Η διοίκηση σε όλα τα επίπεδα, το εμπόριο και η οικονομία, η φροντίδα της υγείας, η εκπαίδευση, είναι μεταξύ των πεδίων της ανθρώπινης δραστηριότητας που επηρεάζονται βαθιά από τις τεχνολογικές προόδους που συντελούνται σήμερα. [7]

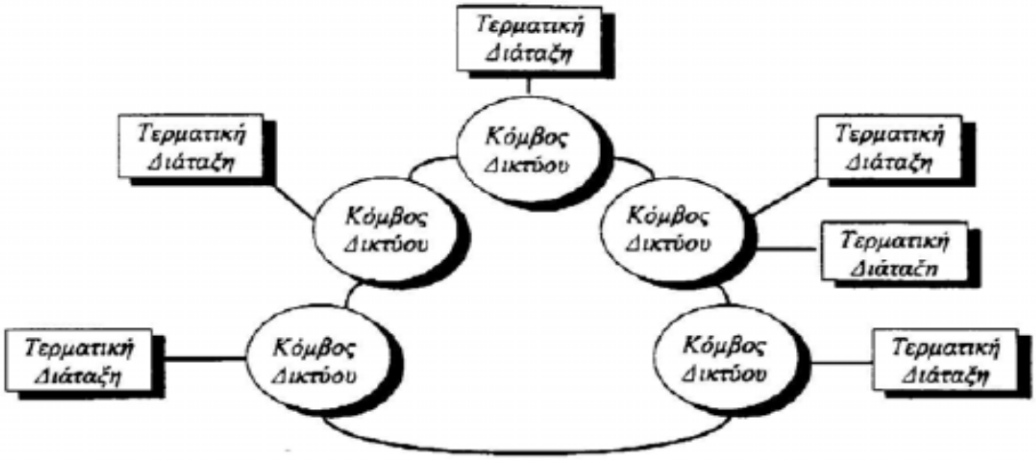
2.2. ΠΕΡΙ ΔΙΚΤΥΩΝ

Σκοπός των τηλεπικοινωνιακών συστημάτων είναι η μεταβίβαση πληροφοριών από ένα σημείο του χώρου που ονομάζεται πομπός σε ένα άλλο σημείο του χώρου που ονομάζεται δέκτης, με τη βοήθεια της διάδοσης της ηλεκτρικής ενέργειας ή του ηλεκτρικού ρεύματος. *Η δομή ενός τυπικού τηλεπικοινωνιακού συστήματος φαίνεται στην εικόνα 2.1.*



Εικόνα 2.1 : Βασικό Τηλεπικοινωνιακό Σύστημα

Το απλό μοντέλο (*σχήμα 2.1*) καλύπτει τις ανάγκες επικοινωνίας μεταξύ δύο συνδρομητών. Για να καλυφθούν όμως οι ανάγκες επικοινωνίας πολλών συνδρομητών γίνεται απαραίτητη η δημιουργία ενός δικτύου (*εικόνα 2.2*). Το δίκτυο δίνει τη δυνατότητα σε ένα συνδρομητή να επικοινωνήσει με οποιονδήποτε άλλο συνδρομητή διαθέτει την κατάλληλη διάταξη πρόσβασης σε κάποιο οριακό σύστημα του δικτύου που ονομάζεται κόμβος ή κέντρο. Βασική ιδιότητα του δικτύου είναι η παροχή ικανοποιητικής επικοινωνίας με τον ελάχιστο δυνατό αριθμό διασυνδέσεων των κόμβων του.



Εικόνα 2.2 : Δίκτυο Επικοινωνίας

Δίκτυο τηλεπληροφορικής είναι ένα σύστημα επικοινωνιών το οποίο διαθέτει συσκευές τηλεπικοινωνιών, τηλεπικοινωνιακούς κόμβους, καθώς και τα φυσικά μέσα διέλευσης της πληροφορίας. Επίσης στην ευρύτερη έννοιά του περιλαμβάνει και τις τερματικές συσκευές, όπως είναι οι υπολογιστές και τα τερματικά κάθε είδους και έχει μια δομή τέτοια ώστε να επιτυγχάνεται η όποια επιθυμητή μεταξύ τους επικοινωνία. ***Στα δίκτυα τηλεπληροφορικής συναντάμε αυστηρούς κανόνες που διέπουν το τηλεπικοινωνιακό τμήμα του δικτύου καθώς επίσης και κανόνες συνομιλίας μεταξύ των υπολογιστών (πρωτόκολλα επικοινωνίας).***

Πολλές φορές στην προσπάθεια των εταιριών υπολογιστών να καλύψουν τα θέματα των τηλεπικοινωνιών, παρατηρείται το φαινόμενο τα σύνορα μεταξύ της πληροφορικής και των τηλεπικοινωνιών να γίνονται δυσδιάκριτα. Άλλωστε ένα μεγάλο μέρος του λογισμικού επικοινωνιών αλλά και των πρωτοκόλλων φιλοξενείται στους υπολογιστές είτε ενσωματωμένο στο λειτουργικό σύστημα είτε

σαν ανεξάρτητα προγράμματα. Γι' αυτό θα δούμε πολλές φορές να μην είναι εύκολος και σαφής ο προσδιορισμός δικτύων.

Από το 1972 αρκετά δίκτυα πληροφορικής έχουν αναπτυχθεί όπως το ARPANET, το CYBERNET, το DCS (Distributed Computing System), το CYCLADES με αποκορύφωμα την τεράστια εξάπλωση του δικτύου INTERNET. [4]

2.3. ΣΚΟΠΟΣ ΤΩΝ ΔΙΚΤΥΩΝ

Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής (προγράμματα, αρχεία, δεδομένα). Πόροι του συστήματος μπορούν να είναι είτε υλικό (hardware), π.χ. υπολογιστές, εκτυπωτές, plotters, σκληροί δίσκοι είτε λογισμικό (software), π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες. **Τα προγράμματα, τα δεδομένα και οι συσκευές (σκληροί δίσκοι, εκτυπωτές, κλπ) είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση.** Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων (electronic mail). Επιπλέον, ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

2.4. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΩΝ ΔΙΚΤΥΩΝ

Η αρχιτεκτονική των δικτύων καθορίζει τον τρόπο με τον οποίο οι υπολογιστές και οι λοιπές συσκευές συνδέονται μεταξύ τους για να σχηματίσουν ένα σύστημα επικοινωνίας που θα επιτρέπει στους χρήστες να διαμοιράζονται πληροφορίες και συσκευές του δικτύου.

Σε ένα δίκτυο δεδομένων περιλαμβάνονται:

1. Τερματικοί Κόμβοι :
Ελέγχουν τους πόρους του δικτύου (λογισμικό και υλικό).

2. Υποδίκτυα :

Φυσικά μέσα μετάδοσης, πρωτόκολλα επικοινωνίας, τοπολογία, τερματικοί κόμβοι, πόροι που μπορούν να διαφέρουν πολύ ανά υποδίκτυο.

3. Συσκευές Διασύνδεσης :

Διασυνδέουν τα ετερογενή υποδίκτυα έτσι ώστε να εξασφαλίζεται η επικοινωνία τερματικών κόμβων που βρίσκονται σε διαφορετικά υποδίκτυα. [5]

2.5. ΚΑΤΗΓΟΡΙΕΣ ΔΙΚΤΥΩΝ

Τα δίκτυα επικοινωνιών κατατάσσονται με βάση την έκταση την οποία εξυπηρετούν, σε τρεις γενικές κατηγορίες :

Τοπικά δίκτυα (LAN: Local Area Networks)

Τα τοπικά δίκτυα (LAN) περιορίζονται συνήθως μέσα σε ένα κτίριο ή κτιριακό συγκρότημα όπου η μέγιστη επιτρεπτή απόσταση είναι μερικές εκατοντάδες μέτρα.

Μητροπολιτικά δίκτυα (MAN: Metropolitan Area Networks)

Τα μητροπολιτικά δίκτυα (MAN) είναι μια μεγαλύτερη εκδοχή ενός LAN. Μπορεί να καλύπτει ομάδα γειτονικών γραφείων ενός νοσοκομείου. Μπορεί να υποστηρίζει δεδομένα και φωνή και ίσως να σχετίζεται με την καλωδιακή τηλεόραση. Περιορίζονται μέσα στα όρια μιας πόλης και μπορούν να καλύπτουν αποστάσεις από 1 έως και 100 km.

Ευρείας περιοχής δίκτυα (WAN: Wide Area Networks)

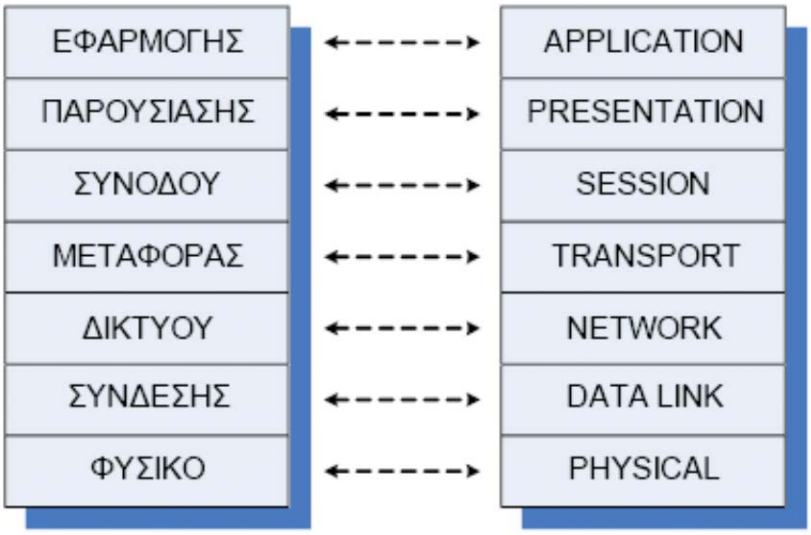
Τα δίκτυα ευρείας περιοχής (WAN) μπορούν να απλώνονται πολλές φορές και σε διαφορετικές ηπείρους . Ένα δίκτυο ευρείας περιοχής μπορεί να απαρτίζεται από υπολογιστές και τοπικά δίκτυα που βρίσκονται διαφορετικές πόλεις ή ακόμα και σε διαφορετικές χώρες. Τα Δίκτυα Ευρείας Περιοχής χρησιμοποιούν καλώδια υψηλής ταχύτητας, οπτικές ίνες, και δορυφόρους για τη μεταφορά των δεδομένων και των αρχείων. Τα δίκτυα ευρείας περιοχής χρησιμοποιούνται συνήθως από μεγάλες εταιρείες, κυρίως πολυεθνικές, οι οποίες έχουν δραστηριότητες σε πολλές πόλεις χώρες. Το Internet θεωρείται το μεγαλύτερο δίκτυο ευρείας περιοχής στον κόσμο. [7]

2.6. ΜΟΝΤΕΛΟ ISO/OSI

Το 1977 ο διεθνής οργανισμός τυποποιήσεων ISO ξεκίνησε μια προσπάθεια, που τα πρώτα της αποτελέσματα εμφανίσθηκαν το 1983 με την ανακοίνωση του προτύπου OSI (Open System Interconnection reference model), που ερμηνεύεται *«Πρότυπο διασύνδεσης ανοικτών συστημάτων»*. Το OSI αποτελεί το πλαίσιο μέσα στο οποίο κινούνται οι λεπτομερείς πλέον τυποποιήσεις, για την επίλυση όλων των επί μέρους προβλημάτων που εμφανίζονται στις επικοινωνίες υπολογιστών διαφορετικών κατασκευαστών.

Ο στόχος του προτύπου αυτού είναι η δημιουργία τυποποίησης ώστε να είναι δυνατή η επικοινωνία μεταξύ υπολογιστών διαφορετικών κατασκευαστών. Στο ακρωνύμιο OSI το **O** που οφείλεται στο **Open** και σημαίνει ανοικτό, εννοεί ελεύθερη επικοινωνία σε αντιδιαστολή προς τα κλειστά (της αυτής εταιρίας) συστήματα. Με το πρότυπο αυτό τίθεται ένα πλαίσιο, μέσα στο οποίο καθορίζονται standard και πρωτόκολλα για την επικοινωνία των διαφόρων επιπέδων που ορίζονται από το OSI.

Η βασική φιλοσοφία που το διέπει είναι της επιπεδοποίησης (layering). Όλες οι απαιτούμενες για επικοινωνία λειτουργίες ομαδοποιούνται σε επτά μεγάλα επίπεδα. Οι λειτουργίες αυτές είναι ανεξάρτητες μεταξύ τους έτσι ώστε αλλαγές σε ένα επίπεδο να μην έχουν επίδραση στα άλλα. Στην *εικόνα 2.3* βλέπουμε τα επτά επίπεδα, έτσι όπως έχουν τιτλοφορηθεί από τον ISO με παράλληλη παράθεση της Ελληνικής ορολογίας.



Εικόνα 2.3 : Πρότυπο OSI [4]

2.7. ΦΥΣΙΚΑ ΜΕΣΑ ΜΕΤΑΔΟΣΗΣ

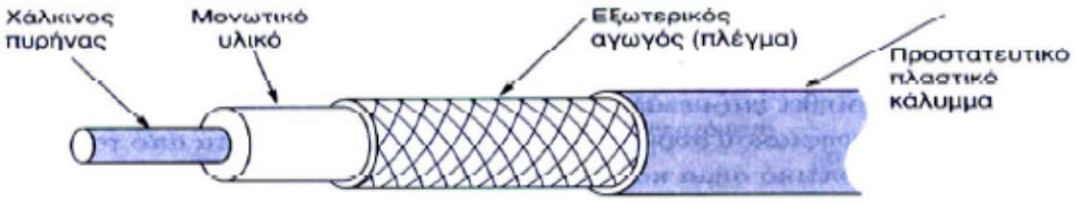
Η μετάδοση της ψηφιακής πληροφορίας μπορεί να γίνει διαμέσου πολλών ειδών φυσικών μέσων. Σε κάθε περίπτωση, ζητείται ένας τρόπος αναπαράστασης των **0** και **1** με χρήση σημάτων που μπορούν να διαδοθούν μέσα στο μέσο.

Διακρίνουμε δύο βασικούς τύπους μέσων μετάδοσης:

- **Επίγεια (terrestrial)** και
- **Εναέρια (aerial).**

Στην κατηγορία των **επίγειων μέσων** περιλαμβάνονται **τα μεταλλικά καλώδια (metallic cables)** και **οι οπτικές ίνες (optical fibers).**

Τα μεταλλικά καλώδια είναι δύο τύπων: ομοαξονικά (coaxial) και twisted pair (TP). Τα καλώδια του δεύτερου τύπου είναι είτε θωρακισμένα (Shielded twisted pair, STP) είτε αθωράκιστα (Unshielded Twisted Pair, UTP). Τα ψηφία μεταφέρονται μέσα στα μεταλλικά καλώδια με την μορφή ηλεκτρικών παλμών. Λόγω των αντιστάσεων του καλωδίου και των παρεμβολών, το ηλεκτρικό σήμα εξασθενεί κατά τη διάδοση του μέσα στο καλώδιο. Σε γενικές γραμμές, τα ομοαξονικά καλώδια έχουν μικρότερες εξασθενίσεις και μπορούν να επιτύχουν μεγαλύτερες ταχύτητες σε σχέση με τα UTP και τα STP. Όταν χρησιμοποιούνται TP καλώδια για μεταφορά δεδομένων σε μεγάλες αποστάσεις, απαιτούνται σημεία αναγέννησης του ηλεκτρικού σήματος. Τα καλώδια TP και ειδικότερα τα UTP, είναι ευαίσθητα στο θόρυβο και στις ηλεκτρομαγνητικές ακτινοβολίες γειτονικών συσκευών, ενώ έχουν και περισσότερες εκπομπές χαμηλών ραδιοφωνικών συχνοτήτων. Στην *εικόνα 2.4* μπορούμε να δούμε πως είναι ένα ομοαξονικό καλώδιο.



Εικόνα 2.4 : Ομοαξονικό καλώδιο

Οι οπτικές ίνες προσφέρουν πολύ μεγαλύτερες ταχύτητες μετάδοσης. Τα bits μεταδίδονται ως διαμορφωμένο φως και όχι ως ηλεκτρικό σήμα.

Η αναγέννηση του σήματος στις οπτικές ίνες γίνεται είτε απευθείας είτε με ενδιάμεση μετατροπή του φωτός σε ηλεκτρικό σήμα. Οι επιδόσεις των οπτικών ινών μπορούν να αποδοθούν από το γινόμενο του bit rate τους με τη μέγιστη απόσταση που μπορεί να διανύσει το σήμα χωρίς να απαιτηθεί αναγέννηση. Αυτός ο δείκτης διπλασιάζεται κάθε χρόνο και αυτή τη στιγμή βρίσκεται στα 100 εκατομμύρια Mbps ΄ km. Στην *εικόνα 2.5* βλέπουμε πως είναι μια οπτική ίνα.

(α) Πλευρική όψη μίας ίνας. (β) Εγκάρσια όψη περιβλήματος με τρεις ίνες.

Εικόνα 2.5 : Οπτική ίνα

Οι **εναέριες μεταδόσεις** διακρίνονται σε δύο τύπους: επιφανείας (surface), όπως **οι ραδιοφωνικές**, και **δορυφορικές (satellite)**. Και οι δυο τύποι έχουν μεγαλύτερους ρυθμούς εμφάνισης λαθών σε σχέση με τις επίγειες μεταδόσεις. Η δορυφορική μετάδοση παρουσιάζει ένα επιπλέον μειονέκτημα, μια καθυστέρηση μισού περίπου δευτερολέπτου για κάθε πακέτο πληροφορίας που μεταδίδεται. *Αναλυτικότερα για τις εναέριες μεταδόσεις θα μιλήσουμε στο Κεφάλαιο 3 οπού εκεί θα γίνει εκτενέστερη η ανάλυση των ασύρματων δικτύων.* **[6] [7]**

2.8. ΜΕΤΑΔΟΣΗ ΒΑΣΙΚΗΣ ΚΑΙ ΕΥΡΕΙΑΣ ΖΩΝΗΣ

Στην **μετάδοση βασικής ζώνης (baseband transmission) διαμέσου ηλεκτρικών καλωδίων, το ηλεκτρικό σήμα εφαρμόζεται απευθείας ανάμεσα στους δυο αγωγούς.** Ένα μόνο bit μπορεί να μεταδοθεί κάθε φορά. Η πολυπλεξία μπορεί να επιτευχθεί μόνο με χρονικό καταμερισμό (Time Division Multiplexing, TDM).

Η **μετάδοση ευρείας ζώνης** (broadband transmission) δεν χρησιμοποιεί το ηλεκτρικό σήμα απευθείας. Το ηλεκτρικό σήμα χρησιμοποιείται στη **διαμόρφωση** κάποιου χαρακτηριστικού (πχ του πλάτους) ενός άλλου ηλεκτρικού σήματος, που ονομάζεται **φέρον** (carrier) και που αποτελεί το σήμα που τελικά θα μεταδοθεί. Συνήθως, το φέρον έχει πολύ μεγαλύτερη συχνότητα από το σήμα που μεταφέρει την πληροφορία. Στην μετάδοση ευρείας ζώνης η πολυπλεξία μπορεί να επιτευχθεί και με καταμερισμό του πεδίου συχνοτήτων (Frequency Division Multiplexing, FDM). Αυτό σημαίνει ότι σε κάθε ροή δεδομένων διατίθεται φέρον διαφορετικής συχνότητας. Στην πολυπλεξία FDM, η μετάδοση των ροών δεδομένων μπορεί να γίνει ταυτόχρονα και με μικρότερες απαιτήσεις αναγέννησης σε σχέση με τη μετάδοση βασικής ζώνης. Η ανάκτηση της πληροφορίας στον προορισμό, γίνεται με την αντίστροφη διαδικασία, που ονομάζεται αποδιαμόρφωση. Οι συσκευές που διαμορφώνουν το φέρον κατά την μετάδοση και το αποδιαμορφώνουν στην λήψη, ονομάζονται modems. [6]

2.9. ΤΟΠΟΛΟΓΙΕΣ ΔΙΚΤΥΩΝ

Η τοπολογία ορίζει τον τρόπο με τον οποίο γίνεται η φυσική διασύνδεση των κόμβων ενός δικτύου. Η τοπολογία επηρεάζεται από τους εξής παράγοντες:

- Αν το δίκτυο είναι ενσύρματο ή ασύρματο.
- Από τον τρόπο σύνδεσης των κόμβων (ένας προς έναν ή ένας προς πολλούς).

Σε αυτό το κεφάλαιο θα αναφερθούμε μόνο στις τοπολογίες των ενσύρματων δικτύων. Για τις τοπολογίες ασύρματων δικτύων θα γίνει αναφορά στο επόμενο κεφάλαιο «Κεφάλαιο 3 : Ασύρματα δίκτυα» .

Οι βασικές τοπολογίες των ενσύρματων τοπικών δικτύων είναι:

- **Ο δίαυλος**
- **Το δέντρο**
- **Ο δακτύλιος**
- **Το άστρο (ή αστέρας)**

Υπάρχουν τοπολογίες οι οποίες προκύπτουν από παραλλαγές και βελτιώσεις των παραπάνω. Για παράδειγμα, παραλλαγή της τοπολογίας διαύλου είναι το δέντρο, και παραλλαγή της τοπολογίας δακτυλίου είναι ο διπλός δακτύλιος.

Υπάρχουν τοπολογίες που προκύπτουν από συνδυασμούς άλλων όπως άστρο-δακτύλιος και τοπολογίες που δεν έχουν κάποιο συγκεκριμένο σχήμα (δικτυωτά) και συναντώνται περισσότερο σε δίκτυα ευρείας περιοχής.

Βασικοί παράγοντες που επηρεάζουν την επιλογή μιας τοπολογίας στην υλοποίηση ενός δικτύου είναι:

- Το είδος των εφαρμογών.
- Η πολυπλοκότητα των διαδικασιών ελέγχου που επιβάλλει η τοπολογία και η επίδραση που μπορεί αυτή να έχει στην απόδοση του δικτύου.
- Η ευκολία με την οποία μπορεί να επεκταθεί (π.χ. να προστεθούν και άλλες θέσεις εργασίας) αν υπάρχει ανάγκη.

Σε ένα δίκτυο στο οποίο ένας κόμβος Α μπορεί να επικοινωνήσει με ένα άλλο κόμβο Β με περισσότερες από μία διαδρομές, η εύρεση της συντομότερης διαδρομής αποτελεί το πρόβλημα της δρομολόγησης. Το πρόβλημα αυτό μέχρι σήμερα παραμένει ανοικτό (δεν υπάρχει κάποιος άμεσος τρόπος επίλυσης μέχρι στιγμής αλλά ούτε έχει αποδειχθεί ότι το πρόβλημα δεν λύνεται).

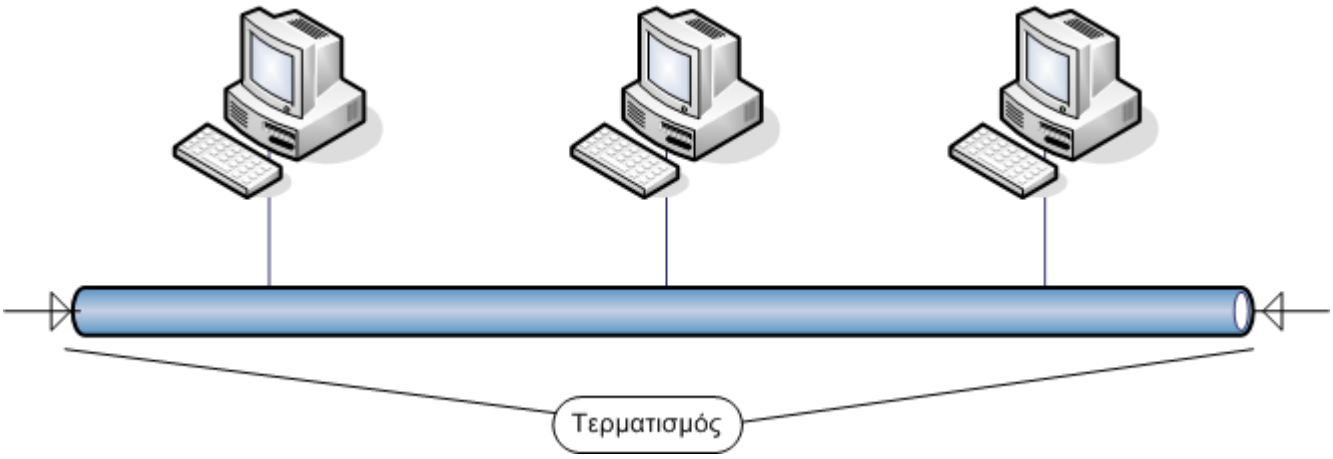
2.9.1. Τοπολογία Διαύλου :

Σχεδιαστικά αυτή η τοπολογία είναι αρκετά απλή, αφού όλοι οι κόμβοι του δικτύου συνδέονται άμεσα (με την βοήθεια κατάλληλων συνδετήρων (βυσμάτων) και τερματισμών) σε μια κοινή γραμμή επικοινωνίας που ονομάζεται δίαυλος (bus). Τα πακέτα που στέλνονται από ένα κόμβο διαδίδονται σε όλη την κοινή γραμμή επικοινωνίας και λαμβάνονται από όλους τους κόμβους. Κάθε κόμβος ελέγχει την διεύθυνση παραλήπτη που αναγράφεται στο πακέτο, και αν ανακαλύψει ότι απευθύνεται σε αυτόν το αντιγράφει, διαφορετικά το αγνοεί.

Επειδή οι κόμβοι που βρίσκονται πιο κοντά σε αυτόν που εκπέμπει κάθε φορά λαμβάνουν ισχυρότερο σήμα από τους πιο απομακρυσμένους υπάρχουν κάποιοι περιορισμοί οι οποίοι αφορούν:

- Το μήκος του καλωδίου.
- Το πλήθος των συνδέσεων.
- Το είδος / ποιότητα των υλικών που χρησιμοποιούνται στις συνδέσεις.

Πέρα από κάποιο όριο εξασθένησης (το οποίο μπορεί να προκληθεί για παράδειγμα από πολύ μεγάλο μήκος καλωδίου) μπορεί να έχουμε απώλεια δεδομένων. Τα δίκτυα διαύλου δεν παρουσιάζουν πολυπλοκότητα στην κατασκευή και μπορούμε εύκολα να τους αλλάξουμε διάταξη ή να τα επεκτείνουμε. *Ένα παράδειγμα τοπολογίας Διαύλου φαίνεται στην εικόνα 2.6.*



Εικόνα 2.6. : Τοπολογία Διαύλου

Στο τέλος της γραμμής του διαύλου υπάρχει ένα απλό εξάρτημα, που ονομάζεται *τερματιστής* (terminator). Ο τερματιστής αναλαμβάνει να εμποδίσει το σήμα του δικτύου που φτάνει στην άκρη του καλωδίου από το να ανακλαστεί και να γυρίσει πίσω στο καλώδιο – παρεμβάλλοντας έτσι την κανονική μετάδοση. Ο τερματιστής ουσιαστικά καταναλώνει το σήμα του δικτύου που φτάνει στην άκρη του καλωδίου. Αν ο δίαυλος κοπεί σε ένα σημείο, τυπικά διακόπτεται η λειτουργία όλου του δικτύου ακριβώς επειδή χάνεται ο τερματισμός. Ωστόσο η βλάβη ενός κόμβου δεν επηρεάζει το υπόλοιπο δίκτυο.

Τα δίκτυα διαύλου είναι κατάλληλα όταν:

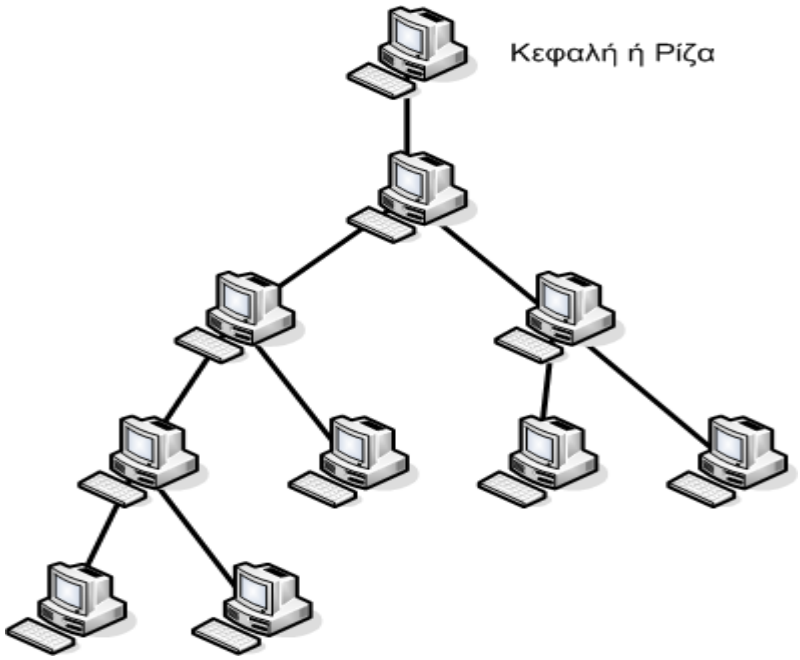
- Έχουμε μικρό αριθμό κόμβων.
- Η κυκλοφορία δεδομένων είναι μικρή.

Αντίθετα, είναι κακή επιλογή όταν:

- Έχουμε μεγάλο αριθμό κόμβων.
- Η κυκλοφορία στο δίκτυο είναι μεγάλη.

2.9.2. Τοπολογία Δέντρου :

Η τοπολογία δέντρου αποτελεί παραλλαγή της τοπολογίας διαύλου. Σχηματικά μοιάζει με ένα ανεστραμμένο δέντρο. Ο κορμός και τα κλαδιά του δέντρου αυτού αποτελούνται από δίκτυα διαύλου.



Εικόνα 2.7. : Τοπολογία Δέντρου

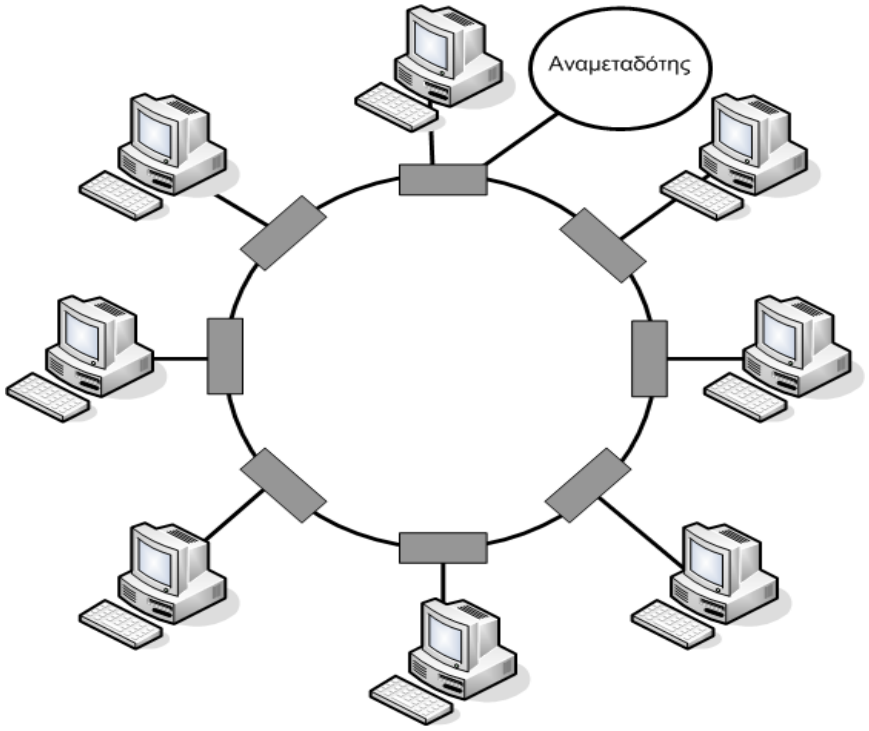
Το καλώδιο στην τοπολογία δέντρου διακλαδίζεται αλλά ποτέ δεν σχηματίζει κλειστούς βρόχους (δακτυλίους). Ξεκινά από ένα κόμβο που βρίσκεται στην κορυφή και ονομάζεται *κεφαλή ή ρίζα*. Η ρίζα αναμεταδίδει στο δίκτυο το σήμα που λαμβάνει από κάθε κόμβο που εκπέμπει και για το λόγο αυτό το τμήμα του διαύλου που περνάει από τη ρίζα έχει μεγαλύτερο φόρτο κίνησης σε σχέση με το υπόλοιπο δίκτυο. Ο δίαυλος που ξεκινά από τη ρίζα μπορεί να έχει διακλαδώσεις και αυτές με τη σειρά τους δικές τους διακλαδώσεις κ.ο.κ.

Επειδή η τοπολογία δέντρου αποτελεί παραλλαγή της τοπολογίας διαύλου, έχει περίπου τα ίδια πλεονεκτήματα και μειονεκτήματα με αυτή. Ωστόσο πρέπει να σημειώσουμε ότι είναι κατασκευαστικά πιο δύσκολο να φτιαχτεί (και να συντηρηθεί) και έχει ακόμα το μειονέκτημα ότι **σε περίπτωση βλάβης της ρίζας καταρρέει όλο το τμήμα του δικτύου που ελέγχει (αφού όλα τα δεδομένα περνάνε από τη ρίζα).**

2.9.3. Τοπολογία Δακτυλίου :

Στην τοπολογία δακτυλίου οι κόμβοι συνδέονται μεταξύ τους με συνδέσεις σημείο προς σημείο. Τα δύο άκρα του καλωδίου ενώνονται ώστε να σχηματίσουν ένα κλειστό βρόχο. Οι κόμβοι συνδέονται στο δίκτυο μέσω μιας διάταξης που ονομάζεται *αναμεταδότης*. *Παράδειγμα δακτυλίου φαίνεται στην εικόνα 2.8.*

Ο αναμεταδότης είναι μια απλή διάταξη που λαμβάνει το σήμα του δικτύου, το ενισχύει και το μεταδίδει ξανά στο δίκτυο. Ο αναμεταδότης λαμβάνει τα δυαδικά ψηφία από την είσοδο του, αναδημιουργεί το σήμα του δικτύου, και το μεταδίδει ξανά στην έξοδο του, με τον ίδιο ρυθμό μετάδοσης που τα έλαβε. Ο αναμεταδότης δεν έχει δυνατότητα προσωρινής αποθήκευσης.



Εικόνα 2.8. : Τοπολογία Δακτυλίου

Η ροή των πακέτων στο δακτύλιο ακολουθεί συγκεκριμένη και από πριν συμφωνημένη φορά η οποία μπορεί να είναι είτε αυτή των δεικτών του ρολογιού ή αντίστροφη. Τα πακέτα μεταδίδονται από κόμβο σε κόμβο χωρίς ιδιαίτερη καθυστέρηση. Δεν υπάρχουν πληροφορίες δρομολόγησης. Κάθε πακέτο περιέχει την διεύθυνση του παραλήπτη. Όλοι οι κόμβοι βλέπουν όλα τα πακέτα και αυτός για τον οποίο προορίζεται το αντιγράφει.

Επειδή όλοι οι κόμβοι μεταδίδουν και μοιράζονται το ίδιο φυσικό μέσο, χρειάζεται κάποιο είδος ελέγχου πρόσβασης ώστε να αποφασίζεται κάθε φορά ποιος κόμβος έχει δικαίωμα μετάδοσης.

Η τοπολογία δακτυλίου είναι καλή επιλογή όταν:

- Απαιτείται ισοκατανομή της χωρητικότητας του δικτύου στους κόμβους. Ισοκατανομή σημαίνει ότι κάθε κόμβος έχει δυνατότητα να στείλει με ίδιους ρυθμούς μετάδοσης με τους υπόλοιπους και η καθυστέρηση μετάδοσης του είναι επίσης ίδια.
- Όταν ο αριθμός κόμβων είναι μικρός και σε μικρή απόσταση ο ένας από τον άλλο, αλλά απαιτείται υψηλός ρυθμός μετάδοσης.
- Όταν κάθε κόμβος πρέπει να μεταδώσει οπωσδήποτε πριν από κάποιο συγκεκριμένο χρονικό διάστημα.

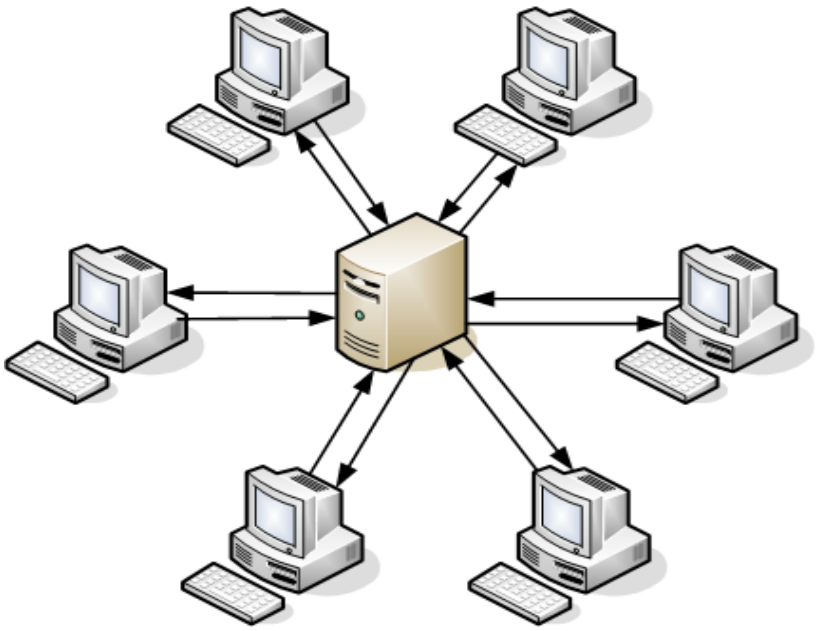
Γενικά τα δίκτυα δακτυλίου:

- Παρουσιάζουν καθυστέρηση μετάδοσης η οποία μπορεί να είναι σημαντική ακόμα και σε μικρό φορτίο κίνησης.
- Η μέση καθυστέρηση μετάδοσης δεν αυξάνει ανάλογα με το φορτίο του δικτύου.
- Υπάρχει σταθερή χρήση του καναλιού ακόμα και κάτω από μεγάλα φορτία κίνησης.

Το δίκτυο δακτυλίου υπάρχει και σε παραλλαγή με διπλό δακτύλιο όπου τα δεδομένα κινούνται με αντίθετη κατεύθυνση σε κάθε δακτύλιο. Ο διπλός δακτύλιος χρησιμοποιείται στα δίκτυα υψηλών επιδόσεων.

2.9.4. Τοπολογία Άστρου (ή Αστέρα) :

Στην τοπολογία άστρου οι κόμβοι συνδέονται ο καθένας με δικό του καλώδιο σε ένα κεντρικό κόμβο. Έχουμε δηλ. συνδέσεις σημείου προς σημείο από κάθε κόμβο του δικτύου προς τον κεντρικό. Μάλιστα κάθε κόμβος έχει μια σύνδεση ανά κατεύθυνση μετάδοσης. *Παράδειγμα φαίνεται στο εικόνα 2.9.*



Εικόνα 2.9. : Τοπολογία Άστρου (ή Αστέρα)

Η τοπολογία έχει τα χαρακτηριστικά της τοπολογίας διαύλου:

- Κάθε φορά μπορεί μόνο ένας κόμβος να μεταδώσει.
- Κάθε κόμβος μπορεί να δει τις μεταδόσεις οποιουδήποτε άλλου κόμβου.

Τα μηνύματα όλων των κόμβων μεταδίδονται στον κεντρικό κόμβο. Ανάλογα με το είδος του ελέγχου που εφαρμόζεται, ο κεντρικός κόμβος έχει διαφορετικό κάθε φορά ρόλο.

Υπάρχουν τρεις μορφές ελέγχου που μπορούν να εφαρμοστούν στην τοπολογία άστρου:

- Στην πρώτη μορφή ελέγχου (***κεντρικός έλεγχος***) ο κεντρικός κόμβος είναι υπεύθυνος για όλες τις διαδικασίες δρομολόγησης. Τα μηνύματα που φτάνουν στον κεντρικό κόμβο, αποστέλλονται μετά από επεξεργασία στον κόμβο παραλήπτη.
- Στην δεύτερη μορφή ελέγχου (***περιφερειακός έλεγχος***) ο έλεγχος δεν ασκείται από τον κεντρικό κόμβο αλλά από κάποιον από τους άλλους κόμβους (περιφερειακό κόμβο) ενώ ο κεντρικός αναλαμβάνει να αποκαταστήσει απλώς τις συνδέσεις λειτουργώντας σαν μεταγωγικός διακόπτης (ενώνει τους κόμβους μεταξύ τους).

Μπορείτε να φανταστείτε τη λειτουργία του κεντρικού κόμβου σε αυτή την περίπτωση όπως τη λειτουργία του τηλεφωνικού κέντρου του ΟΤΕ: Συνδέει μεταξύ τους τις συσκευές τηλεφώνων των συνδρομητών που θέλουν να συνομιλήσουν.

- Στην τρίτη μορφή ελέγχου (***κατανεμημένος έλεγχος***) ο έλεγχος δεν ασκείται συγκεκριμένα από κάποιον κόμβο, αλλά όλοι μαζί οι κόμβοι είναι υπεύθυνοι ενώ ο κεντρικός κόμβος είναι υπεύθυνος για την δρομολόγηση και την αποφυγή των συγκρούσεων.

Τα δίκτυα με τοπολογία άστρου αποτελούν καλή επιλογή όταν:

- Χρειαζόμαστε υψηλούς ρυθμούς μετάδοσης.
- Χρειαζόμαστε ολοκληρωμένες υπηρεσίες, κατάλληλες τόσο για μεταφορά φωνής όσο και δεδομένων (Μην ξεχνάμε ότι και συσκευές όπως τηλέφωνα και φαξ χρειάζονται συνδέσεις που ξεκινάνε από την κάθε συσκευή και καταλήγουν σε ένα κεντρικό σημείο, δηλ. τοπολογία άστρου).

Η υλοποίηση των δικτύων άστρου μπορεί να είναι πολύπλοκη. Κάποιοι κόμβοι μπορεί να έχουν απλό ρόλο τερματικής συσκευής και κάποιοι να ασκούν έλεγχο. Πολλά χαρακτηριστικά του δικτύου εξαρτώνται από τις δυνατότητες του κεντρικού κόμβου. Τέτοια χαρακτηριστικά είναι η χωρητικότητα του δικτύου, ο μέγιστος ρυθμός μεταφοράς δεδομένων, η δυνατότητα επέκτασης (προσθήκη και άλλων κόμβων), η αξιοπιστία κλπ. Δεν πρέπει επίσης να ξεχνάμε ότι το πλήθος των καλωδίων θα είναι μεγάλο, αφού χρειάζεται ένα καλώδιο από κάθε κόμβο προς τον κεντρικό. [1]

2.10. ΜΕΤΡΑ ΑΞΙΟΛΟΓΗΣΗΣ ΕΝΟΣ ΔΙΚΤΥΟΥ

Η αξιολόγηση μιας αρχιτεκτονικής δικτύου είναι πολύπλοκη υπόθεση και απαιτεί την εξέταση πολλών παραμέτρων. Όσον αφορά στην ικανότητα ενός δικτύου να υποστηρίξει εφαρμογές πολυμέσων, μπορούμε να διακρίνουμε **έξι παράγοντες καθοριστικής σημασίας:**

1. Ρυθμός Εξυπηρέτησης (Throughput)

Το δείκτη αυτό τον έχουμε ήδη χρησιμοποιήσει με τα ονόματα bit rate, ρυθμό μεταφοράς δεδομένων (transfer rate) ή εύρος ζώνης (bandwidth). Ο τελευταίος όρος τυπικά αναφέρεται στο εύρος συχνοτήτων ενός μέσου μετάδοσης, αλλά γενικεύεται κατά αναλογία και στην περίπτωση του δικτύου. Ο ρυθμός εξυπηρέτησης μπορεί να οριστεί ως εξής:

Ο ρυθμός μεταφοράς των δεδομένων μεταξύ δύο συστημάτων ορίζεται ως το πλήθος των δυαδικών ψηφίων (ή πακέτων) που μπορεί να δεχτεί και μεταδώσει το δίκτυο στη μονάδα του χρόνου.

Ο ορισμός αυτό έχει ένα κρυφό σημείο. Δεν καθορίζει ακριβώς τον τρόπο μέτρησης του ρυθμού εξυπηρέτησης. Έτσι μια τιμή μπορεί να αναφέρεται στο μέγιστο ρυθμό εξυπηρέτησης είτε στο ρυθμό εξυπηρέτησης που μπορεί να διατηρηθεί σταθερός από το δίκτυο.

Οι συνήθεις μονάδες μέτρησης είναι τα πολλαπλάσια του bps (bits per second): Kbps, Mbps, Gbps. Σε δίκτυα όπου η πληροφορία μεταδίδεται σε πακέτα, μπορούμε να μιλήσουμε για packets/sec.

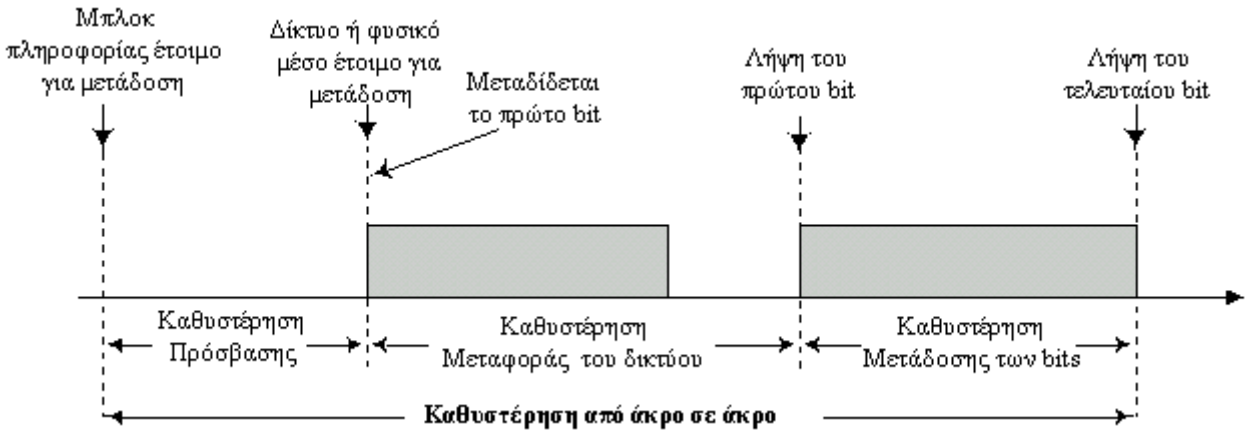
Στο ορισμό παρατηρούμε μια διαφοροποίηση μεταξύ του μέγιστου δυνατού ρυθμού αποδοχής των δεδομένων, που θα ονομάσουμε ρυθμό ή ταχύτητα πρόσβασης (access speed), και του ρυθμού μετάδοσης τους από το δίκτυο. Πράγματι, υπάρχουν δίκτυα, όπως τα περισσότερα από αυτά που χρησιμοποιούν διαμεταγωγή με πακέτα, που δέχονται δεδομένα τα οποία όμως, για διάφορους λόγους, δεν μπορούν να μεταδοθούν αμέσως και τοποθετούνται σε ουρές αναμονής. Αντίθετα, τα δίκτυα μεταγωγής κυκλώματος μπορούν να εξασφαλίσουν σταθερό bit rate παρόμοιο με αυτό του ρυθμού εισόδου πελατών.

2. Καθυστέρηση Μεταφοράς (Transit Delay)

Ορίζουμε την καθυστέρηση μεταφοράς ως εξής:

Η καθυστέρηση μεταφοράς του δικτύου είναι το χρονικό διάστημα μεταξύ της αποστολής του πρώτου bit ενός κομματιού πληροφορίας και της λήψης του από το άλλο άκρο της επικοινωνίας.

Κανένα δίκτυο δεν μπορεί να αποφύγει την καθυστέρηση μεταφοράς λόγω της καθυστέρησης μετάδοσης του σήματος στο φυσικό μέσο. Υπάρχουν και περιπτώσεις δικτύου που αυτή η καθυστέρηση οφείλεται και σε άλλους παράγοντες όπως η δρομολόγηση και η αναγέννηση.



Εικόνα 2.10. : Καθυστερήσεις κατά τη μετάδοση της πληροφορίας σε ένα δίκτυο

Η καθυστέρηση μεταφοράς αποτελεί ένα χαρακτηριστικό του δικτύου. Για τις περισσότερες εφαρμογές υπάρχει μια πιο σημαντική παράμετρος: η καθυστέρηση από άκρο σε άκρο, η οποία έχει τρεις συνιστώσες:

- Το χρόνο που απαιτείται για να ελευθερωθεί το μέσο, ώστε να επιτραπεί η αποστολή των δεδομένων από το δίκτυο. Αυτή η καθυστέρηση ονομάζεται καθυστέρηση πρόσβασης (access delay)
- Το χρόνο διάδοσης των δεδομένων πάνω στο φυσικό μέσο.
- Την καθυστέρηση μεταφοράς που ορίσαμε πριν.

Για τις interactive εφαρμογές ιδιαίτερη σημασία έχει και ο χρόνος απάντησης από τον λήπτη (round trip delay). Ο χρόνος αυτός δεν εξαρτάται πλήρως από το δίκτυο αλλά και από την ταχύτητα με την οποία απαντά ο λήπτης.

3. Μεταβλητότητα της Καθυστέρησης (Delay Variation)

Κανένα δίκτυο δεν μπορεί να εγγυηθεί σταθερή καθυστέρηση μεταφοράς ή από άκρο σε άκρο. Υπάρχουν δίκτυα με ελάχιστες καθυστερήσεις της τάξης του nanosecond στα οποία η μεταβλητότητα δεν παίζει καθοριστικό ρόλο. Όταν όμως αυξάνει η καθυστέρηση και η μεταβλητότητα είναι μεγάλη, όπως στα δίκτυα IP (Internet Protocol), τότε η παράμετρος αυτή είναι σημαντική. Η μεταβλητότητα μετράται με διάφορες στατιστικές μεθόδους.

Στη τεχνολογία μετάδοσης σημάτων ορίζεται η έννοια του jitter, ως η μεταβλητότητα της καθυστέρησης μετάδοσης που οφείλεται αποκλειστικά στις συσκευές μετάδοσης. Στα δίκτυα το jitter που οφείλεται στις ατέλειες των συσκευών μετάδοσης είναι αναπόφευκτο, αλλά συνήθως μικρό. Σε κυκλώματα μεγάλων αποστάσεων μπορεί να φτάσει την τάξη των microsecond, ενώ συνήθως κυμαίνεται στην τάξη των nanosecond.

Εκτός από το jitter του υλικού, υπάρχει και μεταβλητότητα που οφείλεται στην αρχιτεκτονική του δικτύου. Για παράδειγμα, σε τοπικά δίκτυα αρτηρίας η μεταβλητότητα του χρόνου πρόσβασης ή σε δίκτυα IP της δρομολόγησης, προστίθενται σε αυτή του jitter.

4. Ισοχρονισμός (Isochronism)

Αυτό το χαρακτηριστικό έχει ιδιαίτερη σημασία, όσον αφορά στην καταλληλότητα ενός δικτύου για εφαρμογές πολυμέσων. Δεν αποτελεί εγγενές χαρακτηριστικό του δικτύου, αλλά έναν συνδυασμό ορισμένων βασικών χαρακτηριστικών.

Μια από άκρο σε άκρο επικοινωνία ονομάζεται ισόχρονη, εάν το bit rate της σύνδεσης είναι εξασφαλισμένο και αν η μεταβλητότητα της καθυστέρησης είναι επίσης εξασφαλισμένη και μικρή.

Αυτή η απαίτηση επιτρέπει την μετάδοση συνεχών ροών πληροφορίας, όπως για παράδειγμα video και ήχου πραγματικού χρόνου. Τέτοιου είδους μεταδόσεις απαιτούν ένα σταθερό ρυθμό μεταφοράς δεδομένων, ώστε η πληροφορία να διατηρεί τη χρονική της εξάρτηση στο άλλο άκρο αναλλοίωτη. Επίσης, σταθερή μεταβλητότητα, που βρίσκεται σε καθορισμένα όρια, μπορεί να αντιμετωπιστεί ή να περάσει απαρατήρητη.

5. Mutlticasting

Ο ορισμός του multicasting είναι ο εξής:

Multicasting είναι η ιδιότητα ενός δικτύου να αντιγράφει, σε καθορισμένα σημεία του δικτύου, τα δεδομένα που εκπέμπει μια πηγή. Τα δεδομένα που αντιγράφονται προωθούνται στα συστήματα-παραλήπτες που αποτελούν μέλη ενός multicast group, με τέτοιο τρόπο ώστε να ελαχιστοποιηθούν τα τμήματα του δικτύου, στα οποία περνούν πολλά αντίγραφα της ίδιας πληροφορίας.

Η αντιγραφή μπορεί να γίνεται σε επίπεδο μεμονωμένων bits, μπλοκ πληροφορίας όπως τα πακέτα ή και σε επίπεδο αντικειμένων όπως έγγραφα, ηλεκτρονικά μηνύματα κ.λ.π.

6. Ρυθμοί Λαθών (Error Rates)

Το πιο προφανές ζητούμενο από ένα δίκτυο είναι η σωστή μετάδοση της πληροφορίας. Τα είδη των λαθών μπορούν να προκύψουν κατά τη μετάδοση της πληροφορίας μέσα από ένα δίκτυο είναι:

- **Αλλοίωση των δεδομένων.**

  Συνήθως εμφανίζεται με τη μορφή αντεστραμμένων bits.

- **Χάσιμο δεδομένων.**

  Αυτό μπορεί να οφείλεται στην αλλοίωση των δεδομένων. Ορισμένα δίκτυα ανιχνεύουν τα λάθη και απορρίπτουν τα μπλοκ πληροφορίας που έχουν επηρεαστεί. Στην συνέχεια, είτε ενημερώνουν τον αποστολέα να επαναλάβει την αποστολή, είτε αφήνουν την εφαρμογή να αντιμετωπίσει την απώλεια. Σε σύγχρονα δίκτυα μεταγωγής με πακέτα, όπως τα IP, η απώλεια μπορεί να οφείλεται και στην υπερφόρτωση των κόμβων ή των γραμμών.

- **Data Duplication.**

  Ένα λάθος που συναντάται σπάνια, είναι η λήψη του ίδιου μπλοκ πληροφορίας περισσότερες από μια φορές.

- **Λήψη σε λάθος σειρά.**

Σε δίκτυα που μεταφέρουν την πληροφορία σε κάποιας μορφής πακέτα και προσφέρουν εναλλακτικούς δρόμους μετακίνησης των δεδομένων, είναι δυνατόν τα δεδομένα να φτάσουν στον προορισμό τους με λανθασμένη σειρά. Αυτό συμβαίνει συνήθως σε δίκτυα που εφαρμόζουν επικοινωνία χωρίς σύνδεση. [6]

ΚΕΦΑΛΑΙΟ 3 :

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ
(WIRELESS NETWORKS)

3.1. ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Από την επιτυχία του Ethernet στις αρχές της δεκαετίας του '70 και άλλων παρόμοιων ψηφιακών πρωτοκόλλων, η βασική τεχνολογία για τα δίκτυα τοπικής περιοχής (LANs) ήταν έτοιμη να εφαρμοστεί τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Τα Standard LAN πρωτόκολλα , όπως το Ethernet, που λειτουργούν σε υψηλές ταχύτητες με φτηνό υλισμικό σύνδεσης (απλώς την εξασφάλιση ενός modem ή μιας κάρτας δικτύου) μπορούν να φέρουν την ψηφιακή δικτύωση σχεδόν σε οποιοδήποτε υπολογιστή. Σήμερα, οργανισμοί κάθε μεγέθους έχουν πρόσβαση και μοιράζονται τις πληροφορίες μέσω ψηφιακών δικτύων. ***Όμως μέχρι πρόσφατα, τα LANs περιορίζονταν στη φυσική, συνδεμένη με καλώδιο (wired infrastructure), υποδομή του κτηρίου.*** **Πολλοί χρήστες δικτύων, ειδικά κινητοί χρήστες σε επιχειρήσεις, στον ιατρικό κλάδο, σε εργοστάσια, και πανεπιστήμια, είναι μερικοί, από τους επαγγελματίες και όχι μόνο, που έχουν όφελος από τις προστιθέμενες ικανότητες των ασύρματων LANs.** *Πλέον οι συνθήκες ήταν ώριμες ώστε στις αρχές της δεκαετίας του '90 να αρχίσουν οι πρώτες προσπάθειες προτυποποίησης των ασύρματων δικτύων.* **[3]**

Ένας πολύ απλός και εύκολα κατανοητός ορισμός για τα ασύρματα δίκτυα (wireless networks) είναι **δίκτυα στα οποία η πληροφορία δε μεταφέρεται μέσω καλώδιων, επιτρέπωντας έτσι ευελιξία στο χρήστη για ανταλλαγή δεδομένων.** Αν θέλουμε όμως να είμαστε λίγο πιο ακριβής θα λέγαμε ότι **είναι ο τύπος δικτύου όπου χρησιμοποιούνται υπέρυθρα, υπεριώδη ή ραδιο κύματα για να συνδέσουν τα υπολογιστικά συστήματα στο δίκτυο.**

Ένα ασύρματο τοπικό δίκτυο (Wireless Local Area Network ή WLAN) αποτελεί ένα επικοινωνιακό σύστημα που δεν αποσκοπεί στην αντικατάσταση του κοινού ενσύρματου δικτύου (Ethernet). Αντιθέτως, λειτουργεί συμπληρωματικά ή εναλλακτικά, καθώς επιτρέπει την επέκταση της γεωγραφικής κάλυψης του προϋπάρχοντος δικτύου. Τα WLANs είναι κατάλληλα για τη σύνδεση χρηστών μέσα σε ένα κτήριο ή με άλλα γειτονικά χωρίς να απαιτούνται καλώδια.

Όμως γιατί στραφήκαμε στα ασύρματα δίκτυα; Τι παραπάνω μας προσφέρουν σε σχέση με τα ενσύρματα;

Παρακάτω παρουσιάζονται δέκα καλοί λόγοι για να χρησιμοποιήσουμε ασύρματα δίκτυα :

I. Τα ασύρματα δίκτυα είναι μια απλή γρήγορη και ευέλικτη πρόταση που έχει όλα τα πλεονεκτήματα της ενσύρματης δικτύωσης και προσφέρεται σε χαμηλό κόστος χωρίς να σε περιορίζει σε μια σταθερή και αμετάβλητη εγκατάσταση.

II. Τα ασύρματα δίκτυα δίνουν λύση εκεί που η τοποθέτηση καλωδίων είναι ανεπιθύμητη ή ακόμα πολύ δύσκολο να πραγματοποιηθεί. Πιθανόν αυτό να συμβαίνει σε κάποιο περιορισμένο χώρο γραφείου, ή ακόμα εκεί όπου κάποιο φυσικό όριο δεν επιτρέπει την τοποθέτηση καλωδίων.

III. Για ομάδες εργαζομένων οι οποίοι χρειάζονται να επικοινωνούν και να συνεργάζονται από διαφορετικό τόπο σε διαφορετική χρονική στιγμή τα ασύρματα δίκτυα αποτελούν μια πολύτιμη λύση.

IV. Μπορούμε σίγουρα να φανταστούμε πόσο χρόνο θα κέρδιζε κάποιος αν ακόμα και στην καφετέρια είχε την δυνατότητα να διαβάσει το ηλεκτρονικό του ταχυδρομείο.

V. Τα ασύρματα δίκτυα είναι επιπλέον δίκτυα πολύ εύκολο να επεκταθούν και να εξυπηρετήσουν περισσότερο κόσμο.

VI. Εκτός από τη επεκτασιμότητα ένα ασύρματο δίκτυο είναι πολύ εύκολο να αλλάξει την τοποθεσία που βρίσκεται (relocate).

VII. Επίσης ένα ασύρματο δίκτυο είναι πολύ εύκολο να συνδεθεί σε κάποιο άλλο (πιθανόν ενσύρματο) δίκτυο για κάποια επείγουσα εργασία.

VIII. Όταν το δίκτυο σου δεν έχει καλώδιο είναι εύκολο να μεταφέρεις τον υπολογιστή σου να καταγράφεις δεδομένα και να τα στέλνεις αμέσως προς επεξεργασία.

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

X. Τέλος τα ασύρματα δίκτυα σου δίνουν τη δυνατότητα να υλοποιείς εύκολα οποιαδήποτε κινητή υπηρεσία (mobile service). **[2] [8]**

<u>Που δεν χρειάζονται τα ασύρματα δίκτυα :</u>

I. Όταν ο χρήστης έχει κατευθείαν εύκολη πρόσβαση στο ενσύρματο δίκτυο, για παράδειγμα η σύνδεση ενός δύο υπολογιστών που βρίσκονται δίπλα δίπλα σε ένα γραφείο με ένα απλό ethernet καλώδιο.

II. Στις περιπτώσεις όπου ο χρήστης - εφαρμογή απαιτεί αρκετά μεγάλο ρυθμό μετάδοσης, όπου δεν μπορεί να καλυφθεί από το ασύρματο δίκτυο. Έτσι για παράδειγμα εάν θέλουμε μία διασύνδεση με ρυθμό 1Gbps, μπορούμε να την υλοποιήσουμε με πολύ χαμηλό κόστος με συσκευές που να υποστηρίζουν Gigabit Ethernet και την κατάλληλη καλωδίωση. Η ασύρματη τεχνολογία δεν προβλέπεται να φτάσει ποτέ αυτές τις ταχύτητες. Επιπλέον ήδη έχουν κυκλοφορήσει λύσεις ενσύρματης δικτύωσης που φτάνουν στα 10Gbps αν και δεν είναι κοινή ακόμα η χρήση τους.

III. Σε δίκτυα που απαιτούν μεγάλο βαθμό ασφαλείας, οι ενσύρματες λύσεις είναι σαφώς καλύτερες. Σε ένα καλώδιο το οποίο είναι προστατευμένο κάτω από ψευδοπατώματα, δεν είναι δυνατή η φυσική πρόσβαση στο καλώδιο προκειμένου να γίνει υποκλοπή. Αντίθετα, στην περίπτωση ασύρματης υλοποίησης, επειδή δεν είναι δυνατό να περιορίσουμε τα ραδιοκύματα, είναι εύκολο να γίνει ανίχνευση της μεταδιδόμενης πληροφορίας. Σε περίπτωση δε, που η πληροφορία δεν είναι κωδικοποιημένη μπορεί να γίνει ανάκτηση της. Για να φτάσουν σε παρόμοιο βαθμό ασφαλείας τα ασύρματα δίκτυα, πρέπει να εφαρμοστούν σε αυτά περίπλοκες τεχνικές αυθεντικοποίησης και κωδικοποίησης και μάλιστα σε επίπεδο εφαρμογής. Άλλωστε αυτός είναι και ένας από τους λόγους που δεν χρησιμοποιούνται σε κρίσιμες στρατιωτικές εφαρμογές οι συμβατικές ασύρματες τεχνολογίες (για παράδειγμα επικοινωνία συσκευών, εφαρμογών, προσωπικού, σε ένα πολεμικό πλοίο ή εντός μιας στρατιωτικής βάσης).

IV. Σε περιοχές που έχουν μεγάλο ηλεκτρομαγνητικό θόρυβο, γεγονός που έχει ως αποτέλεσμα προβληματικές και μη αξιόπιστες συνδέσεις. **[9]**

3.2. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Από τα αρχαία χρόνια οι άνθρωποι έβρισκαν τρόπους να επικοινωνούν από απόσταση. Ξεκινώντας από τους αγγελιοφόρους, δρομείς δηλαδή, που έκαναν τη μεταφορά προφορικών και γραπτών μηνυμάτων, περνώντας στις φρυκτωρίες που ήταν ένα σύστημα μεταβίβασης φωτεινών σημάτων με διαδοχικό άναμμα φωτιάς στις κορυφές βουνών και που χρησιμοποιήθηκαν για στρατιωτικούς κυρίως σκοπούς από την εποχή του τρωικού πόλεμου έως τους βυζαντινούς χρόνους από τους έλληνες, και στις πυρσίες που ήταν ο πρώτος οπτικός τηλέγραφος που αναφέρεται στην ιστορία, μέχρι τα ταχυδρομικά περιστέρια και τα τύμπανα των αφρικανικών φυλών και τα σήματα καπνού των ινδιάνων, φτάσαμε τελικά στο πρώτο πραγματικά ασύρματο τρόπο επικοινωνίας σύμφωνα με τον ορισμό που χρησιμοποιούμε και σήμερα.

Η έννοια του ασύρματου δικτύου και ποιο συγκεκριμμένα της ασύρματης επικοινωνίας δεν είναι νέα ιδέα. **Ήδη από το 1901 ο Ιταλός φυσικός Γουλιέλμος Μαρκόνι επέδειξε στο κοινό έναν ασύρματο τηλέγραφο ανάμεσα στα πλοία και στη ξηρά. Ως κώδικα ο Μαρκόνι χρησιμοποίησε το κώδικα μορς (οι τελείες και οι παύλες είναι άλλωστε δυαδικό σύστημα).** Συχνά δε τον ασυρματιστή του πλοίου τον αποκαλούσαν μαρκόνι. Τα σύγχρονα ψηφιακά ασύρματα έχουν βέβαια πολύ καλύτερη απόδοση, αλλά η βασική ιδέα είναι η ίδια.

Συνεχίζοντας την αναδρομή μετά τον Marconi, τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) τεχνολογίας TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν γύρω στο 1964, ενώ ο όρος Packet" προτάθηκε από τον D. W. Davies του National Physical Laboratory της Μεγ. Βρετανίας. Οι έρευνες του εργαστηρίου αυτού οδήγησαν στο σημερινό διεθνές δημόσιο δίκτυο μεταγωγής πακέτων X.25, ενώ το ίδιο έτος ο οργανισμός ARPA (Advanced Research Projects Agency) των Η.Π.Α. άρχισε να χρηματοδοτεί τα προγράμματα που οδήγησαν στη δημιουργία του ARPAnet (πυρήνα του σημερινού Internet) το 1969.

Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Εδώ αξίζει να αναφέρουμε ότι το πρώτο ολοκληρωμένο ασύρματο LAN κατασκευάστηκε στο πανεπιστήμιο της Χαβάης στα πλαίσια ενός project που λέγονταν *ALOHANET*.

Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).

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

Τα τελευταία χρόνια γίνονται σταθερά βήματα προόδου για την βελτίωση της ποιότητας των ασυρμάτων δικτύων με όλο και αυξανόμενες ταχύτητες και νέα πρότυπα από οργανισμούς και συμμαχίες γνωστών εταιρειών. Χαρακτηριστικά είναι τα παραδείγματα του Bluetooth, GPRS (General Packet Radio Service), ενώ σε εξέλιξη βρίσκονται και άλλα δύο πρότυπα. Το ένα αναπτύσσεται στην Ευρώπη από το ETSI (European Telecommunications Standard Institute) και ονομάζεται HIPERLAN (High – Performance European Radio LAN). Το άλλο αναπτύσσεται από την IEEE (Institute of Electrical and Electronics Engineers) και ονομάζεται 802.11 WLAN. Και τα δύο αυτά πρότυπα καλύπτουν τις προδιαγραφές για το φυσικό στρώμα και το υπόστρωμα MAC (Medium Access Control). **[2] [10]**

3.3. ΤΟΠΟΛΟΓΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

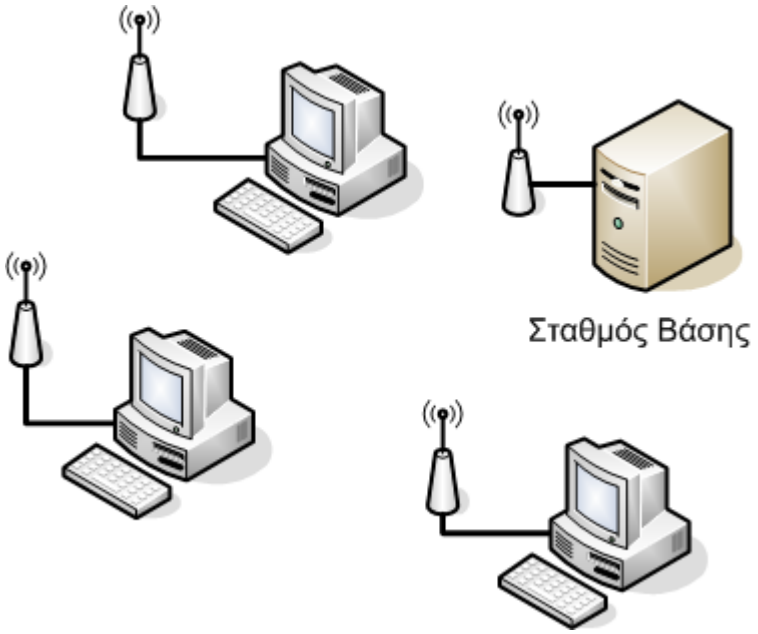
Οι τοπολογίες ασύρματων τοπικών δικτύων διαχωρίζονται ανάλογα με το αν χρησιμοποιούν *συνδέσεις σημείου προς σημείο* ή *συνδέσεις εκπομπής*.

Θα εξετάσουμε πρώτα τις τρεις περιπτώσεις ασύρματων δικτύων με συνδέσεις εκπομπής:

3.3.1. <u>Σύνδεση εκπομπής – 1ος Τρόπος</u> :

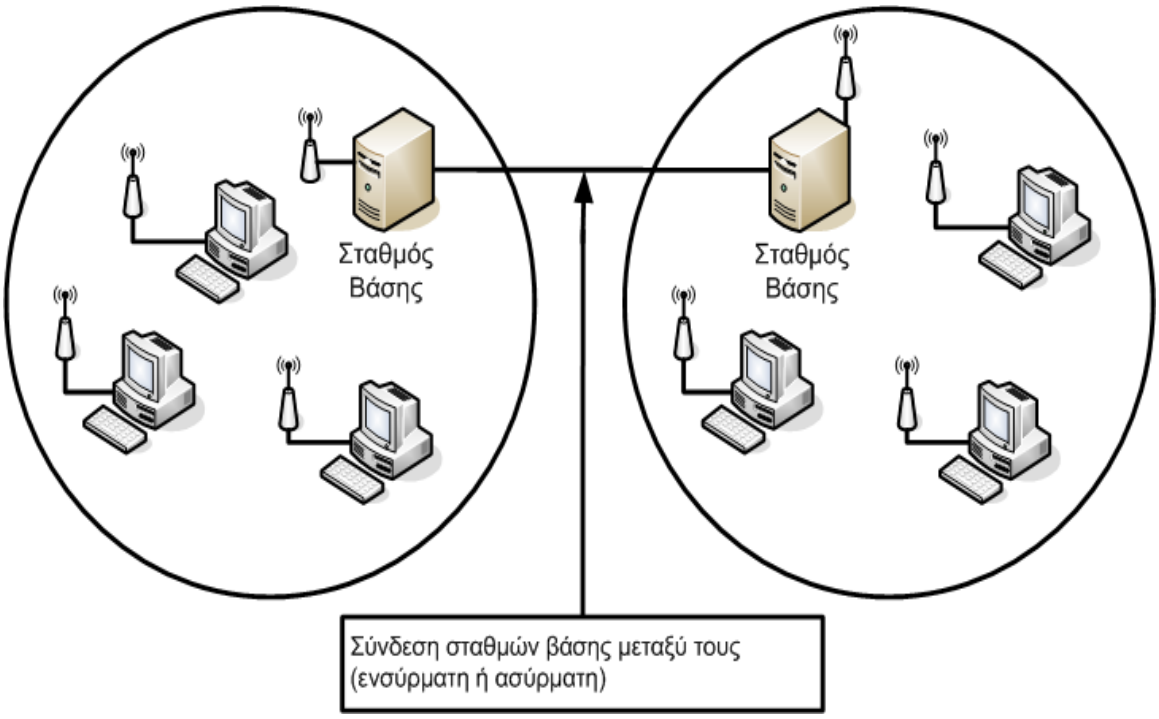
Στην πρώτη περίπτωση (*<u>εικόνα 3.1.</u>*), χρησιμοποιούνται ραδιοκύματα σχετικά χαμηλής συχνότητας (που μπορούν να διαπεράσουν αδιαφανή αντικείμενα). Όλοι οι κόμβοι συνδέονται με ένα κεντρικό κόμβο επικοινωνίας ο οποίος ονομάζεται *σταθμός βάσης*. Οι κόμβοι τυπικά είναι κατανεμημένοι σε μια

σχετικά μικρή περιοχή γύρω από το σταθμό βάσης, μπορεί όμως να είναι πολλοί σε αριθμό. Αν και αυτός ο τρόπος είναι ο πιο παλιός, χρησιμοποιείται ακόμα και σήμερα και μάλιστα όχι μόνο σε συνδέσεις υπολογιστών. Σύγχρονες παραλλαγές του χρησιμοποιούνται σήμερα για παράδειγμα στην κινητή τηλεφωνία.



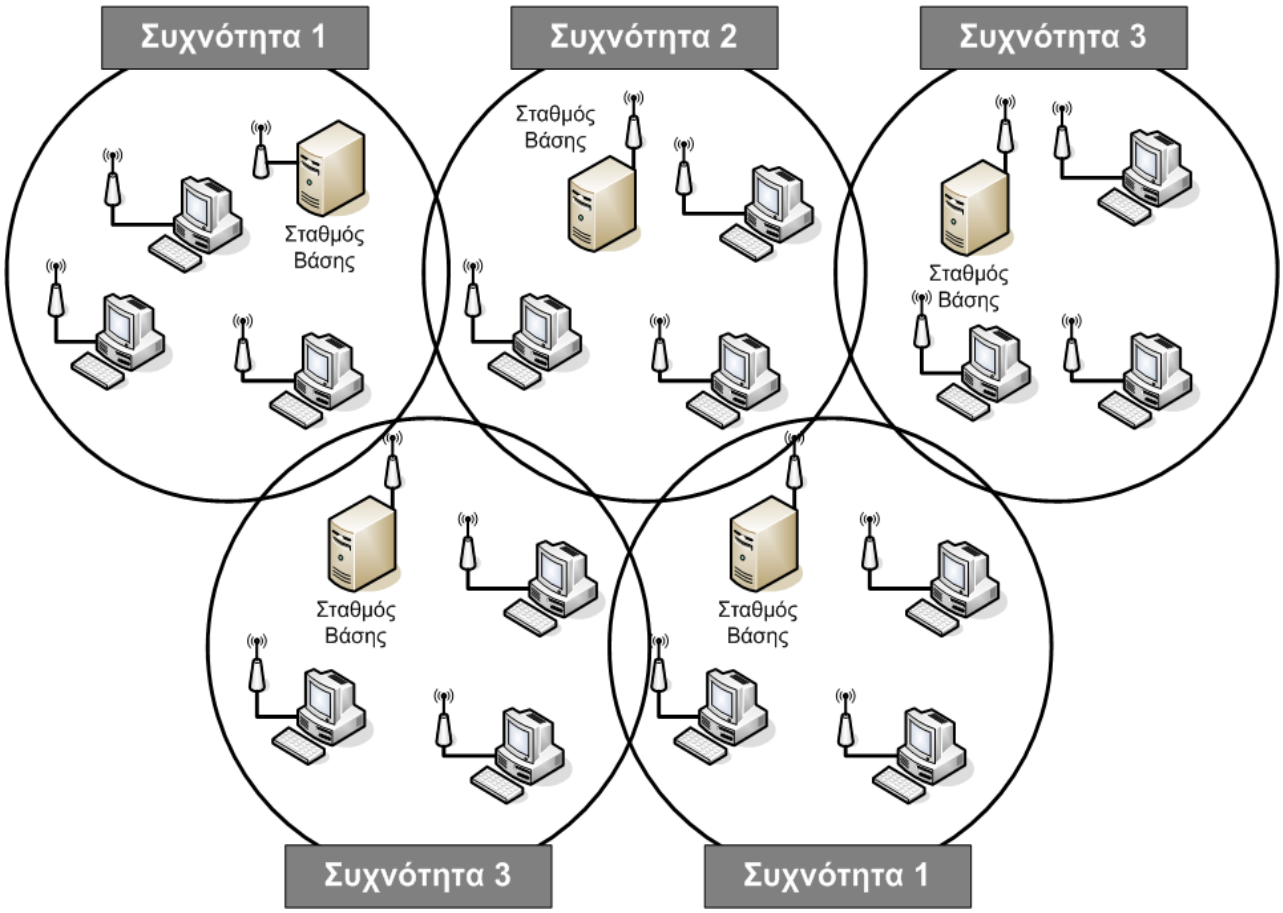
Εικόνα 3.1. : Σύνδεση εκπομπής – 1ος Τρόπος

Για να μοιραστεί η διαθέσιμη χωρητικότητα του δικτύου σε πολλούς χρήστες, ομάδες χρηστών ομαδοποιούνται σε *κυψέλες*. Κάθε κυψέλη έχει το δικό της σταθμό βάσης που εξυπηρετεί ένα αριθμό από χρήστες – αυτούς που βρίσκονται στην περιοχή εμβέλειας της. Η βάση της κάθε κυψέλης συνδέεται με τις βάσεις των υπόλοιπων τυπικά μέσω ενσύρματου δικτύου. Η διασύνδεση αυτή εξασφαλίζει την μετάδοση των δεδομένων από τους κόμβους μιας κυψέλης σε κόμβους μιας άλλης, και επίσης χρησιμοποιείται για τον συντονισμό των μεταδόσεων των κόμβων. (*εικόνα 3.2.*)



Εικόνα 3.2. : Κυψέλες

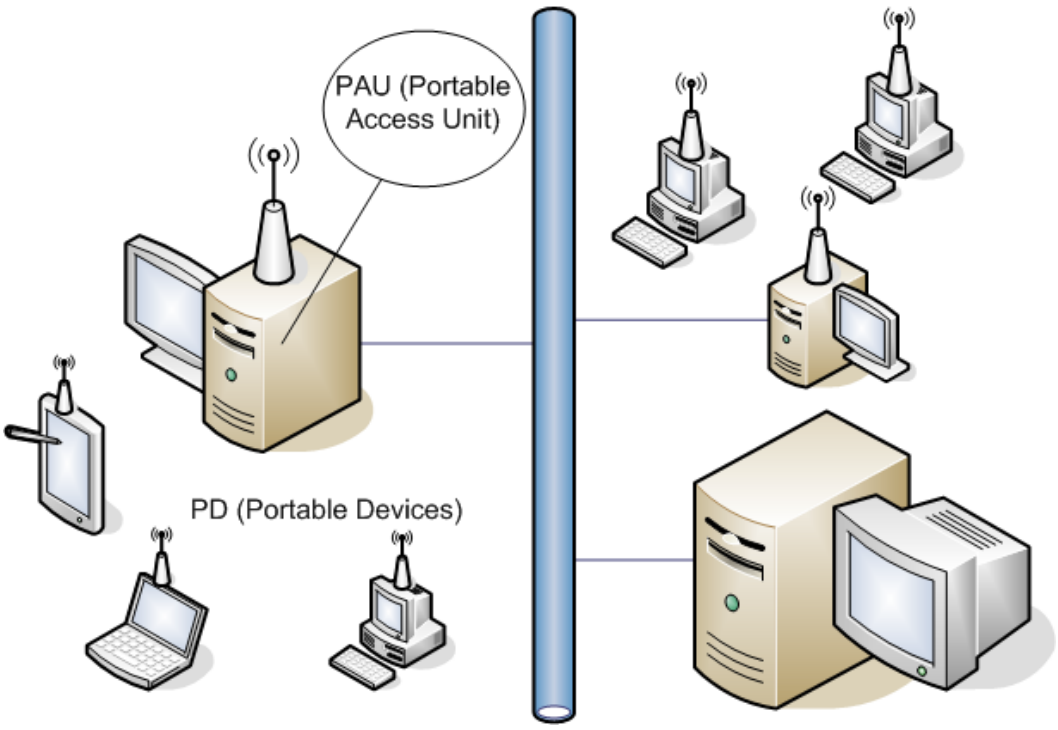
Κάθε κόμβος της κυψέλης εκπέμπει με σχετικά χαμηλά επίπεδα ισχύος (μη ξεχνάμε ότι οι κόμβοι βρίσκονται σε σχετικά μικρές αποστάσεις από το σταθμό βάσης). Έτσι αποφεύγονται οι παρεμβολές με άλλες κυψέλες. Λόγω επίσης της μικρής ισχύος εκπομπής, είναι δυνατόν να χρησιμοποιήσουμε ξανά την ίδια συχνότητα σε μια άλλη κυψέλη η οποία βρίσκεται μακρύτερα (όχι γειτονική). Η *επαναχρησιμοποίηση συχνοτήτων* (*βλέπε εικόνα 3.3.*) μας εξυπηρετεί γιατί διαφορετικά θα έπρεπε να σχεδιάσουμε ένα σύστημα το οποίο να χρησιμοποιεί εκατοντάδες διαφορετικές συχνότητες κάτι το οποίο είναι ασύμφορο οικονομικά (αλλά επίσης σύντομα θα μέναμε και χωρίς διαθέσιμες συχνότητες).



Εικόνα 3.3. : Επαναχρησιμοποίηση συχνοτήτων

3.3.2. Σύνδεση εκπομπής – 2ος τρόπος :

Στον δεύτερο τρόπο σύνδεσης με διάταξη εκπομπής χρησιμοποιούνται μικροκύματα ή υπέρυθρες ακτίνες και χρησιμοποιείται κυρίως σε μεγάλες εγκαταστάσεις όπως συνεδριακά κέντρα κλπ. Οι κατανεμημένες τερματικές διατάξεις (μπορεί να είναι φορητοί υπολογιστές) γνωστές σαν Portable Devices (PD) των χρηστών συνδέονται μέσω ασύρματων ζεύξεων με μια ενδιάμεση μονάδα πρόσβασης (PAU, Portable Access Unit).(*εικόνα 3.4.*)



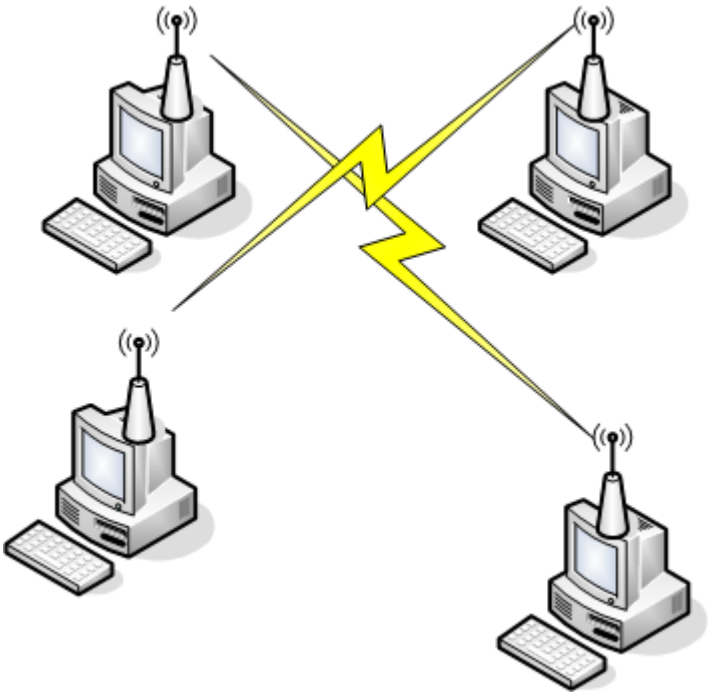
Εικόνα 3.4. : Σύνδεση εκπομπής – 2ος Τρόπος

Η ενδιάμεση μονάδα πρόσβασης έχει το ρόλο της βάσης. Αυτή συνδέεται με τη σειρά της σε ένα ενσύρματο δίκτυο στο οποίο μπορεί να είναι συνδεδεμένες και άλλες μονάδες πρόσβασης, κεντρικός υπολογιστής εξυπηρέτησης (server), το διαδίκτυο κλπ.

Η μέγιστη απόσταση που μπορεί να απέχει μια τερματική διάταξη από την μονάδα πρόσβασης κυμαίνεται από 50 ως 400 μέτρα και εξαρτάται από την ισχύ με την οποία εκπέμπει η βάση και η τερματική μονάδα.

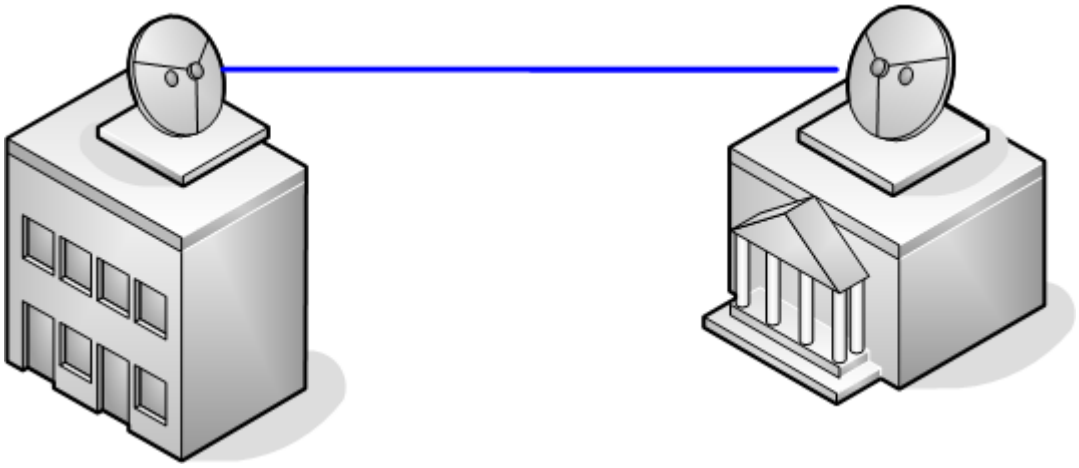
3.3.3. Σύνδεση Εκπομπής – 3ος τρόπος :

Στην τρίτη περίπτωση σύνδεσης εκπομπής, έχουμε άμεση σύνδεση κάποιων τερματικών που βρίσκονται εγκατεστημένες σε μικρούς χώρους (όπως χώροι συνεδρίων, εκθέσεων κλπ). Στις περιπτώσεις αυτές δεν υπάρχει σταθμός βάσης αλλά οι κόμβοι συνδέονται μεταξύ τους άμεσα. (*εικόνα 3.5.*)



Εικόνα 3.5. : Σύνδεση Εκπομπής – 3ος τρόπος

3.3.4. Σύνδεση Σημείο προς Σημείο :



Εικόνα 3.6. : Σύνδεση σημείο προς σημείο

Αν χρησιμοποιούμε συνδέσεις σημείου προς σημείο, τότε η επικοινωνία πραγματοποιείται (*εικόνα 3.6.*):

- Είτε μεταξύ δύο σταθερών σημείων.
- Είτε ενός σταθερού και ενός που βρίσκεται σε κίνηση.
- Είτε δύο σημείων που βρίσκονται σε κίνηση.

Σε επικοινωνίες μεγάλων αποστάσεων (και ειδικά σε σταθερά σημεία) προτιμώνται ιδιαίτερα τα μικροκύματα τα οποία όπως έχουμε ήδη πει διαδίδονται πρακτικά ευθύγραμμα και μπορούν να καλύψουν μεγάλες αποστάσεις (αλλά χρειάζεται οι κεραίες να έχουν οπτική επαφή). Παρόμοια αποτελέσματα μπορούμε να επιτύχουμε και με χρήση οπτικών επικοινωνιών π.χ. με χρήση LASER. Μικροκύματα επίσης μπορούν να χρησιμοποιηθούν και σε ορισμένες ασύρματες εφαρμογές μικρής εμβέλειας (συστήματα ασφαλείας, ενεργοποίησης ηλεκτρονικών συσκευών κλπ). [1]

3.4. Η ΠΡΩΤΗ ΠΕΡΙΟΔΟΣ ΑΝΑΠΤΥΞΗΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Ενώ η IEEE έχει συστήσει την επιτροπή 802.11 Wireless Local Area Networks Standards Working Group το 1990 ήταν μέχρι το 1997 όταν η IEEE έδωσε σε δημοσιότητα το πρότυπο 802.11 για τους κατασκευαστές WLAN συσκευών που λειτουργούσαν κάνοντας χρήση του φάσματος των 2.4 GHz, έτσι δημιουργήθηκε το πρώτο πρότυπο για την βιομηχανία των WLANs. Το πρότυπο δεν περιλάμβανε πληροφορίες για την τεχνολογία ή για συγκεκριμένες εφαρμογές μόνο για το φυσικό και το MAC επίπεδο. Τα πρώτα WLANs έτρεχαν σε ταχύτητες της τάξεως 1 και 2 Mbps (megabits per second), μια ταχύτητα που ήταν χρήσιμη για κάποιες εφαρμογές αλλά ήταν πολύ πιο αργή από το ενσύρματο αντίπαλο του, το Ethernet, που έτρεχε με ταχύτητες 10πλάσιες ή ακόμα και 50πλάσιες (10 και 100 Mbps). Δύο χρόνια αργότερα (1999), το αναθεωρημένο πρότυπο 802.11b αύξησε την ταχύτητα των ασύρματων δικτύων σε 11Mbps και κατέστησε τα ασύρματα δίκτυα ανταγωνιστικά έναντι των αντίστοιχων ενσύρματων.

Εκείνη η χρόνια αποτέλεσε ορόσημο για αυτό που χαρακτηρίζουμε ρυθμιστικό καθεστώς των ασύρματων δικτύων καθώς έγινε αντιληπτό από πολλούς βιομηχανικούς παίκτες ότι η τεχνολογία ήταν αρκετά ώριμη και γρήγορη ώστε να διεκδικήσει μερίδιο της αγοράς δικτύων και τηλεπικοινωνιών.

Έτσι, το 1999 συνίσταται η επιτροπή Wireless Ethernet Compatibility Alliance (τώρα πλέον γνωστή ως (Wi-Fi Alliance http://www.wi-fi.org/) που ως πρωταρχικό στόχο της είχε να διασφαλίσει την ταχύτατη υιοθέτηση από πλευράς αγοραστικού ενδιαφέροντος των προϊόντων της σειράς 802.11b. Μέσω της δράσης του συγκεκριμένου οργανισμού δημιουργήθηκε, και πλέον έχει υιοθετηθεί από όλη την επιστημονική κοινότητα στο χώρο των δικτύων και των τηλεπικοινωνιών, το λογότυπο Wi-Fi (Wireless Fidelity), το οποίο στα ελληνικά αποδίδεται «ασύρματη πιστότητα», προκείμενου να συνοδεύει τα προϊόντα και να αποτελεί ένδειξη ότι αυτά είναι εγκεκριμένα και συμβατά μεταξύ τους.

Το συγκεκριμένο εγκεκριμένο λογότυπο έδωσε ώθηση στην υιοθέτηση και εφαρμογή των προϊόντων της οικογένειας 802.11b και αποτέλεσε εφαλτήριο ώστε να εξελιχθεί η ασύρματη τεχνολογία δικτύων σε μια εκρηκτική τεχνολογία που διείσδυσε τόσο στα οικιακά όσο και στα επιχειρηματικά δίκτυα. Το 2002, η επιτροπή αδειών της ασύρματης πιστότητας (Wi-Fi Alliance) άρχισε την πιστοποίηση των προϊόντων μιας ακόμα αναθεωρημένης έκδοσης της οικογένειας 802.11 και συγκεκριμένα της 802.11a. Η μόνη τροχοπέδη στην επικράτηση των ασύρματων δικτύων στην αγορά ήταν πλέον η ασφάλεια, καθώς οι υποκλοπές θα ήταν πολύ εύκολες στην μη αδειοδοτημένη μπάντα και έχοντας ως μέσο μεταφοράς τον αέρα.

Οι ολοένα αυξανόμενες ανάγκες για ασφάλεια που εντάθηκαν μετά και τα τραγικά γεγονότα του 2001 στην Νέα Υόρκη κατέστησαν την ασφαλή διακίνηση δεδομένων μέσω δικτύων επιτακτική. Κινούμενη προς αυτή την κατεύθυνση, η επιτροπή (Wi-Fi Alliance) ρύθμισε το 802.11 ως ένα πρότυπο που θα έχει μηχανισμούς κρυπτογράφησης ώστε να διασφαλίζεται η ασφάλεια μετάδοσης των δεδομένων ακόμα και μέσω ασύρματων ζεύξεων. Ο μηχανισμός κρυπτογράφησης ονομάστηκε Wired Equivalent Privacy (WEP), και έχει την πρόθεση να καταστήσει ένα ασύρματο δίκτυο εξίσου ασφαλές με ένα «όχι και τόσο ασφαλές» ενσύρματο δίκτυο. Αρχικά η ομάδα εργασίας για το WEP είχε μια δυσάρεστη έκπληξη να αντιμετωπίσει, καθώς προσέκρουσε στην νομοθεσία των Η.Π.Α για εξαγωγές στο χώρο της κρυπτογράφησης, εδώ όμως και λίγο διάστημα η Αμερικανική κυβέρνηση έχει άρει αυτούς τους νομοθετικούς περιορισμούς, καθιστώντας τα ασύρματα LANs ένα αναπόσπαστο κομμάτι των καθημερινών δραστηριοτήτων πολλών οργανισμών, επιχειρήσεων αλλά και ιδιωτών.

Το σημαντικότερα κίνητρο και όφελος από τα ασύρματα LANs είναι η αυξανόμενη κινητικότητα. Χωρίς να περιορίζονται από τις συμβατικές συνδέσεις δικτύων, οι χρήστες κινητών δικτύων μπορούν να έχουν πρόσβαση σε LANs σχεδόν από οπουδήποτε. Οι κατάλογοι αποθηκών εμπορευμάτων μπορούν να ελεγχθούν γρήγορα και αποτελεσματικά με τους ασύρματους ανιχνευτές που συνδέονται με την κύρια βάση δεδομένων καταλόγων (RFID). Ακόμη και οι ασύρματες "έξυπνες" ετικέτες τιμών, εφοδιασμένες με οθόνες LCD, επιτρέπουν στους εμπόρους να προλάβουν τις αποκλίσεις μεταξύ της τιμολόγησης των αποθεμάτων και των τιμών στην checkout line και πολλές άλλες εφαρμογές.

Εκτός από την αυξανόμενη κινητικότητα, τα ασύρματα LANs αύξησαν πολύ και την ευελιξία. Κάποιος μπορεί να απεικονίσει χωρίς μεγάλη δυσκολία μια συνεδρίαση στην οποία οι υπάλληλοι χρησιμοποιούν απλούς υπολογιστές και ασύρματες συνδέσεις για να μοιραστούν και να συζητήσουν τα μελλοντικά τους σχέδια. Αυτό το ad-hoc δίκτυο μπορεί να σχεδιαστεί κατάλληλα και να σχηματιστεί σε πολύ σύντομο χρονικό διάστημα, είτε γύρω από τον πίνακα διασκέψεων ή / και σε όλο τον κόσμο. Οι χρηματιστές στη Wall Street είναι σε θέση να χρησιμοποιήσουν τα ασύρματα τερματικά για να κάνουν τις αγοροπωλησίες τους. Ακόμη και οι σπουδαστές έχουν πρόσβαση στις σημειώσεις διαλέξεων και στο υλικό των μαθημάτων περιπλανώμενοι στους εσωτερικούς και εξωτερικούς χώρους της πανεπιστημιούπολης. Μερικές φορές είναι πιο οικονομικό να χρησιμοποιηθεί το ασύρματο τοπικό LAN. Παραδείγματος χάριν, στα παλαιά κτίρια, το κόστος του καθαρισμού αμιάντων ή η αφαίρεσή του, αντισταθμίζει το κόστος για μια ασύρματη λύση τοπικού LAN. Σε άλλες καταστάσεις, όπως ένα πάτωμα εργοστασίου, μπορεί να μην είναι εφικτό να ''περαστεί'' το παραδοσιακό συνδεμένο με καλώδιο LAN. [3]

3.5. Το Πρότυπο 802.11

3.5.1. Εισαγωγή :

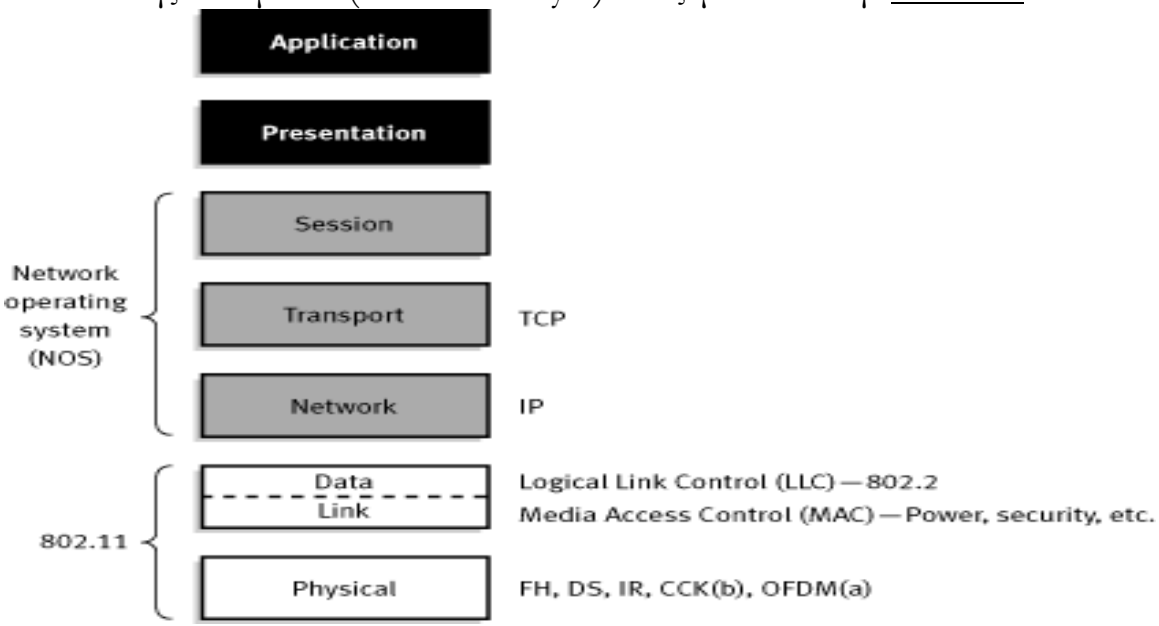
Ένα ασύρματο τοπικό δίκτυο είναι αυτό στο οποίο ένας κινούμενος χρήστης μπορεί να συνδεθεί σε ένα τοπικό δίκτυο μέσω μια ασύρματης σύνδεσης.

Το πρότυπο IEEE 802.11 περιγράφει τις τεχνολογίες που χρησιμοποιούνται στα ασύρματα τοπικά δίκτυα. Το 802.11 είναι το όνομα του project της ομάδας εργασίας του IEEE (Institute of Electrical and Electronics Engineers, Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών). **Δημιουργήθηκε τον Ιούνιο του 1997,** έχει ταχύτητα 2Mbps, αποτελεί το πρώτο πρότυπο για ασύρματη δικτύωση και ακολουθείται από τα περισσότερα ασύρματα δίκτυα μέχρι και σήμερα. Περιγράφονται τα δύο πρώτα επίπεδα του OSI, δηλαδή το φυσικό επίπεδο (PHY, Physical Layer) και το επίπεδο σύνδεσης δεδομένων (MAC, Medium Access Control). Τα πρωτόκολλα αυτά δημοσιεύονται από την IEEE γεγονός που είναι σημαντικό για την διαλειτουργικότητα των συσκευών που το ακολουθούν.

Περιγράφοντας μόνο τα δύο κατώτερα επίπεδα, επιτρέπει σε οποιαδήποτε εφαρμογή να εργάζεται πάνω σε συσκευή 802.11 όπως ακριβώς θα εργαζόταν πάνω από Ethernet. Δηλαδή τα πιο πάνω επίπεδα δεν γνωρίζουν και δεν απασχολούνται από το τι βρίσκεται πιο κάτω. **[2] [10]**

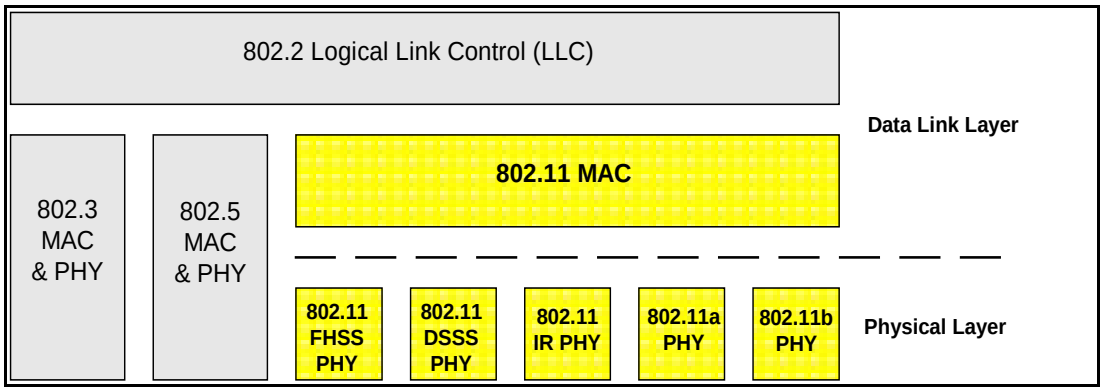
3.5.2. Διαστρωμάτωση :

Όπως όλα τα 802.x πρότυπα, έτσι και το 802.11 επικεντρώνεται στα δύο χαμηλότερα στρώματα του μοντέλου OSI (Open System Interconnection), δηλαδή στο φυσικό στρώμα (Physical Layer-PHY) και στο υπόστρωμα MAC (Medium Access Control-Ελέγχου προσπέλασης Μέσων) του στρώματος διασύνδεσης δεδομένων (Data Link Layer) όπως φαίνεται στην *εικόνα 3.7*.



Εικόνα 3.7. : Μοντέλο Αναφοράς OSI

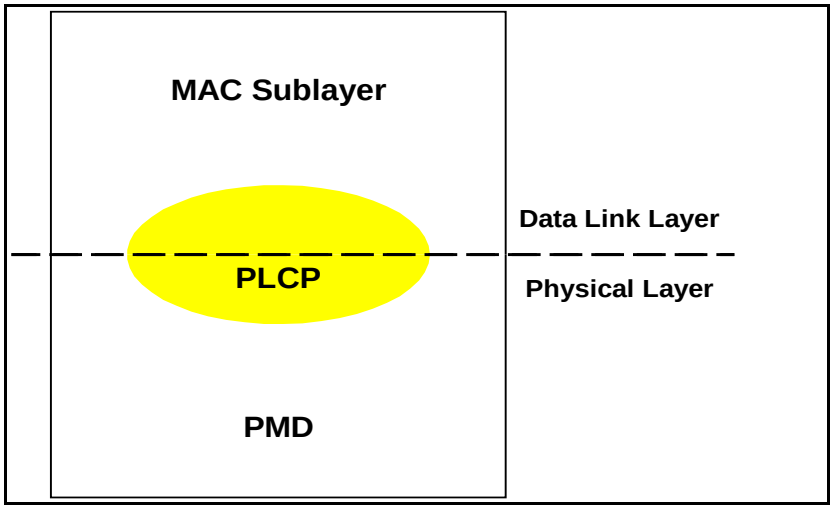
Το άλλο υπόστρωμα του στρώματος ζεύξης δεδομένων, δηλαδή το υπόστρωμα ελέγχου λογικής ζεύξης (Logical Link Control – LLC), είναι αυτό που έχει προτυποποιηθεί ως IEEE 802.2 και χρησιμοποιείται σε συνδυασμό με όλα τα διαφορετικά MAC της σειράς IEEE 802, όπως φαίνεται στην *εικόνα 3.8.*



Εικόνα 3.8. : Διαστρωμάτωση του Προτύπου 802.11

Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Κάθε φυσικό στρώμα χωρίζεται σε δύο υποστρώματα, όπως φαίνεται στην *εικόνα 3.9*.

Το υπόστρωμα PLCP (Physical Layer Convergence Procedure) χρησιμεύει στην προσαρμογή των διαφόρων φυσικών στρωμάτων στο κοινό MAC. Το υπόστρωμα PMD (Physical Medium Dependent) περιέχει όλες τις λειτουργίες που απαιτούνται για τη μετάδοση της πληροφορίας από το εκάστοτε φυσικό στρώμα.



Εικόνα 3.9. :Φυσικό στρώμα του προτύπου 802.11

3.5.3. Βασικές Μονάδες :

Τα ασύρματα δίκτυα 802.11 αποτελούνται από τις κάτωθι τέσσερις βασικές μονάδες :

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

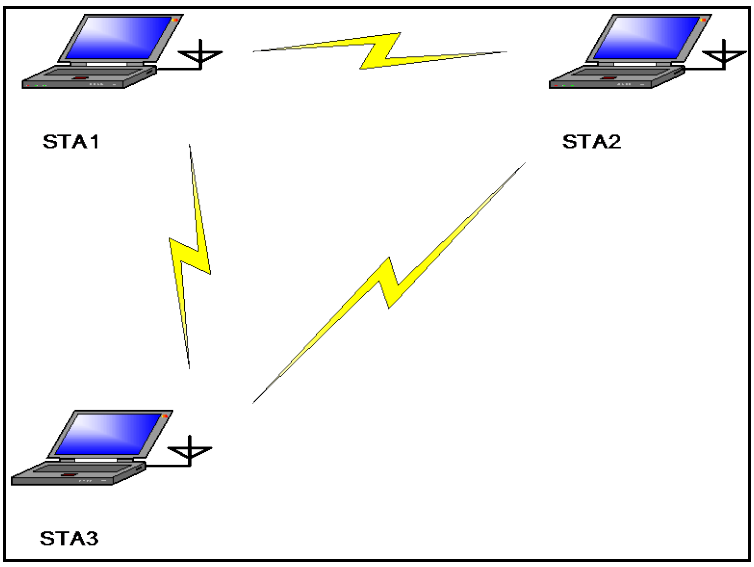
Η βασική δομική μονάδα κάθε 802.11 δικτύου αποκαλείται **Basic Service Set (BSS)** και αποτελείται από μία ομάδα σταθμών που επικοινωνούν μεταξύ τους. Τα όρια του BSS καθορίζονται από την περιοχή ραδιοκάλυψης, που ονομάζεται **Basic Service Area (BSA)**. Ένας σταθμός σε ένα BSS μπορεί να επικοινωνεί με οποιονδήποτε άλλο σταθμό στο ίδιο BSS.

3.5.4. Τοπολογία - Αρχιτεκτονική :

Είναι γνωστό πως υπάρχουν δύο βασικές τοπολογίες, βάσει των οποίων ορίζονται δύο είδη ασυρμάτων δικτύων. Πρόκειται για τα **ανεξάρτητα δίκτυα (independent networks)** και τα **δίκτυα υποδομής (infrastructure networks)**.

Σε ένα **independent** δίκτυο κάθε σταθμός επικοινωνεί απευθείας με όλους τους υπόλοιπους. Το BSS σε αυτήν την περίπτωση ονομάζεται και IBSS (Independent BSS) ή ad-hoc BSS ή πιο απλά ad-hoc δίκτυο. Το IBSS αποτελείται το λιγότερο από δύο σταθμούς και συνήθως είναι προσωρινό,

δηλαδή δημιουργείται για κάποιο σκοπό και μετά διαλύεται. Είναι ο απλούστερος τύπος ασύρματου δικτύου**. Ένα IBSS φαίνεται στην *εικόνα 3.10.***

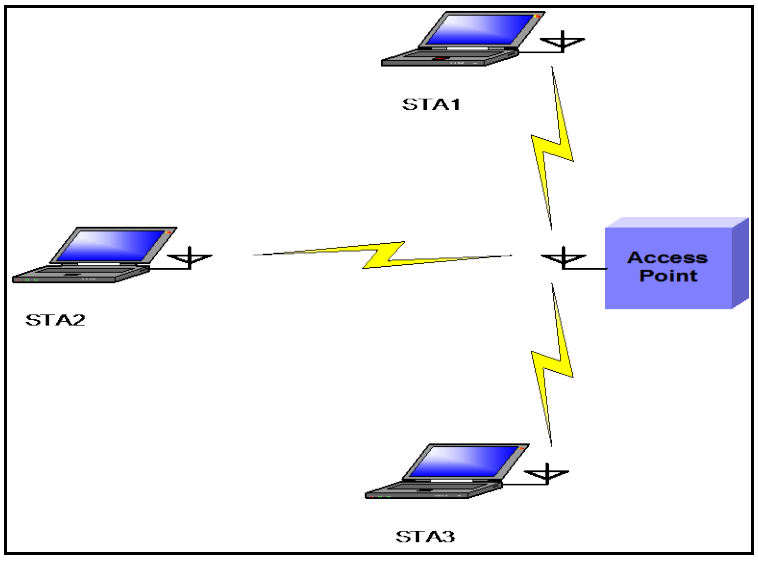


Εικόνα 3.10. : Τοπολογία IBSS

Ο άλλος τύπος δικτύου είναι το **infrastructure** δίκτυο. Σε αυτήν την περίπτωση το BSS διακρίνεται από την παρουσία ενός AP σε αυτό. Το AP, εκτός από το ότι συνδέει το BSS με το ενσύρματο δίκτυο, είναι υπεύθυνο για την ανταλλαγή πλαισίων μεταξύ των σταθμών και γενικότερα για τον κεντρικό έλεγχο της λειτουργίας του BSS. Όταν ένας σταθμός θέλει να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, το πλαίσιο αρχικά αποστέλλεται στο AP και αυτό με την σειρά του το στέλνει στον τελικό προορισμό του. **Η BSA σε αυτήν την περίπτωση είναι η περιοχή όπου υπάρχει ραδιοκάλυψη από το AP.**

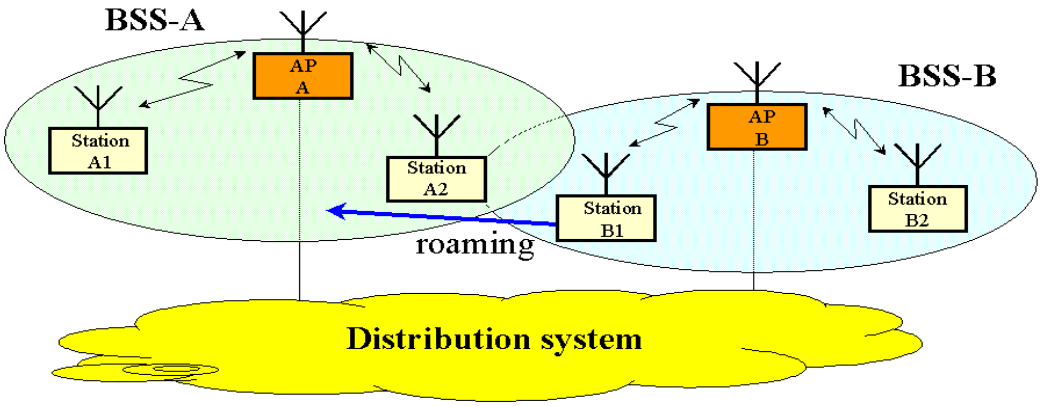
Έτσι σε αντίθεση με το IBSS, όπου όλοι οι σταθμοί πρέπει να βρίσκονται στην περιοχή ραδιοκάλυψης των υπολοίπων, για να επικοινωνήσουν με αυτούς, εδώ αρκεί να βρίσκονται στην περιοχή ραδιοκάλυψης του AP, άσχετα με την μεταξύ τους απόσταση.

Για να συμμετέχει ένας σταθμός στο BSS πρέπει να ακολουθήσει τη διαδικασία του association (στην οποία θα αναφερθούμε παρακάτω) με το AP. Η διαδικασία αυτή ξεκινάει πάντα με πρωτοβουλία του σταθμού και είναι απόφαση του AP αν ο σταθμός θα γίνει τελικά δεκτός στο BSS. Το 802.11 δεν ορίζει μέγιστο αριθμό σταθμών που μπορούν να συμμετάσχουν σε ένα BSS, αλλά τίθενται περιορισμοί στις διάφορες υλοποιήσεις AP. **Ένα infrastructure δίκτυο φαίνεται στην *εικόνα 3.11.***



Εικόνα 3.11. : Τοπολογία infrastructure BSS

Στην περίπτωση infrastructure δικτύων ένας αριθμός από BSSs μπορούν να συνδεθούν και να αποτελέσουν ένα **Extended Service Set (ESS)**. Αυτό δημιουργείται ενώνοντας τα APs των BSSs μέσω ενός ενσύρματου δικτύου κορμού, που ονομάζεται **Σύστημα Διανομής (Distribution System –DS)**. Με αυτόν τον τρόπο είναι εφικτή η επικοινωνία μεταξύ σταθμών που ανήκουν σε διαφορετικά BSSs αλλά στο ίδιο ESS. Σε αυτήν την περίπτωση πρέπει τα APs να επικοινωνούν στο στρώμα ζεύξης δεδομένων μέσω του δικτύου κορμού, επιτελώντας τη λειτουργία της γέφυρας για τους σταθμούς διαφορετικών BSSs. Το ESS τελειώνει όταν παρεμβληθεί μεταξύ των AP's οντότητα δικτύου που λειτουργεί σε υψηλότερο στρώμα, όπως είναι ο δρομολογητής (router). **Τα παραπάνω φαίνονται καλύτερα στην παρακάτω *εικόνα 3.12*.**



Εικόνα 3.12. : Τοπολογία infrastructure δύο BSSs

Το 802.11 προσφέρει κινητικότητα σε ένα ESS, αρκεί το δίκτυο κορμού να είναι ένα απλό LAN ή και VLAN (Virtual LAN). Σε κάθε άλλη περίπτωση η σύνδεση στα ανώτερα επίπεδα θα χαθεί, εκτός κι αν χρησιμοποιείται κάποια άλλη τεχνολογία όπως το Mobile IP. [2] [3]

Πόσους ασύρματους σταθμούς πρέπει να έχει ένα AP ;

Ισοδύναμα το ερώτημα αφορά το πλήθος των ασύρματων συσκευών σε μια κυψέλη. Όσο περισσότερους πελάτες έχει ένα AP, τόσο ελαττώνεται ο ρυθμός μετάδοσης που μπορεί να έχει ο καθένας. Το συνολικό εύρος που έχει διαθέσιμο ένα AP έχει ανώτατο όριο και αυτό το εύρος πρέπει να το μοιραστούν οι πελάτες. Έτσι αν ένας πελάτης μόνο στέλνει και λαμβάνει δεδομένα με το AP, όλο το εύρος είναι διαθέσιμο σε αυτόν, αν δύο πελάτες θελήσουν να ανταλλάξουν δεδομένα το διαθέσιμο εύρος, αυτόματα μοιράζεται στους δύο.

Μάλιστα, το εύρος θα μοιραστεί στους χρήστες όχι όμως με ισοδύναμο τρόπο, αλλά ανάλογα με την ποιότητα ζεύξης που έχει ο καθένας με το AP. Έτσι κάποιος πελάτης που βρίσκεται πιο κοντά και μπορεί να επικοινωνεί χρησιμοποιώντας ρυθμό 11Mbps θα πάρει περισσότερο εύρος από κάποιον που είναι σε μεγαλύτερη απόσταση και λειτουργεί με άλλο ρυθμό, π.χ 2Mbps.
Επίσης, όσον αυξάνεται ο αριθμός των πελατών τόσο αυξάνεται και η πιθανότητα συγκρούσεων και άρα μειώνεται ο συνολικός ρυθμός μετάδοσης του συστήματος.

Από την άλλη πλευρά, αν έχουμε πολύ λίγους πελάτες σε ένα AP δεν το αξιοποιούμε πλήρως. Έτσι θα υπάρχουν μεγάλοι χρονικοί περίοδοι όπου το AP θα μπορεί να υποστηρίξει κάποιο ρυθμό αλλά οι υπάρχοντες χρήστες δεν θα το εκμεταλλεύονται. Αυτό, προφανώς, δεν είναι καθόλου αποδοτικό από οικονομική άποψη.

Κατά συνέπεια, υπάρχει ένας βέλτιστος αριθμός χρηστών ανά AP. Αυτός ο αριθμός εξαρτάται από τα χαρακτηριστικά των χρηστών. Αν, δηλαδή, χρησιμοποιούν μεγάλο εύρος πρέπει να εγκαταστήσουμε περισσότερα AP.

Ένας τυπικός αριθμός όπου το AP μπορεί να λειτουργεί αποτελεσματικά είναι 15-50 πελάτες. [9]

3.5.5. Υπηρεσίες Ασύρματου Δικτύου 802.11 :

Το ασύρματο δίκτυο 802.11 προσφέρει εννέα βασικές υπηρεσίες. Οφείλουμε να επισημάνουμε ότι τρεις από αυτές σχετίζονται με τη μεταφορά δεδομένων και οι υπόλοιπες έξι σχετίζονται με τη διαχείριση. **Οι υπηρεσίες αυτές είναι οι εξής :**

- ***Distribution :*** Η υπηρεσία αυτή είναι απαραίτητη για την παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του. Συνίσταται στον εντοπισμό του παραλήπτη, ώστε να γίνει εφικτή η τελική παράδοση του πλαισίου. Έτσι λαμβάνεται απόφαση αν ένα πλαίσιο πρέπει να σταλεί στο ίδιο BSS ή πρέπει να σταλεί στο DS προς παράδοση σε σταθμό συσχετιζόμενο με άλλο AP.
- ***Integration :*** Η υπηρεσία αυτή παρέχεται από το σύστημα διανομής. Είναι υπεύθυνη για τη διασύνδεση του συστήματος διανομής DS σε ένα δίκτυο διαφορετικό του 802.11. Στην ουσία είναι υπεύθυνη για την μετάφραση των πλαισίων από τον ένα τύπο στον άλλο.
- ***MSDU Delivery :*** Η παράδοση των πλαισίων MAC (MAC Service Data Unit) στον τελικό προορισμό τους.
- ***Association :*** Απαραίτητη διαδικασία συσχετισμού ενός σταθμού με το AP, προκειμένου να είναι σε θέση να στείλει και να δεχτεί πλαίσια μέσω του ασυρμάτου δικτύου. Όταν ένας σταθμός είναι συσχετισμένος με ένα AP, δημιουργείται τότε μια λογική σχέση μεταξύ τους, ώστε το DS να γνωρίζει που και πώς να παραδώσει δεδομένα σε έναν ασύρματο σταθμό.
- ***Reassociation :*** Χρησιμοποιείται από τους κινητούς σταθμούς σε περίπτωση μετακίνησης από μία BSS σε μία άλλη. Είναι μέρος του μηχανισμού της διαπομπής.
- ***Disassociation :*** Η διαδικασία αυτή αφαιρεί έναν σταθμό από το δίκτυο. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να κάνουν πρώτα disassociation.
- ***Authentication :*** Αν απαιτείται από το διαχειριστή του δικτύου, πρέπει κάθε χρήστης να πιστοποιεί την ταυτότητά του πριν να προχωρήσει στη διαδικασία του association.
- ***Deauthentication :*** Τερματισμός μιας ισχύουσας κατάστασης authentication. Τερματίζει επίσης και το association, εφόσον το authentication είναι προαπαιτούμενο αυτού.

- ***Privacy :*** Λόγω του ασύρματου περιβάλλοντος μετάδοσης έχει οριστεί από το 802.11 μια προεραιτική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (Wired Equivalent Privacy). Το WEP δεν προσφέρει σε καμία περίπτωση ασφαλής μεταφορά δεδομένων και ήδη μελετάται η αντικατάσταση του. [3]

3.5.6. Υπόστρωμα MAC του 802.11 :

Το υπόστρωμα MAC του 802.11 είναι ίσως το πιο σημαντικό κομμάτι της προτυποποίησης. Υποστηρίζει όλα τα φυσικά στρώματα και προσφέρει υπηρεσίες αξιόπιστης μεταφοράς δεδομένων και πρόσβασης στο μέσο στα ανώτερα στρώματα. Οι όποιες διαφοροποιήσεις του από το αντίστοιχο MAC ενσύρματων δικτύων οφείλονται στις ιδιαιτερότητες του ασύρματου μέσου μετάδοσης που χρησιμοποιείται στο φυσικό επίπεδο.

Σαν μηχανισμός πρόσβασης στο μέσο έχει επιλεχτεί ο **CSMA (Carrier Sense Multiple Access)**. Για να αποφευχθούν όσο το δυνατόν περισσότερο οι συγκρούσεις αντί για το μηχανισμό ανίχνευσης συγκρούσεων **CD (Collision Detection)** που χρησιμοποιείται στο 802.3 επιλέχτηκε ο μηχανισμός αποφυγής συγκρούσεων **CA (Collision Avoidance).** Αιτία για την επιλογή αυτή είναι η αδυναμία του δέκτη να αντιλαμβάνεται την κατάσταση του ασύρματου μέσου την χρονική στιγμή που μεταδίδει κάποια πληροφορία. Επομένως, το φαινόμενο της σύγκρουσης (που λαμβάνει χώρα όταν δυο ή περισσότεροι σταθμοί μεταδίδουν την ίδια ακριβώς χρονική στιγμή) γίνεται αντιληπτό από τους σταθμούς εργασίας μόνο εκ του αποτελέσματος που είναι φυσικά η μη παράδοση των πακέτων της πληροφορίας.

Επιπλέον η αξιόπιστη μεταφορά δεδομένων μεταξύ των διαφόρων σταθμών δυσχεραίνεται ακόμα περισσότερο εξαιτίας του ασύρματου φυσικού μέσου. Προβλήματα όπως η κακή ποιότητα της ασύρματης ζεύξης λόγω θορύβου ή παρεμβολών, η πιθανότητα κάποιος κόμβος να βγει προσωρινά εκτός της περιοχής κάλυψης του δικτύου και η ύπαρξη κρυμμένων κόμβων (hidden nodes) δεν υπάρχουν σε ενσύρματα δίκτυα. Για να αντιμετωπιστούν τα παραπάνω το 802.11 MAC προσφέρει τους κατάλληλους μηχανισμούς, όπως η θετική επιβεβαίωση (positive acknowledgment) κάθε πλαισίου και την ανταλλαγή πλαισίων RTS (Request To Send) και CTS (Clear To Send) πριν την μετάδοση κάποιου πλαισίου. [2]

3.5.7. Φυσικό Στρώμα του 802.11 :

Στο φυσικό στρώμα προδιαγράφονται τρεις τεχνικές διαμόρφωσης:

- *Infrared (Υπέρυθρες Ακτίνες)* σε μήκη κύματος μεταξύ 850 και 950 nm με ρυθμούς μετάδοσης 1 και 2 Mbps.

- *Frequency Hopping Spread Spectrum-FHSS (Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας)* στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.

- *Direct Sequence Spread Spectrum-DSSS (Εξάπλωση Φάσματος Άμεσης Ακολουθίας)* στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.

3.5.7.1 Infrared (Υπέρυθρες Ακτίνες):

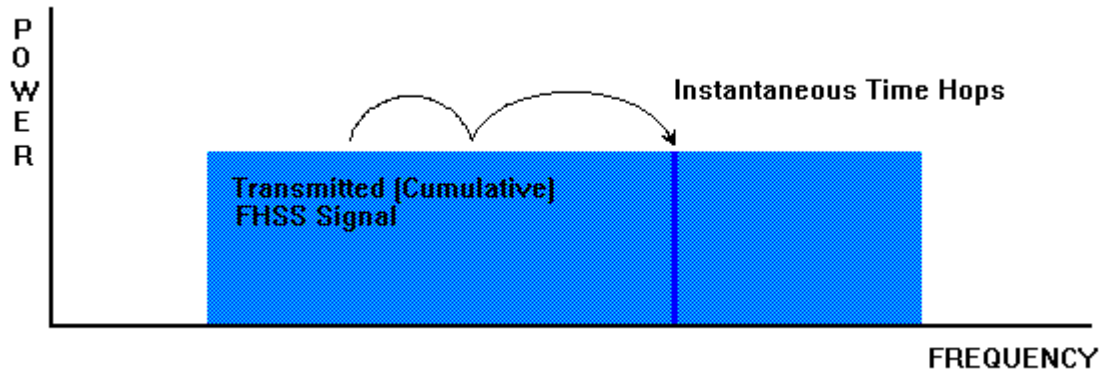
Η τεχνική των υπέρυθρων ακτινών δεν χρησιμοποιείται ιδιαίτερα λόγω του χαμηλού εύρους ζώνης και του γεγονότος ότι το φως του ήλιου εξαφανίζει τα υπέρυθρα σήματα.

Η υπέρυθρη επιλογή χρησιμοποιεί διάχυτη (δηλαδή όχι σε ευθεία γραμμή) μετάδοση στα 0,85 ή στα 0,95 micron. Στα 1 Mbps χρησιμοποιείται μία μέθοδος κωδικοποίησης στην οποία κάθε ομάδα των 4 bit κωδικοποιείται ως μία κωδικολέξη των 16 bit που περιέχει δεκαπέντε 0 και ένα 1, χρησιμοποιώντας τον Gray code (κώδικα Gray) ο οποίος έχει την ιδιότητα ότι ένα μικρό σφάλμα συγχρονισμού οδηγεί σε ένα σφάλμα του ενός bit στην έξοδο.

Στα 2 Mbps η κωδικοποίηση παίρνει 2 bit και παράγει μία κωδικολέξη των 4 bit όπου πάλι υπάρχει ένα μόνο 1, δηλαδή δίνει μία από τις κωδικολέξεις 0001, 0010, 0100, 1000. Τα υπέρυθρα σήματα δεν μπορούν να διαπεράσουν τους τοίχους, έτσι οι κυψέλες (BSS) που βρίσκονται σε ξεχωριστά δωμάτια είναι καλά απομονωμένες η μία από την άλλη.

3.5.7.2 Frequency Hopping Spread Spectrum-FHSS :

Πρόκειται για τεχνική εξάπλωσης φάσματος. Η τεχνική FHSS βασίζεται στην ιδέα της αλλαγής της φέρουσας ενός σήματος μέσα σε ένα μεγάλο εύρος συχνοτήτων και σύμφωνα με μία συγκεκριμένη ψευδοτυχαία ακολουθία (hopping pattern). Χρησιμοποιείται μία γεννήτρια ψευδοτυχαίων (PN) αριθμών για την παραγωγή της ακολουθίας συχνοτήτων στις οποίες μεταβαίνουν διαδοχικά οι σταθμοί, όπως φαίνεται στην *εικόνα 3.13*.



Εικόνα 3.13. : Φάσμα FHSS

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

Σε μεγαλύτερες αποστάσεις μπορεί να δημιουργήσει πρόβλημα η εξασθένιση πολλαπλών διαδρομών, η τεχνική FHSS όμως παρέχει αρκετή αντοχή σε αυτό το φαινόμενο.

Πλεονέκτημα είναι ότι είναι σχετικά ανθεκτική στις ραδιοκυματικές παρεμβολές, γεγονός που την κάνει δημοφιλή για συνδέσεις από κτίριο σε κτίριο.

Πλεονεκτήματα έναντι της εναλλακτικής DSSS είναι τα απλούστερα και φθηνότερα ηλεκτρονικά για την υλοποίηση των ανάλογων συσκευών, η χαμηλότερη κατανάλωση ενέργειας και η δυνατότητα συνύπαρξης πολλών τέτοιων δικτύων στην ίδια περιοχή χωρίς να επηρεάζεται η συνολική διέλευση.

Βασικό πλεονέκτημα είναι η δυνατότητα συνύπαρξης διαφορετικών ασυρμάτων δικτύων, αρκεί τα hopping patterns τους να είναι διαφορετικά, δηλαδή σε κάθε χρονική στιγμή κάθε σύστημα να μεταδίδει σε διαφορετική φέρουσα. Τότε τα hopping patterns ονομάζονται *ορθογώνια* και η συνολική διέλευση μεγιστοποιείται.

Το κύριο μειονέκτημα της τεχνικής FHSS είναι το χαμηλό εύρος ζώνης της.

Η FHSS χρησιμοποιεί κανάλια, το καθένα με εύρος 1 MHz, ξεκινώντας από το κάτω όριο της ζώνης ISM στα 2,4 GHz. Ο *Πίνακας 1* παρουσιάζει τα κανάλια και τα hopping patterns που χρησιμοποιούνται σε διάφορες γεωγραφικές περιοχές.

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

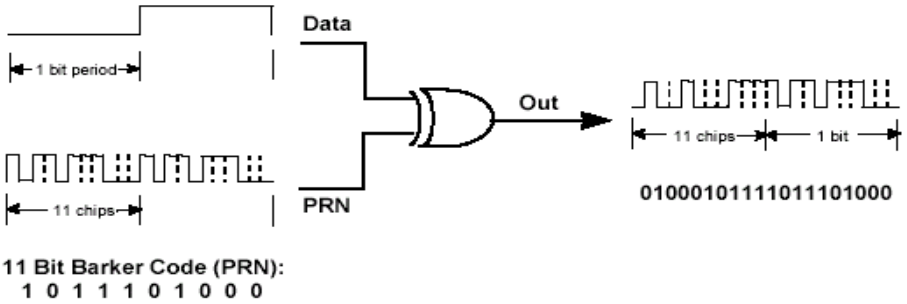
Πίνακας 1. Διαθέσιμα κανάλια και hopping patterns ανά περιοχή για το φυσικό στρώμα.

3.5.7.3 Direct Sequence Spread Spectrum-DSSS :

Πρόκειται για τεχνική εξάπλωσης φάσματος. **Η DSSS τεχνική είναι η πιο επιτυχημένη που έχει χρησιμοποιηθεί σε συνδυασμό με τα ασύρματα δίκτυα.** Σε σχέση με την FHSS τεχνική μετάδοσης απαιτεί περισσότερη ενέργεια για να επιτύχει παρόμοια διέλευση, όμως το μεγάλο πλεονέκτημά της είναι ότι μπορεί εύκολα να αναβαθμιστεί για την επίτευξη υψηλότερων ρυθμών μετάδοσης.

Η DSSS περιορίζεται και αυτή σε 1 ή 2 Mbps. Η τεχνική αυτή αντικαθιστά κάθε bit πληροφορίας με μία σειρά από bits που ονομάζεται spreading code (κώδικας εξάπλωσης).

Κάθε bit μεταδίδεται ως 11 θραύσματα (chips), χρησιμοποιώντας την ονομαζόμενη ακολουθία Barker (Barker sequence) η οποία είναι ο spreading code. Για την ακρίβεια, κάθε bit πληροφορίας συνδέεται μέσω μίας XOR με μία ψευδοτυχαία αριθμητική (Pseudo-random Numerical ή PN) ακολουθία όπως δείχνει η *εικόνα 3.14*. Το αποτέλεσμα είναι ένα ψηφιακό φέρον σήμα υψηλής ταχύτητας το οποίο διαμορφώνεται σε ένα κατά τη φάση φέρον σήμα χρησιμοποιώντας Differential Phase Shift Keying-DPSK (διαφορική μεταλλαγή ολίσθησης φάσης).



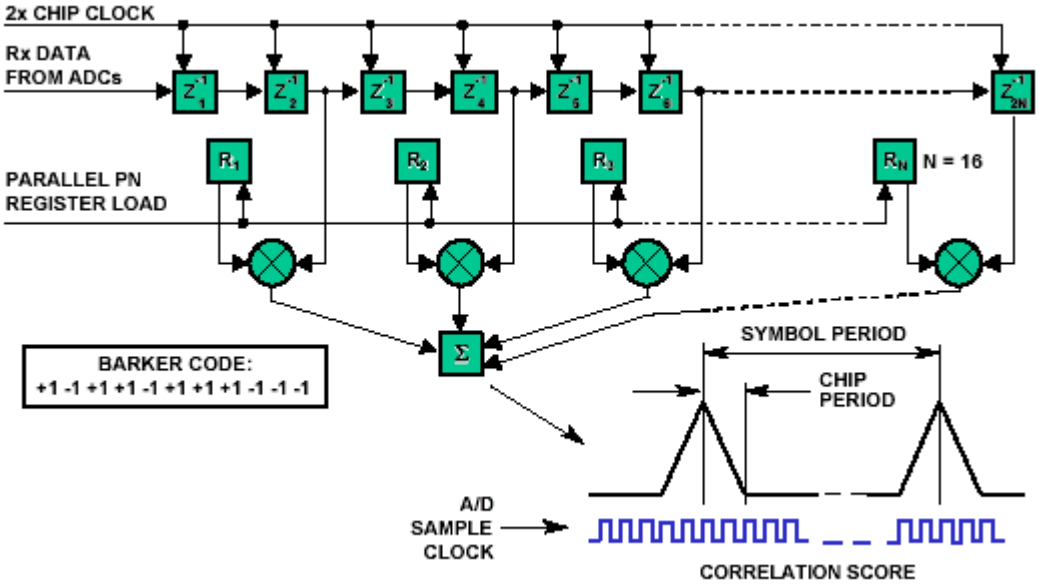
Εικόνα 3.14. :Ψηφιακή Διαμόρφωση Δεδομένων με μία PN

Ο δέκτης εκτελεί την αντίστροφη διαδικασία. Κατά τη λήψη του DSSS σήματος, χρησιμοποιεί ένα συσχετιστή (φίλτρο αντιστοίχησης) όπως φαίνεται στην *εικόνα 3.15*. Ο συσχετιστής αφαιρεί την PN ακολουθία και ανακτά το αρχικό σήμα.

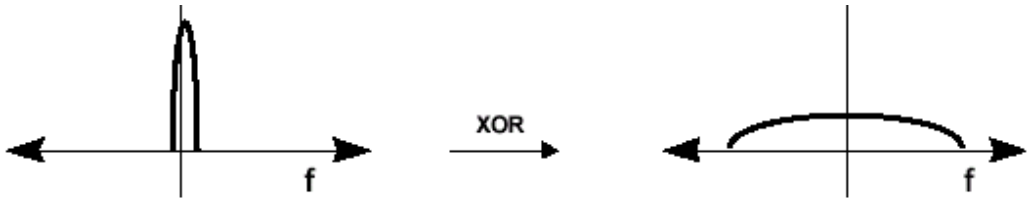
Τα αποτελέσματα της χρησιμοποίησης PN ακολουθιών για την δημιουργία εξάπλωσης φάσματος φαίνονται στις *εικόνες 3.16* και *3.17*.

Όπως παρατηρούμε στην *εικόνα 3.16* η ακολουθία PN διευρύνει το φάσμα του προς μετάδοση σήματος, μειώνοντας ταυτόχρονα το πλάτος του, δηλαδή απλώνει την ισχύ του σήματος σε πολύ μεγαλύτερο φασματικό εύρος. Βλέπουμε όμως ότι η συνολική ισχύς δεν μεταβάλλεται. Στην *εικόνα 3.17* παρατηρούμε μετά τη λήψη του σήματος, το σήμα συσχετίζεται με την ίδια PN ακολουθία για να ανακτηθεί το αρχικό σήμα.

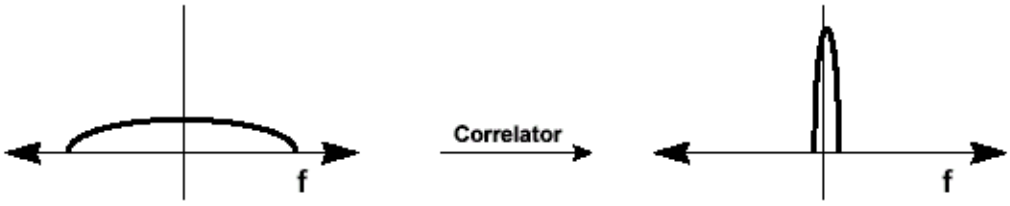
Ένα πλεονέκτημα της τεχνικής DSSS είναι η ανοχή σε παρεμβολές στενής ζώνης, καθώς και μεγαλύτερη ασφάλεια, εφόσον το "απλωμένο" σήμα μοιάζει σαν απλός θόρυβος σε πομπό που λαμβάνει μόνο σήμα στενής ζώνης.



Εικόνα 3.15. : Συσχετιστής (φίλτρο αντιστοίχησης) κατά τη λήψη του DSSS σήματος.



Εικόνα 3.16. : Επίδραση της PN ακολουθίας στο μεταδιδόμενο σήμα.



Εικόνα 3.17. :Το λαμβανόμενο σήμα συσχετίζεται με την PN ακολουθία για την ανάκτηση του αρχικού σήματος.

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

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

Πίνακας 2. : Διαθέσιμα κανάλια ανά περιοχή για το φυσικό στρώμα.

3.5.8. Πρόσβαση στο Μέσον :

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

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

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

Ως όρος προκειμένου να υπάρξει πρόσβαση στο μέσον, το υπόστρωμα MAC ελέγχει την τιμή που έχει ο Network Allocation Vector (NAV), ο οποίος είναι ένας καταμετρητής που εδρεύει σε κάθε σταθμό και που αντιπροσωπεύει το χρόνο

που ο προηγούμενος σταθμός χρειάζεται για να στείλει ένα πλαίσιο. Το NAV πρέπει να είναι μηδέν προτού ένας σταθμός να επιχειρήσει να στείλει ένα πλαίσιο. Πριν τη μετάδοση ενός πλαισίου, ο σταθμός υπολογίζει το χρόνο που απαιτείται για να σταλεί το πλαίσιο λαμβάνοντας υπόψη το μήκος και το ρυθμό μετάδοσης του πλαισίου. Όταν οι σταθμοί λάβουν το πλαίσιο, εξετάζουν τη διάρκειά του και χρησιμοποιούν αυτή την τιμή ως βάση για τον καθορισμό των αντίστοιχων δικών τους NAV. Αυτή η διαδικασία καθιστά αποκλειστικό χρήστη του μέσου, το σταθμό που κάνει μετάδοση εκείνη τη στιγμή.

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

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

Για την υποστήριξη χρονικά περιορισμένης παράδοσης πλαισίων δεδομένων, το πρότυπο 802.11 ορίζει προαιρετικά τον αλγόριθμο Point Coordination Function (**PCF**) σύμφωνα με τον οποίο το σημείο πρόσβασης (access point) παραχωρεί την πρόσβαση στο μέσον για ένα σταθμό, σφυγμομετρώντας (polling) το σταθμό κατά τη περίοδο χωρίς ανταγωνισμό (contention free period).

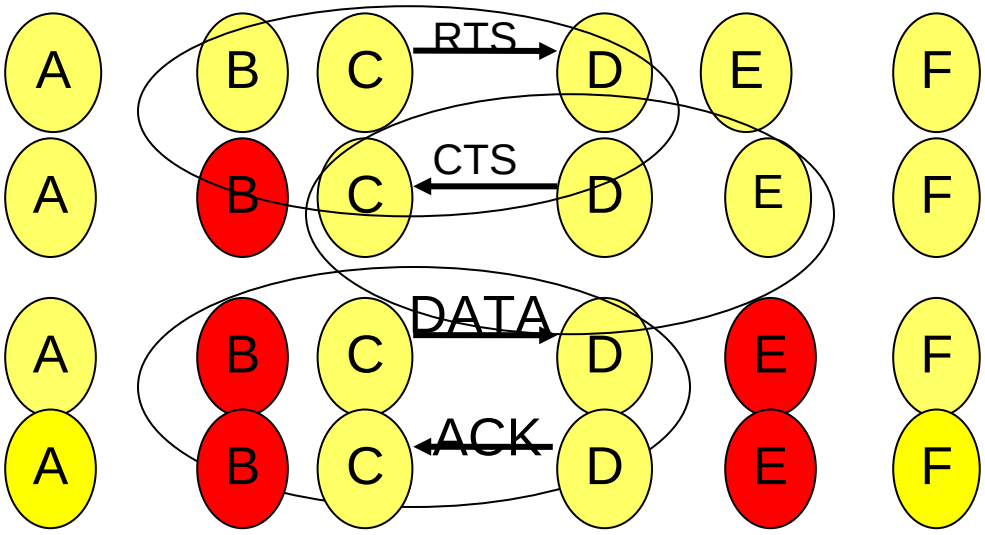
Οι σταθμοί δεν μπορούν να μεταδώσουν πλαίσια μέχρις ότου το access point τους σφυγμομετρήσει. Το χρονικό διάστημα για κίνηση δεδομένων που έχουν βάση τον αλγόριθμο PCF (αν είναι ενεργοποιημένος) συμβαίνει εναλλάξ ανάμεσα σε περιόδους ανταγωνισμού DCF.

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

Για να εξασφαλιστεί ότι μία συγκεκριμένη ανταλλαγή πλαισίων θα γίνει χωρίς διακοπή λόγω μετάδοσης τρίτου σταθμού, το πρότυπο 802.11 υποστηρίζει το μηχανισμό RTS/CTS. Αυτός ο μηχανισμός διαφοροποιεί την διαδικασία αποστολής πλαισίου εισάγοντας δύο επιπλέον πλαίσια, τα RTS (Ready To Send) και CTS (Clear To Send). Προστατεύοντας την ανταλλαγή πλαισίων, ο μηχανισμός RTS/CTS βελτιώνει την απόδοση της χρήσης του ασύρματου δικτύου σε περιπτώσεις μεγάλου φόρτου εξαιτίας της ύπαρξης πολλών τερματικών και αντιμετωπίζει το πρόβλημα του κρυμμένου κόμβου. Αν όμως χρησιμοποιείται χωρίς λόγο, έχει το ακριβώς αντίθετο αποτέλεσμα, εφόσον προσθέτει επιπλέον φορτίο στο ασύρματο δίκτυο.

Ο αποστολέας στέλνει αρχικά ένα πλαίσιο RTS στον παραλήπτη το οποίο δεν περιέχει δεδομένα. Αυτό το πλαίσιο έχει ως σκοπό να δεσμεύσει ο αποστολέας το μέσο μετάδοσης για όσο χρόνο υπολογίζει ότι θα διαρκέσει η αποστολή του πλαισίου δεδομένων και να το ανακοινώσει στους υπόλοιπους σταθμούς μέσω του μετρητή NAV στο πλαίσιο RTS. Ο παραλήπτης λαμβάνοντας το RTS απαντάει με ένα πλαίσιο CTS. Υπενθυμίζεται ότι η αποστολή πλαισίου CTS γίνεται με το συντομότερο χρόνο αναμονής SIFS. Τότε ο αποστολέας στέλνει το πλαίσιο δεδομένων και περιμένει την επιβεβαίωση ορθής λήψης του από τον παραλήπτη. Έτσι η διαδικασία αποστολής πλαισίου απαιτεί την ανταλλαγή τεσσάρων πλαισίων για να ολοκληρωθεί σωστά.

Η παραπάνω διαδικασία γίνεται κατανοητή με το ακόλουθο παράδειγμα :
Όσοι σταθμοί ακούν το πλαίσιο CTS παραμένουν σιωπηλοί για να μη δημιουργηθεί σύγκρουση κατά την μετάδοση του πλαισίου δεδομένων από τον σταθμό C στον σταθμό D. Επίσης σιωπηλοί παραμένουν και όσοι σταθμοί ακούν το πλαίσιο RTS, προκειμένου να μην δημιουργήσουν σύγκρουση κατά την μετάδοση της επιβεβαίωσης ACK από τον σταθμό D στον C. Το διάστημα στο οποίο οι σταθμοί παραμένουν σιωπηλοί περιλαμβάνεται σε ένα πεδίο RTS/CTS πλαισίων και εξαρτάται από την διάρκεια του πλαισίου πληροφορίας. Το πλαίσιο επιβεβαίωσης χρησιμοποιείται, διότι παρά την ύπαρξη του RTS/CTS μηχανισμού, υπάρχει πάντα η πιθανότητα λαθών λόγω του θορύβου του καναλιού καθώς επίσης και η πιθανότητα σύγκρουσης. Αν ένας σταθμός δεν λάβει πλαίσιο επιβεβαίωσης, επαναμεταδίδει τότε το πλαίσιο.

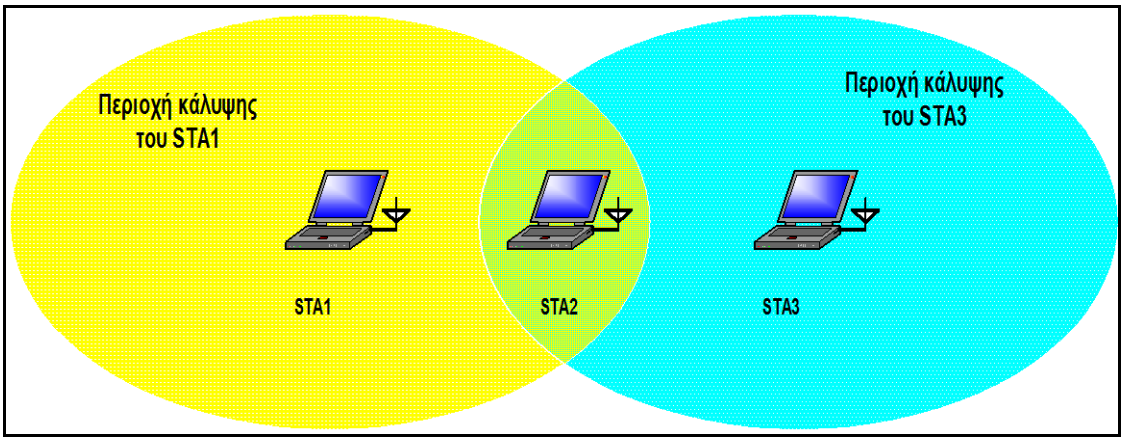


Εικόνα 3.18. : Μηχανισμός RTS/CTS

Ο μηχανισμός αυτός ενεργοποιείται αυτόματα όταν το μέγεθος ενός πλαισίου είναι μεγαλύτερο από το RTS threshold για να διασφαλίσει την ομαλή αποστολή μεγάλων πλαισίων. Επίσης μπορεί να χρησιμοποιηθεί σε συνδυασμό με τον κατακερματισμό. Συνήθως τα κατώφλια RTS threshold και Fragmentation threshold τίθενται στην ίδια τιμή. Αυτό έχει σαν αποτέλεσμα όλα τα fragments ενός πλαισίου να μεταδίδονται με τη σειρά προστατευμένα από το μηχανισμό RTS/CTS. Σε αυτήν την περίπτωση το πλαίσιο RTS που στέλνει ο αποστολέας στην αρχή της διαδικασίας δεσμεύει το μέσο για όσο χρόνο απαιτεί η αποστολή και η επιβεβαίωση του πρώτου τμήματος του πλαισίου.

Όταν ο αποστολέας πάρει το CTS αρχίζει να στέλνει διαδοχικά τα τμήματα περιμένοντας φυσικά κάθε φορά για το αντίστοιχο πλαίσιο ACK, του οποίου η αποστολή γίνεται με χρήση του χρόνου SIFS. Ο αποστολέας και ο παραλήπτης ανανεώνουν το NAV κατά τη διάρκεια της ανταλλαγής πλαισίων, εξασφαλίζοντας ότι θα διατηρήσουν τον έλεγχο του μέσου. Το μέσο αποδεσμεύεται με την λήψη από τον αποστολέα του τελευταίου πλαισίου ACK από τον παραλήπτη. Ένας άλλος τρόπος μετάδοσης των τμημάτων ενός πλαισίου είναι να δεσμεύσει ο αποστολέας το μέσο με χρήση του μετρητή NAV στο πρώτο τμήμα που θα στείλει.

Ο εν λόγω μηχανισμός αντιμετωπίζει αποτελεσματικά το πρόβλημα ύπαρξης κρυμμένου κόμβου (hidden node). **Το πρόβλημα αυτό απεικονίζεται στην παρακάτω *εικόνα 3.19.***



Εικόνα 3.19. : Πρόβλημα κρυμμένου κόμβου

Πρόβλημα κρυμμένου κόμβου :

Όπως φαίνεται στην παραπάνω εικόνα, ο σταθμός STA1 δεν γνωρίζει την ύπαρξη του STA3, εφόσον αυτός είναι έξω από την περιοχή κάλυψής του. Το ίδιο συμβαίνει και με τον STA3, ο οποίος δεν γνωρίζει την ύπαρξη του STA1, για τον ίδιο λόγο με την προηγούμενη περίπτωση. Ο STA2 βρίσκεται στην κοινή περιοχή κάλυψης των STA1 και STA3 και συνεπώς μπορεί να ανταλλάσσει πλαίσια και με τους δύο. Το πρόβλημα δημιουργείται στην περίπτωση που οι STA1 και STA3 επιχειρούν να επικοινωνήσουν με τον STA2 ταυτόχρονα. Το αποτέλεσμα είναι η δημιουργία συγκρούσεων και τα πλαίσια που έχουν εκπεμφθεί χάνονται.

Τη λύση λοιπόν σ' αυτό το πρόβλημα έρχεται μας δώσει ο μηχανισμός RTS/CTS. Σύμφωνα μ' αυτόν, ο κόμβος STA2 θα εκπέμψει ένα πλαίσιο CTS σε απάντηση του RTS που θα του έχει στείλει νωρίτερα ο STA1. Αυτό το πλαίσιο CTS θα το λάβει και ο STA3 (καθώς «ακούει»)και έτσι θα αποφύγει να μεταδώσει κι αυτός κάποιο πλαίσιο που θα προκαλούσε σύγκρουση. Τον ίδιο ρόλο παίζει και το πλαίσιο RTS που μεταδίδει ο STA1, δηλαδή ενημερώνει άλλους κρυφούς κόμβους που μπορεί να βρίσκονται γύρω του και δεν βλέπουν τον STA2. [2]

3.5.9. Υποπρότυπα του 802.11 :

Τα νέα υποπρότυπα IEEE 802.11x αρχίζουν να κάνουν την εμφάνισή τους. Πρόκειται για την απόρροια επιστημονικών ερευνών των μελών της ομάδας

εργασίας του IEEE, που συνεργάζονται για να φέρουν σε πέρας την προτυποποίηση των προσπαθειών τους. Στην συνέχεια παραθέτουμε αυτά τα υποπρότυπα ανά κωδικό ομάδας εργασίας, που στην ουσία αποτελούν και τα μέλη της οικογένειας του προτύπου IEEE 802.11.

3.5.9.1 Οι αναθεωρήσεις του Πρότυπου 802.11 :

Από τότε που έγινε η επικύρωση του αρχικού προτύπου, η ομάδα εργασίας του IEEE 802.11 έκανε αρκετές αναθεωρήσεις μέσω διαφόρων ομάδων αναθεώρησης. Οι ομάδες αναθεώρησης εντός της ομάδας εργασίας του 802.11 έχουν ως αποστολή την ενίσχυση – εμπλουτισμό τμημάτων του προτύπου 802.11. Ένα ειδικό γράμμα του αλφαβήτου που αντιστοιχεί σε κάθε αναθεώρηση, όπως π.χ. 802.11a, 802.11b κλπ, αντιπροσωπεύει τις διάφορες ομάδες αναθεώρησης. Ως παράδειγμα μπορούμε να αναφέρουμε την ομάδα αναθεώρησης B (δηλαδή 802.11b) που είναι υπεύθυνη για την αναβάθμιση του αρχικού πρότυπου 802.11 έτσι ώστε να συμπεριλάβει λειτουργία υψηλότερου ρυθμού μετάδοσης δεδομένων χρησιμοποιώντας DSSS στη μπάντα των 2,4 GHz. Το πρότυπο 802.11 της IEEE αποτελείται από διάφορες εκδόσεις όπως θα δούμε παρακάτω που πολλές φορές ο εξοπλισμός τους είναι συμβατός μεταξύ τους.

3.5.9.2 802.11a – OFDM στην μπάντα των 5 Ghz :

Η IEEE αναγνωρίζοντας ότι οι τηλεοπτικές, όπως και οι 'βαριές' εφαρμογές πολυμέσων θα απαιτούσαν ταχύτητες υψηλότερες από 11 Mb/s, εξέδωσε το 1999 το πρότυπο IEEE 802.11a, το οποίο είναι βελτιστοποιημένο για υψηλή απόδοση στα εσωτερικά περιβάλλοντα. Παρέχει ρυθμούς μετάδοσης δεδομένων μέχρι 54 Mb/s, ενώ χρησιμοποιεί την μπάντα των 5GHz. Ένας κατασκευαστής μάλιστα έχει δηλώσει ότι είναι σε θέση να προχωρήσει το πρότυπο ώστε να υποστηρίζει ταχύτητες μέχρι 108 Mb/s, με κάποιες μικρές αλλαγές.

Το 802.11a βασίζεται στην τεχνική πολυπλεξίας OFDM (Orthogonal Frequency Division Multiplexing / Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας).

Η βασική ιδέα πίσω από την OFDM είναι η διαίρεση ενός κύριου υψηλού ρυθμού σε πολλούς μικρότερους ρυθμούς και η χρήση αυτών για την αποστολή των δεδομένων ταυτόχρονα. Όλα τα «αργά» κανάλια πολυπλέκονται τελικά σε ένα «γρήγορο» κανάλι και μεταδίδονται.

Με την ορθογονοποίηση λύνεται το πρόβλημα της σπατάλης του εύρους ζώνης, προκειμένου να διαχωρίσουμε τα κανάλια μεταξύ τους.

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

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

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

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

3.5.9.3 802.11b – Υψηλός Ρυθμός Μετάδοσης DSSS στα 2,4 GHz:

Το 802.11b είναι σήμερα, το πιο δημοφιλές από τα μέλη της οικογένειας των προτύπων ασύρματης δικτύωσης IEEE 802.11, με υποστήριξη από πολλούς κατασκευαστές. Το πρώτο 802.11 πρότυπο παρείχε αρκετά χαμηλή ταχύτητα μεταφοράς δεδομένων με αρκετά υψηλό κόστος για να υιοθετηθεί ευρέως. Έτσι το 1999, η IEEE εξέδωσε ένα νέο πρότυπο, το 802.11b, το οποίο υποστηρίζει ταχύτητες μέχρι 11 Mb/s και χρησιμοποιεί την ελεύθερη μπάντα συχνοτήτων των 2,4 GHz. Επίσης είναι το πιο διαδεδομένο στην αγορά ανεξάρτητα από το γεγονός ότι το 802.11a, προσφέρει υψηλότερους ρυθμούς μετάδοσης.

Όταν η ποιότητα επικοινωνίας είναι φτωχή, το σύστημα μπορεί να ρίξει την ταχύτητα σε 5,5 Mb/s, 2 Mb/s ή 1 Mb/s προκειμένου να διατηρηθεί η σύνδεση μεταξύ των ασύρματων συσκευών.

Χρησιμοποιεί το ίδιο υπόστρωμα MAC όπως και τα άλλα πρότυπα, την τεχνική HR/DSSS (High Rate/ Direct Sequence Spread Spectrum) και την διαμόρφωση CCK (Complementary Code Keying - χρησιμοποιεί το πλήρες εύρος ζώνης συχνοτήτων κάθε υποκαναλιού για να διαμορφώσει τα σήματά του). Μπορεί να θεωρηθεί σαν επέκταση του αρχικού DSSS φυσικού στρώματος που ορίστηκε στο 802.11 και μάλιστα χρησιμοποιεί τα ίδια κανάλια με αυτό, πετυχαίνοντας αρκετά μεγαλύτερους ρυθμούς μετάδοσης

Τα περισσότερα 802.11 προϊόντα προορίζονται ώστε να χρησιμοποιηθούν σε ενδοκτιριακές εφαρμογές, όπου επιτυγχάνουν κάλυψη ως 150 μέτρα κάτω από τις βέλτιστες συνθήκες (ειδικές κεραίες είναι διαθέσιμες για την επέκταση της κάλυψης για ανοικτές περιοχές ή από σημείο σε σημείο επικοινωνίες). Εντούτοις, πολλοί πελάτες χρησιμοποιούν το πρότυπο για κάλυψη έκτασης όχι παραπάνω από 30 μέτρα, ώστε να εξασφαλίσουν καλή απόδοση χωρίς να χρειάζεται να κάνουν εκτενείς μελέτες για την εξασφάλιση των αναγκών τους.

Το IEEE 802.11 πρότυπο υποστηρίζει πιστοποίηση ταυτότητας των συσκευών και κρυπτογράφηση των δεδομένων. Η πιστοποίηση ταυτότητας μπορεί να βασιστεί σε έναν καθορισμένο από το χρήστη κατάλογο έγκυρων μελών ή σε ένα κοινό κλειδί. Ούτε όλοι οι κατασκευαστές, ούτε όλα τα προϊόντα από τον ίδιο κατασκευαστή, υποστηρίζουν τα ίδια επίπεδα ασφάλειας. Το IEEE 802.11b πρότυπο επιτάσσει την ύπαρξη ενός ελάχιστου επιπέδου ασφάλειας, αλλά καθορίζει και άλλα ασφαλέστερα επίπεδα τα οποία μπορούν να χρησιμοποιηθούν προαιρετικά. Εντούτοις, η πιστοποίηση Wi-Fi (Wireless Fidelity) απαιτεί τα προϊόντα να υποστηρίζουν τουλάχιστον ένα μήκους 40 bits κλειδί κρυπτογράφησης(WEP key).

Η προαιρετική δυνατότητα κρυπτογράφησης WEP είναι διαθέσιμη στις ασύρματες συσκευές των περισσότερων κατασκευαστών, αλλά όχι απαραιτήτως στην πλήρη γραμμή των προϊόντων τους. Μόνο τα δεδομένα κρυπτογραφούνται πριν την μετάδοση, ενώ οι επικεφαλίδες μεταδίδονται χωρίς κάποια επεξεργασία.

3.5.9.4 802.11c – Λειτουργίες Γεφύρωσης (Bridge Operation Procedures) :

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

3.5.9.5 802.11d – Καθολική Εναρμόνιση (Global Harmonization):

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

3.5.9.6 802.11e – Εμπλουτισμός του MAC για Ποιότητα Υπηρεσιών (MAC Enhancements For QoS) :

Η IEEE δημιούργησε το 802.11e ένα καθολικό ασύρματο standard - το οποίο προσφέρει seamless interoperability μεταξύ επιχειρήσεων, σπιτιών και σε δημόσιους χώρους και το οποίο ακόμα προσφέρει τα χαρακτηριστικά γνωρίσματα που ικανοποιούν τις μοναδικές ανάγκες κάθε κοινωνικής ομάδας. Αντίθετα από άλλες ασύρματες πρωτοβουλίες, αυτό είναι το πρώτο ασύρματο πρότυπο που εκτείνεται σε περιβάλλοντα σπιτιών και επιχειρήσεων. Προσθέτει QoS και υποστήριξη πολυμέσων στα υπάρχοντα ασύρματα πρότυπα 802.11b, 802.11a και 802.11g, διατηρώντας full backward compatibility (πλήρη προς τα πίσω συμβατότητα) με αυτά τα πρότυπα.

Χωρίς ισχυρή ποιότητα υπηρεσιών - QoS (Quality of Service), η υπάρχουσα έκδοση του πρότυπου 802.11 δεν βελτιστοποιεί τη μετάδοση φωνής και εικόνας. Επί του παρόντος δεν υπάρχει κανένας αποτελεσματικός μηχανισμός

που να καθορίζει την προτεραιότητα κίνησης εντός του 802.11. Ως εκ τούτου, η εργασία της ομάδας αναθεώρησης 802.11e, είναι να διυλίσει – καθαρίσει το 802.11 MAC (Medium Access Layer) για να βελτιωθεί το Quality of Service (QoS) προκειμένου να υπάρξει καλύτερη υποστήριξη στις εφαρμογές audio και video (όπως οι MPEG-2).

Επειδή το 802.11e είναι εντός των ορίων του MAC υποστρώματος, είναι κοινό και σε όλα τα φυσικά υποστρώματα του 802.11 και επομένως συμβατό προς τα πίσω με όλα τα υπάρχοντα 802.11 WLANs.

3.5.9.7 802.11f – Πρωτόκολλο Διασύνδεσης Σημείων Πρόσβασης (Inter Access Point Protocol) :

Το υπάρχον πρότυπο 802.11 δεν προδιαγράφει τις επικοινωνίες μεταξύ των Access Points και τούτο για να υποστηρίζονται οι χρήστες που περιπλανώνται από το ένα στο άλλο Access Point. Η ομάδα εργασίας του 802.11 εσκεμμένα δεν καθόρισε αυτό το στοιχείο για να υπάρχει ελαστικότητα όταν εργαζόμαστε με διαφορετικά συστήματα διανομής, δηλαδή ενσύρματα backbones που διασυνδέουν Access Points.

Το πρόβλημα ωστόσο είναι ότι Access Points από διαφορετικούς κατασκευαστές μπορεί να μη έχουν διαλειτουργικότητα όταν υποστηρίζουν περιαγωγή (roaming). Το 802.11f προδιαγράφει ένα Inter Access Point Protocol το οποίο παρέχει τις αναγκαίες πληροφορίες που χρειάζονται να ανταλλάξουν τα Access Points προκειμένου να υποστηριχθούν οι λειτουργίες των συστημάτων διανομής του προτύπου 802.11, δηλαδή περιαγωγή.

Εν απουσία του προτύπου 802.11f, θα πρέπει να χρησιμοποιείται ο ίδιος κατασκευαστής για τα Access Points έτσι ώστε να διασφαλίζεται η διαλειτουργικότητα για τους περιπλανώμενους χρήστες. Σε ορισμένες περιπτώσεις μία ανάμιξη από Access Points διαφορετικών κατασκευαστών μπορεί να λειτουργήσει, ειδικά αν τα Access Points έχουν πιστοποίηση Wi – Fi. Η προσμέτρηση του προτύπου 802.11f στο σχεδιασμό των Access Points ενδεχομένων να αυξήσει τις εναλλακτικές λύσεις και να προσθέσει μερικώς ασφάλεια διαλειτουργικότητας όταν πρόκειται να γίνει επιλογή για Access Points διαφορετικών κατασκευαστών.

3.5.9.8 802.11g – Υψηλότεροι Ρυθμοί Μετάδοσης στην μπάντα των 2,4 GHz :

Τον Ιούνιο του 2003 η ομάδα εργασίας IEEE ολοκλήρωσε τις εργασίες τις και εξέδωσε το πρότυπο 802.11g, το οποίο επεκτείνει το 802.11b προσφέρει ρυθμούς μετάδοσης μέχρι 54 Mbps αλλά και συμβατότητα με το 802.11b. Χρησιμοποιεί και αυτό την ISM μπάντα των 2,4 GHz. Σε αντίθεση με το 802.11b χρησιμοποιεί την OFDM για να πετύχει τους επιθυμητούς ρυθμούς μετάδοσης.

Το πιο σημαντικό χαρακτηριστικό του 802.11g είναι η συμβατότητά του με το 802.11b. Το 802.11b ως γνωστών αποτελεί σήμερα το φυσικό στρώμα που υλοποιείται στα περισσότερα προϊόντα ασύρματης δικτύωσης. Το 802.11g λειτουργώντας ταυτόχρονα με το 802.11b μπορεί να το αντικαταστάσει σταδιακά εξολοκλήρου.

Σημειώνεται τέλος ότι προϊόντα που βασίζονται στο 802.11g είχαν αρχίσει να κυκλοφορούν στην αγορά αρκετά πριν την ανακοίνωση του τελικού προτύπου. Βασίζονταν σε ενδιάμεσες εκδόσεις του προτύπου και οι κατασκευαστές τους υπόσχονταν πλήρη συμβατότητα με την τελική μορφή.

3.5.9.9 802.11h – Διαχείριση Φάσματος στο 802.11a (Spectrum Managed 802.11a) :

Το 802.11h απευθύνεται και καλύπτει τις απαιτήσεις των Ευρωπαϊκών κανονισμών. Παρέχει Dynamic Channel Selection (DCS) – δυναμική επιλογή καναλιών και Transmit Power Control (TPC) – έλεγχο μετάδοσης ισχύος, για συσκευές που λειτουργούν στη μπάντα των 5 GHz (802.11a). Στην Ευρώπη υπάρχει εν δυνάμει πιθανότητα το 802.11a να έχει παρεμβολές με τις δορυφορικές επικοινωνίες. Με τη χρήση των DCS και TPC, το 802.11h θα αποφύγει τις παρεμβολές.

Προκειμένου να υλοποιήσει το DCS και TCP, το 802.11h αναπτύσσει πρακτικές που επηρεάζουν αμφότερα τα υποστρώματα MAC και PHY. Με το να συμπεριληφθούν το DCS και το TPC, το 802.11h θα μπορέσει να γίνει ο διάδοχος του 802.11a. Ευτυχώς, δεν υπάρχουν ζητήματα μη καλής διαλειτουργικότητας ανάμεσα σε υπάρχοντα 802.11a και 802.11h χρήστες και access points. Τα καλά νέα είναι ότι το 802.11h ενισχύει πωλήσεις 802.11a δικτύων στην Ευρώπη, πράγμα που ενδεχομένως να έχει ως αποτέλεσμα υψηλότερους όγκους πωλήσεων και χαμηλότερες τιμές.

3.5.9.10 802.11i – Ενίσχυση των Χαρακτηριστικών του MAC για Ενισχυμένη Ασφάλεια:

Πρόκειται για το πρότυπο που μελετά θέματα ασφαλείας στα WLAN. Είναι σαφές ότι τα ενσύρματα LAN είναι πιο ασφαλή από ότι τα ασύρματα και αυτό οφείλεται στους παρακάτω δύο λόγους :

Στα WLAN το μέσο μετάδοσης (Ασύρματο κανάλι) έχει συγκεκριμένες δυνατότητες απόδοσης και εμφανίζει σημαντικές και μεγάλες διαφορές συγκρινόμενο με το ασύρματο κανάλι των LANs. Κάτι τέτοιο οφείλεται προφανώς στην ασύρματη φύση του καναλιού και στο ότι παρουσιάζει μεγάλες μεταβολές με το πέρασμα του χρόνου.

Ο οποιοσδήποτε μπορεί να έχει πρόσβαση στο κανάλι μετάδοσης (αέρας), κάτι που δεν ισχύει στα ενσύρματα δίκτυα.

Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται σήμερα, όπως ο WEP (Wired Equivalent Privacy), ο WPA (Wi-Fi Protected Access) και IP SEC παρουσιάζουν κάποια προβλήματα.

Για παράδειγμα ο πρώτος εμφανίζει σημαντικά κενά ασφαλείας, ο WPA ενώ έρχεται να καλύψει τα κενά του WEP, στην πραγματικότητα δεν καλύπτει την ουσιαστική ασφάλεια στα ασύρματα τοπικά δίκτυα. Τέλος ο IP SEC εφαρμόζεται τοπικά σε κάθε χρήστη και καλύπτει Point-to-Point συνδέσεις.

Η ομάδα εργασίας θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου πρωτοκόλλου ασφαλείας προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του. Η αρχική προσέγγιση προσανατολίζεται στην αύξηση του μήκους κλειδιού, έτσι ώστε brute force επιθέσεις σε αυτόν να έχουν απαγορευτικούς χρόνους επιτυχίας με την υπάρχουσα τεχνολογία. Δυστυχώς και πάλι μπορούν να χρησιμοποιηθούν σχεδιαστικές ατέλειες που θα καταστήσουν έναν τέτοιο αλγόριθμο ανασφαλή. Έτσι η ομάδα εργασίας προσανατολίζεται στην δημιουργία του προτύπου IEEE 802.11i (Extensible Authentication Protocol-EAP, Advanced Encryption Standard-AES, Temporal Key Integrity Protocol-TKIP, Robust Security Network-RSN). [3]

3.6. ΑΣΦΑΛΕΙΑ ΑΣΥΡΜΑΤΩΝ ΤΟΠΙΚΩΝ ΔΙΚΤΥΩΝ

Τα πλεονεκτήματα που προκύπτουν από τις τεχνολογίες WLAN είναι αναμφίβολα πολλά, με σημαντικότερο, στις περισσότερες περιπτώσεις, την ευελιξία που παρέχουν. **Παρόλα αυτά, ο τρόπος με τον οποίο πραγματοποιείται η διακίνηση της πληροφορίας παρουσιάζει κάποιες αδυναμίες, κυρίως όσον αφορά στην ασφάλεια.** Στο πρότυπο 802.11 b, τα δεδομένα εκπέμπονται, όπως αναφέρθηκε, στη φασματική περιοχή των 2,4GHz, σε συχνότητες που μπορούν εύκολα να διαπεράσουν κάποια τυπική τοιχοποιία και μεταλλική κατασκευή.

Το γεγονός ότι τα δεδομένα που διακινούνται ανά πάσα στιγμή στο δίκτυο, διαχέονται "ελεύθερα" στον περιβάλλοντα χώρο, επιτρέπει σε κάθε περαστικό, με ένα laptop να συνδεθεί στο δίκτυο και να το χρησιμοποιήσει με καλούς ή κακούς σκοπούς.

Γενικά, οι "επιθέσεις" που είναι πιθανόν να δεχτεί ένα ασύρματο δίκτυο, χωρίζονται σε δύο βασικούς τύπους. :

Ο πρώτος αποτελείται από επιθέσεις που έχουν βασικό σκοπό την υποκλοπή των πληροφοριών που διακινούνται. Στόχος των παραπάνω επιθέσεων είναι τις περισσότερες φορές τα εταιρικά δίκτυα, στα οποία ανταλλάσσονται αρκετά "ευαίσθητες", τόσο για την εταιρεία όσο και τους ανταγωνιστές της, πληροφορίες.

Ο δεύτερος τύπος περιλαμβάνει επιθέσεις, με τις οποίες ένας "κακόβουλος" επισκέπτης προσπαθεί να αποκτήσει πρόσβαση και να χρησιμοποιήσει "προσωρινά" ένα ασύρματο δίκτυο. Δεδομένων των παραπάνω κινδύνων και έχοντας ως στόχο την αύξηση της ασφάλειας των ασύρματων δικτύων, το IEEE έχει ενσωματώσει στο πρότυπο 802.11 μεθόδους, που συντελούν στην αύξηση της ασφάλειας του ασυρμάτου δικτύου (Basic Industry Standard Security).

Η πρώτη και λιγότερο ασφαλής, είναι η χρήση του **"κωδικού του δικτύου" SSID (Secure Set Identifier).** Πρόκειται για το χαρακτηριστικό όνομα ενός ασύρματου δικτύου, το οποίο χρησιμοποιείται για να διαφοροποιούνται τα δίκτυα, που ενδεχομένως λειτουργούν στον ίδιο χώρο. Γενικά, όλες οι συσκευές ασύρματης σύνδεσης έχουν μια προκαθορισμένη τιμή του SSID, τυπική για κάθε μοντέλο. Για να διευκολυνθεί η διαδικασία σύνδεσης δύο συσκευών WLAN, κάθε συσκευή εκπέμπει ανά τακτά χρονικά διαστήματα το SSID της.

Έτσι, όταν δύο συσκευές βρεθούν μέσα στα όρια εμβέλειας τους, αυτομάτως αναγνωρίζουν η μία την άλλη και στη συνέχεια, μπορούν, εφόσον έχουν το ίδιο SSID, να συνδεθούν. Αν και ο παραπάνω μηχανισμός απλοποιεί σημαντικά τη διαδικασία σύνδεσης δύο ή περισσότερων "φιλικών" υπολογιστών, εγκυμονεί κινδύνους, διότι βοηθά σημαντικά πιθανούς "εχθρούς" να εντοπίσουν το εν λόγω δίκτυο. Ο μόνος τρόπος με τον οποίο μπορεί να περιοριστεί ο παραπάνω κίνδυνος είναι να αποτραπεί η αυτόματη εκπομπή του SSID, μια δυνατότητα που προσφέρεται μόνο από τα Σημεία Πρόσβασης. Συνοψίζοντας, **όταν χρησιμοποιείται ένα Σημείο Πρόσβασης, ένα πρώτο μέτρο ασφάλειας που μπορεί κανείς να πάρει, είναι να απενεργοποιήσει την εκπομπή του SSID και να αλλάξει το όνομα του δικτύου, με κάποιο δύσκολα προβλεπόμενο.**

3.6.1 Κρυπτογράφηση Δεδομένων :

Το πρότυπο 802.11b περιλαμβάνει, μία μέθοδο κρυπτογράφησης δεδομένων, που ονομάζεται **WEP (Wireless Equivalent Privacy).** Η WEP βασίζεται στον αλγόριθμο κρυπτογράφησης RC4, ο οποίος χρησιμοποιεί ένα κλειδί μεγέθους 40bit ή 104bit και έναν τυχαίο αριθμό, που ονομάζεται "διάνυσμα έναρξης" Initialization Vector και έχει μήκος 24bit.

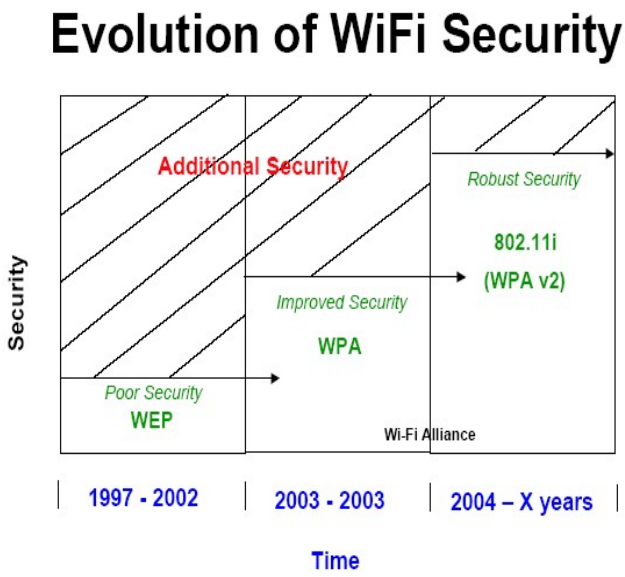
Οι συσκευές μάλιστα που ακολουθούν το πρότυπο 802.11b+ της Texas Instruments, υποστηρίζουν κωδικοποίηση με κλειδί μήκους 256bit (τυχαίος αριθμός 24bit και κλειδί 232bit). Λόγω όμως κάποιων εγγενών αδυναμιών του αλγορίθμου RC4, η υποκλοπή του χρησιμοποιούμενου κλειδιού είναι εφικτή. **Μια τακτική που μπορεί να δυσκολέψει τους πιθανούς "εισβολείς" είναι να χρησιμοποιείται κλειδί μεγάλου μεγέθους (128bit ή 256bit), το οποίο πρέπει να αλλάζει αρκετά συχνά.** Ένας οργανωμένος cracker, μπορεί, χρησιμοποιώντας τα κατάλληλα εργαλεία λογισμικού, όπως το AirSnort (airsnort.shmoo.com), να συλλέξει μερικά εκατομμύρια πακέτα κλειδιών και να "σπάσει" το WEP.

Βλέποντας τη μάλλον απαράδεκτη κατάσταση, οι εταιρείες προχώρησαν στην ενίσχυση της ασφάλειας, σχεδιάζοντας το WiFi Protected Access (WPA), το οποίο βελτιώνει το WEP. Η βελτίωση έχει δύο πυλώνες. Ο πρώτος συνίσταται στην αύξηση του μήκους του διανύσματος έναρξης σε 48bit (από 24), αυξάνοντας εκθετικά το χρόνο που απαιτείται για την παραβίαση του. Ο δεύτερος είναι η αλλαγή του αλγόριθμου κρυπτογράφησης από τον πεπαλαιωμένο και αδύναμο πλέον RC4, στον TKIP (Temporal Key Integrity Protocol). Ο TKIP επιτρέπει το συχνό μετασχηματισμό των κλειδιών κρυπτογράφησης, με χρήση μιας συνάρτησης κατακερματισμού (hash function).

Στη συνέχεια, διασφαλίζει ότι τα κλειδιά αυτά είναι αυθεντικά και όχι κάποια που προσπάθησε να "βάλε" στο κανάλι κάποιος "κακόβουλος". Παράλληλα, η πιστοποίηση όσων έχουν πρόσβαση στο δίκτυο, γίνεται με ένα σύστημα δημόσιου κλειδιού, ανάλογου με αυτό που χρησιμοποιείται στην κινητή τηλεφωνία.

Το WPA είναι αρκετά πιο ασφαλές από το διάτρητο WEP, αλλά σχετικές έρευνες έδειξαν ότι έχει και αυτό τις αδυναμίες του, ιδιαίτερα όταν χρησιμοποιείται συνθηματική φράση με λιγότερους από 20 χαρακτήρες. Η ασφάλεια σε απαιτητικά εταιρικά περιβάλλοντα, βελτιώνεται με τη χρήση κεντρικού διακομιστή ελέγχου της πρόσβασης. Η διαδικασία είναι περίπλοκη και περιγράφεται από την προδιαγραφή ασφαλείας RADIUS. Δυστυχώς, τέτοιοι μηχανισμοί δεν μπορούν εύκολα να προσαρμοσθούν σε μικρά "οικιακά" ασύρματα δίκτυα. [10]

Στην παρακάτω εικόνα γίνεται μια αναδρομή στους διάφορους αλγορίθμους κρυπτογράφησης : [2]



Εικόνα 3.20. : Αλγόριθμοι Κρυπτογράφησης

ΚΕΦΑΛΑΙΟ 4 :
WLAN HOTSPOTS

4.1. ΕΙΣΑΓΩΓΗ

Η δωρεάν ασύρματη πρόσβαση στο Δίκτυο σε δημόσιους χώρους προτάθηκε από τον Μπρετ Στιούαρτ σε ένα συνέδριο στο Σαν Φρανσίσκο το 1993. Ο όρος « hotspot » επινοήθηκε από τη Nokia πέντε χρόνια μετά. Από τότε, τα hotspots αυξάνονται και πληθύνονται παγκοσμίως τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Πολλές επιχειρήσεις, μεγάλα ξενοδοχεία, ενοικιαζόμενες εξοχικές κατοικίες, ακόμη και αεροδρόμια παρέχουν πρόσβαση στους πελάτες τους, προκειμένου να αποκτήσουν πλεονέκτημα έναντι των ανταγωνιστών τους. ***Στις πόλεις, τα* hotspots *βρίσκονται συνήθως σε εστιατόρια, σιδηροδρομικούς σταθμούς, αεροδρόμια, βιβλιοθήκες, καφετερίες, βιβλιοπωλεία, βενζινάδικα, ακόμη και σούπερ μάρκετ!***

Η πόλη της Σιγκαπούρης είναι πρωτοπόρος στην πρόσβαση στο Διαδίκτυο. Τον περασμένο Δεκέμβριο η κυβέρνηση ανακοίνωσε ότι σε λίγο καιρό όλο το νησί θα έχει δωρεάν ασύρματη πρόσβαση στο Ιντερνετ και περισσότεροι από 400.000 Σιγκαπούριοι έχουν ήδη εγγραφεί στην υπηρεσία.

Ο δήμαρχος του Σαν Φρανσίσκο υποσχέθηκε δωρεάν ασύρματη πρόσβαση στο Ιντερνετ από κάθε σημείο της πόλης μέσα στον επόμενο χρόνο.

Στην πρωτεύουσα της Εσθονίας, το Ταλίν, υπάρχουν hotspots σε όλη την πόλη, στα μπαρ, τα ξενοδοχεία, τα πάρκα, παντού! Ο κάτοικος ή επισκέπτης του Ταλίν μπορεί εύκολα να τα εντοπίσει. Το μόνο που έχει να κάνει είναι να ακολουθήσει τις πινακίδες που υπάρχουν σε κάθε δρόμο της πόλης.

Όσο για τη Νέα Υόρκη, το Παρίσι και το Λονδίνο οι πόλεις αυτές χορεύουν στους ρυθμούς της ευρυζωνικότητας και τα wifi hotspots υπάρχουν σε κάθε γωνιά τους.

Το παράδειγμα ξένων αγορών δείχνει ότι η δημιουργία των hotspots αποτελεί πεδίο δράσης τόσο για τους παραδοσιακούς τηλεπικοινωνιακούς οργανισμούς όσο και για τους παρόχους υπηρεσιών διαδικτύου (ISP). **Στην Ελλάδα δραστηριοποιούνται ήδη αρκετοί πάροχοι, ISP και εναλλακτικοί πάροχοι τηλεφωνίας, εγκαθιστώντας δίκτυα hotspots με το brand του παρόχου.** Παράλληλα, στο χώρο δραστηριοποιούνται και ένα πλήθος μικρών μελετητικών γραφείων που αναλαμβάνουν την ανάπτυξη ιδιωτικών hotspot σε ιδιωτικές εταιρείες και οργανισμούς τοπικής αυτοδιοίκησης.

Οι κυριότεροι λόγοι οι οποίοι οδηγούν στην ανάπτυξη υποδομών WiFi Hotspot είναι :

- Η ευρυζωνικότητα διαδίδεται με πολύ γρήγορους ρυθμούς και είναι πλέον ιδιαίτερα δημοφιλής.
- Αυξάνεται η ανάγκη του κοινού για ασύρματη πρόσβαση στο Internet μέσω φορητών συσκευών.
- Καθιερώνεται ο συνεδριακός τουρισμός, με υψηλές τηλεπικοινωνιακές απαιτήσεις, ως βασική στρατηγική επιλογή των μεγάλων ξενοδοχείων.
- Εντείνεται ο ανταγωνισμός για παροχή πρόσβασης στο Internet με αξιοποίηση όλων των τεχνολογιών. [11] [12]

4.2. ΕΠΙΧΕΙΡΗΣΕΙΣ, ΠΟΛΙΤΕΣ ΚΑΙ HOTSPOTS

Η δομή των σύγχρονων, ανοιχτών, οικονομιών βασίζεται ολοένα και περισσότερο σε ευέλικτες δικτυακές υποδομές, καινούργιες υπηρεσίες, με νέα μοντέλα χρήσης, καθώς και σε εφαρμογές προστιθέμενης αξίας, των οποίων η επιτυχία αλλά και η, εν γένει, αποδοχή, εξαρτάται από την ύπαρξη και ευρεία διάδοση τέτοιων υποδομών.

Η παροχή, λοιπόν, ευρυζωνικών υπηρεσιών σε μετακινούμενους πολίτες – επισκέπτες δημοσίων ή και ιδιωτικών χώρων, σε πελάτες και εργαζόμενους επιχειρήσεων, είναι αναγκαία ώστε να έχουν τη δυνατότητα μεταφοράς μεγάλου όγκου πληροφοριών, με έμφαση στη δυνατότητα σύνδεσης με παρόχους πολυμεσικού περιεχομένου και εφαρμογών (multimedia content), καθώς επίσης και τη μετάδοση καλής ποιότητας video με δυνατότητα διαδραστικότητας με το χρήστη.

Άλλοι χώροι, εκτός των εγκαταστάσεων επιχειρήσεων για την περίπτωση των εργαζομένων σε αυτές, που μπορούν να προσφέρονται τέτοιου είδους υπηρεσίες περιλαμβάνουν ξενοδοχεία, εμπορικά κέντρα, πολυκαταστήματα, χώρους αναψυχής, συνεδριακά κέντρα, καφέ, εστιατόρια κλπ. **Οι χώροι αυτοί ονομάζονται και Σημεία Ασύρματης Ευρυζωνικής Πρόσβασης (Wireless Hotspots).**

Λαμβάνοντας υπόψη ότι ο ρόλος των ευέλικτων ασυρματικών δικτύων στην δραστηριότητα των επιχειρήσεων είναι, σε διεθνές επίπεδο αναγνωρισμένος, ως ιδιαίτερα σημαντικός, οι τρόποι με τους οποίους θα διαδοθεί και θα μεγιστοποιηθεί η χρήση τους πρέπει να αποτελούν θέμα προβληματισμού μιας ευρύτερης κοινότητας συμμετοχόντων και συνεργατών. Η δυναμική αλλά και η εξέλιξη του ζητήματος, τόσο σε τεχνολογικό όσο και σε θεσμικό επίπεδο, υποχρεώνει όλους, κατά κάποιο τρόπο, προς μια τέτοια αντίληψη.

Σε κάθε περίπτωση, τα HotSpots μπορούν να βρουν εφαρμογή σε πλήθος περιπτώσεων. Μπορούν, δηλαδή, να αποτελέσουν χρήσιμο εργαλείο για:

- μικρές και ατομικές επιχειρήσεις, αντικαθιστώντας ουσιαστικά την ενσύρματη δικτυακή υποδομή στο χώρο της επιχείρησης.
- οικιακούς χρήστες για την πρόσβαση σε κοινές δικτυακές υποδομές (π.χ. σύνδεση ADSL) ή και για την διευκόλυνση της επικοινωνίας χωρίς καλώδια.
- χρήστες και επιχειρήσεις οι οποίοι επιθυμούν μια σημειακή σύνδεση με κάποιον κοντινό χρήστη ή υποκατάστημα.
- ιδιοκτήτες δημόσιων χώρων συγκέντρωσης (καφετέριες, αεροδρόμια, πλατείες κτλ.) οι οποίοι επιθυμούν να παρέχουν υπηρεσίες πρόσβασης σε υπηρεσίες περιεχομένου ή διαδικτύου στους επισκέπτες τους. **[13]**

4.3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΕΝΟΣ ΔΗΜΟΣΙΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΑΝΟΙΧΤΟΥ ΧΩΡΟΥ

Για ένα τυπικό δημόσιο ασύρματο δίκτυο ανοιχτού χώρου, τα χαρακτηριστικά που θα πρέπει να ληφθούν υπόψη κατά το σχεδιασμό του είναι τα ακόλουθα :

- **Ελάχιστος Ρυθμός Μετάδοσης Χρηστών**: Της τάξης των 50-100Kbps ανά χρήστη. Ο μέγιστος ρυθμός μπορεί να φτάσει στο όριο της χρησιμοποιούμενης ασύρματης τεχνολογίας (π.χ. 802.11b, 802.11g) σε συνδυασμό με το μέγιστο ρυθμό παροχής της σύνδεσης με το Διαδίκτυο.

- **Πυκνότητα Χρηστών**: Μικρή, με δυνατότητα επέκτασης

- **Υπηρεσίες**: Πρόσβαση στο Διαδίκτυο, μέσω της οποίας παρέχονται όλες οι αντίστοιχες υπηρεσίες όπως: Παγκόσμιος Ιστός (www), Ηλεκτρονική Αλληλογραφία (e-mail), Σύγχρονη Γραπτή Επικοινωνία (chat), Μεταφορά Αρχείων (ftp), κ.α.

- **Περιαγωγή**: Λόγω της έκτασης ενός τέτοιου δικτύου, υπάρχει απαίτηση για δυνατότητα περιαγωγής (roaming). Με αυτό τον τρόπο θα είναι εφικτό για κάθε χρήστη να μετακινείται μεταξύ των διαφορετικών σημείων πρόσβασης κρατώντας τα ίδια συνθηματικά και όνομα.

- **Ασφάλεια**: Συνήθως δεν παρέχεται ασφάλεια στο επίπεδο του ασύρματου δικτύου. Ο χρήστης προειδοποιείται για το συγκεκριμένο χαρακτηριστικό του δικτύου και του προτείνεται η λήψη καταλλήλων μέτρων (κυρίως η επίτευξη ασφάλειας με τη χρήση κατάλληλων εφαρμογών). Ασφάλεια μπορεί να επιτευχθεί μέσω της τεχνικής Μετάφρασης Διευθύνσεων (Network Address Translation), ενώ για την περαιτέρω προστασία των χρηστών προτείνεται η χρήση προσωπικού firewall από τους ίδιους.

- **Διαθεσιμότητα**: Παρέχεται συνήθως υψηλή διαθεσιμότητα όσον αφορά την καλυπτόμενη περιοχή (αλληλοεπικάλυψη με πολλαπλά hotspot) και όσον αφορά την προσβασιμότητα στο Διαδίκτυο με συνδεσιμότητα ανάνηψης από σφάλματα (fail-over) και κατανομής φορτίου (load-balancing).

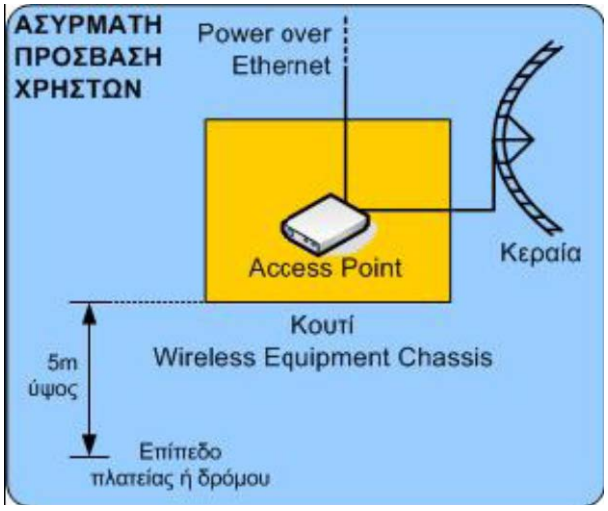
Οι παραπάνω επιλογές ουσιαστικά περιορίζουν και αποκλείουν κάποιες υπηρεσίες και χαρακτηριστικά, όπως π.χ. αποδοτική μετάδοση ζωντανού video σε υψηλή ανάλυση λόγω σχετικά χαμηλού ρυθμού μετάδοσης, αποδοτική απομακρυσμένη εργασία μέσω δικτύου (NFS, κλπ.) λόγω ενδεχομένων διακοπών στη σύνδεση, μαζική λήψη μεγάλων αρχείων μέσω συστημάτων Peer-to-Peer λόγω σχετικά χαμηλού ρυθμού μετάδοσης, ασφαλή μετάδοση ευαίσθητων πληροφοριών (π.χ. ιατρικών) λόγω μη παροχής ασφάλειας στο επίπεδο του δικτύου, κλπ.

4.4. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΕΝΟΣ ΔΗΜΟΣΙΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΑΝΟΙΧΤΟΥ ΧΩΡΟΥ

Το Δημόσιο Ασύρματο Δίκτυο Ανοιχτού Χώρου σχεδιάζεται ως ένα ολοκληρωμένο πληροφοριακό σύστημα, το οποίο προσφέρει ασύρματη πρόσβαση στο Διαδίκτυο. Το συνολικό σύστημα χωρίζεται σε επιμέρους υποσυστήματα, καθένα από τα οποία εξυπηρετεί κάποια ξεχωριστή λειτουργία που είναι απαραίτητη για την ολοκλήρωση των υπηρεσιών που παρέχονται στους τελικούς χρήστες. Η μεταφορά των δεδομένων από τα Σημεία Ασύρματης Πρόσβασης Χρηστών στα Περιφερειακά Σημεία Συλλογής γίνεται ενσύρματα (Ethernet), ενώ από τα Περιφερειακά Σημεία Συλλογής προς το Κεντρικό Σημείο Διασύνδεσης ασύρματα (IEEE 802.11b).

4.4.1. Υποσύστημα Ασύρματης Πρόσβασης Χρηστών :

Η παροχή τελικών ασύρματων δικτυακών υπηρεσιών προς το χρήστη επιτυγχάνεται με τη χρήση των Hotspot. **Κάθε Hotspot, αποτελείται ουσιαστικά από μία συσκευή Access Point, ένα κουτί (wireless equipment chassis) μέσα στο οποίο τοποθετείται το Access Point και μία κεραία** (*βλ. Εικόνα 4.1*). Σκοπός των κουτιών είναι η προστασία των Access Point από τις καιρικές συνθήκες, αλλά και η κατάλληλη εμφάνιση προκειμένου να μην έρχονται σε αντίθεση με τη αισθητική του χώρου εγκατάστασης. Η κατάλληλη εμφάνιση μπορεί να επιτευχθεί με κατάλληλη διακόσμηση ή χρωματισμό.



Εικόνα 4.1. : Wireless Hotspot

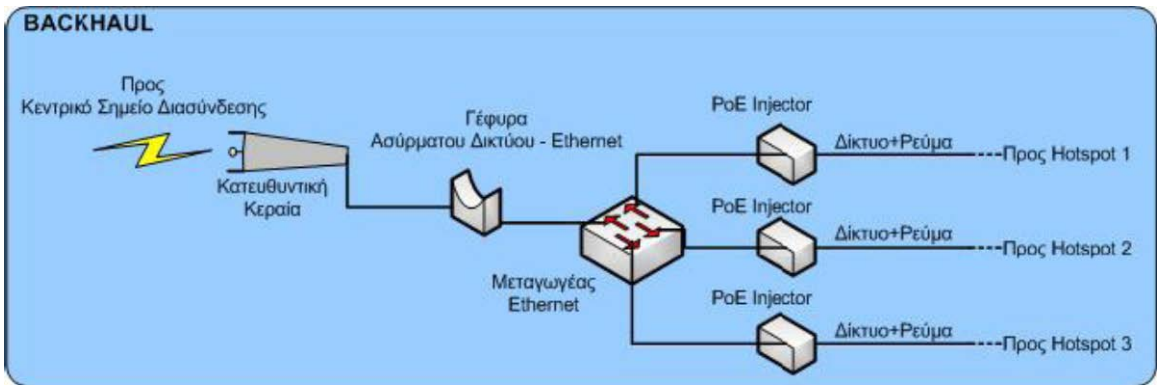
Τα κουτιά που θα φιλοξενούν τα Hotspot εγκαθίστανται σε ύψος το πολύ 5 μέτρων από το επίπεδο των χρηστών στο συγκεκριμένο σημείο. Σε κάθε κουτί καταλήγει ένα καλώδιο δικτύου (cat. 5e). Μέσα από το καλώδιο αυτό θα μεταφέρονται και τα δικτυακά δεδομένα, αλλά και η απαραίτητη ισχύς για την λειτουργία του hotspot. **Η τεχνολογία που επιτρέπει την μεταφορά ηλεκτρικής ισχύς μέσα από τυπικά καλώδια δικτύου ονομάζεται Power Over Ethernet (PoE) και είναι ιδιαίτερα διαδεδομένη σε τέτοιου είδους εφαρμογές.** Το καλώδιο αυτό ξεκινά από το σημείο όπου έχει εγκατασταθεί ένα Περιφερειακό Σημείο Συλλογής (Υποσύστημα Backhaul).

Η λειτουργία που επιτελεί κάθε ένα από τα ασύρματα hotspot είναι να συλλέγει την ασύρματη κίνηση που βρίσκεται στην ακτίνα κάλυψής του, να την μετατρέπει σε ενσύρματη κίνηση τύπου Ethernet και να την προωθεί προς το Υποσύστημα Backhaul.

4.4.2. Υποσύστημα Backhaul :

Το Υποσύστημα Backhaul (*βλ. Εικόνα 4.2*) **περιλαμβάνει μία ασύρματη γέφυρα (wireless bridge), μια κατευθυντική κεραία, ένα μικρό μεταγωγέα (switch) και συσκευές power-over-ethernet injectors.** Η ασύρματη γέφυρα είναι μια δικτυακή συσκευή η οποία ενσωματώνει το κατάλληλο λογισμικό για την υλοποίηση ασύρματων πρωτοκόλλων, προκειμένου να ενώσει το τοπικό δίκτυο που δημιουργείται από τα Hotspot με το κεντρικό δίκτυο.

Ο μεταγωγέας χρησιμεύει για την διασύνδεση των δικτύων των Hotspot, ενώ οι συσκευές power-over-ethernet injectors αναλαμβάνουν να πολυπλέξουν το σήμα του δικτύου και την παροχή ρεύματος για κάθε Hotspot σε ένα μόνο καλώδιο (cat 5e).



Εικόνα 4.2. : Υποσύστημα Backhaul

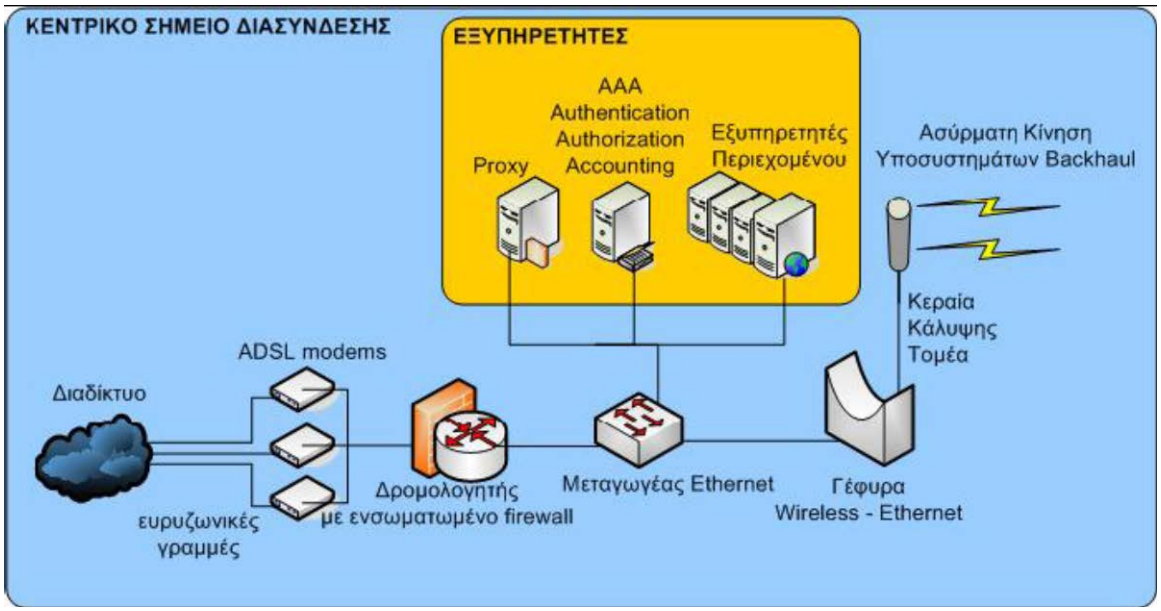
Το Υποσύστημα Backhaul είναι τοποθετημένο σε σχετικά μεγάλο ύψος (π.χ. στην ταράτσα ενός κτιρίου) όσο το δυνατόν πιο κοντά σε μία ομάδα Σημείων Ασύρματης Πρόσβασης (hotspot). *Χρησιμοποιώντας την κατευθυντική κεραία, το Υποσύστημα Backhaul συνδέεται με το Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.*

Η λειτουργία που επιτελεί κάθε ένα από τα υποσυστήματα Backhaul είναι να συλλέγει τη κίνηση από το επιμέρους hotspot που είναι τοποθετημένα στο επίπεδο των χρηστών (π.χ. επίπεδο κάποιας πλατείας), να την μετατρέπουν σε ασύρματη μορφή τύπου 802.11b και να την προωθούν προς το Κεντρικό Σημείο Διασύνδεσης.

Για να μην υπάρχουν παρεμβολές ανάμεσα στις συχνότητες των Σημείων Ασύρματης Πρόσβασης με τις συχνότητες επικοινωνίας των συστημάτων Backhaul με το Κεντρικό Σημείου Διασύνδεσης, καλό είναι να χρησιμοποιηθεί το κανάλι 13. Λαμβάνοντας υπόψη ότι τα κανάλια που έχουν χρησιμοποιηθεί για τα Σημεία Ασύρματης Πρόσβασης είναι τα 1, 6 και 11, η χρήση του καναλιού 13 είναι η καλύτερη επιλογή. Στην περίπτωση που παρατηρηθούν παρεμβολές από τη χρήση των συγκεκριμένων καναλιών, μπορεί να γίνει χρήση διαφορετικών καναλιών για την κάθε περίπτωση. Συγκεκριμένα μπορούν να χρησιμοποιηθούν τα κανάλια 1, 5 και 9 για τα Σημεία Ασύρματης Πρόσβασης και το 13 για την επικοινωνία των συστημάτων Backhaul με το Κεντρικό Σημείου Διασύνδεσης.

4.4.3. Υποσύστημα Κεντρικού Σημείου Διασύνδεσης :

Το Κεντρικό Σημείο Διασύνδεσης (*βλ. Εικόνα 4.3*) είναι το υποσύστημα που συνδέει όλη την δικτυακή υποδομή με το δίκτυο κορμού (Διαδίκτυο). Εκεί γίνεται η εγκατάσταση των ευρυζωνικών γραμμών πρόσβασης στο Διαδίκτυο (ευρυζωνικές υπηρεσίες σταθερής πρόσβασης μεσαίας ταχύτητας - xDSL). Επίσης, εκεί εγκαθίστανται ένας κεντρικός εξυπηρετητής, που αναλαμβάνει να ενοποιεί τις ευρυζωνικές γραμμές σε μία εικονική πύλη στο Διαδίκτυο – Internet gateway, ο εξυπηρετητής AAA που αναλαμβάνει την πιστοποίηση της ταυτότητας των χρηστών του δικτύου, οι εξυπηρετητές περιεχομένου που φιλοξενούν διάφορες ηλεκτρονικές υπηρεσίες για τους χρήστες και ο κεντρικός μεταγωγέας.



Εικόνα 4.3 : Κεντρικό Σημείο Διασύνδεσης

Ο παραπάνω εξοπλισμός συνδέεται σε κάποιο σημείο σε μεγάλο ύψος (π.χ. ταράτσα κτιρίου) όπου εγκαθίσταται και η κεντρική ασύρματη γέφυρα, η οποία μέσω μιας κεραίας κάλυψης τομέα (sector antenna) θα επικοινωνεί με τις αντίστοιχες γέφυρες στις οροφές των διάφορων περιφερειακών κτιρίων (point-to-multipoint communication). Λόγω των κατευθυντικών κεραιών που χρησιμοποιούν τα Υποσυστήματα Backhaul, η επικοινωνία με την κεντρική Κεραία Κάλυψης Τομέα πραγματοποιείται χωρίς ιδιαίτερες παρεμβολές.

4.4.3.1. Γραμμές Ευρυζωνικής Πρόσβασης :

Ο κεντρικός εξυπηρετητής διαμοιράζει τον φόρτο των εξερχόμενων πακέτων δικτύου στις ευρυζωνικές γραμμές – τύπου ADSL, μέσω των αντίστοιχων, ανεξάρτητων συνδέσεων που θα έχει με κάθε μια από τις συσκευές ADSL modem/router (modem/δρομολογητές ADSL). Σε κάθε μια από τις συσκευές αυτές θα καταλήγει και από μία γραμμή ευρυζωνικής πρόσβασης.

4.4.3.2. Λογισμικό Εξυπηρετητών :

Εκτός από τη ρύθμιση των ασύρματων συσκευών, ώστε αυτές να λειτουργούν όπως περιγράφεται παραπάνω, θα πρέπει να γίνει εγκατάσταση και ρύθμιση του λογισμικού των εξυπηρετητών του Κ.Σ.Δ.

Συνοπτικά σε κάθε έναν από τους εξυπηρετητές θα πρέπει εκτός από το λειτουργικό σύστημα, να είναι εγκατεστημένες και να λειτουργούν απρόσκοπτα οι παρακάτω εφαρμογές:

4.4.3.2.1. Λογισμικό Κεντρικού Εξυπηρετητή

Εφαρμογή διαμοιρασμού του φόρτου εξερχόμενης κίνησης στους τρεις από τους προσαρμογείς δικτύου που θα είναι συνδεδεμένοι οι ASDL modem/δρομολογητές (load-balancing). Σε περίπτωση που οποιαδήποτε γραμμή σταματήσει να λειτουργεί για οποιαδήποτε λόγο, θα πρέπει ο εξυπηρετητής να την παρακάμπτει και να χρησιμοποιεί όσες λειτουργούν (fail-over).

4.4.3.2.2. Λογισμικό Εξυπηρετητή AAA

Εφαρμογή ελέγχου της ταυτότητας των χρηστών μέσω ζευγαριών ονόματος και κωδικού πρόσβασης (username/password pair). Η εφαρμογή αυτή θα πρέπει να επικοινωνεί με κάποιου είδους τοπικό Firewall σε επίπεδο λογισμικού, το οποίο δεν θα επιτρέπει στους μη διαπιστευμένους χρήστες να χρησιμοποιούν το ασύρματο δίκτυο για να προσπελαύνουν το Διαδίκτυο (captive portal). Επίσης, θα πρέπει η εφαρμογή να αποθηκεύει όλες τις πληροφορίες των χρηστών σε κάποιο τρίτο ανεξάρτητο σύστημα, όπως για παράδειγμα μια σχεσιακή βάση δεδομένων ή έναν εξυπηρετητή LDAP.

4.4.3.2.3. Λογισμικό Εξυπηρετητών Περιεχομένου

Πρόκειται για λογισμικό τύπου Εξυπηρετητή Ιστοσελίδων (web server) καθώς και λογισμικό προσωρινής αποθήκευσης ιστοσελίδων (web proxy). Οι Εξυπηρετητές ιστοσελίδων περιέχουν το σύνολο των ιστοσελίδων που είναι αναγκαίες για την παροχή των υπηρεσιών στους χρήστες. Ανάλογα με το είδος του περιεχομένου (δυναμικό, στατικό, κλπ.) ενδέχεται να είναι απαραίτητοι και Εξυπηρετητές Εφαρμογών (Application server) ή/και Εξυπηρετητής Βάσης Δεδομένων (Database Server) προκειμένου να υλοποιηθούν οι διάφορες δικτυακές υπηρεσίες. Θεωρούμε ότι ένα σύνολο τεσσάρων εξυπηρετητών περιεχομένου καλύπτει το σύνολο των υπηρεσιών που θα ήταν χρήσιμες για ένα περιβάλλον δημόσιας ασύρματης δικτυακής πρόσβασης.

4.4.3.2.4. Λογισμικό Ανοιχτού Κώδικα

Όσον αφορά στο είδος του λογισμικού που θα χρησιμοποιηθεί, προτείνεται η χρήση Ελεύθερου Λογισμικού / Λογισμικού Ανοιχτού Κώδικα (ΕΛ/ΛΑΚ) καθώς οι λύσεις αυτές αποτελούν παγκόσμια το εκ των πραγμάτων πρότυπο για αντίστοιχες εγκαταστάσεις. Στο Διαδίκτυο υπάρχει διαθέσιμο λογισμικό ικανό να παρέχει όλες τις υπηρεσίες που χρειάζεται ένα τέτοιο δίκτυο. Προφανώς, απαιτείται η κατάλληλη παραμετροποίηση, εγκατάσταση και ρύθμιση προκειμένου το λογισμικό να καταστεί λειτουργικό για ένα συγκεκριμένο περιβάλλον ασύρματου δικτύου.

4.5. ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

Το δίκτυο θα πρέπει να είναι πλήρως συμβατό με το πρότυπο WiFi (IEEE 802.11b). Οι ασύρματες συνδέσεις και οι ασύρματες γέφυρες στις οροφές των κτιρίων θα πρέπει να λειτουργούν σύμφωνα με το πρότυπο αυτό. Τα Wireless Hotspot θα πρέπει να απαγορεύουν συνδέσεις στο πρότυπο IEEE 802.11g, και να ενημερώνουν τις συσκευές πελάτη να χρησιμοποιήσουν το πρότυπο IEEE 802.11b (όλες οι συσκευές που είναι συμβατές με το πρότυπο IEEE 802.11g έχουν τη δυνατότητα επικοινωνίας και με το πρότυπο IEEE 802.11b). Όλος ο ασύρματος τηλεπικοινωνιακός εξοπλισμός θα πρέπει να είναι συμβατός με το πρότυπο IEEE 802.11g, ώστε να είναι δυνατή η μελλοντική επέκταση της χωρητικότητας του δικτύου χωρίς την ανάγκη προμήθειας επιπλέον εξοπλισμού ή λογισμικού. (Αρχικά προτιμάται το πρότυπο IEEE 802.11b επειδή έχει μεγαλύτερη εμβέλεια λειτουργίας και προκαλεί λιγότερες παρεμβολές στα γειτονικά κανάλια του).

4.6. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

Στο υπο δημιουργία δίκτυο δεν θα υποστηρίζονται ασφαλείς συνδέσεις στο επίπεδο του ασύρματου δικτύου. Τα συστήματα που υλοποιούν πραγματική ασφάλεια σε ασύρματα δίκτυα, έχουν υψηλό κόστος και απαιτούν αντίστοιχη υποστήριξη και από τις συσκευές των χρηστών.

Από την άλλη, ο χρήστης μπορεί εύκολα να χρησιμοποιεί τεχνικές κρυπτογραφίας και κωδικοποίησης δεδομένων στο επίπεδο των εφαρμογών (π.χ. συνδέσεις με secure sockets, εξυπηρετητές που υποστηρίζουν HTTPS, SFTP αντί για FTP, κ.λπ.) καθώς το σύνολο των τερματικών συσκευών υποστηρίζει πλέον αντίστοιχες τεχνικές.

Οι χρήστες θα ενημερώνονται για αυτό με την είσοδό τους στο δίκτυο, μέσω ειδικής ιστοσελίδας που θα τους παρουσιάζει ένα συμφωνητικό χρήσης του δικτύου και μια προειδοποίηση ότι το ίδιο το δίκτυο δεν είναι ασφαλές (welcome screen από το σύστημα captive portal).

Για παράδειγμα, η σχετική προειδοποίηση μπορεί να αναφέρει:

« Στο Ασύρματο Δίκτυο στο οποίο θα συνδεθείτε δεν κρυπτογραφούνται τα δεδομένα σας κατά την μετάδοσή τους. Η ασφάλεια του συστήματός σας και των προσωπικών σας δεδομένων είναι αποκλειστικά δική σας ευθύνη. Σας συνιστούμε την χρήση πρωτοκόλλων ασφαλούς μετάδοσης όπως SMTPs, POPs, IMAPs, SSH, HTTPS, κτλ .».

4.7. ΥΨΗΛΗ ΔΙΑΘΕΣΙΜΟΤΗΤΑ

Για τις ανάγκες ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου, υψηλή διαθεσιμότητα παρέχεται σε 3 διακριτά σημεία του συνολικού συστήματος:

- **Ασύρματη Πρόσβαση Χρηστών**
- **Πρόσβαση στο Διαδίκτυο**
- **Σύστημα Εξυπηρετητών**

Υψηλή διαθεσιμότητα παρέχεται στο κομμάτι της ασύρματης πρόσβασης χρηστών μέσω της ύπαρξης πολλαπλών hotspot. Στην περίπτωση που κάποιο hotspot παρουσιάσει βλάβη, τότε ο χρήστης συνεχίζει να εξυπηρετείται από κάποιο άλλο hotspot. Αν εκείνη η περιοχή δεν καλύπτεται από δεύτερο hotspot, τότε ο χρήστης θα πρέπει να μετακινηθεί σε κάποιο άλλο σημείο της περιοχής όπου συνεχίζει να υπάρχει ασύρματη δικτυακή κάλυψη.

Στο κομμάτι που αφορά στην σύνδεση με το Διαδίκτυο πρέπει να έχει προβλεφθεί η ύπαρξη διαφορετικών ευρυζωνικών γραμμών xDSL. Αν κάποια από τις γραμμές αστοχήσει, τότε η συνολική κίνηση δρομολογείται μέσω των υπολοίπων γραμμών, επιτυγχάνοντας έτσι την συνέχιση της παροχής υπηρεσιών, έστω και με μικρότερο συνολικό ρυθμό μετάδοσης.

Οι κεντρικοί εξυπηρετητές, βρίσκονται μέσα σε ειδικά διαμορφωμένα χώρο και υποστηρίζονται από μηχάνημα αδιάλειπτης παροχής ηλεκτρικού ρεύματος (UPS). Με τον τρόπο αυτό εξασφαλίζεται ότι δεν θα πάψουν να

λειτουργούν εξαιτίας σύντομων διακοπών ρεύματος. Σε περίπτωση διακοπής ρεύματος μεγάλης διάρκειας, δεν προβλέπεται η συνέχιση της παροχής υπηρεσιών. Ο εξοπλισμός των εξυπηρετητών προστατεύεται μέσω της ομαλής τους απενεργοποίησης, μετά από εντολή του συστήματος αδιάλειπτης παροχής ρεύματος. Ειδικά στο θέμα των εξυπηρετητών, υψηλή διαθεσιμότητα μπορεί να επιτευχθεί μέσω χρήσης επιπλέον εφεδρικών μηχανημάτων (σε διατάξεις active-active ή active-passive). Αν και τέτοιες διατάξεις χρησιμοποιούνται ευρέως σε άλλου είδους εφαρμογές, έχουν υψηλό κόστος και εφαρμόζονται κυρίως σε συστήματα mission critical. Δεν προτείνονται λοιπόν για έργα με τις συγκεκριμένες λειτουργικές προδιαγραφές.

Τέλος, η σύνδεση με το Διαδίκτυο ενέχει και κινδύνους όσον αφορά την διαθεσιμότητα των υπηρεσιών, εξαιτίας των δικτυακών επιθέσεων από κακόβουλους τρίτους. **Στην περίπτωση αυτή, υψηλή διαθεσιμότητα παρέχεται μέσω συστήματος firewall,** το οποίο πρέπει να είναι προγραμματισμένο να αποτρέπει το σύνολο των γνωστών Διαδικτυακών επιθέσεων και να παρέχει τη δυνατότητα για την προσθήκη επιπλέον κανόνων για την αντιμετώπιση μελλοντικών τύπων επιθέσεων. Εντούτοις δεν είναι δυνατό να προστατευθεί ένα τέτοιο σύστημα από επιθέσεις τύπο DoS (Denial of Service) καθώς και DDoS (Distributed Denial of Service). Συστήματα τα οποία να προστατεύουν από τέτοιες επιθέσεις είναι σαφώς εκτός των στόχων των συγκεκριμένων έργων και αφορούν κυρίως ιδιαίτερα κρίσιμες υποδομές παροχής υπηρεσιών.

Τέτοιες υποδομές είναι για παράδειγμα Web εξυπηρετητές εμπορικών επιχειρήσεων οι οποίες πραγματοποιούν μεγάλο όγκο πωλήσεων μέσω διαδικτύου, επιχειρήσεων και εταιριών ενημέρωσης – ειδήσεων και ψυχαγωγίας καθώς και κρατικών φορέων οι οποίοι παρέχουν υπηρεσίες προς τους πολίτες ή/και τις επιχειρήσεις κ.λπ.

4.8. ΡΥΘΜΟΣ ΜΕΤΑΔΟΣΗΣ ΔΕΔΟΜΕΝΩΝ

Το πρωτόκολλο IEEE 802.11b είναι σχεδιασμένο για ταχύτητες 11 Mbit/sec. Η ταχύτητα αυτή είναι ονομαστική. Η πραγματική ταχύτητα είναι περίπου η μισή. Όταν η απόσταση είναι μεγάλη ή υπάρχει θόρυβος και παρεμβολές, η ονομαστική ταχύτητα μπορεί να πέσει στα 5.5, 2 και 1 Mbit/sec.

Το πρωτόκολλο IEEE 802.11g είναι σχεδιασμένο για ταχύτητες 54 Mbit/sec. Η ταχύτητα αυτή είναι ονομαστική και η πραγματική είναι πολύ μικρότερη. Όμως παρότι το 802.11g είναι πιο ελκυστικό πρωτόκολλο εξαιτίας του

μεγαλύτερου ρυθμού παροχής δεδομένων που επιτυγχάνει, έχει μικρότερη ακτίνα κάλυψης. *Συνεπώς για την κάλυψη της ίδιας περιοχής απαιτείται η χρήση περισσότερων hotspot 802.11g από ότι 802.11b.*

Οι ευρυζωνικές γραμμές που επιτρέπουν την πρόσβαση στο Διαδίκτυο συνδυάζονται προσφέροντας κάποια συνολική χωρητικότητα και κατ' επέκταση δυνατότητα μετάδοσης δεδομένων. Το σύνολο της συγκεκριμένης χωρητικότητας θα πρέπει να μοιράζεται στο σύνολο των χρηστών του ασύρματου δικτύου Wi-Fi. Αυτό σημαίνει ότι κανένας χρήστης δεν θα έχει προτεραιότητα έναντι κάποιου άλλου. Αν όλοι οι χρήστες μεταφέρουν δεδομένα με τον μέγιστο ρυθμό, τότε κάθε χρήστης θα πάρει το ίδιο ποσοστό του συνολικού ρυθμού μετάδοσης.

Παράδειγμα: Αν ο συνολικός ρυθμός μετάδοσης (download) που προσφέρει το σύνολο των ευρυζωνικών γραμμών είναι 3Mbps, τότε σε ένα σύνολο 30 χρηστών κάθε χρήστης μπορεί να κατεβάζει δεδομένα με ρυθμό 102Kbps. Όμως, στην περίπτωση όπου μόνο ένας χρήστης χρησιμοποιεί την πρόσβαση στο Διαδίκτυο, τότε θα μπορεί να αξιοποιήσει το σύνολο του εύρους, δηλ. και τα 3Mbps.

4.9. ΠΛΗΘΟΣ ΕΞΥΠΗΡΕΤΟΥΜΕΝΩΝ ΧΡΗΣΤΩΝ

Σύμφωνα με τα χαρακτηριστικά ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου, η πολιτική που ακολουθείται όσον αφορά την πρόσβαση είναι η ελεύθερη χρήση του από το σύνολο των χρηστών. Παρ' όλα αυτά, ενδεχομένως να υπάρχουν κάποια σημεία τα οποία περιορίζουν τον συνολικό αριθμό χρηστών που είναι ταυτόχρονα συνδεδεμένοι στο δίκτυο.

Συγκεκριμένα τα σημεία στα οποία μπορεί να παρουσιαστεί το φαινόμενο της στενωπού (bottleneck) είναι δύο (2):

- **Τα Σημεία Πρόσβασης (Access Points) στο υποσύστημα ασύρματης πρόσβασης χρηστών.**
- **Οι ασύρματες συνδέσεις μεταξύ των Υποσυστημάτων Backhaul με το Κεντρικό Σημείο Διανομής (Κ.Σ.Δ.).**

Κάθε Υποσύστημα Ασύρματης Πρόσβασης Χρηστών περιέχει ένα Access Point για την ασύρματη επικοινωνία με τους χρήστες. Κάθε Access Point μπορεί να υποστηρίξει συνολικό ονομαστικό ρυθμό μετάδοσης 11Mbps, ενώ λόγω της πλεονάζουσας πληροφορίας για την σωστή αποστολή των δικτυακών πακέτων ο

πραγματικός ρυθμός μετάδοσης είναι μισός, δηλ. περίπου 5.5Mbps. Αυτός ο ρυθμός μετάδοσης μοιράζεται στους χρήστες που είναι συνδεδεμένοι σε κάθε Access Point, πράγμα που σημαίνει ότι σε σύνολο 20 συνδεδεμένων «ενεργών» χρηστών (στο ίδιο Access Point), κάθε χρήστες θα λαμβάνει δεδομένα με 275Kbps ή 34KBps. Αυτή η ταχύτητα είναι η μέγιστη στην περίπτωση που όλοι οι χρήστες κατεβάζουν δεδομένα την ίδια χρονική στιγμή. Συνήθως οι περισσότεροι χρήστες περιηγούνται στον Παγκόσμιο Ιστό ή διαβάζουν την Ηλεκτρονική Αλληλογραφία τους. Αυτό σημαίνει ότι για ένα μικρό χρονικό διάστημα κατεβάζουν πληροφορίες στην συσκευή τους και στη συνέχεια τις επεξεργάζονται. Εκείνη τη στιγμή δεν χρησιμοποιούν το δίκτυο, πράγμα που σημαίνει ότι κάποιοι άλλοι χρήστες, που κατεβάζουν δεδομένα, μπορούν να απολαμβάνουν καλύτερη δικτυακή εμπειρία. Δεδομένου ότι κάθε χρονική στιγμή, κατά μέσο όρο 5 χρήστες χρησιμοποιούν το δίκτυο για το κατέβασμα πληροφοριών, τότε κάθε χρήστης μπορεί θεωρητικά να λάβει πληροφορίες με ρυθμό μεγαλύτερο από 1Mbps.

Όσον αφορά στην ασύρματη σύνδεση μεταξύ του Υποσυστήματος Backhaul με το Κ.Σ.Δ. αναφέρεται ότι ο συνολικός ρυθμός μετάδοσης πληροφορίας είναι αυτός του 802.11b, δηλ. 11Mbps ονομαστικά και περίπου 5.5Mbps πρακτικά. Στην περίπτωση που στο Σύστημα Backhaul υπάρχει συνδεδεμένο μόνο ένα Υποσύστημα Ασύρματης Πρόσβασης Χρηστών, δεν παρουσιάζεται πρόβλημα. Πρόβλημα ενδεχομένως να παρουσιαστεί στην περίπτωση που 2 hotspot είναι συνδεδεμένα στο ίδιο Υποσύστημα Backhaul. Τότε ο μέγιστος συνολικός ρυθμός μετάδοσης μειώνεται στο μισό.

Εξετάζοντας συνολικά τα παραπάνω σημεία, γίνεται σαφές ότι ο συνολικός αριθμός των χρηστών που μπορούν να «συνδεθούν» στο σύστημα δεν περιορίζεται, χωρίς να εγγυάται κάποια συγκεκριμένη ποιότητα υπηρεσίας. Όμως, εκ των πραγμάτων, ο αριθμός περιορίζεται λόγω του πιλοτικού χαρακτήρα του έργου. Ένας αριθμός 75 ταυτόχρονα «πολύ ενεργών» χρηστών θα απολαμβάνει εμπειρία δικτυακής πρόσβασης με ταχύτητες όμοιες με εκείνες των συσκευών modem. Στην τυπική περίπτωση που οι χρήστες έχουν τα προαναφερθέντα χαρακτηριστικά (www, e-mail, chat, μικρά αρχεία), τότε ο συνολικός αριθμός των χρηστών μπορεί να διπλασιαστεί.

4.10. ΤΕΚΜΗΡΙΩΣΗ

Κατά την παραλαβή ενός τέτοιου συστήματος, πρέπει να υπάρχει ένα πλήρως λειτουργικό ασύρματο δίκτυο και ένα Κεντρικό Σημείο Διασύνδεσης

(όπως αυτά περιγράφονται παραπάνω). Επίσης, είναι πολύ σημαντικό να υπάρχει και η κατάλληλη τεκμηρίωση, στην οποία θα υπάρχουν όλες οι πληροφορίες σχετικά με την κάλυψη του δικτύου, την αρχιτεκτονική, τη λειτουργικότητα του, τα σημεία που έχουν τοποθετηθεί τα hotspot και τα συστήματα backhaul, καθώς και όλες οι παράμετροι του λογισμικού που χρησιμοποιείται για τη λειτουργία του δικτύου. Με τον τρόπο αυτό διασφαλίζεται η ομαλή μετάβαση από πειραματική σε επιχειρησιακή (κανονική) λειτουργία. **[14]**

4.11. ΑΣΥΡΜΑΤΟΣ ΕΞΟΠΛΙΣΜΟΣ

Οι μονάδες προσπέλασης που συνθέτουν τον απαραίτητο ασύρματο εξοπλισμό, προκειμένου να γίνει εφικτή η πρόσβαση σε ένα δίκτυο, είναι οι παρακάτω:

- *Κεραία*
- *NIC*
- *Καλώδιο RF*
- *Connectors*
- *Pigtail*
- *Καλώδιο UTP*
- *POE*
- *Bridge*
- *Router*

4.11.1. ΚΕΡΑΙΑ :

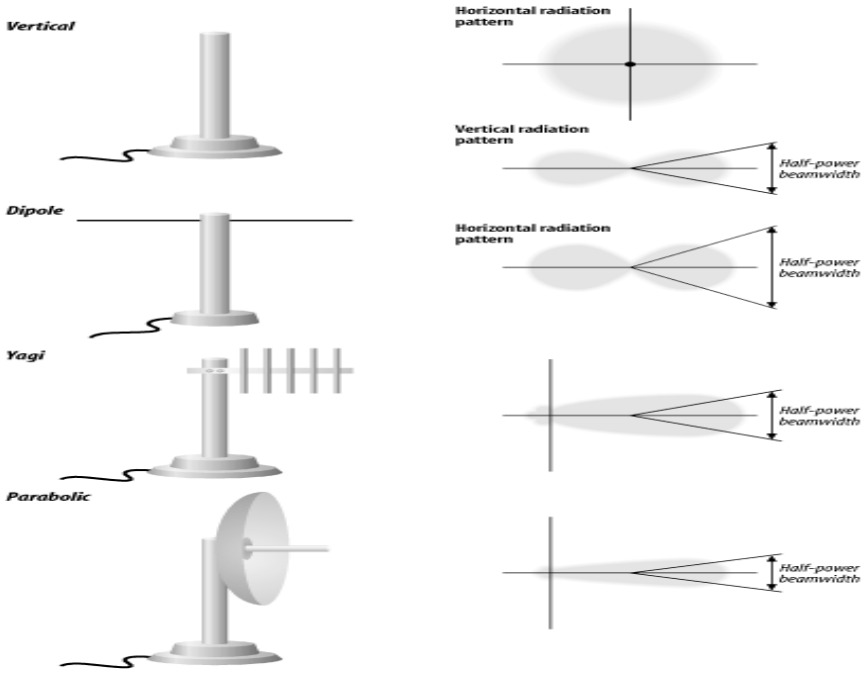
Για την δημιουργία ενός client θα πρέπει να γίνει σύνδεση με ένα AP. Αυτό σημαίνει ότι η κεραία χρειάζεται να σημαδεύει ένα AP. Τυπικά χρειαζόμαστε μία κατευθυντική κεραία (grid, yagi, ελικοειδείς, πιάτο κλπ), για τον απλούστατο λόγο ότι οι συνδέσεις με κατευθυντικές κεραίες καλύπτουν μικρότερη περιοχή, χρησιμοποιούν το φάσμα πιο αποτελεσματικά, απαιτούν μικρότερη ισχύ για να φτάσουν σε μεγαλύτερη απόσταση και μειώνουν το θόρυβο στην περιοχή.

Ο τύπος της κεραίας καθορίζει την μορφή ακτινοβολίας. Οι κεραίες διακρίνονται σε μη κατευθυντικές που είναι κατάλληλες για την κάλυψη των μεγάλων περιοχών, δικατευθυντικές που είναι κατάλληλες για την κάλυψη των

διαδρόμων και μονοκατευθυντικές, που ενδείκνυνται για την σύνδεση μεταξύ κτηρίων (point-to-point). Έτσι διακρίνουμε τους κάτωθι τύπους κεραιών.

- *Vertical* : Έχει κέρδος από 3-10 dBi. Είναι μη κατευθυντική σε οριζόντια κατεύθυνση. Είναι μεγαλύτερη από κάθε άλλη κεραία καθώς επίσης και ακριβότερη. Την χρησιμοποιούμε για να καλύψουμε μια περιοχή στην οποία υπάρχουν αρκετά κτήρια που θέλουμε να συνδεθούν ασύρματα.
- *Dipole* : Χρησιμοποιείται για να καλύψει ένα διάδρομο, μία μεγάλη ή και μικρή περιοχή.
- *Yagi* : Είναι μια υψηλούς κέρδους (12-18dBi) μονοκατευθυντική κεραία.
- *Parabolic* : Έχει πολύ υψηλό κέρδος μέχρι και 24 dBi (very narrow beam widths). Χρησιμοποιείται στην περίπτωση που θέλουμε να συνδέσουμε δύο κτήρια. Μια τέτοια κεραία έχει εμβέλεια μέχρι και 20 miles. Και οι δύο πλευρές αυτής της ασύρματης σύνδεσης έχουν την ίδια κεραία, οι οποίες πρέπει και να σημαδεύονται σωστά. Παραβολική είναι και η κεραία τύπου grid.

Η παραβολική και η yagi κεραία χρησιμοποιείται για την διασύνδεση δυο κτηρίων. Το πρόβλημα είναι να σημαδεύονται οι κεραίες από τις δύο πλευρές σωστά. Στην <u>*εικόνα 4.4*</u> που ακολουθεί φαίνεται η μορφή αυτών των κεραιών, ενώ υπάρχει και το διάγραμμα ακτινοβολίας τους.



Εικόνα 4.4. : Τύποι Κεραιών

4.11.1.1. Εγκατάσταση της Κεραίας :

Η κεραία πρέπει να τοποθετείται στο καλύτερο σημείο και όσο πιο ψηλά γίνεται. Είναι πολύ σημαντικό να στοχεύει όσο γίνεται καλύτερα το AP, αφού ακόμα και να αστοχήσει κατά 5-6 μοίρες αδυνατίζει πολύ το σήμα. Χρησιμοποιείται κάθετη πόλωση, δηλαδή ο λοβός της κεραίας να είναι κάθετος.

Ένας ιστός 1.5-2.5 m, πάνω στον οποίο θα τοποθετηθεί η κεραία είναι αρκετός. Μάλιστα θα πρέπει να είναι όσο το δυνατό πιο σταθερός, έτσι ώστε να αποφευχθούν οι ταλαντώσεις. Αυτό γιατί ακόμα και μικρές ταλαντώσεις μειώνουν την ισχύ αλλά και ο ιστός παθαίνει κόπωση και μειώνει την ικανότητά του στις ανεμοπιέσεις στο ελάχιστο.

4.11.2. NIC (NIC – NETWORK INTERFACE CARD) :

Πρόκειται για υλικό που ενσωματώνεται στην κεντρική μητρική κάρτα του υπολογιστή μας (motherboard) ή εισάγεται στο δίαυλο διασύνδεσης (bus) και έχει ως σκοπό τη σύνδεση του υπολογιστή μας με το υποσύστημα επικοινωνίας (καλωδίωση) του δικτύου μας.

Υπάρχουν τέσσερις μορφές με τις οποίες μπορούμε να βρούμε ασύρματες συσκευές (NIC's) των πρωτοκόλλων που μας ενδιαφέρουν:

1. ***PCI κάρτες*** **:** Είναι μόνο clients και τοποθετούνται στο PCI bus του Η/Υ και διαθέτουν μικρή εξωτερική κεραία.
2. ***PCMCIA κάρτες*** **:** Επίσης είναι μόνο clients, χρησιμοποιούνται σε φορητούς Η/Υ και δεν έχουν εμφανή κεραία.
3. ***USB*** **:** Αποτελεί την πιο ευέλικτη λύση καθώς συνδέεται σε κάθε τύπο Η/Υ.
4. ***Bridges*** **:** Σε αυτή τη μορφή βρίσκουμε και clients αλλά και access points. Πρόκειται για αυτόνομη συσκευή η οποία παρέχει συνήθως δύο διεπαφές, μία ασύρματη και μία ενσύρματη (Ethernet). Και λειτουργεί σαν level 2 bridge .

Ο εξοπλισμός αυτός είναι κατασκευασμένος για χρήση εντός εσωτερικών χώρων, οπότε οι μετατροπές για εξωτερική χρήση γίνονται αναγκαίες. Ταυτόχρονα σε μεγάλες αποστάσεις σε αστικό περιβάλλον, για να πετύχει μία ζεύξη, είναι αναγκαία η οπτική επαφή.

Η προφανής λύση είναι η επέκταση του καλωδίου σύνδεσης με την κεραία μας μέχρι το σημείο που επιτυγχάνεται η οπτική επαφή. Αυτό δεν είναι πάντοτε αποδοτικό, καθώς το καλώδιο RF έχει μεγάλες απώλειες ανά μέτρο. Άλλωστε μεγάλα μήκη εκμηδενίζουν το σήμα. Οι συνθήκες αυτές μας οδηγούν και στις αντίστοιχες υλοποιήσεις. **Συνεπώς ανάλογα με τις ιδιομορφίες του κάθε κόμβου υπάρχουν οι εξής δύο περιπτώσεις :**

1. Εάν το σημείο που επιτυγχάνεται σύνδεση με την κεραία μας είναι μακριά από το Η/Υ του χρήστη, τότε χρησιμοποιούμε Wireless to Ethernet Bridge ή USB. Σ' αυτή λοιπόν την περίπτωση, οι δύο τελευταίες συσκευές τοποθετούνται στο στύλο της κεραίας μας και η σύνδεση με αυτές γίνεται με utp ή usb καλώδιο. Κάτι τέτοιο συνεπάγεται τόσο πλεονεκτήματα, όσο και μειονεκτήματα.

   Πλεονεκτήματα **:**

   - Μήκος καλωδίου RF μικρό οπότε θα έχουμε και μικρές απώλειες.
   - Ευέλικτη λύση καθώς συνδέεται σε κάθε τύπο Η/Υ.
   - Η απόσταση μεταξύ κόμβου και Η/Υ μπορεί να φτάσει μέχρι και 100 μέτρα για μια Ethernet σύνδεση ή 36 μέτρα για μια USB.
   - Αυτόνομη λειτουργία στη περίπτωση Ethernet συσκευών.

   Μειονεκτήματα :

   - Οι ιδιοκατασκευές και οι μετατροπές είναι απαραίτητες, για τη προστασία της συσκευής από την εξωτερική χρήση καθώς και για τη μεταφορά ρεύματος από το σπίτι στον κόμβο μέσω POE (power over Ethernet).
   - Μεγαλύτερο κόστος σε σχέση με τις PCMCIA ή PCI συσκευές.
   - Περιορισμός στις λειτουργίες που προσφέρει το ενσωματωμένο σε αυτό λογισμικό.

Στην περίπτωση που ο εξοπλισμός είναι USB ή Ethernet to wireless bridge, τότε είναι απαραίτητο να τοποθετηθεί η συσκευή σε αδιάβροχο κουτί έτσι ώστε να είναι δυνατή η τοποθέτησή του στο στύλο της κεραίας.

Για την τροφοδοσία (στην περίπτωση bridge) πρέπει να κάνουμε τις κατάλληλες μετατροπές ώστε να περάσει από το καλώδιο utp. Αυτός ο μηχανισμός ονομάζεται POE (Power Over Ethernet), όπως θα δούμε πιο κάτω. Τέλος χρειάζεται ένα pigtail για να το συνδέσουμε με την κεραία μας. Εάν το σημείο που επιτυγχάνεται σύνδεση είναι κοντά στον Η/Υ του χρήστη, τότε χρησιμοποιούμε μια pci ή pcmcia κάρτα. Σ' αυτή την περίπτωση τα πλεονεκτήματα υπερτερούν των μειονεκτημάτων.

Πλεονεκτήματα :

- Χαμηλό κόστος.
- Επεκτασιμότητα – ευελιξία.
- Πλήρης έλεγχος από λογισμικό
- Οι PCMCIA προσφέρουν τον πολύ δημοφιλή τρόπο διασύνδεσης περιφερειακών σε φορητούς.
- Δημιουργία access point με τη χρήση καρτών client.

Μειονεκτήματα :

- Μετά τα 15-20 μέτρα το κόστος και οι απώλειες στο σήμα γίνονται απαγορευτικές.

<u>Στην συνέχεια παρατίθεται ένα μοντέλο NIC's :</u>

EZ Connect SMC2835W - ΑΣΥΡΜΑΤΗ ΚΑΡΤΑ ΔΙΚΤΥΟΥ για ΦΟΡΗΤΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ 54 Mbps Wireless Cardbus Adapter

Έχει τα κάτωθι χαρακτηριστικά :

- Είναι μια PCMCIA Card εξαιρετικά γρήγορη, προσφέρει πολύ υψηλές ταχύτητες μεταφοράς δεδομένων, μπορεί να διακινήσει streaming video, πολυμέσα και όλες τις εφαρμογές που χρειάζονται μεγάλο bandwidth.
- Παρέχει σύνδεση στα 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54Mbps.
- Η συχνότητα εκπομπής / λήψης είναι στα 2.4 GHz (2400MHz – 2483.5MH).

- Παρέχει υψηλό επίπεδο ασφάλειας, με κρυπτογράφηση 64/128 bit καθώς και τη νέα κρυπτογράφηση 256-bit WEP (Wired Equivalent Privacy).
- Ενδείκτης LED (Activity/Link)
- Κατανάλωση: 480mA Tx, 380mA Rx.
- Διαθέτει ενσωματωμένη κεραία (1.5 dBi).
- Καλύπτει απόσταση έως 350 μέτρα.
- 13 κανάλια.
- Λειτουργεί σε θερμοκρασία περιβάλλοντος από 0º έως +60ºC.
- Διαστάσεις 12.8 cm x 5.4 cm x 0.9 cm.
- Συμβατή με λειτουργικά συστήματα Win 98, WinME, Win 2000, WinXP. Η μορφή της φαίνεται στην *εικόνα 4.5.* :

Εικόνα 4.5. : EZ Connect SMC2835W

4.11.3. ΚΑΛΩΔΙΟ RF :

Πρόκειται για το ένα από τα δύο καλώδια που απαιτούνται. Η μορφή του φαίνεται στην *εικόνα 4.6*. Όταν η απόσταση της κεραίας από την κάρτα δικτύου είναι μεγαλύτερη από 50cm χρειάζεται ένα καλώδιο κεραίας που να συνδέει την υποδοχή της κεραίας με το pigtail. Η υποδοχή στις περισσότερες κεραίες των 2.4GHz είναι συνήθως τύπου N-type θηλυκό (N-type female), οπότε χρειάζεται το ένα άκρο να είναι N-type αρσενικό και το άλλο συμβατό με το άκρο του pigtail που αντιστοιχεί στην κεραία.

Εικόνα 4.6. : Καλώδιο RF

Υπάρχουν τα κάτωθι είδη καλωδίων :

- ***Σειρά LMR* :** Πρόκειται για καλώδια καλής ποιότητας. Το εξωτερικό τους κέλυφος αποτελείται από συμπαγή χαλκό (που είναι όμως αυλακωτός για ευλυγισία) και ο κεντρικός αγωγός είναι ένας συμπαγής πυρήνας χαλκού/αλουμινίου. Λυγίζεται εύκολα σε μία ακτίνα 20cm. Στην *εικόνα 4. 7.* φαίνονται καλώδια αυτής της σειράς.

Εικόνα 4.7. : Σειρά LMR

- *RG213*
- *Aircom+*
- *H2000*

Ιδιαίτερη σημασία πρέπει να δίδεται στην προστασία των καλωδίων. Έτσι θα πρέπει να αποφεύγονται τα λυγίσματα των καλωδίων, διότι μια απότομη γωνίαση μπορεί να καταστρέψει το καλώδιο.

4.11.4. CONNECTORS (ΣΥΝΔΕΤΗΡΕΣ) :

Πρόκειται για υλικό που απαιτείται για την διασύνδεση αλλά και την προσαρμογή των επαφών (ακροδεκτών) της κάρτας δικτύου με το σύστημα καλωδίωσης. Στην περίπτωση μάλιστα εξωτερικής χρήσης οι connectors, πρέπει να είναι σωστά τοποθετημένοι, έτσι ώστε τα καλώδια να είναι απόλυτα στεγνά και προστατευμένα. Και αυτό γιατί η υγρασία που μπορεί να εισχωρήσει να ενδεχομένως να μειώσει ή και να εξαφανίσει το σήμα. Το μικρό βύσμα στο καλώδιο στην *εικόνα 4.8.* είναι ένας Connector.

4.11.5. PIGTAIL :

Pigtail ονομάζεται το καλώδιο στην *εικόνα 4.8* . Αυτό το εξάρτημα συναντάται με πολλά ονόματα. Είναι απλά ένα μικρό κομμάτι καλώδιο με connectors προσαρμογής για την ένωση του αποκλειστικού connector της κάρτας Wi-Fi με το καλώδιο της εξωτερικής κεραίας.

Ένας RF connector πρέπει να είναι τοποθετημένος σε κάθε άκρο του pigtail. Στο ένα άκρο ένας κατάλληλος connector για την κάρτα Wi-Fi και στο άλλο άκρο ένας τυποποιημένος RF connector (στην γενική περίπτωση N-type). Πολλοί αποκλειστικοί connectors μπορούν να βρεθούν σε καταστήματα του εξωτερικού. Είναι ακριβοί γιατί είναι αποκλειστικοί. Θα πρέπει να βεβαιωθείς ότι θα πάρεις τους σωστούς connectors για το ομοαξονικό καλώδιο (coaxial cable) που διαθέτεις.

Το καλώδιο που χρησιμοποιείται γι' αυτό το εξάρτημα είναι γενικά λεπτό (συνήθως 4.9mm) και συνεπώς με αρκετές απώλειες, οπότε καλύτερα το μήκος να είναι όσο πιο μικρό γίνεται (συνήθως μικρότερο από 60 cm).

Εικόνα 4.8. : Pigtail

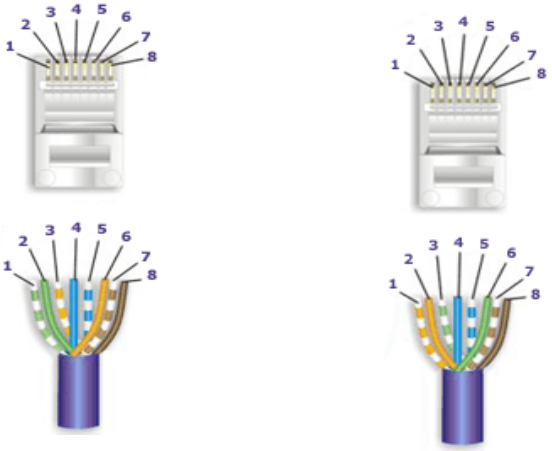
Στο Pigtail του παραπάνω σχήματος, το μικρό βύσμα είναι αποκλειστικός connector Lucent, ενώ το ογκώδες είναι N-type βύσμα που καταλήγει στην κεραία.

4.11.6. ΚΑΛΩΔΙΟ UTP (UNSHIELDED TWISTED PAIR) :

Αποτελούνται από 4 συνεστραμένα ζεύγη που περιβάλλονται από τον πλαστικό μανδύα του καλωδίου. Είναι τα πιο συχνά χρησιμοποιούμενα καλώδια εύκολα στην εγκατάσταση και τα πιο οικονομικά. Στην *εικόνα 4.9* εικονίζεται ένα τέτοιο καλώδιο. Χρησιμοποιείται την διασύνδεση των συσκευών Wireless to Ethernet Bridge ή USB που τοποθετούνται στην κεραία (όταν το σημείο σύνδεσης με την κεραία μας είναι μακριά από το Η/Υ).

Εικόνα 4.9. : Καλώδιο UTP

Ένα τέτοιο καλώδιο υποστηρίζει εφαρμογές φωνής και δεδομένων με ρυθμό μετάδοσης 100Mbps. Η τυποποίηση EIA/TIA 568 (EIA electronic industries association - Αμερικάνικος οργανισμός που ασχολείται με τυποποιήσεις) προδιαγράφει λεπτομέρειες υλοποίησης όλων των τμημάτων ενός δομημένου καλωδιακού συστήματος και όσον αφορά την καλωδίωση UTP, προβλέπει τη χρήση καλωδίου UTP CAT5 τεσσάρων ζευγών, πρίζα RJ-45 και συστήνει μήκος καλωδίου όχι μεγαλύτερο από 3 μέτρα. Η τυποποίηση εκτείνεται και στα χρώματα των καλωδίων για ασφαλέστερη κατασκευή και καλύτερη διαχείριση. Σήμερα έχουν επικρατήσει δυο παραλλαγές καλωδίωσης η EIA/TIA 568A και EIA/TIA 568B τις οποίες βλέπουμε στην παρακάτω *εικόνα 4.10*.

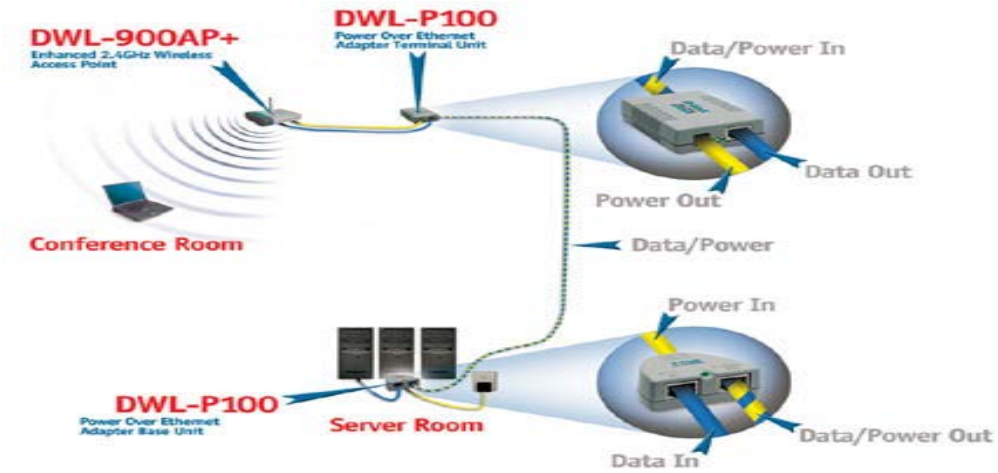


Εικόνα 4.10. : UTP 568-A και UTP-568B

4.11.7. POE (POWER OVER ETHERNET) :

Σε περίπτωση που μία συσκευή Ethernet βρίσκεται κάπου μακριά (και υπάρχει και έλλειψη τροφοδοσίας στο τελικό σημείο), το να μεταφέρουμε ρεύμα 220V με πολλά μέτρα καλώδιο δεν είναι και πολύ καλή ιδέα, για λόγους ασφαλείας. Σε αυτή λοιπόν την περίπτωση χρησιμοποιούμε την τεχνολογία PoE (Power Over Ethernet). Η συσκευή Ethernet τροφοδοτείται μέσω του UTP ή FTP καλωδίου που το συνδέει με τον υπολογιστή.

Δηλαδή, μέσω ενός adapter «βάζουμε» ρεύμα και data στο ίδιο καλώδιο και στο τέλος, μέσω ενός splitter, τα διαχωρίζουμε. Η όλη διαδικασία φαίνεται στην παρακάτω *εικόνα 4.11*.



Εικόνα 4.11. : Λειτουργία POE

Παραθέτουμε έπειτα ένα μοντέλο ενός adapter.

EZ Connect Wireless Ethernet Adapter SMC2670W 11 Mbps Wireless Ethernet Adapter

Η συγκεκριμένη μονάδα, που φαίνεται στην *εικόνα 4.12* έχει τα παρακάτω χαρακτηριστικά :

- Συνδέεται σε οποιαδήποτε μονάδα διαθέτει Ethernet θύρα (RJ-45) και την μετατρέπει σε ασύρματη.
- Παρέχει σύνδεση στα 11, 5.5, 2, και 1Mbps, με αυτόματη υποχώρηση.
- Plug-n-Play-Δεν χρειάζεται οδηγούς.
- Η συχνότητα εκπομπής/λήψης είναι στα 2.4 GHz (2412MHz – 2472MHz).
- Εξασφαλίζει υψηλό επίπεδο ασφάλειας με κρυπτογράφηση 64/128 bit WEP (Wired Equivalent Privacy).
- Ενδείκτης LED (Power, Wireless, Ethernet).
- Κατανάλωση 800mA Tx, 350mA Rx).
- Δίπολη κεραία.

- 13 κανάλια.
- Καλύπτει απόσταση έως 250 m.
- Μια Ethernet θύρα (RJ45).
- Λειτουργεί σε θερμοκρασία περιβάλλοντος από -10º έως +65ºC.
- Διαστάσεις 11.7 cm x 6.2 cm x 2.2 cm.
- Συμβατή με λειτουργικά συστήματα Win 98, WinME, Win 2000, WinXP.

Εικόνα 4.12. : EZ Connect Wireless Ethernet Adapter SMC2670W 11 Mbps Wireless Ethernet Adapter

4.11.8. BRIDGE (ΓΕΦΥΡΑ) :

Η γέφυρα είναι μία συσκευή η οποία ουσιαστικά κάνει αυτό που περιγράφει το όνομά της, δηλαδή γεφυρώνει μεταξύ τους δύο τοπικά δίκτυα. Η διαφορά μεταξύ μιας γέφυρας και ενός router (δρομολογητή), έγκειται στον τρόπο με τον οποίο συνδέουν τα δίκτυα. Σε ένα τηλεπικοινωνιακό δίκτυο, μία γέφυρα είναι είτε μία συσκευή, είτε λογισμικό το οποίο αντιγράφει πακέτα στο δεύτερο στρώμα του μοντέλου OSI. και συνδέει τα δίκτυα σε επίπεδο hardware.

Ακολουθεί ένα μοντέλο μιας γέφυρας.

EZ Connect Turbo SMC2482W 11/22 Mbps Auto-Sensing Wireless Bridge

Έχει τα ακόλουθα χαρακτηριστικά :

- Σε συνδυασμό με το SMC2455W 11/22 Mbps Wireless Access Point έχει σχεδιασθεί να συνδέει δυο ή περισσότερα διαφορετικά Τοπικά Δίκτυα (συνήθως ευρισκόμενα σε διαφορετικά κτίρια). Η νέα αυτή ασύρματη γέφυρα είναι η ευκολότερη εναλλακτική στο παραδοσιακό ενσύρματο δίκτυο, μιας και αποτελεί μια γρήγορη και αξιόπιστη λύση η οποία εξαλείφει τις καλωδιώσεις και τις μισθωμένες γραμμές.

- Ρυθμός ροής δεδομένων έως 22Mbps, με αυτόματη υποχώρηση.
- Η συχνότητα εκπομπής / λήψης είναι στα 2.4 GHz.
- Υποστηρίζει έως 253 χρήστες.
- RJ45 - 10/100 Mbps.
- Αποσπώμενη διπλή δίπολη κεραία (2 dBi) με δυνατότητα σύνδεσης εξωτερικής κατευθυντικής κεραίας μεγάλης εμβέλειας.
- Καλύπτει απόσταση έως 350 μέτρα.
- 13 κανάλια.
- Παρέχει κρυπτογράφηση μεταφοράς δεδομένων 64-bit/128/256-bit.
- Λειτουργεί σε θερμοκρασία περιβάλλοντος από 0º έως +70ºC.
- Διαστάσεις 19.8 cm x 15 cm x 6.15 cm και ζυγίζει 600 gr.
- Τέλος είναι συμβατή με λειτουργικά συστήματα Win 98, WinME, Win 2000, WinXP.

Στην παρακάτω εικόνα 4.13. φαίνεται η μορφή του.

Εικόνα 4.13. : EZ Connect Turbo SMC2482W

4.11.9. ROUTER (ΔΡΟΜΟΛΟΓΗΤΗΣ) :

Ένας router είναι μία συσκευή που συνδέει δύο ή περισσότερα δίκτυα (που μπορεί να είναι διαφορετικού τύπου) και έτσι ανήκει σε δύο ή περισσότερα δίκτυα ταυτόχρονα. Η δουλειά των routers είναι να δρομολογούν τα πακέτα των δεδομένων μέσα από τα διάφορα δίκτυα που αποτελούν το Internet μέχρις ότου τα επιδώσουν στον προορισμό τους.

Ακολουθεί στην συνέχεια το μοντέλο ενός router.

ΑΣΥΡΜΑΤΟΣ ROUTER Barricade SMC2804WBR V.2 Wireless Cable/DSL Broadband Router - 54 Mbps

Η μορφή του φαίνεται στην παρακάτω *εικόνα 4.14*. και παρουσιάζει τα χαρακτηριστικά :

- Ροή δεδομένων έως 54Mbs, με αυτόματη υποχώρηση (1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 και 54 Mbps).
- Η συχνότητα εκπομπής / λήψης είναι στα 2.4 GHz.
- Υποστηρίζει έως 253 χρήστες.
- Ενσωματωμένο Switch με 4 θύρες 10/100 Mbps συν μία θύρα 10/100 Mbps για σύνδεση με DSL Modem.
- Αποσπώμενη διπλή δίπολη κεραία (2dBi) με δυνατότητα σύνδεσης εξωτερικής κατευθυντικής κεραίας μεγάλης εμβέλειας (SMA connectors).
- Καλύπτει απόσταση έως 350 m.
- Παρέχει κρυπτογράφηση μεταφοράς δεδομένων WEP 64-bit/128-bit, WPA και MAC Address Filtering.
- Ενσωματωμένο Firewall.
- Υποστήριξη Dynamic DNS.
- URL Blocking για απαγόρευση της πρόσβασης σε συγκεκριμένες ιστοσελίδες με βάση μια λέξη κλειδί ή τη διεύθυνση.
- 13 κανάλια.
- Ενδείκτες LED (Power, WLAN, LAN και WAN).
- Λειτουργεί σε θερμοκρασία περιβάλλοντος από 0º έως +55ºC.
- Διαστάσεις 22 cm x 13.5 cm x 2.5 cm και ζυγίζει 680 gr.
- Συμβατό με λειτουργικά συστήματα Win 98, WinME, Win 2000, WinXP, Linux, Unix, MacOS.

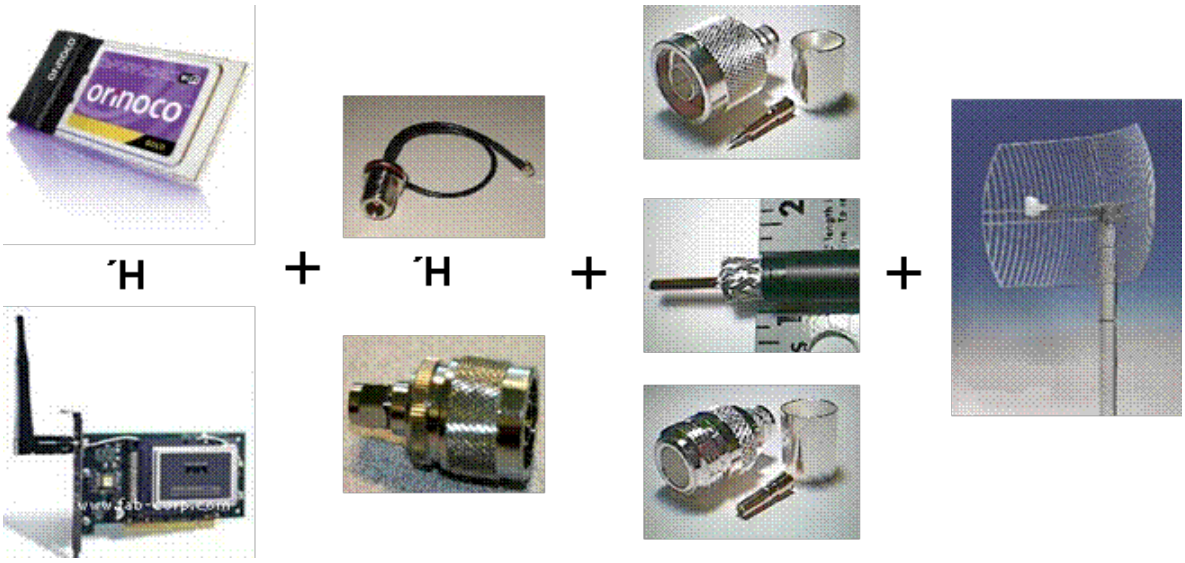
Εικόνα 4.14. : ΑΣΥΡΜΑΤΟΣ ROUTER Barricade SMC2804WBR V.2

4.12. ΠΑΡΑΔΕΙΓΜΑ ΔΙΑΣΥΝΔΕΣΗΣ

Με το παράδειγμα αυτό επιχειρείται να γίνει κατανοητός ο τρόπος με τον οποίο συνδέονται οι μονάδες που περιγράψαμε προηγουμένως. Θεωρούμε λοιπόν την περίπτωση όπου το σημείο που γίνεται εφικτή η σύνδεση με την κεραία μας είναι σχετικά μακριά από τον Η/Υ μας. Σ' αυτή την περίπτωση μπορούμε να επιλέξουμε όσον αφορά την κάρτα NIC, είτε μια PCI, η οποία τοποθετείται στο PCI bus του Η/Υ και διαθέτει μικρή εξωτερική κεραία, είτε μια PCMCIA, η οποία ενδείκνυται σε φορητούς υπολογιστές και δεν έχει εμφανή κεραία (ενσωματωμένη). Το επόμενο βήμα είναι να επιλέξουμε μεταξύ ενός pigtail ή ενός connector, που καταλήγει σε βύσμα τύπου Ν. Με τον τρόπο αυτό γίνεται η διασύνδεση των ακροδεκτών (connectors) της κάρτας NIC με το σύστημα καλωδίωσης και πιο συγκεκριμένα με το καλώδιο της κεραίας μας, το οποίο διαθέτει βύσματα τύπου Ν. Η κεραία πρέπει να τοποθετηθεί όσο πιο ψηλά γίνεται και να σημαδεύει το AP όσο γίνεται καλύτερα.

Η παραπάνω διαδικασία περιγράφεται στην *εικόνα 4.15*.

Στην περίπτωση που το σημείο που επιτυγχάνεται σύνδεση με την κεραία μας είναι μακριά από το Η/Υ, τότε χρησιμοποιούμε Wireless to Ethernet Bridge ή USB. Οι συσκευές αυτές τοποθετούνται στο στύλο της κεραίας μας και η σύνδεση με αυτές γίνεται με utp ή usb καλώδιο. Τότε είναι απαραίτητο να τοποθετηθεί η συσκευή σε αδιάβροχο κουτί έτσι ώστε να είναι δυνατή η τοποθέτησή του στο στύλο της κεραίας. Η συσκευή τροφοδοτείται μέσω του UTP καλωδίου που το συνδέει με τον υπολογιστή. Εδώ γίνεται χρήση της τεχνολογίας POE (Power Over Ethernet), που παρουσιάσαμε λίγο πιο πάνω. Υπενθυμίζουμε ότι μέσω ενός adapter «βάζουμε» ρεύμα και data στο ίδιο καλώδιο και στο τέλος, μέσω ενός splitter, τα διαχωρίζουμε. Τέλος χρειάζεται ένα pigtail για να το συνδέσουμε την συσκευή με την κεραία μας. [2]



Εικόνα 4.15. : Διασύνδεση ασύρματων μονάδων

4.13. ΕΞΟΠΛΙΣΜΟΣ ΧΡΗΣΤΩΝ ΓΙΑ ΠΡΟΣΒΑΣΗ ΣΕ HOTSPOTS

Από την πλευρά των χρηστών για τη σύνδεση σε δίκτυα τεχνολογίας WiFi απαιτείται η ύπαρξη ειδικού εξοπλισμού μικρού σχετικά κόστους (*εικόνα 4.16*). Στη μεγάλη τους πλειοψηφία οι τελικοί χρήστες χρησιμοποιούν τους φορητούς υπολογιστές τους για πρόσβαση σε ασυρματικά δίκτυα. Οι σύγχρονοι φορητοί υπολογιστές έχουν στη μεγάλη τους πλειοψηφία ενσωματωμένες τις δυνατότητες για πρόσβαση σε ασυρματικά δίκτυα τα οποία στηρίζονται στο πρωτόκολλα 802.11b της IEEE το οποίο είναι συμβατό και με τον εξοπλισμό του 802.11g χωρίς όμως να εκμεταλλεύεται τις υψηλότερες ταχύτητες που προσφέρει το τελευταίο. **Για την υποστήριξη του 802.11g ή για τη δυνατότητα πρόσβασης μέσω παλαιότερων φορητών υπολογιστών αρκεί μία μικρή κάρτα πρόσβασης η οποία υποστηρίζει τα πρωτόκολλα 802.11b ή / και 802.11g.** Το κόστος μιας τέτοιας κάρτας είναι της τάξης των **100€**, πολύ μικρό σε σχέση με το κόστος ενός καινούριου υπολογιστή. **Μία άλλη εναλλακτική, λιγότερο διαδεδομένη, για την πρόσβαση του χρήστη στις υπηρεσίες που προσφέρει ένα Wireless Hotspot είναι η χρήση κάποιου υπολογιστή παλάμης.** Ο αριθμός των συσκευών αυτών είναι γενικά πολύ μικρός άλλα αναμένεται να αυξηθεί δραματικά τα επόμενα χρόνια.

Τέλος στο πλαίσιο της σύγκλισης των τεχνολογιών και της ανάπτυξης της κινητής τηλεφωνίας τρίτης γενιάς αναμένονται στην αγορά οι νέες συσκευές κινητών τηλεφώνων οι οποίες θα συνδυάζουν τόσο τις τεχνολογίες δικτύων τρίτης γενιάς όσο και τις τεχνολογίες των δικτύων WiFi. Σε μία τέτοια περίπτωση η συσκευή θα επιλέγει αυτόματα τη χρήστη του Wireless Hotspot όπου αυτό είναι διαθέσιμο.

Άλλωστε στις επιχειρήσεις οι οποίες αναμένεται να παίξουν σημαντικό ρόλο στην ευρεία παροχή υπηρεσιών πρόσβασης σε υπηρεσίες και υποδομής μέσω δικτύων WiFi είναι οι σημερινές επιχειρήσεις κινητών επικοινωνιών. Οι επιχειρήσεις αυτές διαθέτουν ήδη την κατάλληλη τεχνογνωσία και πελατειακή βάση για την ανάπτυξη και διάδοση τέτοιων υπηρεσιών. **[13]**

Εικόνα 4.16. : Εξοπλισμός χρηστών για πρόσβαση σε HotSpots **[15]**

ΠΑΡΑΡΤΗΜΑ :

Δίκτυο AthensWiFi: "Δημόσιο Δίκτυο Ασύρματης Πρόσβασης στο Διαδίκτυο στην πλατεία Συντάγματος" (www.athenswifi.gr)

Στη συνέχεια παρουσιάζουμε ένα συγκεκριμένο παράδειγμα υλοποίησης ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου το οποίο θα αναπτυχθεί στην περιοχή της Πλατείας Συντάγματος στην Αθήνα, στο πλαίσιο του έργου «**Ανάπτυξη Ασύρματων Ευρυζωνικών Υποδομών και Προώθηση Ζήτησης Ασύρματων Υπηρεσιών Διαδικτύου σε Πολυσύχναστους Εξωτερικούς Χώρους**», του ΕΠ ΚτΠ, αποφάσεις ένταξης: 151.369/ΚτΠ9371-Β3 24/2/2004 και 152.679/ΚτΠ7356-Β3 23/7/2004, κωδικός ΟΠΣ: 91016. Σκοπός του δικτύου είναι η πιλοτική παροχή ασύρματης πρόσβασης στο διαδίκτυο σε όλους τους χρήστες του εξωτερικού χώρου, με στόχο την προώθηση της ιδέας της ευρυζωνικότητας. Η επιτυχία του έργου βασίζεται στην μεγάλη αποδοχή που θα έχει από τους πολίτες. Για το λόγο αυτό έπρεπε να επιλεγεί ανοικτός χώρος μεταξύ δημόσιων χώρων συνάθροισης, όπως είναι πλατείες, σταθμοί μητροπολιτικού σιδηροδρόμου, μεγάλοι εμπορικοί πεζόδρομοι, σταθμοί λεωφορείων, εμπορικά κέντρα, χώροι αναψυχής, κ.λπ. Η Πλατεία Συντάγματος καλύπτει πλήρως την απαίτηση για πολυσύχναστο δημόσιο χώρο, καθημερινά επισκέψιμο από μεγάλο αριθμό πολιτών όλων των ηλικιών, ώστε να γνωρίσουν από κοντά τις δυνατότητες της ασύρματης ευρυζωνικότητας.

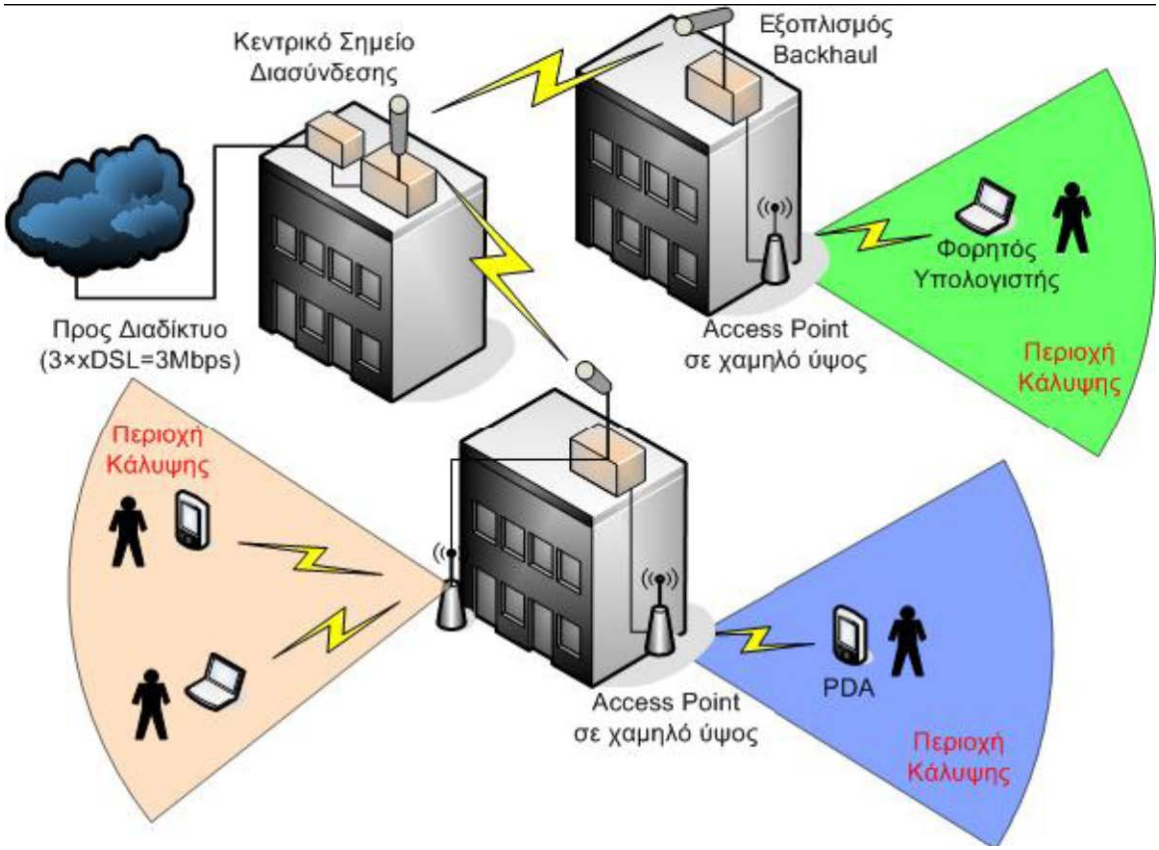
Επομένως, στο πλαίσιο της προώθησης ζήτησης ασύρματων ευρυζωνικών υποδομών για μεγάλο αριθμό πολιτών, θα πραγματοποιηθεί, η προμήθεια, εγκατάσταση και δοκιμαστική λειτουργία εξοπλισμού για τη δημιουργία ασύρματων τοπικών δικτύων (Wireless Hotspots) στην Πλατεία Συντάγματος της Αθήνας, εγκαθιστώντας το πρώτο «**Δημόσιο Δίκτυο Ασύρματης Πρόσβασης στο Διαδίκτυο στην πλατεία Συντάγματος (www.athenswifi.gr)**». Μέσω των Wireless Hotspots θα παρέχονται, σε δοκιμαστική – πιλοτική βάση, ευρυζωνικές υπηρεσίες Internet στους πολίτες, καθώς και στους επισκέπτες της Πλατείας.

Κάθε Wireless Hotspot θα επικοινωνεί ασύρματα με τις συσκευές των χρηστών του δικτύου (φορητοί υπολογιστές, υπολογιστές παλάμης, κτλ.), εφόσον αυτές διαθέτουν τον κατάλληλο εξοπλισμό (ενσωματωμένους προσαρμογείς, ειδικές κάρτες επέκτασης κτλ.) που να είναι συμβατός με το πρότυπο WiFi (ειδικότερα IEEE 802.11b και IEEE 802.11g). Ένα Wireless Hotspot θα επικοινωνεί με πολλαπλές συσκευές χρηστών, ενώ κρίνεται απαραίτητο να εγκατασταθούν πολλά Hotspot (περί τα δέκα), περιμετρικά ή και στο κέντρο της πλατείας, ώστε αφενός να καλύπτεται ομοιόμορφα όλος ο χώρος της πλατείας και αφετέρου να μην απαιτείται αυξημένη ένταση εκπομπής από κάθε Wireless Hotspot χωριστά.

Επιπρόσθετα, θα πρέπει να ληφθεί υπόψη ότι η εγκατάσταση των Wireless Hotspot θα πρέπει να γίνει με τέτοιο τρόπο ώστε να μειωθούν όσο το δυνατόν περισσότερο οι παρεμβολές μεταξύ τους. Επίσης οι χρήστες του δικτύου θα πρέπει να μπορούν να περιφέρονται στην Πλατεία, αλλάζοντας ανάλογα με τη θέση τους σημείο εξυπηρέτησης, χωρίς να αποσυνδέονται και να επανασυνδέονται στο ασύρματο δίκτυο (roaming).

Α. Περιγραφη Λειτουργιας του Ασυρματου Δικτυου AthensWiFi

Η λειτουργία του Ασύρματου Δικτύου AthensWiFi είναι όμοια με εκείνη του γενικού Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου που περιγράφηκε παραπάνω. Οι χρήστες που βρίσκονται στην Πλατεία Συντάγματος μπορούν μέσω μιας ασύρματης δικτυακής συσκευής (π.χ. φορητού υπολογιστή, PDA, κλπ.) να χρησιμοποιήσουν τις υπηρεσίες του δικτύου. Οι φορητές συσκευές συνδέονται με τα Σημεία Πρόσβασης (hotspot) που βρίσκονται στο επίπεδο της Πλατείας. Η κίνηση από τα hotspot μεταφέρεται ενσύρματα (Ethernet) στην οροφή ενός κτιρίου όπου υπάρχει ένα υποσύστημα Backhaul. Το υποσύστημα Backhaul συγκεντρώνει την κίνηση από όλα τα hotspot που είναι συνδεδεμένα με αυτό. Στη συνέχεια προωθεί όλη την κίνηση με ασύρματο τρόπο (IEEE 802.11b) προς το Κεντρικό Σημείο Διασύνδεσης, όπου υπάρχουν τρεις (3) ευρυζωνικές γραμμές τύπου ADSL (1Mbps), μέσω των οποίων όλη η κίνηση του ασύρματου δικτύου προωθείται στο Διαδίκτυο. Όλα αυτά φαίνονται σχηματικά στην *Εικόνα 1*.



Εικόνα 1. : Λειτουργία Ασύρματου Δικτύου AthensWiFi

Β. ΠΕΡΙΟΧΗ ΚΑΛΥΨΗΣ ΔΙΚΤΥΟΥ ATHENSWIFI

Προκειμένου να επιτύχει το συγκεκριμένο έργο παροχής ασύρματων δικτυακών υπηρεσιών, θα πρέπει η καλυπτόμενη από το ασύρματο δίκτυο περιοχή να είναι όσο γίνεται μεγαλύτερη και με όσο το δυνατόν ισχυρότερο σήμα σε κάθε σημείο. **Οι πλέον πολυσύχναστες περιοχές, οι οποίες θα πρέπει να καλύπτονται, είναι οι ακόλουθες:**

1. Η Πλατεία Συντάγματος

2. Τα πεζοδρόμια μπροστά από τον χώρο του Υπουργείου Οικονομικών

3. Το πάνω τμήμα της οδού Ερμού που καταλήγει στην Πλατεία

4. Το πεζοδρόμιο μπροστά από την Εθνική Τράπεζα και η κατάληξη της οδού Σταδίου στην Πλατεία

5. Το πάνω τμήμα της οδού Μητροπόλεως που καταλήγει στην Πλατεία

6. Ο επίπεδος χώρος μπροστά από το Μνημείο του Άγνωστου Στρατιώτη

7. Το τμήμα της Λεωφόρου Βασιλίσσης Αμαλίας που περνάει από την πλατεία

8. Η αρχή της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου)

9. Ένα τμήμα της Λεωφόρου Βασιλίσσης Σοφίας που ξεκινάει από την Πλατεία

Για να επιτευχθεί η προτεινόμενη κάλυψη, θα πρέπει να τοποθετηθούν αρκετά hotspot, ένα ανά υπο-περιοχή του συνολικού χώρου κάλυψης. Τα σημεία αυτά αντιστοιχίζονται σε κτίρια, στο κάτω μέρος των οποίων τοποθετούνται τα hotspot και στην ταράτσα κάθε κτιρίου τοποθετείται από ένα υποσύστημα Backhaul. Τα κτίρια αυτά θα πρέπει να βρίσκονται περιμετρικά της Πλατείας προκειμένου να επιτευχθεί η κάλυψη που περιγράφηκε παραπάνω.

Είναι προφανές ότι υπάρχουν περισσότεροι από ένας διαφορετικοί συνδυασμοί κτιρίων και σημείων τοποθέτησης hotspot μέσω των οποίων μπορεί να καλυφθεί ο χώρος της Πλατείας. Ένας πιθανός συνδυασμός αποτελείται από το σύνολο των κτιρίων που απεικονίζεται στην *Εικόνα 2*. **Τα κτίρια που φαίνονται είναι τα ακόλουθα:**

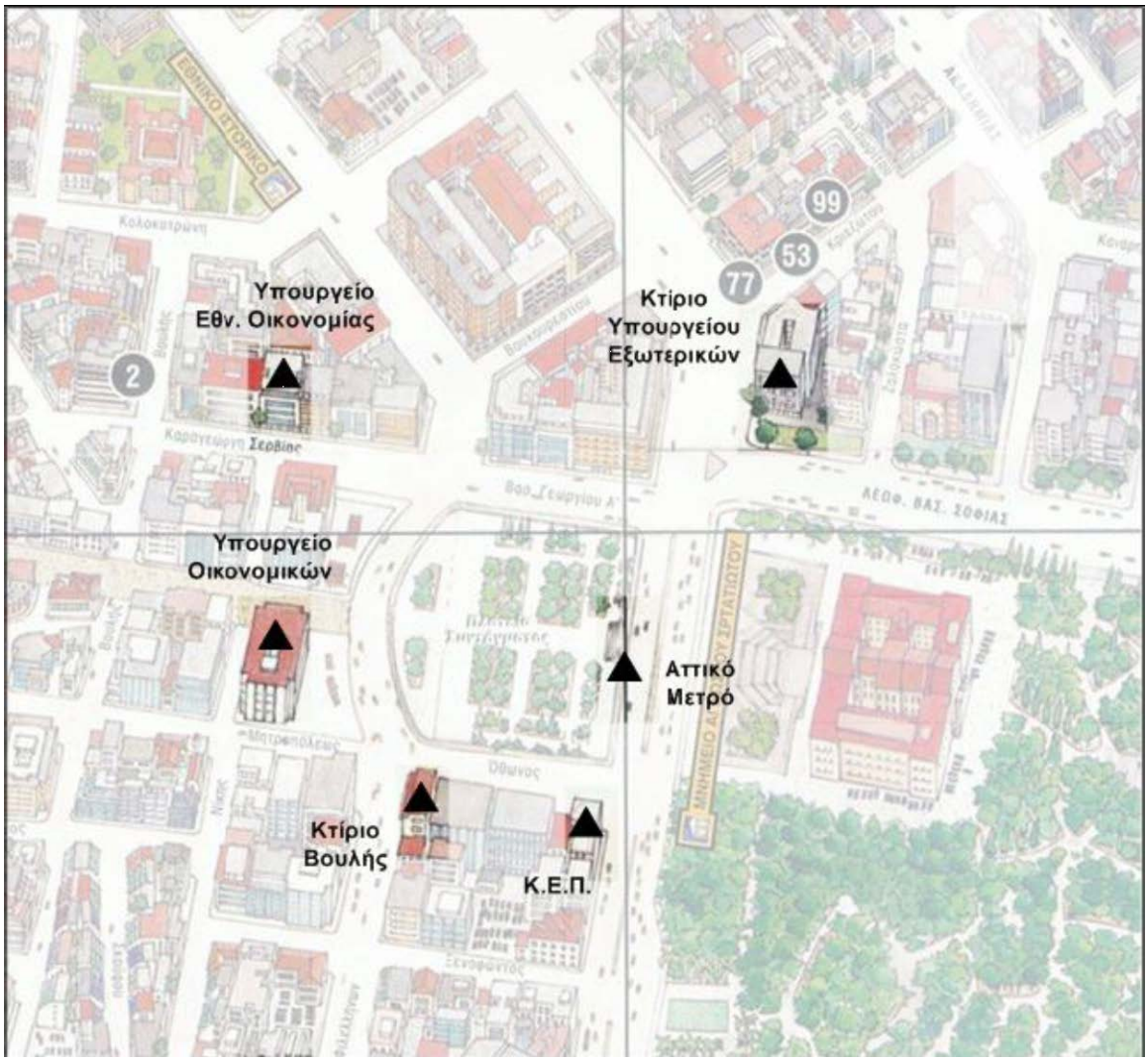
1. Κτίριο Υπουργείου Οικονομικών

2. Κτίριο Κέντρου Εξυπηρέτησης Πολιτών επί των Λεωφόρου Βασιλίσσης Αμαλίας και οδού Όθωνος

3. Κτίριο που ανήκει στη Βουλή επί των οδών Φιλελλήνων και Όθωνος

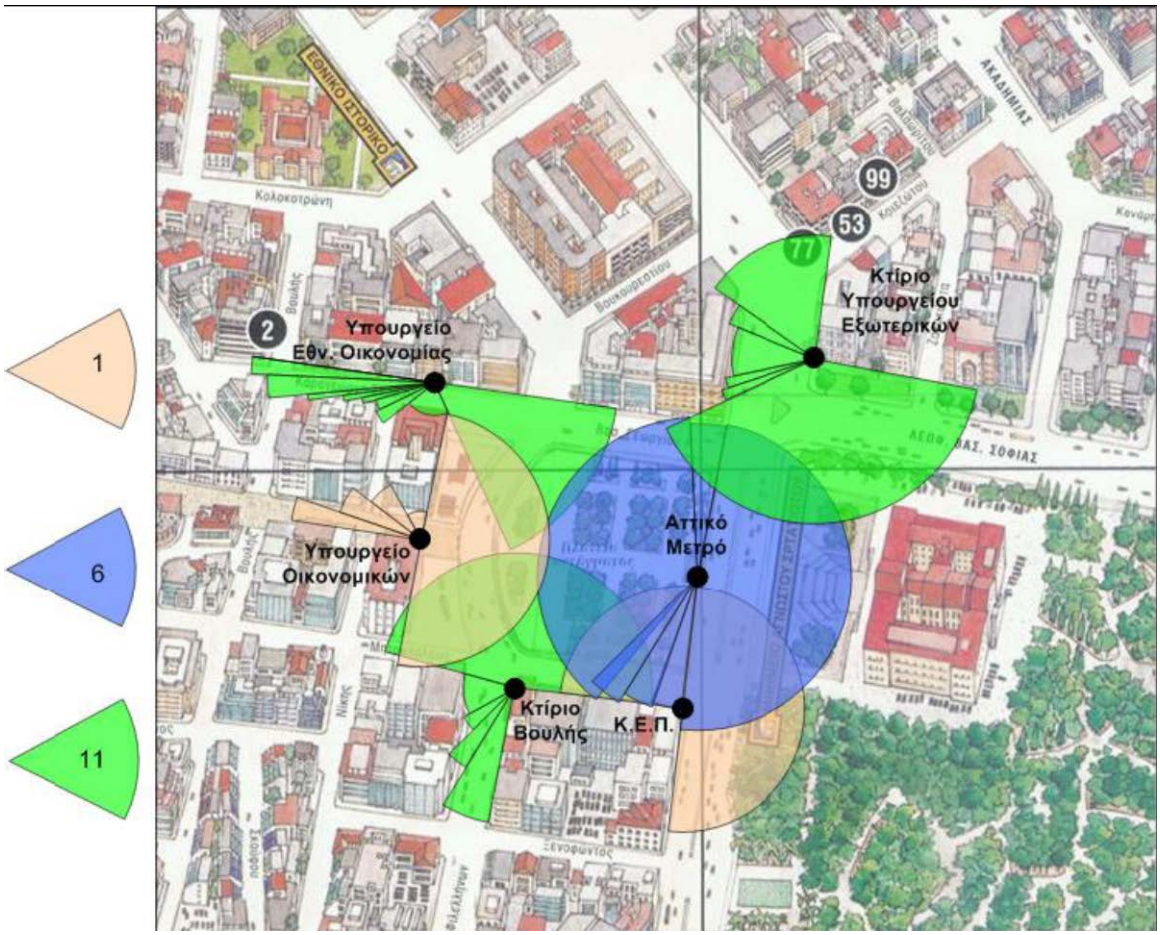
4. Κτίριο Υπουργείου Εθνικής Οικονομίας επί της οδού Καραγεώργη Σερβίας

5. Κτίριο που ανήκει στο Υπουργείο Εξωτερικών επί της λεωφόρου Βασιλίσσης Σοφίας και της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου)



Εικόνα 2. : Ένα σύνολο κτιρίων που μπορούν να επιτύχουν κάλυψη της ζητούμενης περιοχής.

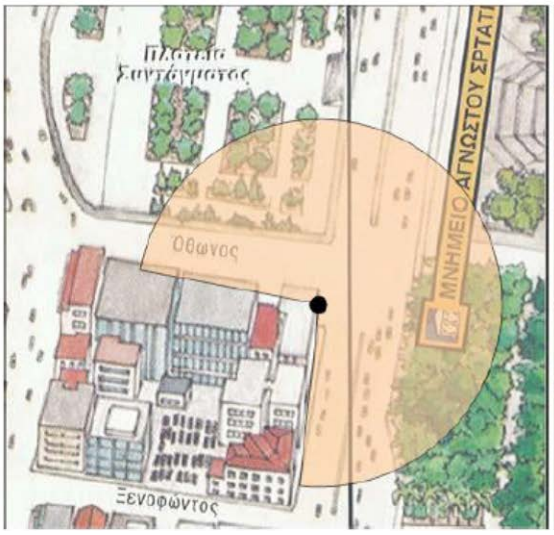
Η περιοχή κάλυψης του ασύρματου δικτύου φαίνεται στην *Εικόνα 3*. Αυτή η κάλυψη επιτυγχάνεται με τον συνδυασμό σημείων πρόσβασης στα κτίρια που προαναφέρθηκαν. Τα σημεία είναι τοποθετημένα με τέτοιο τρόπο ώστε να καλύπτουν τη μέγιστη δυνατή έκταση στην Πλατεία Συντάγματος και γύρω από αυτή. Οι κεραίες που χρησιμοποιούνται στο κομμάτι της ασύρματης πρόσβασης των χρηστών είναι πολυκατευθυντικές (omni) και ακτινοβολούν σε 360° στο οριζόντιο επίπεδο.



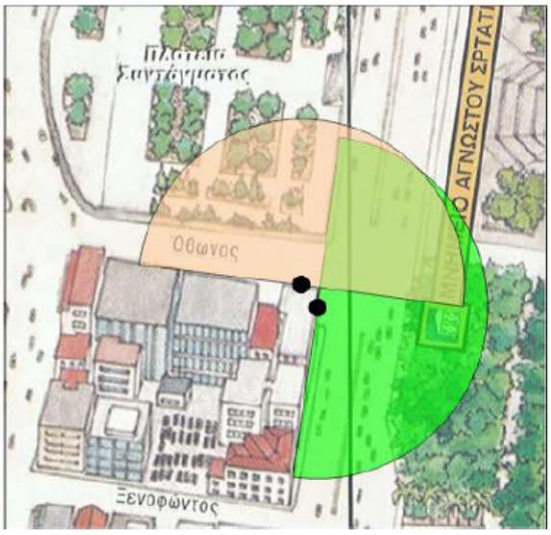
Εικόνα 3. : Συνολική Περιοχή Κάλυψης

Η *Εικόνα 3* παρουσιάζει την τοποθέτηση των hotspot στα προαναφερθέντα κτίρια περιμετρικά της Πλατείας. Τα διαφορετικά κανάλια (1, 6 και 11) που χρησιμοποιούνται για τις περιπτώσεις επικάλυψης φαίνονται με το αντίστοιχα χρώμα. Τα σημεία στα οποία τοποθετούνται τα hotspot (φαίνονται με ένα μαύρο κύκλο στην Εικόνα 3) είναι τα εξής:

1. Κτίριο Κέντρου Εξυπηρέτησης Πολιτών επί της λεωφόρου Βασιλίσσης Αμαλίας και της οδού Όθωνος. Το hotspot τοποθετείται ακριβώς στη γωνία, προκειμένου να καλύψει τμήματα της Πλατείας και της λεωφόρου Βασιλίσσης Αμαλίας. Στην περίπτωση που δεν είναι δυνατόν να τοποθετηθεί ακριβώς στη γωνία (βλ. *Εικόνα 4*), τότε μπορεί να δημιουργηθεί η ίδια κάλυψη με τη χρήση 2 hotspot (βλ. *Εικόνα 5*).

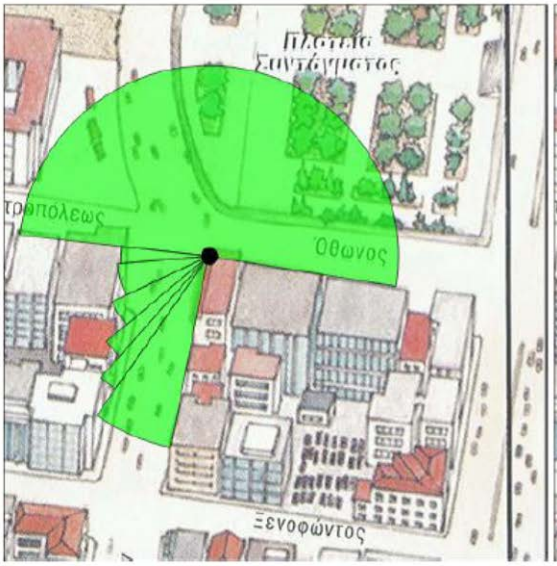


Εικόνα 4. : Κάλυψη από Κ.Ε.Π. με ένα Hotspot ακριβώς στη γωνία.

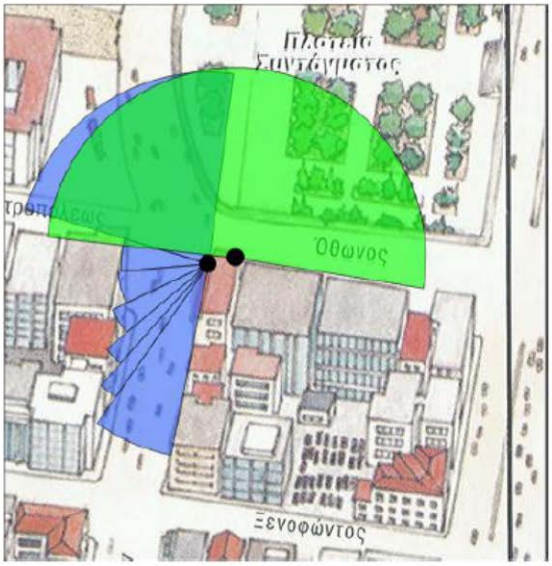


Εικόνα 5. : Κάλυψη από Κ.Ε.Π. με δύο Hotspot

2. Κτίριο της Βουλής επί των οδών Όθωνος και Φιλελλήνων. To hotspot τοποθετείται ακριβώς στη γωνία του κτιρίου, προκειμένου να καλύψει τμήματα τόσο της Πλατείας όσο και της οδού Όθωνος, καθώς και ένα μικρό κομμάτι στην αρχή της οδού Μητροπόλεως (*βλ. Εικόνα 6*). Στην περίπτωση που αυτό δεν καταστεί εφικτό, τοποθετούνται δύο hotspot, το ένα επί της οδού Όθωνος και το δεύτερο επί της οδού Φιλελλήνων, πετυχαίνοντας την ίδια κάλυψη (*βλ. Εικόνα 7*).

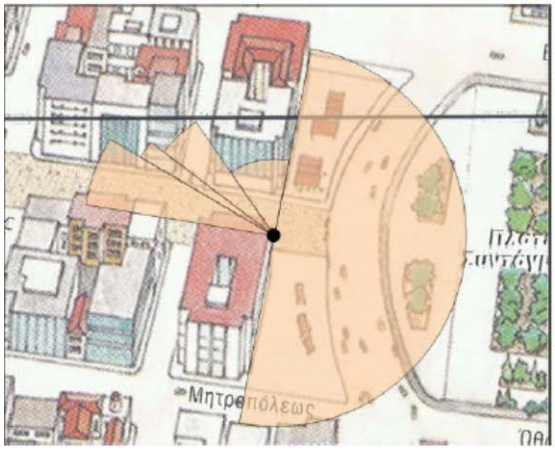


Εικόνα 6. : Κάλυψη από κτίριο Βουλής με ένα hotspot ακριβώς στη γωνία.



Εικόνα 7. : Κάλυψη από κτίριο Βουλής με δύο hotspot.

3. Κτίριο Υπουργείου Οικονομικών. Το hotspot τοποθετείται ακριβώς στη γωνία επί της οδού Ερμού, προκειμένου να καλύψει τόσο τμήμα της Πλατείας όσο και ένα τμήμα στην αρχή της οδού Ερμού (*βλ. Εικόνα 8*). Στην περίπτωση που δεν επιτευχθεί η τοποθέτηση ακριβώς στη γωνία, τότε μπορούν να τοποθετηθούν δύο hotspot, το ένα επί της πλευράς που κτιρίου προς την μεριά της Πλατείας και το άλλο επί της οδού Ερμού, δημιουργώντας την ίδια κάλυψη (*βλ. Εικόνα 9*).



Εικόνα 8.:Κάλυψη από κτίριο Υπ. Οικονομικών με ένα hotspot ακριβώς στη γωνία

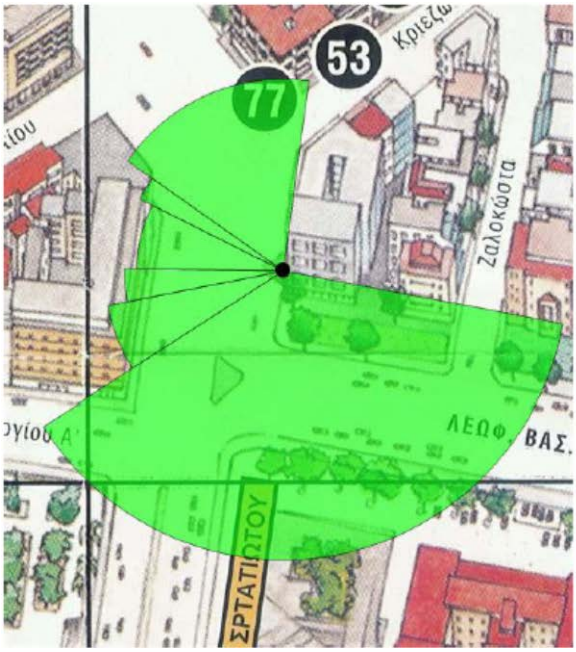
Εικόνα 9.: Κάλυψη από κτίριο Υπ. Οικονομικών με δύο hotspot

4. Κτίριο Υπουργείου Εθνικής Οικονομίας επί της οδού Καραγεώργη Σερβίας. Στη συγκεκριμένη περίπτωση δεν υπάρχει η δυνατότητα κάλυψης μεγάλης περιοχής. Η περιοχή που καλύπτεται είναι ένα τμήμα της Πλατείας, καθώς και το αρχικό τμήμα της οδού Καραγεώργη Σερβίας περίπου μέχρι το ύψος της οδού Βουλής.

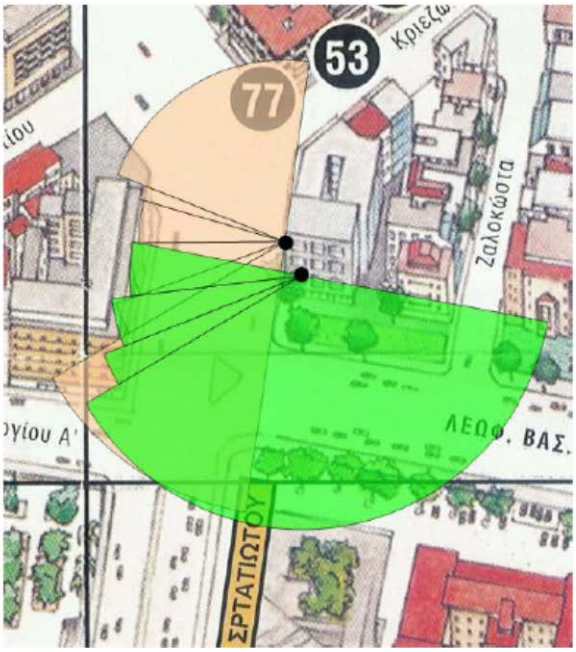
5. Σημείο της «Αττικό Μετρό» επί της Λεωφόρου Βασιλίσσης Αμαλίας. Το συγκεκριμένο hotspot επιτυγχάνει κάλυψη στο κύριο κομμάτι της Πλατείας.

6. Σημείο του Υπουργείου Εξωτερικών επί της Λεωφόρου Βασιλίσσης Σοφίας και της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου). Η περιοχή που καλύπτεται είναι (*βλ. Εικόνα 10*) ένα τμήμα της Πλατείας, ένα τμήμα στην αρχή της οδού Βασιλίσσης Σοφίας και ένα τμήμα στην αρχή της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου). Στην περίπτωση αυτή τοποθετείται ένα hotspot ακριβώς στη γωνία επί της λεωφόρου Βασιλίσσης Σοφίας και Ελευθερίου Βενιζέλου. Στην περίπτωση που αυτό δεν καταστεί δυνατό, τότε μπορούν να

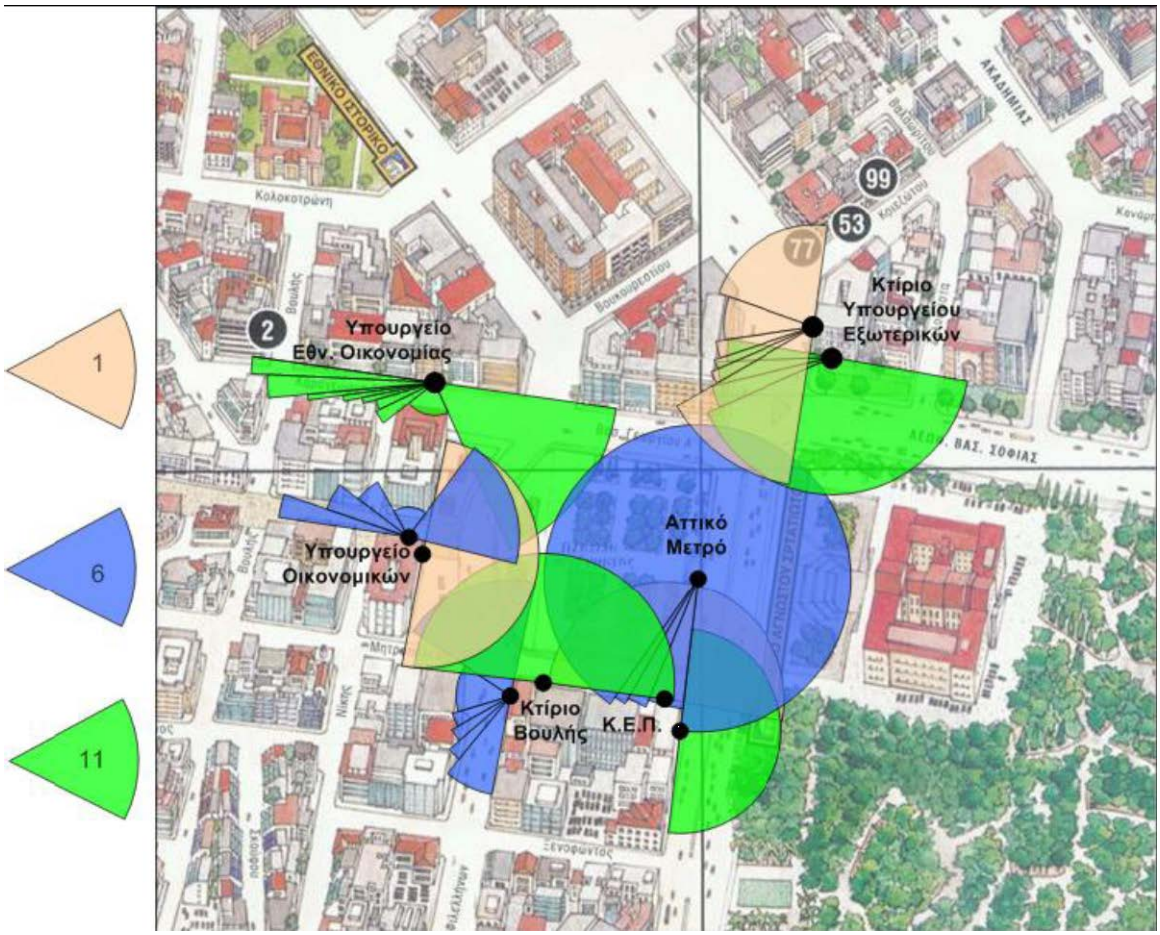
τοποθετηθούν δύο hotspot, ένα επί της Λεωφόρου Βασιλίσσης Σοφίας και ένα επί της οδού Ελευθερίου Βενιζέλου (*βλ. Εικόνα 11*).



Εικόνα 10. : Κάλυψη από κτίριο Υπ.Εξωτερικών με ένα hotspot ακριβώς στη γωνία.



Εικόνα 11.:Κάλυψη από κτίριο Υπ.Εξωτερικών με δύο hotspot



Εικόνα 12. : Περιοχή Συνολικής Κάλυψης χρησιμοποιώντας 2 hotspot στα κτίρια Κ.Ε.Π., Υπ. Οικονομικών, Βουλής και Υπ. Εξωτερικών.

Στην Εικόνα 12 φαίνεται η συνολική περιοχή κάλυψης χρησιμοποιώντας το μέγιστο αριθμό hotspot, δηλ. 2 hotspot σε κάθε γωνιακό σημείο εξυπηρέτησης. Παρατηρούμε ότι στην περίπτωση αυτή απαιτούνται 10 hotspot προκειμένου να καλυφθεί η περιοχή που μας ενδιαφέρει. Από την εικόνα γίνεται εμφανές ότι η καλυπτόμενη περιοχή είναι η πλέον πολυσύχναστη, γεγονός που αυξάνει την αξία του συγκεκριμένου έργου, προωθώντας σημαντικά τη χρήση ασύρματων δικτυακών τεχνολογιών στους πολίτες.

C. ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ATHENSWIFI

Η αρχιτεκτονική του Ασύρματου Δικτύου AthensWiFi είναι όμοια με εκείνη του γενικού Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου που περιγράφηκε παραπάνω. Το συνολικό δίκτυο χωρίζεται σε επιμέρους υποσυστήματα, καθένα από τα οποία πραγματοποιεί και μια ιδιαίτερη λειτουργία.

Τα υποσυστήματα αυτά είναι τα εξής:

- **Υποσύστημα Ασύρματης Πρόσβασης Χρηστών (hotspot)**
- **Υποσύστημα Περιφερειακού Σημείου Συλλογής κίνησης (Backhaul)**
- **Υποσύστημα Κεντρικού Σημείου Διασύνδεσης**

Τα συστήματα αυτά έχουν περιγραφεί αναλυτικά προηγουμένως. Παρακάτω περιγράφουμε τα ιδιαίτερα χαρακτηριστικά που έχουν τα υποσυστήματα του συγκεκριμένου δικτύου.

i. Υποσύστημα Ασύρματης Πρόσβασης Χρηστών (hotspot)

Στην περίπτωση του Ασύρματου Δικτύου AthensWiFi τα σημεία ασύρματης πρόσβασης βρίσκονται κοντά στο επίπεδο της Πλατείας. Επειδή τα hotspot δεν πρέπει να είναι φυσικώς προσβάσιμα από τον κόσμο που βρίσκεται στην Πλατεία (για λόγους προστασίας του εξοπλισμού), τοποθετούνται σε ένα ύψος 5μ από το επίπεδο της Πλατείας. Κάθε hotspot περιέχει ένα κουτί μέσα στο οποίο βρίσκεται κλειδωμένο το Access Point. Εκτός του κουτιού υπάρχει μια πολυκατευθυντική κεραία (omni) και ένα καλώδιο ethernet (cat 5e) που μεταφέρει και το ρεύμα (power-over-ethernet). Το καλώδιο συνδέεται με ένα υποσύστημα backhaul που βρίσκεται στην ταράτσα του κτιρίου στο οποίο είναι τοποθετημένο το hotspot.

ii. Υποσύστημα Backaul

Κάθε υποσύστημα Backhaul είναι τοποθετημένο στην ταράτσα του κτιρίου στο οποίο είναι τοποθετημένα 1-2 hotspot. Χρησιμοποιώντας την κατευθυντική κεραία, το Υποσύστημα Backhaul συνδέεται με το Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.

Η λειτουργία που επιτελεί κάθε ένα από τα υποσυστήματα Backhaul είναι να συλλέγουν τη κίνηση από τα επιμέρους hotspot που είναι τοποθετημένα στο επίπεδο των χρηστών (π.χ. επίπεδο κάποιας πλατείας), να τη μετατρέπουν σε ασύρματη μορφή τύπου 802.11b και να την προωθούν προς το Κεντρικό Σημείο Διασύνδεσης.

iii. Υποσύστημα Κεντρικού Σημείου Διασύνδεσης

Το Κεντρικό Σημείο Διασύνδεσης είναι το υποσύστημα που συνδέει όλη τη δικτυακή υποδομή με το δίκτυο κορμού (Διαδίκτυο). Στην περίπτωση του ασύρματου Δικτύου AthensWiFi, το Κ.Σ.Δ. είναι τοποθετημένο σε ειδικά εξοπλισμένο χώρο στο **Υπουργείο Οικονομικών** (*βλ. Εικόνα 8*).

Στο σημείο του Κεντρικού Σημείου Διασύνδεσης, εκτός από τον δικτυακό εξοπλισμό για την συγκέντρωση της κίνησης από τα επιμέρους Υποσυστήματα Backhaul, τοποθετείται εξοπλισμός Backhaul προκειμένου να καταστεί εφικτή η τοποθέτηση hotspot (ενός ή δύο), κοντά στο επίπεδο της Πλατείας. Στην περίπτωση αυτή δεν απαιτείται η προμήθεια κατευθυντικής κεραίας.

URL ‘s

1) http://users.sch.gr/sonic2000gr/files/thebook/thebook.html

2) http://ru6.cti.gr/bouras/

3) 3)http://mm.aueb.gr/technicalreports/2006-MMLAB-TR-04.pdf

4) http://ru6.cti.gr/bouras/lessons.php?id=1&action=dialekseis

5) http://www.cnc.uom.gr/services/pdf/section1(2).pdf

6) http://www.it.uom.gr/project/MultimediaTechnologyNotes/chap2d_1.htm#_ftnref1

7) mpl.med.uoa.gr/ekpaideytiko-yliko/i-y-stin-iatrik/diktya-ilektronikon-ypologiston.pdf

8) http://www.papaki.panteion.gr/teuxos18/diktya.htm

9) www.ebusinessforum.gr/engine/index.php?op=modload&modname=Downloads&action=downloadsviewfile...

10) http://2tee-n-smyrn.att.sch.gr/texn_site/texn2.htm

11) infoweb.ote.gr/intranet/index.htm

12) http://www.athenswifi.gr/110707-ET-pg26-27.pdf

13) www.ebusinessforum.gr/index.php?op=modload&modname=Downloads&pageid=1423 -

14) http://www.athenswifi.gr/meleti-public-wireless.pdf

15) www.entelia.gr/el/node/42 - 9k