Πανεπιστήμιο Θεσσαλίας

Τμήμα Μηχανικών Ηλεκτρονικών υπολογιστών, Τηλεπικοινωνιών και Δικτύων

Διπλωματική Εργασία:

WI-FI

Συγγραφεύς: Γιώργος Καρνιαβούρας

1ος Επιβλέπων καθηγητής: Κατσαρός Δημήτριος

2ος Επιβλέπων καθηγητής: Σταμούλης Γεώργιος

ΕΠΙΤΡΟΠΗ ΕΞΕΤΑΣΗΣ

1ος Εξεταστής – Επιβλέπων Καθηγητής

Δρ. Κατσαρός Δημήτριος
Τμήμα Μηχανικών Η/Υ, Τηλεπικοινωνιών & Δικτύων
Πανεπιστήμιο Θεσσαλίας

2ος Εξεταστής

Δρ. Σταμούλης Γεώργιος
Τμήμα Μηχανικών Η/Υ, Τηλεπικοινωνιών & Δικτύων
Πανεπιστήμιο Θεσσαλίας

Ευχαριστίες.

Ολοκληρώνοντας την παρούσα διπλωματική μου εργασία, θα ήθελα να αναγνωρίσω, την πραγματικά πολύτιμη βοήθεια που μου προσφέρθηκε, και να πω, ένα μεγάλο **«ευχαριστώ»** στον επιβλέποντα καθηγητή μου, Δρ. Κατσαρό Δημήτριο. Επίσης οφείλω ένα «ευχαριστώ» στον δεύτερο επιβλέποντα καθηγητή μου, Σταμούλη Γεώργιο για την άψογη συνεργασία.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΕΣ ΕΙΚΟΝΕΣ

ΠΕΡΙΕΧΟΜΕΝΟΙ ΠΙΝΑΚΕΣ

ΠΡΟΛΟΓΟΣ

Στην παρούσα πτυχιακή εργασία πραγματοποιείται μια περιγραφή των δικτύων Wi-Fi. Αρχικά γίνεται μια αναφορά στα είδη και την χρησιμότητα των ασύρματων δικτύων που χρησιμοποιούνται ευρέως. Στην συνέχεια δίνεται ιδιαίτερη βάση στο πρωτόκολλο 802.11b, του οποίου περιγράφεται η αρχιτεκτονική, δηλαδή οι βασικές αρχές λειτουργίας του, η μεταφορά δεδομένων, οι συσκευές που χρησιμοποιούνται για να υλοποιηθεί το δίκτυο οι τρόποι σύνδεσης καθώς και η εμβέλεια και οι επιδόσεις του συστήματος και τέλος τα RF στοιχεία του δικτύου. Παρουσιάζονται επισης οι βασικές τεχνικές που χρησιμοποιούνται για την ασφάλεια κατά την μεταφορά των δεδομένων σε ένα τέτοιο δίκτυο [Network Name(SSID), Κρυπτογράφιση WEP, Τείχος Προστασίας, Εικονικά Ιδιωτικά Δίκτυα(VPN)] καθώς και των αδυναμιών που παρουσιάζουν αυτές οι τεχνικές. Επισημαίνεται πως οι σύγχρονες τεχνικές δεν μπορούν να προσφέρουν επαρκή προστασία από επίδοξους υποκλοπείς. Στην εργασία περιγράφονται επίσης , σύντομα ,οι παράμετροι που πρέπει να ληφθούν υπ' όψην κατά την κατασκευή ενός δικτύου 802.11(Τοπολογία, είδος συνδέσμων, Περιβάλλον, Διαπερατότητα, κανάλια πολλαπλών διαδρομών κ.λ.π). Επίσης γίνεται σύντομη αναφορά στον τρόπο σωστής λειτουργίας και συντήρησης ενός δικτύου. Η εργασία κλείνει με αναφορά σε μια σημαντική εφαρμογή του Wi-Fi, το Voice over IP.

1. ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Ο όρος ασύρματο δίκτυο αναφέρεται σε κάθε δίκτυο, το οποίο είναι υλοποιημένο χωρίς την χρήση καλωδίων. Συνήθως ένα τέτοιο τηλεπικοινωνιακό δίκτυο υλοποιείται με κάποιο είδος απομακρυσμένου συστήματος μετάδοσης πληροφοριών που χρησιμοποιεί ηλεκτρομαγνητικά κύματα, όπως ραδιοκύματα. Υπάρχουν διάφορα είδη ασύρματων δικτύων.

1.1. Είδη Ασύρματων Δικτύων

Wireless PAN

Τα Wireless Personal Area Networks (WPANs) συνδέουν συσκευές σε ένα σχετικά μικρό χώρο, γενικά στην εμβέλεια ενός ανθρώπου. Το Bluetooth για παράδειγμα παρέχει ένα WPAN που μπορεί να χρησιμοποιηθεί για συνδέσεις όπως ακουστικών με κινητό τηλέφωνο.

Wireless LAN

Τα Wireless Local Area Networks (WLANs) παρέχουν ένα LAN χρησιμοποιώντας ραδιοκύματα αντί για καλώδια σε μία μικρή περιοχή όπως ένα σπίτι, ένα γραφείο ή ένα σχολείο. Τα περισσότερα WLANs βασίζονται στο IEEE 802.11. Ο όρος WI-Fi χρησιμοποιείται όλο και περισσότερο ως συνώνυμο για τα 802.11 WLANs , αν και στην πραγματικότητα είναι μια πιστοποίηση της συνεργασίας 802.11 συσκευών.

Wireless MAN

Τα Wireless Metropolitan Area Networks είναι ένας τύπος δικτύου που συνδέει περισσότερα WLANs. Ένας όρος που χρησιμοποιείται για να αναφερθούμε στα WMANs είναι το WiMAX.

Mobile devices networks

Με την ανάπτυξη των έξυπνων τηλεφώνων (smart phones) τα δίκτυα κινητών επικοινωνιών μεταφέρουν πολλών ειδών δεδομένα εκτός της φωνής.

- **Global System for Mobile Communications (GSM):** Το δίκτυο GSM χωρίζεται σε τρία κύρια συστήματα: το σύστημα εναλλαγής, το σύστημα σταθμού βάσης και το σύστημα λειτουργίας και υποστήριξης. Το κινητό τηλέφωνο συνδέεται στο σύστημα σταθμού βάσης που εν συνεχεία συνδέεται στο σταθμό λειτουργίας και υποστήριξης. Τέλος συνδέεται στο σταθμό εναλλαγής όπου η κλήση μεταφέρεται εκεί που πρέπει να πάει.
- Personal Communications Service (PCS): Το PCS είναι ένα είδος δικτύου που χρησιμοποιείται από κινητά τηλέφωνα στην Βόρειο Αμερική και την Νότιο Ασία.
- D-AMPS: Το Digital Advanced Mobile Phone Service είναι ένα είδος δικτύου που έχει πλέον ξεπεραστεί από την ανάπτυξη της τεχνολογίας και του GSM.

1.2. Χρήσεις και Εφαρμογές Ασύρματων Δικτύων

Τα ασύρματα δίκτυα είχαν εφαρμογές και αποδοχή αποδοχή από τον κόσμο εδώ και πολλά χρόνια. Από τον δεύτερο παγκόσμιο πόλεμο χρησιμοποιήθηκαν για αποστολή πληροφοριών. Από τότε τα ασύρματα δίκτυα αναπτύσσονται και εξελίσσονται συνεχώς και οι χρήσεις τους έχουν αυξηθεί και εξαπλωθεί σε πολλούς τομείς.

- Τα κινητά τηλέφωνα είναι μέρος τεράστιων ασύρματων δικτύων.
- Οι δορυφόροι επιτρέπουν την αποστολή πληροφοριών, εικόνων, ήχου και κάθε μορφής δεδομένων σε όλο τον κόσμο.
- Υπηρεσίες όπως η αστυνομία και η πυροσβεστική χρησιμοποιούν ασύρματη δικτύωση για γρήγορη και εύκολη επικοινωνία.
- Γραφεία, υπηρεσίες και επιχειρήσεις χρησιμοποιούν ασύρματη δικτύωση για κοινή χρήση δεδομένων.
- Το internet στα περισσότερα σπίτια πλέον φτάνει ενσύρματα αλλά μέσα σε αυτά χρησιμοποιούνται συσκευές (wireless routers) που στέλνουν το σήμα στον υπολογιστή ασύρματα. Επίσης με τον ίδιο τρόπο πολλές βιβλιοθήκες, καφετέριες πανεπιστήμια κ.α. παρέχουν στους παρευρισκόμενους φορητές υπολογιστές ασύρματη δικτύωση

Εικόνα 1 : Συσκευές που λειτουργούν με βάση το 802.11

2. ΠΡΩΤΟΚΟΛΛΟ 802.11 (WI-FI)

2.1. Ιστορική Ανασκόπηση

Το Wi-Fi(Wireless Fidelity) είναι απόρροια της απόφασης που πήρε το 1985 η κρατική επιτροπή επικοινωνιών των Η.Π.Α. να ανοιχτούν πολλές περιοχές του ασύρματου φάσματος για χρήση χωρίς κρατική άδεια. Για να λειτουργήσουν συσκευές όμως σε αυτές τις περιοχές έπρεπε να χρησιμοποιήσουν τεχνολογία διευρυμένου φάσματος. Η τεχνολογία αυτή απλώνει ένα σήμα σε ένα ευρύ φάσμα συχνοτήτων κάνοντας το λιγότερο επιρρεπές σε παρεμβολές.

Το 1990 μια νέα επιτροπή του IEEE(Institute of Electrical and Electronics Engineers) δημιουργήθηκε υπό το όνομα 802.11 για να ερευνήσει με σκοπό τη δημιουργία ενός νέου προτύπου. Η έκδοση αυτού του προτύπου έγινε τελικά το 1997. Δύο παραλλαγές εγκρίθηκαν μέσα στα επόμενα δύο χρόνια. Το 802.11b που λειτουργεί στην βιομηχανική, ιατρική και επιστημονική συχνότητα των 2.4 GHz και το 802.11a που λειτουργεί στις συχνότητες των 5.3 GHz και 5.8 GHz.

Η δημοτικότητα του Wi-Fi απογειώθηκε με την ανάπτυξη του γρήγορου ευρυζωνικού Internet στα σπίτια. Ήταν και παραμένει ο ευκολότερος τρόπος για να μοιραστεί ένας ευρυζωνικός σύνδεσμος μεταξύ πολλών υπολογιστών σε διάφορα σημεία ενός σπιτιού. Η ανάπτυξη δημόσιων σημείων παροχής δωρεάν ή έναντι αμοιβής Internet έχει συμβάλει στην δημοτικότητα του Wi-Fi. Μια Τρίτη παραλλαγή το 802.11g εγκρίθηκε τον Ιούνιο του 2003. Όπως το 802.11a, χρησιμοποιεί μία πιο εξελιγμένη μορφή διαμόρφωσης που λέγεται ορθογωνική πολυπλεξία με διαίρεση συχνότητας. Ή 802.11g χρησιμοποιώντας την ζώνη των 2.4 GHz μπορεί να πετύχει ταχύτητες ως 54 Mbps. Κι άλλες παραλλαγές έχουν εγκριθεί από τότε όπως το 802.11i για ασφάλεια, αλλά κανένα που να έχει στόχο την απόδοση.

Θα πρέπει να αναφέρουμε εδώ δύο ονόματα που σχετίζονται με τα πρότυπα ασύρματης δικτύωσης: το WECA και το WI-Fi.Η WECA (Wireless Ethernet Compatibility Alliance) είναι μια βιομηχανική ομάδα που περιλαμβάνει όλους τους κύριους κατασκευαστές 802.11b εξοπλισμού. Αποστολή τους είναι ο

έλεγχος και η πιστοποίηση ότι συσκευές ασύρματης δικτύωσης από όλες τις εταιρίες-μέλη μπορούν να λειτουργήσουν μαζί στο ίδιο δίκτυο και να προωθήσουν τα δίκτυα 802.11 ως το παγκόσμιο πρότυπο για τα WLANs. Η WECA για λόγους μάρκετινγκ υιοθέτησε το πιο "φιλικό" όνομα Wi-Fi που αποτελεί σύντομη γραφή του Wireless Fidelity για τα χαρακτηριστικά του 802.11 και άλλαξε το δικό της όνομα σε Wi-Fi Alliance. Μία ή δύο φορές το χρόνο, η Wi-Fi Alliance διεξάγει έναν έλεγχο "διαλειτουργεικότητας", όπου μηχανικοί από πολλούς κατασκευαστές επιβεβαιώνουν ότι οι συσκευές τους επικοινωνούν σωστά με συσκευές άλλων κατασκευαστών. Εξοπλισμός που έχει περάσει αυτούς τους ελέγχους και είναι επιβεβαιωμένο πως λειτουργεί σωστά φέρει το λογότυπο Wi-Fi που φαίνεται στην εικόνα 2.

Εικόνα 2 : Το λογότυπο Wi-Fi

2.2. Αρχιτεκτονική του Πρωτοκόλλου 802.11

Η υποενότητα αυτή περιγράφει τα πρότυπα και τις αρχές που διέπουν τα ασύρματα δίκτυα, και εξηγεί πως τα δεδομένα μετακινούνται μεταξύ των συσκευών που ανήκουν στο εκάστοτε δίκτυο.

2.2.1. Βασικές Αρχές και Τρόπος Λειτουργίας

Η μετακίνηση δεδομένων μέσω ενός ασύρματου δικτύου συνδυάζει τρία ξεχωριστά στοιχεία: τα ραδιοσήματα, την μορφή των δεδομένων και την δομή του δικτύου. Κάθε ένα από αυτά τα στοιχεία είναι ανεξάρτητο των άλλων δύο, οπότε είναι απαραίτητος ο προσδιορισμός και των τριών κατά την δημιουργία ενός νέου δικτύου. Κατά το μοντέλο αναφοράς OSI (Open Systems Interconnection), το ραδιοσήμα λειτουργεί στο φυσικό στρώμα και η μορφή των δεδομένων ελέγχει πολλά από τα ανώτερα στρώματα. Η δομή του δικτύου περιλαμβάνει τους αντάπτορες διασύνδεσης και τους σταθμούς βάσης που στέλνουν και λαμβάνουν τα ραδιοσήματα.

Σε ένα ασύρματο δίκτυο, οι αντάπτορες δικτύου σε κάθε υπολογιστή μετατρέπουν ψηφιακά δεδομένα σε ραδιοσήματα, τα οποία αναμεταδίδουν σε άλλες συσκευές του δικτύου, και μετατρέπουν εισερχόμενα ραδιοσήματα που δέχονται από άλλα στοιχεία του δικτύου ξανά σε ψηφιακά δεδομένα. Το IEEE 802.11 είναι ένα σύνολο προτύπων και χαρακτηριστικών για ασύρματα δίκτυα που ορίζουν τη μορφή και τη δομή των σημάτων τους.

Το αυθεντικό πρότυπο 802.11 εκδόθηκε όπως αναφέρθηκε σε προηγούμενο κεφάλαιο το 1997. Καλύπτει πολλά διαφορετικά είδη ασύρματων μέσων: δύο είδη ραδιο εκπομπών και δίκτυα που χρησιμοποιούν υπέρυθρο φως. Το πιο πρόσφατο πρότυπο 802.11 παρέχει πρόσθετα χαρακτηριστικά για ασύρματα δίκτυα Ethernet. Κι άλλα 802.11 πρότυπα ραδιοδικτύωσης με άλλα γράμματα στο όνομα τους κινούνται προς δημόσια έκδοση.

Το πιο ευρέως χρησιμοποιούμενο πρότυπο σήμερα είναι το 802.11b. Είναι το πρότυπο που συναντάται σχεδόν σε όλα τα γραφεία, δημόσιους χώρους και σπίτια. Αξίζει το κόπο να κρατάει κανείς επαφή με τις εξελίξεις των άλλων προτύπων, αλλά προς το παρόν το 802.11 είναι αυτό που χρησιμοποιείται σχεδόν σε όλες τις εφαρμογές. Για την περιγραφή της λειτουργίας θα βασιστούμε κυρίως στο 802.11b αλλά πολλές από τις πληροφορίες ισχύουν και για άλλα πρότυπα 802.11.

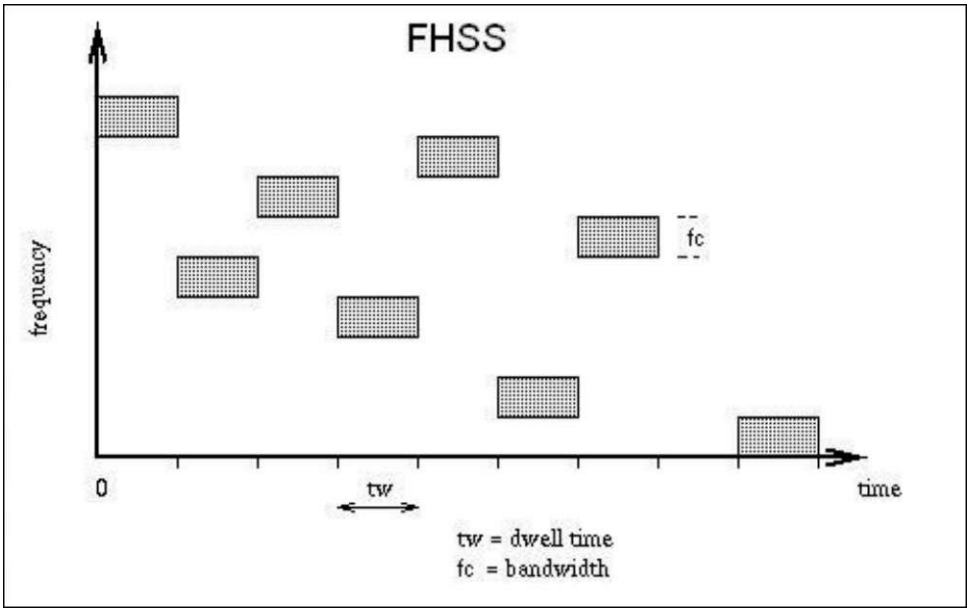
Τα δίκτυα 802.11b λειτουργούν σε μια ειδική ζώνη ραδιοσυχνοτήτων γύρω από τα 2.4 GHz που έχουν "κατοχυρωθεί" στα περισσότερα μέρη του κόσμου για μη-αδειοδοτημένες υπηρεσίες ραδιο-υπηρεσίες διευρυμένου φάσματος. Μη-αδειοδοτημένες σημαίνει ότι οποιοσδήποτε, χρησιμοποιώντας εξοπλισμό σύμφωνο με τις τεχνικές απαιτήσεις μπορεί να στείλει και να λάβει ραδιοσήματα σε αυτές τις συχνότητες, χωρίς να υποχρεούται να έχει άδεια. Αντίθετα με τις περισσότερες ραδιο-υπηρεσίες, που απαιτούν άδειες που αποδίδουν τη χρήση μιας συχνότητας σε έναν χρήστη ή μια ομάδα χρηστών και περιορίζουν την χρήση αυτής της συχνότητας σε ένα συγκεκριμένο είδος υπηρεσίας, μια μη-αδειοδοτημένη υπηρεσία είναι ελεύθερη για όλους και ο κάθε ένας έχει εξίσου δικαίωμα στο ίδιο κομμάτι του φάσματος. Θωρητικά, στην τεχνολογία διευρυμένου φάσματος είναι δυνατή η συνύπαρξη με άλλους χρήστες χωρίς να υπάρχει σημαντική παρεμπόδιση.

Διευρυμένο φάσμα είναι μια οικογένεια τρόπων αναμετάδοσης ενός ραδιοσήματος με χρήση ενός σχετικά ευρέος τμήματος του φάσματος. Τα ασύρματα δίκτυα Ethernet χρησιμοποιούν δύο διαφορετικά συστήματα ραδιο-αναμετάδοσης, το FHSS (FrequencyHopping Spread Spectrum) και το (Direct-Sequence Spread Spectrum). Κάποια παλαιότερα δίκτυα 802.11 χρησιμοποιούν το πιο αργό FHSS, αλλά τα σημερινής γενιάς 802.11b και 802.11a ασύρματα δίκτυα Ethernet κάνουν χρήση του DSSS.

Το διευρυμένο φάσμα προσφέρει σημαντικά πλεονεκτήματα σε σχέση με άλλα είδη ραδιο- σημάτων που χρησιμοποιούν ένα μοναδικό στενό κανάλι. Είναι εξαιρετικά αποδοτικό, ώστε οι ραδιο-αναμεταδότες να μπορούν να λειτουργήσουν με πολύ χαμηλή ισχύ. Λόγω του ότι λειτουργούν σε μια σχετικά ευρεία ζώνη συχνοτήτων, είναι λιγότερο ευαίσθητοι σε παρεμβολές από άλλα ραδιο-σήματα και ηλεκτρικό θόρυβο, που σημαίνει ότι τα σήματα μπορούν συχνά να διεισδύσουν σε περιβάλλοντα όπου ένα συμβατικό σήμα στενής ζώνης θα ήταν αδύνατο να ληφθεί σε κατανοητή μορφή, και επειδή ένα FHSS σήμα εναλλάσσεται μεταξύ πολλών καναλιών μπορεί να είναι πολύ δυσκολότερο να υποκλαπεί και να αποκωδικοποιηθούν οι πληροφορίες που μεταφέρει.

Frequency-Hopping Spread Spectrum (FHSS)

Όπως δείχνει το όνομα της η τεχνολογία FHSS διαιρεί ένα σήμα σε μικρά κομμάτια και "πηδά" από μια συχνότητα σε μία άλλα πολλές φορές το δευτερόλεπτο καθώς μεταδίδει αυτά τα κομμάτια. Ο πομπός και ο δέκτης λειτουργούν με ένα συγχρονισμένο μοτίβο αλμάτων που ορίζει την αλληλουχία με την οποία θα χρησιμοποιήσουν διαφορετικά υποκανάλια.



Εικόνα 3 : Παράδειγμα μετάδοσης πληροφορίας με FHSS

Τα συστήματα FHSS ξεπερνούν τις παρεμβολές από άλλους χρήστες χρησιμοποιώντας ένα στενό σήμα-φορέα που αλλάζει συχνότητα πολλές φορές κάθε δευτερόλεπτο. Πρόσθετα ζεύγη πομπών και δεκτών μπορούν να χρησιμοποιήσουν διαφορετικά μοτίβα αλμάτων στο ίδιο σύνολο από υποκανάλια την ίδια στιγμή. Σε οποιαδήποτε χρονική στιγμή, κάθε μετάδοση μάλλον χρησιμοποιεί διαφορετικό υποκανάλι, ώστε να μην υπάρχουν παρεμβολές μεταξύ των σημάτων. Όταν τελικά προκύψει παρεμβολή, το σύστημα ξαναστέλνει το ίδιο πακέτο μέχρι ο δέκτης να λάβει ένα καθαρό αντίγραφο και να στείλει επιβεβαίωση στο σταθμό εκπομπής.

Για τις υπηρεσίες ασύρματων δεδομένων, η μη-αδειοδοτημένη ζώνη των 2.4 GHz είναι χωρισμένη σε 75 υποκανάλια, κάθε ένα από τα οποία έχει πλάτος 1 MHz. Επειδή κάθε άλμα συχνότητας προσθέτει επιπλέον στη ροή δεδομένων οι αναμεταδόσεις FHSS είναι σχετικά αργές.

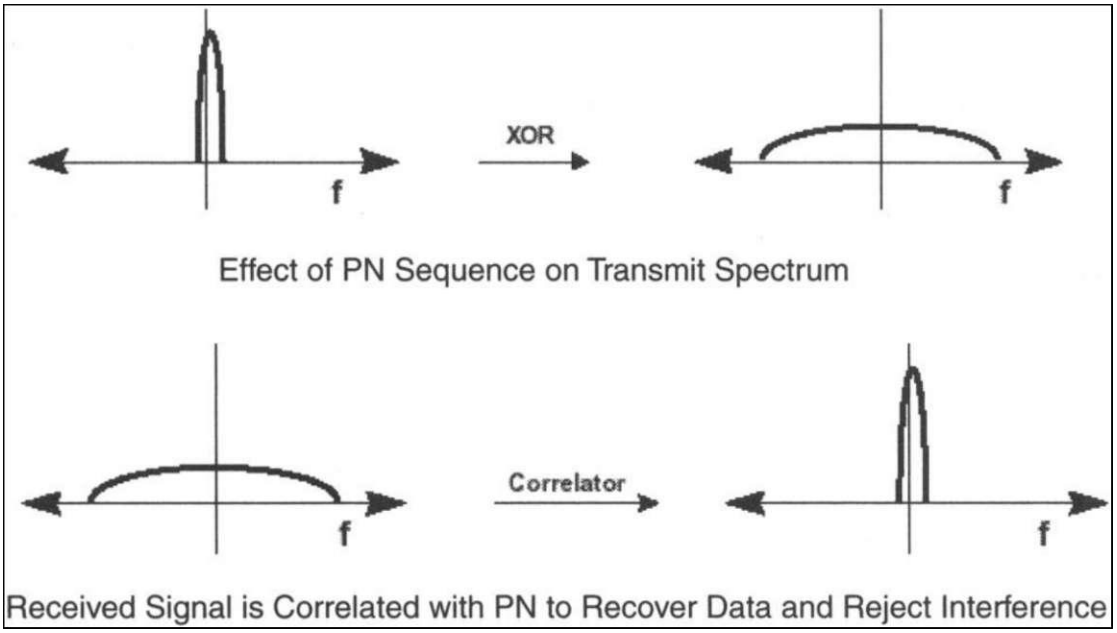
Direct-Sequence Spread Spectrum (DSSS)

Η τεχνολογία DSSS χρησιμοποιεί μία τεχνολογία παρόμοια των δορυφόρων Global Positioning System (GPS). Κάθε bit πληροφορίας συνδυάζεται με ένα μακρύτερο *pseudorandom numerical* (PN) στην διαδικασία αναμετάδοσης. Το αποτέλεσμα είναι μία ψηφιακή ροή μεγάλης ταχύτητας, που μετά διαμορφώνεται σε φέρουσα συχνότητα με χρήση *differential phase-shift keying* (DPSK). Η εικόνα 5 δείχνει πως γίνεται η διαμόρφωση με ακολουθία PN.

Για την διαμόρφωση χρησιμοποιείται μια μέθοδος που ονομάζεται ακολουθία Barker 11-chip (11 κομματιών) για να απλώσει το ραδιοσήμα μέσω ενός καναλιού πλάτους 22 MHz χωρίς να αλλάξει συχνότητα. Κάθε σύνδεσμος DSSS χρησιμοποιεί μόνο ένα κανάλι, χωρίς άλματα μεταξύ συχνοτήτων.

Στον δέκτη, ένα φίλτρο συσχέτισης χρησιμοποιείται για να αφαιρεθεί η ακολουθία PN και να ανακτηθούν τα αρχικά δεδομένα.

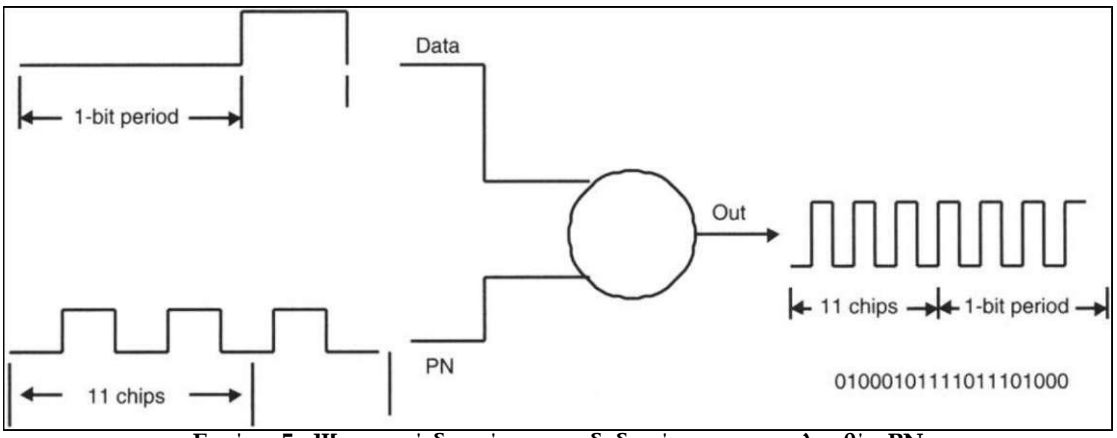
Όπως φαίνεται στην εικόνα 6 η ακολουθία PN απλώνει το μεταδιδόμενο εύρος ζώνης του σήματος (από εδώ προέρχεται και ο όρος διευρυμένο φάσμα) και μειώνει την μέγιστη ισχύ. Η συνολική ισχύς όμως παραμένει η ίδια.



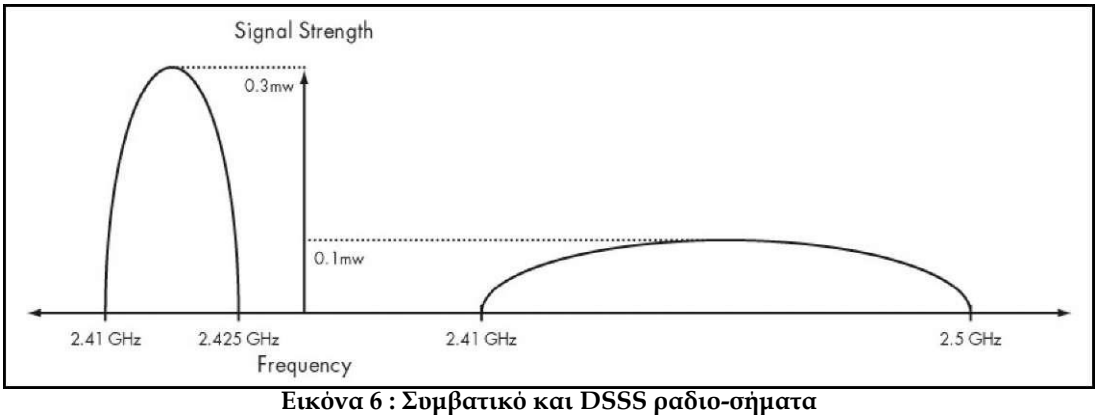
Εικόνα 4 : Διεύρυνση του σήματος με ακολουθία PN και επαναφορά του μετά την λήψη μέσω συσχετιστικού φίλτρου.

Όπως φαίνεται στην εικόνα 7, μια μετάδοση DSSS χρησιμοποιεί μεγαλύτερο εύρος ζώνης, αλλά μικρότερη μέγιστη ισχύ από ένα συμβατικό σήμα. Το ψηφιακό σήμα στα αριστερά είναι ένα μια συμβατική αναμετάδοση, όπου η ισχύς είναι συγκεντρωμένη σε ένα στενό εύρος ζώνης. Το σήμα DSSS στα δεξιά χρησιμοποιεί την ίδια ποσότητα ισχύος, αλλά την απλώνει σε μια πλατύτερη ζώνη από ραδιο-συχνότητες. Προφανώς το κανάλι DSSS των 22 MHz είναι πολύ πλατύτερο από το κανάλι του 1 MHz που χρησιμοποιεί το σύστημα FHSS.

Ένα από τα πλεονεκτήματα της χρήσης κωδίκων που απλώνουν το σήμα είναι ότι ακόμη και αν ένα ή περισσότερα bits χαθούν κατά την αναμετάδοση, στατιστικές τεχνικές μπορούν να ανακτήσουν τα χαμένα δεδομένα χωρίς την ανάγκη επανεκπομπής. Η αναλογία μεταξύ δεδομένων και το εύρος του κώδικα διεύρυνσης λέγεται κέρδος επεξεργασίας. Είναι 16 φορές το εύρος του διευρύνοντος κώδικα και μεγαλώνει τα πιθανά μοτίβα σε 64,000 (2^{16}), μειώντας τι πιθανότητες να "σπάσει" κανείς την μετάδοση.



Εικόνα 5 : Ψηφιακή διαμόρφωση δεδομένων με ακολουθία PN



Εικόνα 6 : Συμβατικό και DSSS ραδιο-σήματα

Ένας πομπός DSSS σπάει κάθε bit της αρχικής ροής δεδομένων σε μία σειρά μοτίβων bit που λέγονται chips και τα αναμεταδίδει σε έναν δέκτη που συναρμολογεί τα chips σε μια ροή δεδομένων που είναι πανομοιότυπη με την αρχική. Επειδή οι περισσότερες παρεμβολές αφορούν στενότερο εύρος ζώνης από ένα σήμα DSSS, και επειδή κάθε bit διαιρείται σε πολλά chips, ο δέκτης μπορεί συνήθως να αναγνωρίσει τον θόρυβο και να τον απορρίψει προτού αποκωδικοποιήσει το σήμα.

Όπως άλλα πρωτόκολλα δικτύωσης ένας ασύρματος DSSS σύνδεσμος ανταλλάσσει μηνύματα αναγνώρισης με κάθε πακέτο δεδομένων για να επιβεβαιώσει ότι ο δέκτης μπορεί να καταλάβει κάθε πακέτο. Ο τυπικός ρυθμός μεταφοράς δεδομένων για ένα δίκτυο DSSS 802.11b είναι 11 Mbps, αλλά όταν η ποιότητα σήματος δεν μπορεί να υποστηρίξει αυτή την ταχύτητα, ο πομπός και ο δέκτης χρησιμοποιούν μια διαδικασία που λέγεται δυναμική εναλλαγή ρυθμού για να ρίξει την ταχύτητα στα 5.5 Mbps. Η ταχύτητα μπορεί να πέσει επειδή υπάρχει μια πηγή ηλεκτρικού θορύβου κοντά στον δέκτη ή επειδή ο πομπός και ο δέκτης είναι πολύ απομακρυσμένη ο ένας από τον άλλο για να υποστηρίξουν λειτουργία μέγιστης ταχύτητας. Αν τα 5.5 Mbps είναι πάλι πολύ υψηλή ταχύτητα για να την υποστηρίξει ο σύνδεσμος, πέφτει πάλι στα 2 Mbps ή ακόμη και στο 1 Mbps.

Καθορισμός περιοχών συχνοτήτων

Με διεθνή συμφωνία, μια ζώνη συχνοτήτων κοντά στα 2.4 GHz έχει καθοριστεί όπως αναφέραμε για μη-αδειοδοτημένη χρήση, για βιομηχανικούς επιστημονικούς και ιατρικούς σκοπούς, περιλαμβάνοντας και τα ασύρματα δίκτυα δεδομένων διευρυμένου φάσματος. Παρ' αυτά, οι ακριβείς καθορισμοί συχνοτήτων διαφέρουν λίγο από ένα μέρος της γης στο άλλο. Ο πίνακας 1 δείχνει ενδεικτικά τις συχνότητες που χρησιμοποιούνται σε κάποιες περιοχές της γης.

Πίνακας 1: Μη *αδειοδοτημένες* συχνότητες διευρυμένου φάσματος ανά περιοχή

Περιοχή	**Ζώνη συχνοτήτων**
Βόρειος Αμερική	2.4000 to 2.4835 GHz
Ευρώπη	2.4000 to 2.4835 GHz
Γαλλία	2.4465 to 2.4835 GHz
Ισπανία	2.445 to 2.475 GHz
Ιαπωνία	2.471 to 2.497 GHz

Σχεδόν κάθε άλλη χώρα χρησιμοποιεί κάποια από αυτές τις ζώνες. Οι μικρές διαφορές που παρατηρούνται στον καθορισμό συχνοτήτων δεν είναι ιδιαίτερα σημαντικές (εκτός αν κανείς σκοπεύει να εκπέμψει πέρα από τα σύνορα της χώρας, ή κάποια άλλη εξίσου απίθανη περίπτωση), γιατί τα περισσότερα δίκτυα λειτουργούν μέσα στα όρια μιας χώρας ή περιοχής, και η συνήθης εμβέλεια σήματος είναι συνήθως μερικές εκατοντάδες μέτρα. Επίσης υπάρχει αρκετή υπερκάλυψη μεταξύ των συχνοτικών περιοχών στις διάφορες χώρες ώστε να μπορούν οι ίδιες συσκευές να λειτουργήσουν οπουδήποτε στον κόσμο. Ίσως χρειαστεί κανείς να θέσει τον αντάπτορα δικτύου του σε άλλο κανάλι

όταν τον χρησιμοποιεί εκτός της χώρας του, αλλά υπάρχει σχεδόν πάντα τρόπος να συνδεθεί, με την προϋπόθεση ότι υπάρχει δίκτυο στην περιοχή.

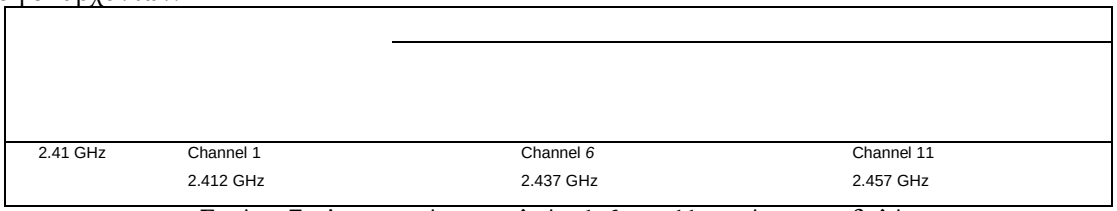
Στην Βόρειο Αμερική, οι συσκευές WI-Fi χρησιμοποιούν 11 κανάλια. Πολλές άλλες χώρες έχουν επικυρώσει 13 κανάλια, αλλά η Ιαπωνία χρησιμοποιεί 14 κανάλια, ενώ η Γαλλία μόνο 4. Ευτυχώς όλος ο κόσμος χρησιμοποιεί το ίδιο σύνολο καναλιών, οπότε το κανάλι 9 στη Νέα Υόρκη χρησιμοποιεί ακριβώς την ίδια συχνότητα με το κανάλι 9 στο Τόκιο και το Παρίσι. Στον πίνακα 2 φαίνονται τα κανάλια και οι αντίστοιχες συχνότητες που χρησιμοποιούν κάποιες περιοχές της γής.

Πίνακας 2 : Κανάλια και συχνότητες

Κανάλι	**Συχνότητα (GHz) και τοποθεσία**
1	2.412 (U.S., Europe, and Japan)
2	2.417 (U.S., Europe, and Japan)
3	2.422 (U.S., Europe, and Japan)
4	2.427 (U.S., Europe, and Japan)
5	2.432 (U.S., Europe, and Japan)
6	2.437 (U.S., Europe, and Japan)
7	2.442 (U.S., Europe, and Japan)
8	2.447 (U.S., Europe, and Japan)
9	2.452 (U.S., Europe, and Japan)
10	2.457 (U.S., Europe, France, and Japan)
11	2.462 (U.S., Europe, France, and Japan)
12	2.467 (Europe, France, and Japan)
13	2.472 (Europe, France, and Japan)
14	2.484 (Japan only)

Η συχνότητα κάθε καναλιού στον πίνακα είναι το μέσον μιας συχνοτικής περιοχής εύρους 22 MHz. Αυτό σημαίνει πως κάθε κανάλι συνυπάρχει σε κάποιο μέρος του φάσματος με το από πάνω και το από κάτω κανάλι. Ολόκληρη η ζώνη των 2.4 GHz έχει χώρο αρκετό μόνο για 3 εντελώς ξεχωριστά κανάλια. Οπότε αν ένα δίκτυο λειτουργεί στο κανάλι 4 και ένα γειτονικό στο κανάλι 5, το κάθε κανάλι θα ανιχνεύει το γειτονικό ως παρεμβολή. Και τα δύο δίκτυα θα λειτουργούν αλλά η απόδοση δεν θα είναι τόσο καλή όσο αν τα κανάλια λειτουγούσαν με μεγαλύτερη συχνοτική απόσταση μεταξύ τους, και αυτό θα αντανακλάται στην ταχύτητα μεταφοράς δεδομένων.

Για να ελαχιστοποιηθεί αυτό το είδος παρεμβολής, θα πρέπει να πρέπει κάθε δίκτυο να χρησιμοποιεί κανάλια που να απέχουν μεταξύ τους το λιγότερο 25 MHz ή 6 κανάλια σε αριθμό. Αν χρειαζόμαστε 3 δίκτυα μπορούμε να χρησιμοποιήσουμε τα κανάλια 1, 6, και 11 οπότε δε θα έχουμε πρακτικά καμία παρεμβολή όπως φαίνεται ξεκάθαρα στην εικόνα 5. Για περισσότερα από 3 δίκτυα θα υπάρχουν αναγκαστικά παρεμβολές, αλλά μπορούν να ελαχιστοποιηθούν ορίζοντας νέα κανάλια στο μέσον των ήδη υπάρχοντων.



Εικόνα 7 : Λειτουργία καναλιών 1, 6 και 11 χωρίς παρεμβολές

Βέβαια στην πράξη ακόμα και σε γειτονικά κανάλια κοντινά δίκτυα λειτουργούν συνήθως χωρίς σοβαρά προβλήματα.

Τα χαρακτηριστικά του 802.11 και πολλές εθνικές υπηρεσίες κανονισμών έχουν επίσης θέσει όρια στην ισχύ πομπών και κέρδος κεραιών που μπορούν να χρησιμοποιούν οι ασύρματες συσκευές Ethernet. Αυτοί οι περιορισμοί έχουν στόχο να περιορίσουν την απόσταση που μπορεί να ταξιδέψει ένας σύνδεσμος δικτύου, και κατ' επέκταση να επιτρέψουν σε περισσότερα δίκτυα να λειτουργούν στο ίδιο κανάλι χωρίς παρεμβολές. Αργότερα θα αναφερθούμε και σε τρόπους επέκτασης της εμβέλειας ενός ασύρματου δικτύου χωρίς παραβίαση νόμων.

2.2.2. Μεταφορά Δεδομένων και τρόποι σύνδεσης

Έχουμε λοιπόν πομπούς και δέκτες που λειτουργούν όλοι στις ίδιες συχνότητες και χρησιμοποιούν το ίδιο είδος διαμόρφωσης (διαμόρφωση είναι η μέθοδος που χρησιμοποιείται για να προστεθεί σε ένα ραδιοκύμα κάποιο είδος περιεχομένου όπως φωνή, ψηφιακά δεδομένα). Το επόμενο βήμα είναι να στείλουμε κάποια δεδομένα μέσω αυτών των συσκευών.

Για να γίνουν κατανοητά τα επόμενα πρέπει πρώτα να αναφερθούμε στην γενική δομή δεδομένων στους υπολογιστές και του τρόπους μεταγωγής δεδομένων των δικτύων.

Τα Bit και τα byte

Η μονάδα επεξεργασίας ενός υπολογιστή μπορεί να αναγνωρίσει μόνο δύο καταστάσεις πληροφορίας : είτε υπάρχει ένα σήμα στην είσοδο του επεξεργαστή, είτε δεν υπάρχει. Αυτές οι καταστάσεις περιγράφονται ως 0 και 1 αντίστοιχα, ή ως on και off. Κάθε κατάσταση 0 ή 1 είναι ένα bit.

Μεμονωμένα bits δεν είναι ιδιαίτερα χρήσιμα, όμως όταν συνδυάζονται 8 μαζί (σχηματίζοντας 1 byte) μπορούμε να έχουμε 256 διαφορετικούς συνδυασμούς. Αυτοί είναι αρκετοί για να συσχετίσουμε διαφορετικές αλληλουχίες bit σε κάθε γράμμα του αλφαβήτου (και στα κεφαλαία και στα μικρά γράμματα), στους αριθμούς από το 0 εώς το 9, στα κενά μεταξύ λέξεων και σε άλλα σύμβολα όπως τα σημεία στίξης και γράμματα από άλλες αλφαβήτους. Ένας σύγχρονος υπολογιστής αναγνωρίζει και μπορεί να επεξεργαστεί πολλά bytes την ίδια χρονική στιγμή. Όταν η επεξεργασία έχει ολοκληρωθεί, ο υπολογιστής χρησιμοποιεί των ίδιο κώδικα bit με την έξοδό του. Η έξοδος μπορεί να είναι συνδεδεμένη σε έναν εκτυπωτή, μια οθόνη ή ένα κανάλι επικοινωνίας δεδομένων. Επίσης μπορεί να είναι κάτι τελείως διαφορετικό όπως μία ακολουθία φώτων που αναβοσβήνουν.

Οι είσοδοι και έξοδοι που μας ενδιαφέρουν εδώ είναι αυτές που σχηματίζουν ένα κύκλωμα επικοινωνίας. Όπως ο επεξεργαστής του υπολογιστή, ένα κανάλι δεδομένων μπορεί να αναγνωρίσει μόνο ένα bit την φορά. Είτε υπάρχει σήμα στην γραμμή είτε όχι.
Σε μικρές αποστάσεις είναι δυνατόν να στείλουμε δεδομένα μέσω καλωδίου που μεταφέρει 8 (ή και πολλαπλάσια του 8) σήματα παράλληλα μέσω ξεχωριστών συρμάτων. Προφανώς, μια παράλληλη σύνδεση μπορεί να είναι 8 φορές γρηγορότερη από το αν στέλνουμε ένα bit μέσω ενός σύρματος. Όταν στέλνουμε δεδομένα σε μεγάλες αποστάσεις όμως το επιπρόσθετο κόστος μπορεί να είναι απαγορευτικό. Και όταν χρησιμοποιούμε υπάρχοντα κυκλώματα όπως τηλεφωνικές γραμμές δεν έχουμε επιλογή. Πρέπει να βρούμε έναν τρόπο να στείλουμε και τα 8 bits μέσω του ίδιου σύρματος (ή άλλο μέσο).

Η λύση είναι να στείλουμε 1 bit την φορά, με μερικά επιπρόσθετα bits και παύσεις που σηματοδοτούν την αρχή του κάθε νέου bit. Αυτό είναι ένα σειριακό κανάλι επικοινωνίας, γιατί στέλνουμε bits το ένα μετά το άλλο. Σ'αυτό το στάδιο, δεν έχει σημασία ποιο μέσο χρησιμοποιούμε για να στείλουμε αυτά τα bits (μπορεί να είναι ηλεκτρικά σήματα σε σύρμα, δύο διαφορετικοί ηχητικοί τόνοι, αλληλουχία φώτων που αναβοσβήνουν κ.α.) αλλά πρέπει να έχουμε τρόπο να μετατρέπουμε την έξοδο του υπολογιστή στο σήμα που χρησιμοποιεί το μέσο για την μεταφορά και στο τέλος να τα μετατρέπουμε ξανά στην αρχική μορφή.

Έλεγχος λαθών

Σε ένα τέλειο κύκλωμα μετάδοσης, το σήμα που εισέρχεται από τη μία πλευρά θα είναι πανομοιότυπο με αυτό που εξέρχεται από την άλλη. Αλλά στην πράξη, υπάρχει σχεδόν πάντα κάποιος θόρυβος που μπορεί να παρεμβληθεί στο αρχικό σήμα. Ως θόρυβος ορίζεται οτιδήποτε που προστίθεται στο αρχικό σήμα. Μπορεί να προκληθεί από έναν κεραυνό, παρεμβολή άλλο κανάλι επικοινωνίας, σκόνη ή άλλου είδους ανεπιθύμητο υλικό πάνω σε κάποιον ηλεκτρικό σύνδεσμο του κυκλώματος. Όποια και να είναι η πηγή , θόρυβος στο κανάλι μπορεί να διακόψει την ροή των δεδομένων. Σε ένα σύγχρονο επικοινωνιακό σύστημα τα bits ρέουν μέσα απ'το κύκλωμα με τεράστια ταχύτητα (εκατομμύρια κάθε δευτερόλεπτο) οπότε θόρυβος για έστω ένα κλάσμα του δευτερολέπτου μπορεί να εξαλείψει αρκετά bits ώστε τα δεδομένα μας να γίνουν ακατανόητα.

Γι'αυτό, πρέπει να συμπεριλάβουμε στη ροή των δεδομένων μια διαδικασία που λέγεται *έλεγχος λαθών.* Ο έλεγχος λαθών επιτυγχάνεται προσθέτοντας κάποιο είδος δεδομένης πληροφορίας που λέγεται checksum σε κάθε byte. Αν η λαμβάνουσα συσκευή ανακαλύψει ότι το checksum δεν είναι το αναμενόμενο, ζητάει το ίδιο byte ξανά από τον πομπό.

Αναγνώριση

Φυσικά, ένας υπολογιστής που στέλνει ένα μήνυμα ή μία ροή δεδομένων δεν μπορεί απλά να αρχίσει να στέλνει bytes. Πρώτα πρέπει να ειδοποιήσει την συσκευή που θα παίξει τον ρόλο του δέκτη ότι είναι έτοιμος να στείλει και να σιγουρευτεί ότι είναι έτοιμη να δεχτεί δεδομένα. Για να επιτευχθεί αυτό μια σειρά από αιτήσεις και απαντήσεις αναγνώρισης πρέπει να υπάρχουν γύρω από τα δεδομένα.

Η διαδικασία μοιάζει με την ακόλουθη :

Πομπός: Αίτημα αποστολής στον δέκτη.

Δέκτης: Απάντηση του δέκτη ότι είναι έτοιμος να δεχτεί δεδομένα.

Πομπός: Εκκίνηση αποστολής δεδομένων. Πομπός: Δεδομένα...

Πομπός: Πληροφορία ότι τελείωσε η αποστολή δεδομένων.

Δέκτης: Έλεγχος checksum και αποστολή πληροφορίας στον δέκτη ότι κάποια byte έχουν καταστραφεί.

Πομπός: Επαναποστολή των bytes. Πομπός: Ερώτηση αν

ελήφθησαν τα δεδομένα. Δέκτης: Απάντηση πως τα δεδομένα

έχουν φτάσει σωστά. *Εύρεση του προορισμού*

Η επικοινωνία μέσω ενός άμεσου φυσικού συνδέσμου μεταξύ της πηγής και του προορισμού δεν χρειάζεται να περιλαμβάνει κανένα είδος διεύθυνσης ως μέρος του μηνύματος. Ίσως χρειαστεί αρχικά να δημιουργηθεί η σύνδεση κάνοντας π.χ. ένα τηλεφώνημα ή βάζοντας καλώδια σε θέσεις ενός πίνακα, αλλά αφού δημιουργηθεί η σύνδεση παραμένει ως έχει μέχρι να δώσουμε εντολή στο σύστημα να την διακόψει. Αυτό το είδος σύνδεσης είναι πολύ καλό για φωνή και απλούς συνδέσμους δεδομένων, αλλά όχι τόσο αποτελεσματικό για ψηφιακά δεδομένα σε ένα περίπλοκο δίκτυο που εξυπηρετεί πολλές πηγές και προορισμούς γιατί απασχολεί το κύκλωμα συνεχώς, ακόμα και όταν δεν υπάρχουν δεδομένα στο κανάλι.

Η εναλλακτική λύση είναι να στείλουμε το μήνυμα σε ένα κέντρο μεταγωγής που θα το κρατήσει μέχρι ένας σύνδεσμος με τον προορισμό να ελευθερωθεί. Αυτό είναι γνωστό ως σύστημα αποθήκευσης και προώθησης. Αν το δίκτυο έχει σχεδιαστεί σωστά για το είδος δεδομένων και την κινητικότητα στο σύστημα ο χρόνος αναμονής θα είναι ασήμαντος. Αν το δίκτυο επικοινωνιών καλύπτει μεγάλη περιοχή, μπορεί το μήνυμα να προωθηθεί σε ένα ή περισσότερα κέντρα μεταγωγής πριν φτάσει στον

τελικό προορισμό. Το μεγάλο πλεονέκτημα αυτής της προσέγγισης είναι ότι πολλά μηνύματα μπορούν να μοιραστούν τα ίδια κυκλώματα.

Για να γίνει το δίκτυο ακόμα πιο αποτελεσματικό, μπορούμε να χωρίσουμε τα μηνύματα που είναι μεγαλύτερα από ένα βασικό όριο σε κομμάτια που ονομάζουμε πακέτα. Πακέτα από διαφορετικά μηνύματα μπορούν να ταξιδεύουν μαζί στο ίδιο κύκλωμα, καθώς κινούνται μεταξύ κέντρων αλλαγής, και να ανασυντάσσονται στο αρχικό μήνυμα όταν φτάσουν το καθένα στον προορισμό του. Κάθε πακέτο δεδομένων πρέπει να περιλαμβάνει ένα σύνολο πληροφοριών : Την διεύθυνση προορισμού του πακέτου ,την σειρά του σε σχέση με τα άλλα πακέτα του αρχικού μηνύματος κ.ο.κ. Κάποιες από αυτές τις πληροφορίες λένε στο κέντρο αλλαγής που πρέπει να σταλεί το μήνυμα και άλλες στην συσκευή-δέκτη πώς να ανακατασκευάσει το μήνυμα από τα πακέτα.

Το ίδιο μοτίβο επαναλαμβάνεται κάθε φορά που προσθέτουμε μια λειτουργία σε ένα σύστημα επικοινωνιών. Κάθε λειτουργία μπορεί να προσθέσει πληροφορίες στο αρχικό μήνυμα και να τις αφαιρέσει αφού έχει κάνει αυτό που του ζητήθηκε από τις επιπρόσθετες πληροφορίες. Μέχρι ένα μήνυμα να ταξιδέψει από έναν υπολογιστή που βρίσκεται σε ασύρματο δίκτυο, μέσω ενός LAN και μία πύλη δικτύου σε έναν απομακρυσμένο υπολογιστή συνδεδεμένο σε ένα άλλο LAN, πολλές επιπρόσθετες πληροφορίες μπορεί να προστεθούν και να αφαιρεθούν, πριν ο παραλήπτης λάβει το αρχικό μήνυμα. Ένα πακέτο δεδομένων που περιέχει πληροφορίες διεύθυνσης και ελέγχου πριν τα bits που περιέχουν το μήνυμα, ακολουθούμενο από μια αλληλουχία ελέγχου λαθών, λέγεται frame. Και τα ασύρματα και τα ενσύρματα δίκτυα χωρίζουν τη ροή δεδομένων σε frames που περιέχουν διάφορες μορφές πληροφοριών χειραψίας μαζί με τα αρχικά δεδομένα.

Το λογισμικό δικτύου προσθέτει και αφαιρεί αυτόματα όλες τις διευθύνσεις, checksums και άλλες πληροφορίες ώστε ο παραλήπτης να βλέπει τελικά μόνο το μήνυμα. Όμως κάθε τι που προστίθεται στα αρχικά δεδομένα αυξάνει το μέγεθος του πακέτου και συνεπώς και τον
χρόνο που απαιτείται για την αποστολή μέσω του δικτύου. Οπότε αν η ονομαστική ταχύτητα ενός δικτύου είναι 11 Mbps, στην πραγματικότητα η ποσότητα "χρήσιμων" δεδομένων που μεταφέρονται μπορεί να είναι μόνο 6 ή 7 Mpbs.

Συσκευές δικτύου

Όταν καθορίσουμε τους συνδέσμους και το είδος των δεδομένων, το επόμενο βήμα είναι να στήσουμε μια δομή δικτύου. Πως χρησιμοποιούν οι υπολογιστές τους πομπούς, τους δέκτες και την μορφή δεδομένων για να ανταλλάξουν δεδομένα;

Τα δίκτυα 802.11b περιλαμβάνουν δύο κατηγορίες πομποδεκτών : τους σταθμούς και τα σημεία πρόσβασης. Ένας σταθμός είναι ένας υπολογιστής, ή μια άλλη συσκευή όπως ένας εκτυπωτής, συνδεδεμένος σε ένα ασύρματο δίκτυο μέσω ενός εσωτερικού ή εξωτερικού αντάπτορα διασύνδεσης δικτύου.Σημείο πρόσβασης είναι ο σταθμός βάσης για ένα ασύρματο δίκτυο και μια γέφυρα μεταξύ του ασύρματου δικτύου και ενός παραδοσιακού ενσύρματου δικτύου.

Network Adapters

Οι αντάπτορες δικτύου για σταθμούς μπορούν να έχουν πολλές μορφές:

- Κάρτες που μπαίνουν σε socket PCMCIA στα περισσότερα Laptop. Λόγω της εσωτερικής θωράκισης συνήθως η κεραία των περισσότερων ασύρματων καρτών εξέχει περίπου 3 εκατοστά από το άνοιγμα της υποδοχής της κάρτας.
- Εσωτερικοί αντάπτορες δικτύου πάνω σε PCI κάρτα για επιτραπέζιους υπολογιστές
- Εξωτερικοί αντάπτορες USB
- Εσωτερικοί ασύρματοι αντάπτορες που είναι ενσωματωμένοι σε laptops. Η κεραίες τους είναι συνήθως κρυμμένες μέσα στην οθόνη
- Άλλες μορφές που έχουν φτιαχτεί για PDAs και άλλες συσκευές

'Ενας αντάπτορας δικτύου πρέπει να λειτουργεί με κάθε λειτουργικό σύστημα, αρκεί να υπάρχει οδηγός (λογισμικό) διαθέσιμος.

Εικόνα 8 : Εσωτερικός αντάπτορας δικτύου

Σημεία πρόσβασης

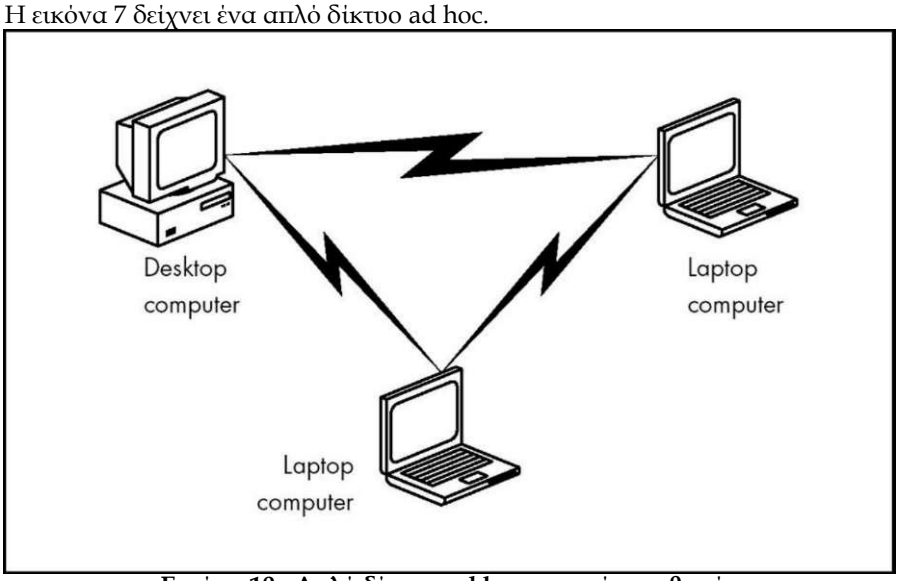
Τα σημεία πρόσβασης συχνά συνδυάζονται με άλλες λειτουργίες δικτύου. Είναι πολύ πιθανό να βρεθεί ένα σημείο πρόσβασης που "μπαίνει" σε ένα ενσύρματο LAN μέσω ενός καλωδίου δεδομένων, αλλά υπάρχουν πολλές άλλες επιλογές. Συχνές επιλογές είναι οι ακόλουθες :

- Απλοί σταθμοί βάσης με γέφυρα για μία Ethernet θύρα σύνδεσης σε LAN
- Σταθμοί βάσης που έχουν διακόπτη, hub, ή router με μια ή περισσότερες θύρες Ethernet μαζί με το ασύρματο σημείο πρόσβασης.
- Ευρυζωνικά routers που παρέχουν γέφυρα μεταξύ του καλωδιακού modem ή θύρα DSL και του ασύρματου σημείου πρόσβασης.
- Σημεία πρόσβασης μέσω λογισμικού που χρησιμοποιούν έναν από τους ασύρματης διασύνδεσης δικτύου ως σταθμό βάσης.

Εικόνα 9 : Σημεία πρόσβασης της Zoom και της D-Link

Καταστάσεις λειτουργίας

Τα δίκτυα 802.11b λειτουργούν σε δύο καταστάσεις : τα **δίκτυα ad hoc** και τα **δίκτυα υποδομής.** Ένα δίκτυο ad hoc είναι συνήθως προσωρινό και αποτελεί ένα δίκτυο από σταθμούς που δεν συνδέονται σε μεγαλύτερο LAN ή στο διαδίκτυο. Περιλαμβάνει δύο ή περισσότερους ασύρματους σταθμούς χωρίς σημείο πρόσβασης ή σύνδεση με τον υπόλοιπο κόσμο. Τα δίκτυα ad hoc ονομάζονται επίσης και peer-to-peer δίκτυα και Independent Basic Service Sets (IBSS), δηλαδή Ανεξάρτητα Σύνολα Βασικών Υπηρεσιών. Η εικόνα 7 δείχνει ένα απλό δίκτυο ad hoc.

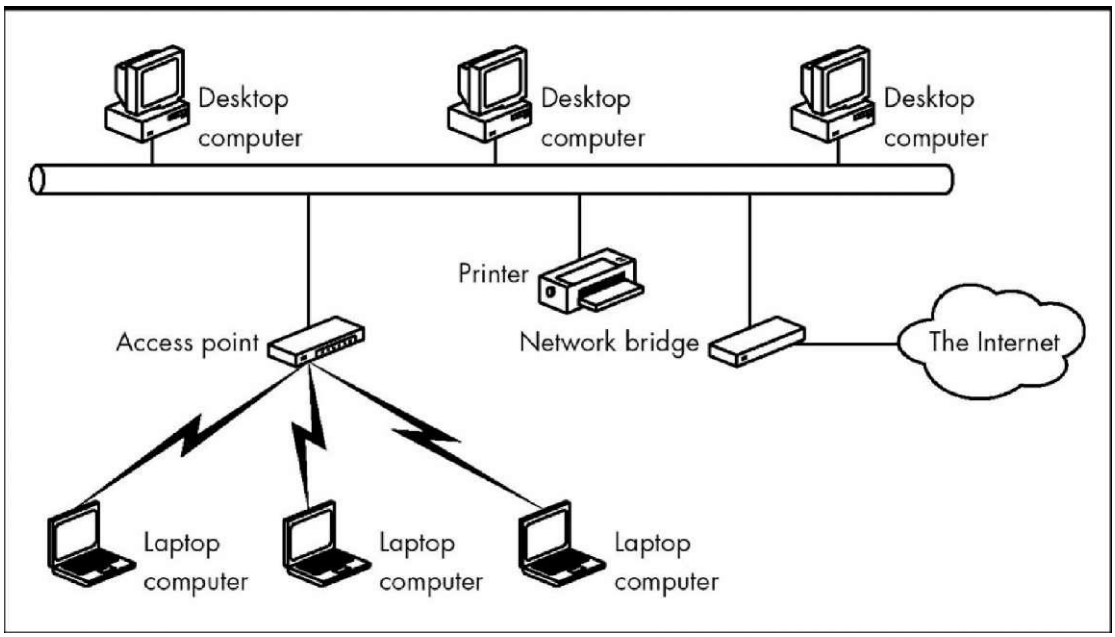


Εικόνα 10 : Απλό δίκτυο ad hoc με τρείς σταθμούς

Σε ένα δίκτυο ad hoc, κάθε αντάπτορας δικτύου ανταλλάσσει δεδομένα με κάθε άλλο τερματικό μέσω άμεσων συνδέσμων, χωρίς ένα σημείο πρόσβασης να δρα ως κεντρικό τερματικό. Τα δίκτυα αυτά είναι χρήσιμα για μικρά, απομονωμένα δίκτυα άμεση κοινή χρήση φακέλων peer-to-peer. Για παράδειγμα κάποιος που χρησιμοποιεί laptop εν κινήσει και επιτραπέζιο υπολογιστή στο γραφείο μπορεί να στήσει ένα δίκτυο ad hoc για να μεταφέρει αρχεία μεταξύ των δύο.

Τα ad hoc ασύρματα δίκτυα που συνδέουν δύο ή περισσότερα τερματικά χωρίς τη χρήση σημείου πρόσβασης είναι πολύ λιγότερο συνηθισμένα από τα δίκτυα υποδομής, αλλά είναι μέρος του προτύπου 802.11b, οπότε σχεδόν κάθε αντάπτορας διασύνδεσης δικτύου και πρόγραμμα ασύρματης παραμετροποίησης προσφέρει επιλογή για δίκτυο ad hoc. Γενικά κάθε αντάπτορας δικτύου με το λογότυπο Wi-Fi δουλεύει σωστά σε ένα δίκτυο ad hoc.

Τα δίκτυα υποδομής έχουν ένα ή περισσότερα σημεία πρόσβασης, που είναι σχεδόν πάντα συνδεδεμένα σε ένα ενσύρματο δίκτυο. Κάθε ασύρματος σταθμός ανταλλάσει μηνύματα με το σημείο πρόσβασης, που τα μεταφέρει σε άλλα σημεία στο ασύρματο δίκτυο ή στο ενσύρματο LAN. Κάθε δίκτυο που χρειάζεται ενσύρματη σύνδεση μέσω ενός σημείου πρόσβασης σε έναν εκτυπωτή, ένας server ή μια πύλη δικτύου είναι ένα δίκτυο υποδομής. Ένα τέτοιο δίκτυο παρουσιάζεται στην εικόνα 11.



Εικόνα 11 : Δίκτυο υποδομής

Ένα δίκτυο υποδομής με μόνο ένα σταθμό βάσης λέγεται και Basic Service-Set (BSS), δηλαδή Βασικό σύνολο υπηρεσιών. Όταν το ασύρματο δίκτυο χρησιμοποιεί δύο ή περισσότερα σημεία πρόσβασης, η δομή δικτύου είναι ένα Extended Service Set (ESS), δηλαδή επεκταμένο σύνολο υπηρεσιών.

Ένα δίκτυο με περισσότερα από ένα σημείο πρόσβασης δημιουργεί πολλές νέες περιπλοκές. Κατ' αρχήν το δίκτυο πρέπει να περιλαμβάνει έναν τρόπο για να χειρίζεται μόνο ο σταθμός βάσης δεδομένα από έναν συγκεκριμένο σταθμό, ακόμα και αν ο σταθμός είναι στην εμβέλεια περισσότερων του ενός σταθμού. Και εάν ο σταθμός κινείται εν μέσω μιας λειτουργίας δικτύου ή αν κάποιο είδος τοπικής παρεμβολής παρουσιαστεί κοντά στο πρώτο σημείο πρόσβασης, το δίκτυο μπορεί να πρέπει να "δώσει" την σύνδεση στο άλλο σημείο πρόσβασης. Ένα δίκτυο 802.11b χειρίζεται αυτό το πρόβλημα συσχετίζοντας έναν σταθμό με ένα μόνο σημείο πρόσβασης κάθε φορά και αγνοώντας σήματα από άλλους μη- συσχετισμένους σταθμούς. Όταν το σήμα ατονεί σε ένα σημείο πρόσβασης και βελτιώνεται σε ένα άλλο, ή η κινητικότητα αναγκάζει το δίκτυο να ανακατανείμει το φορτίο, το δίκτυο επανασυσχετίζει τον σταθμό με ένα νέο σημείο πρόσβασης που μπορεί να παρέχει αποδεκτή υπηρεσία. Αυτός ο τρόπος μοιάζει πολύ με τον τρόπο που το σύστημα κινητής τηλεφωνίας χειρίζεται το roaming και ονομάζεται επίσης roaming.

Ο ραδιο-σύνδεσμος, η δομή δεδομένων και η αρχιτεκτονική δικτύου είναι τα τρία απαραίτητα στοιχεία που διαμορφώνουν ένα 802.11 ασύρματο Ethernet δίκτυο. Όπως τα στοιχεία των περισσότερων δικτύων, αυτά τα στοιχεία θα έπρεπε να είναι εντελώς διάφανα στους ανθρώπους που χρησιμοποιούν το δίκτυο, δηλαδή δεν θα πρέπει ένας χρήστης να χρειάζεται να ασχοληθεί με βαθύτερες λεπτομέρειες του δικτύου. Αρκεί να μπορεί να στείλει και να λάβει δεδομένα και να πραγματοποιήσει της λειτουργίες δικτύωσης που επιθυμεί.

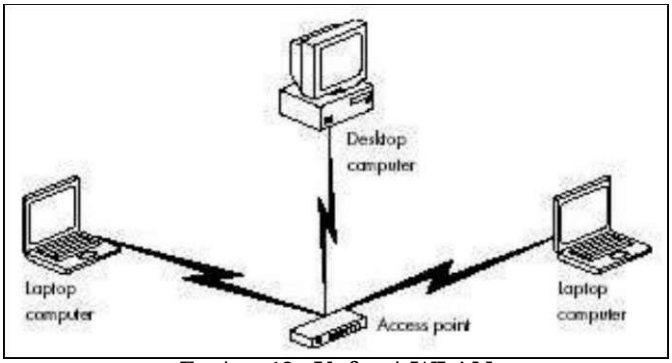
Σημεία πρόσβασης

Οι περισσότεροι αντάπτορες διαούνδεσης ασύρματου δικτύου εκτελούν μόνο μία λειτουργία : ανταλλάσσουν δεδομένα μεταξύ ενός υπολογιστή και ενός δικτύου. Τα σημεία πρόσβασης όμως, προσφέρουν ποικιλία λειτουργιών. Είναι διαθέσιμα ως απλά σημεία πρόσβασης και συνδυάζουν hubs, διακόπτες και routers για ενσύρματες συνδέσεις με κοντινούς υπολογιστές και άλλες συσκευές. Υπάρχει ολόκληρη κατηγορία ασύρματων σημείων πρόσβασης για οικιακά δίκτυα.

Ο σχεδιασμός ενός σημείου πρόσβασης είναι λιγότερο σημαντικός από τον σχεδιασμό ενός αντάπτορα διασύνδεσης γιατί τα σημεία πρόσβασης δεν χρειάζεται να χωρέσουν μέσα σε μια θύρα υπολογιστή. Πιο μεγάλη βάση δίνεται στις λειτουργίες που προσφέρει.

Καθαρό WLAN

Όταν όλα τα τερματικά ενός LAN ανταλλάσουν δεδομένα ασύρματα, το σημείο πρόσβασης δρα ως ένα hub που παρέχει το κεντρικό σημείο ελέγχου για το δίκτυο. Το σημείο πρόσβασης δεν παρέχει πρόσβαση πουθενά αλλού εκτός από άλλα ασύρματα τερματικά.

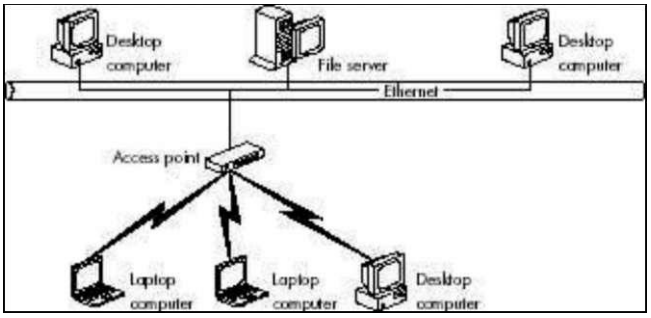


Εικόνα 12 : Καθαρό WLAN

Αυτός ο τύπος απλού ασύρματου δικτύου είναι πιθανός, αλλά δεν υπάρχει ιδιαίτερος λόγος να χρησιμοποιήσουμε σημείο πρόσβασης σε ένα καθαρό WLAN. Μπορούμε να πετύχουμε το ίδιο πράγμα με ένα ασύρματο δίκτυο ad hoc που δημιουργεί άμεσους συνδέσμους σημείου- σημείου χωρίς την ανάγκη ενός κεντρικού hub. Μάλλον η μόνη περίπτωση που έχει νόημα ένα καθαρό ασύρματο δίκτυο υποδομής με σημείο πρόσβασης είναι αν ξεκινήσουμε με ασύρματους συνδέσμους και στη συνέχεια επεκτείνουμε το δίκτυο ώστε να περιλαμβάνει ενσύρματη σύνδεση με έναν διακομιστή αρχείων, μια κοινόχρηστη διαδικτυακή σύνδεση ή περισσότερους υπολογιστές.

Ασύρματη πρόσβαση σε ενσύρματο LAN

Κάθε σημείο πρόσβασης μπορεί να λειτουργήσει σαν σταθμός βάσης, προσθέτοντας ασύρματους συνδέσμους σε ένα υπάρχον ενσύρματο LAN όπως φαίνεται στην εικόνα 13. Το σημείο πρόσβασης παρουσιάζει την ίδια εικόνα στο υπόλοιπο δίκτυο όπως ένας διακόπτης που συνδέει ενσύρματα τερματικά στο δίκτυο.



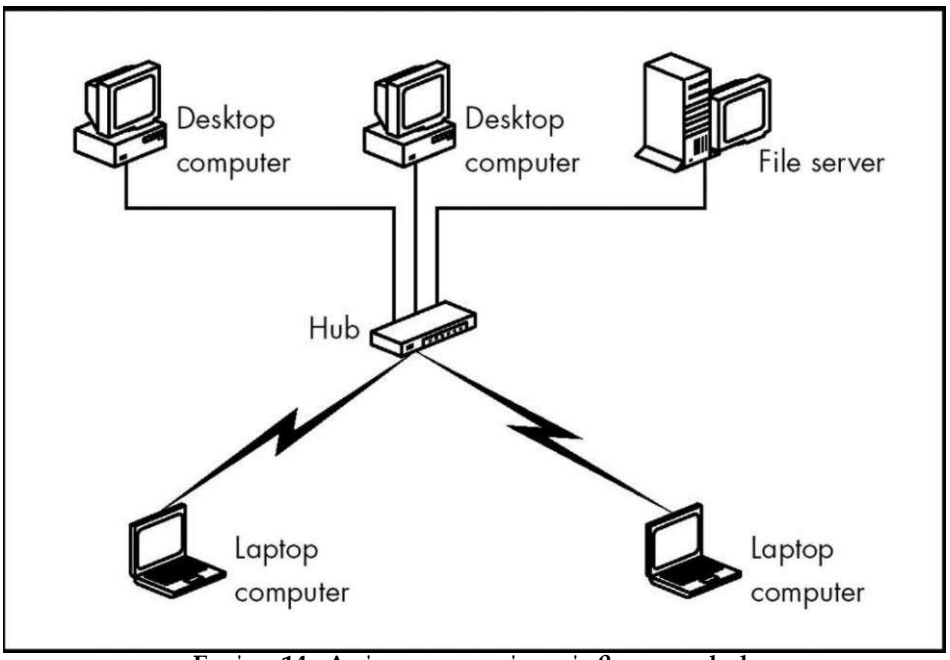
Εικόνα 13 : Ασύρματο σημείο πρόσβασης συνδεδεμένο σε ενσύρματο δίκτυο Ethernet

Σε αυτό το είδος υβριδικού ασύρματου-ενσύρματου LAN, κάθε συσκευή στο δίκτυο μπορεί να ανταλλάξει δεδομένα με κάθε άλλο τερματικό του δικτύου, άσχετα με το πώς αυτό είναι συνδεδεμένο στο δίκτυο.

Ένα σημείο πρόσβασης που δρα σαν γέφυρα μεταξύ του ενσύρματου και ασύρματου τομέα του δικτύου συνήθως έχει μια μονή 10 Mbps ή 100 Mbps RJ-45 θύρα για σύνδεση καλωδίου στο ενσύρματο LAN. Υπάρχει συχνά μια επιπρόσθετη σειριακή θύρα για ένα απομακρυσμένο τερματικό που ο διαχειριστής του δικτύου μπορεί να χρησιμοποιήσει για να εισάγει εντολές παραμετροποίησης και να δεχτεί πληροφορίες κατάστασης.

Συνδυάζοντας το σημείο πρόσβασης με ενσύρματο hub

Σε ένα νέο LAN που περιλαμβάνει και ενσύρματες συνδέσεις και ασύρματους συνδέσμους, η καλύτερη προσέγγιση μπορεί να είναι μια συσκευή που συνδυάζει τις λειτουργίες ενός ασύρματου σημείου πρόσβασης με αυτές ενός ενσύρματου hub ή διακόπτη όπως φαίνεται στην εικόνα 14. Αυτό το είδος σημείου πρόσβασης περιγράφεται και ως ευρυζωνικό router.



Εικόνα 14 : Ασύρματο σημείο πρόσβασης με hub

"Ένα ευρυζωνικό router έχει τυπικά τρία είδη συνδέσεων δικτύου :

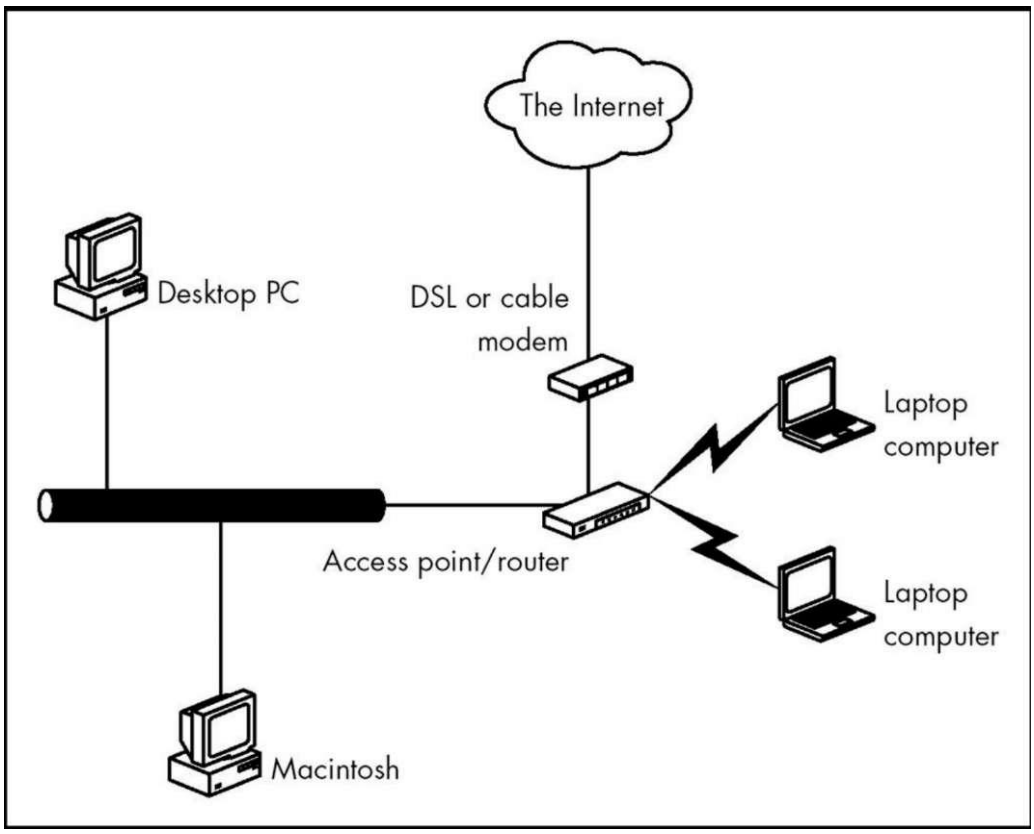
- Συνδέσμους με υπολογιστές εξοπλισμένους με ασύρματους αντάπτορες Ethernet
- Μία ή περισσότερες θύρες για ενσύρματους συνδέσμους με υπολογιστές με κάρτες διασύνδεσης δικτύου
- Μία ευρυζωνική θύρα WAN για σύνδεση του router στο δίκτυο ή για να συνδέσει στο router επιπλέον hubs ή διακόπτες.

Μερικά routers επίσης περιλαμβάνουν διακομιστή εκτύπωσης που μπορεί να μετακινήσει έγγραφα κατ' ευθείαν σε έναν εκτυπωτή δικτύου.

Τα βασικά πλεονεκτήματα συνδυασμένου σημείου πρόσβασης και hub είναι ευκολία και οικονομία σε ένα οικιακό γραφείο ή μικρή επιχείρηση όπου είναι εύκολο να συνδεθούν με καλώδια μερικοί δικτυακοί υπολογιστές. Μπορεί επίσης να είναι και ο γρηγορότερος τρόπος επέκτασης ενός υπάρχοντος δικτύου σε ασύρματα και ασύρματα τερματικά σε απομακρυσμένη τοποθεσία.

Ευρυζωνικές πύλες

Μια ευρυζωνική πύλη είναι ένα σημείο πρόσβασης που περιλαμβάνει θύρα για άπ' ευθείας σύνδεση σε DSL ή καλωδιακό modem που παρέχει γρήγορη σύνδεση στο διαδίκτυο, όπως φαίνεται στην εικόνα 15.



Εικόνα 15 : Σημείο πρόσβασης συνδυασμένο με ευρυζωνική πύλη

Πολλαπλά σημεία πρόσβασης

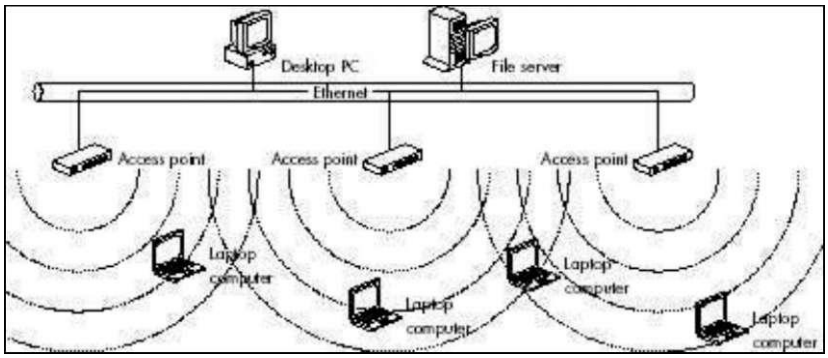
"Ένα σημείο πρόσβασης μπορεί να είναι απόλυτα επαρκές για να υποστηρίξει ένα WLAN σε έναν ανοιχτό μικρό χώρο, με μέτρια κινητικότητα. Αλλά αν το δίκτυο πρέπει να καλύπτει πολύ μεγάλο χώρο (μεγαλύτερο από 25 περίπου μέτρα σε διάμετρο), ή έναν χώρο με εμπόδια (τοίχους, έπιπλα, παρεμβολές από άλλα κανάλια κ.ο.κ.) μάλλον χρειάζονται περισσότερα σημεία πρόσβασης.

Τα περισσότερα οικιακά δίκτυα και πολλά δίκτυα σε πολύ μικρές επιχειρήσεις, χρειάζονται μόνο ένα σημείο πρόσβασης, οπότε η επιλογή ενός σημείου πρόσβασης που να υποστηρίζει roaming (εξηγήθηκε νωρίτερα), πρέπει να απασχολεί μόνο διαχειριστές μεγάλων δικτύων.

Το πρότυπο 802.11b περιλαμβάνει λειτουργία roaming που δίνει έναν σύνδεσμο δικτύου αυτόματα από ένα σημείο πρόσβασης σε άλλο αν διαπιστωθεί ότι η ποιότητα σήματος του νέου σημείου πρόσβασης είναι καλύτερη απ' ότι στο πρώτο. Αφού γίνει η συσχέτιση με ένα σημείο πρόσβασης αυτό αυτόματα κάνει έρευνα σε όλα τα υπόλοιπα κανάλια για να δεί αν κάποιο σημείο πρόσβασης που λειτουργεί σε κάποιο άλλο κανάλι θα παρέχει δυνατότερο σήμα από αυτό που χρησιμοποιείται. Όταν βρεθεί τέτοιο κανάλι γίνεται συσχέτιση με αυτό.
Αυτός είναι και ο λόγος που σημεία πρόσβασης με κοινές περιοχές κάλυψης πρέπει να λειτουργούν σε διαφορετικά κανάλια και μάλιστα για ελάχιστη παρεμβολή πρέπει να απέχουν τουλάχιστον πέντε κανάλια μεταξύ τους.

Στην πλειονότητα των περιπτώσεων ένας πελάτης δικτύου (network client) δεν συσχετίζεται με άλλο σημείο πρόσβασης εκτός αν ο μετακινηθεί ενώ είναι ενεργός ο σύνδεσμος δικτύου, ή αν αυξηθεί το φορτίο του καναλιού.

Όπως δείχνει η εικόνα 14 όλα τα σημεία πρόσβασης πρέπει να είναι συνδεδεμένα μέσω ενός συμβατικού ενσύρματου LAN που μπορεί να περιλαμβάνει επιπρόσθετους υπολογιστές και διακομιστές που δεν χρειάζονται ασύρματη σύνδεση.



Εικόνα 16 : Πολλαπλά σημεία πρόσβασης σε ενσύρματο LAN επιτρέπουν μετακίνηση μέσα σε μεγάλη περιοχή κάλυψης

Στις περισσότερες περιπτώσεις τα πολλαπλά σημεία πρόσβασης πρέπει να τοποθετηθούν ώστε να προσφέρει το καθένα κάλυψη που υπερκαλύπτει κατά 30% περίπου την περιοχή κάλυψης του επόμενου σημείου πρόσβασης. Αν όμως το δίκτυο θέλουμε να υποστηρίξει μεγάλο εριθμό χρηστών είναι καλύτερο σε κάθε σημείο να τοποθετήσουμε δύο σημεία πρόσβασης που το καθένα να λειτουργεί σε άλλο κανάλι.

Η σημασία της εκπομπής διευρυμένου φάσματος

Μία από τις βασικές τεχνολογίες στις οποίες βασίζεται η σειρά προτύπων IEEE 802.11 είναι η εκπομπή διευρυμένου φάσματος. Η βασική ιδέα είναι η χρήση ευρύτερης ζώνης φάσματος από αυτήν που χρειαζόμαστε. Αυτό επιφανειακά φαίνεται σαν "σπατάλη",αλλά όπως διαπιστώνεται επιφέρει πολλά πλεονεκτήματα όπως μικρότερη επιδεκτικότητα σε θόρυβο, υποκλοπές, παρεμβολές και δυνατότητα για ταυτόχρονη παρουσία με αναμεταδόσεις στενής ζώνης

2.2.3. Εμβέλεια και Επιδόσεις

Μια από τις σημαντικότερες εσφαλμένες εκτιμήσεις σχετικά με 802.11b και άλλα ασύρματα πρωτόκολλα είναι ότι η εμβέλεια τους περιορίζεται στα 100 μέτρα και αποδεικνύεται έτσι μη πρακτική ως λύση. Η αλήθεια είναι ότι το 802.11b μπορεί να φθάσει πέρα από τα 20 μίλια από σημείο σε σημείο. Στην αναζήτηση για την παράκαμψη της *Public Switched Telephone Network* (PSTN), αυτή είναι μια από τις πιο συναρπαστικές αποκαλύψεις. Οδηγώντας μια κεραία στην κατεύθυνση του χρήστη ο φορέας παροχής υπηρεσιών μπορεί να φέρει ευρυζωνικό ασύρματο δίκτυο σε μεγάλο αριθμό σπιτιών χωρίς χρήση καλωδίου χαλκού.

Επιπλέον, τα νέα ασύρματα πρωτόκολλα για τα *Metropolitan Area Networks* (MANs) επιτρέπουν την κατασκευή ασύρματων δικτύων που μπορούν να καλύψουν ολόκληρες πόλεις. Τα δίκτυα ad hoc μεγαλώνουν την εμβέλεια ενός ασύρματου δικτύου με το ελάχιστο της κόστος.

Αυτό το κεφάλαιο καλύπτει την επιστήμη των κεραιών και το πώς η κατάλληλη εφαρμοσμένη μηχανική μπορεί να μεγαλώσει τους μετριότερους πόρους για να παραδώσει ουσιαστικές υπηρεσίες στο σπίτι. Επίσης, εξηγεί πώς τα συστήματα κεραιών 802.11b μπορούν να χρησιμοποιηθούν για να μεγαλώσουν την εμβέλεια παράδοσης και να καλύψουν μεγάλες μητροπολιτικές περιοχές και να φτάσουν ακόμη και στις αγροτικές περιοχές.

Το σημαντικότερο μέρος στο σχεδιασμό ενός ευρυζωνικού ασύρματου δικτύου είναι ο συνυπολογισμός του νέου πρωτοκόλλου 802.16 στην επέκταση των WMANs για να τροφοδοτηθούν τα προαστιακά

δίκτυα 802.11b. Άλλες τεχνολογίες όπως τα δίκτυα πλέγματος επεκτείνουν επίσης την εμβέλεια των ευρυζωνικών ασύρματων δικτύων.

Στη δικτύωση δεδομένων, η επιτυχία του 802.11 το έχει συνδέσει με την εφαρμοσμένη μηχανική ραδιοσυχνοτήτων (Radio Frequency ή RF). Ενώ ένα ενσύρματο δίκτυο απαιτεί ελάχιστη ή καμία γνώση εκ μέρους του χρήστη για το πώς τα δεδομένα ταξιδεύουν μέσω του καλωδίου Ethernet, ένα ασύρματο δίκτυο απαιτεί γνώση των πομπών δεκτών και κεραιών. Στις ακόλουθες παραγράφους γίνεται μια επισκόπηση των ασύρματων συστημάτων μετάδοσης.

Στοιχεία RF

Τα συστήματα RF συνεισφέρουν στα ενσύρματα δίκτυα επεκτείνοντας τα. Διαφορετικά στοιχεία μπορεί να χρησιμοποιηθούν ανάλογα με τη συχνότητα και την απόσταση που τα σήματα πρέπει να φτάσουν. Αλλά όλα τα συστήματα είναι στην βάση τους ίδια και φτιάχνονται από έναν μικρό αριθμό στοιχείων. Τρία στοιχεία RF που ενδιαφέρουν πολύ τους χρήστες του 802.11 είναι οι κεραίες, ευαίσθητοι δέκτες, και ενισχυτές. Οι κεραίες είναι γενικού ενδιαφέροντος αφού είναι το πιο απτό κομμάτι ενός RF συστήματος.

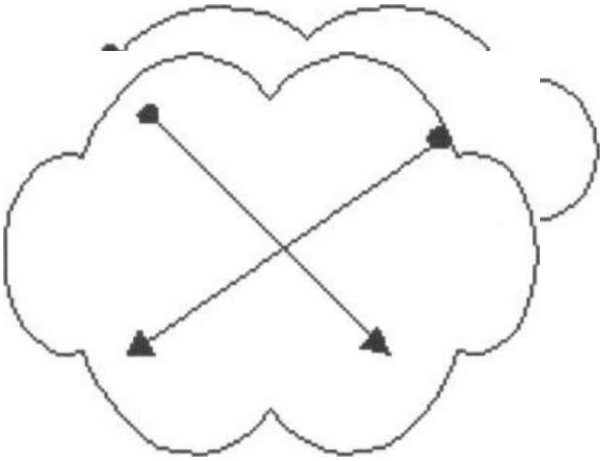
Εικόνα 17 : Στοιχεία RF

Κεραίες

Οι κεραίες είναι το πιο επίμαχο κομμάτι ενός συστήματος RF αφού μεταρέπουν ηλεκτρικά σήματα συρμάτων σε ραδιοκύματα και το αντίστροφο. Για να λειτουργήσει μια κεραία πρέπει να είναι φτιαγμένη από αγώγιμο υλικό. Ραδιοκύματα που χτυπούν μια κεραία προκαλούν ροή ηλεκτρονίων στον αγωγό και δημιουργούν ηλεκτρικό ρεύμα. Παρομοίως, εφαρμόζοντας ηλεκτρικό ρεύμα σε μία κεραία δημιουργεί ηλεκτρικό πεδίο γύρω της. Το ηλεκτρικό πεδίο αλλάζει καθώς το ρεύμα αλλάζει. Ένα μεταβαλλόμενο ηλεκτρικό πεδίο δημιουργεί μαγνητικό πεδίο. Έτσι δημιουργούνται κύματα.

Το μέγεθος της κεραίας που χρησιμοποιείται εξαρτάται από τη συχνότητα. Όσο ψηλότερη είναι αυτή τόσο μικρότερη θα είναι η κεραία. Η μικρότερη δυνατή κεραία σε οποιαδήποτε συχνότητα έχει μήκος ίσο με το μισό μήκος κύματος. Αυτός ο κανόνας είναι υπεύθυνος για το τεράστιο μέγεθος των κεραιών εκπομπής και το μικρό μέγεθος των κινητών τηλεφώνων. Ένας σταθμός AM που εκπέμπει στα 830 kHz σε μήκος κύματος περίπου 360 μέτρα έχει σχετικά μεγάλη κεραία, αλλά ένα δίκτυο 802.11 που λειτουργεί στα 2.4 GHz έχει μήκος κύματος 12.5 εκατοστά, άρα θα έχει και πολύ μικρότερη κεραία.

Οι κεραίες μπορούν επίσης να σχεδιαστούν με συγκεκριμένη διεύθυνση λήψης. Πολλές κεραίες είναι ομοιόμορφης λήψης, που σημαίνει πως μπορούν να στείλουν και να λάβουν σήματα από κάθε κατεύθυνση. Μερικές εφαρμογές όμως μπορεί να ωφεληθούν από χρήση κατευθυντικής κεραίας. Η εικόνα 17 συγκρίνει την ακτινοβολούμενη ισχύ κεραιών ομοιόμορφης εκπομπής και κατευθυντικών κεραιών.



Omnidirectional

Antenna

Directional Antenna

Εικόνα 18 : ακτινοβολούμενη ισχύς κεραιών κυκλικής εκπομπής και κατευθυντικών κεραιών

Για δεδομένη ποσότητα ισχύος εισόδου, μια κατευθυντική κεραία μπορεί να φτάσει πολύ μακρύτερα και με καθαρότερο σήμα. Η κεραία πρέπει επίσης να έχει πολύ μεγαλύτερη ευαισθησία σε ραδιοσήματα στην κύρια κατεύθυνση. Όταν ασύρματοι σύνδεσμοι χρησιμοποιούνται για να αντικαταστήσουν ενσύρματα δίκτυα, συχνά χρησιμοποιούνται κατευθυντικές κεραίες. Τα δίκτυα 802.11 τυπικά χρησιμοποιούν κεραίες ομοιόμορφης λήψης και στις δύο πλευρές τις σύνδεσης.

Όταν θέλουμε να χρησιμοποιήσουμε κεραίες πρέπει να δίνουμε προσοχή στα παρακάτω χαρακτηριστικά.

Τύπος κεραίας

Ο τύπος κεραίας καθορίζει το μοτίβο εκπομπής της: ομοιόμορφης λήψης, δικατευθυντική ή μονοκατευθυντική. Οι ομοιόμορφης λήψης είναι καλές για κάλυψη μεγάλων περιοχών, οι δικατευθυντικές προσφέρονται ιδιαίτερα για κάλυψη διαδρόμων και οι μονοκατευθυντικές είναι οι καλύτερες για στήσιμο σύνδεσης σημείου-σημείου μεταξύ κτιρίων ή άλλων τοποθεσιών. Συνήθως ισχύει πως όσο μεγαλύτερο είναι η απολαβή της κεραίας, τόσο πιο στενή είναι η δέσμη της.

Παράγοντες που επηρεάζουν την εμβέλεια

Είναι δελεαστικό να σκεφτεί κανείς ότι μπορούμε να στήσουμε μια κεραία υψηλής απολαβής με έναν ενισχυτή ισχύος και να καλύψουμε μια τεράστια περιοχή εξυπηρετώντας έτσι μεγάλο αριθμό χρηστών. Αυτή όμως δεν είναι καλή ιδέα. Όσο μεγαλύτερη είναι η περιοχή που καλύπτεται, τόσο περισσότερους χρήστες πρέπει να εξυπηρετήσουν τα σημεία πρόσβασης. Ένα καλό άνω όριο είναι 20-30 χρήστες ανά ασύρματη κάρτα ανά σημείο πρόσβασης. Ένα μοναδικό σημείο πρόσβασης για μεγάλη περιοχή θα δούλευε καλά αρχικά, αλλά μόλις αυξανόταν ο αριθμός των χρηστών δε θα μπορούσε να τους εξυπηρετήσει. Όταν συμβεί αυτό πρέπει να εγκατασταθούν περισσότερα σημεία πρόσβασης και να χωριστεί το αρχικό κελί σε άλλα μικρότερα με μικρότερη ισχύ εκπομπής στο κάθε ένα.

Συνεχίζοντας θα πούμε κάποια πράγματα για τους ευαίσθητους δέκτες και τους ενισχυτές και το πώς μπορούμε να αυξήσουμε την εμβέλεια ενός δικτύου.

Ευαίσθητοι δέκτες

Εκτός από την κεραία, το πιο σημαντικό στοιχείο ενός συστήματος Wi-Fi είναι ο δέκτης. Συγκεκριμένα, είναι σημαντικό να προσέξουμε την ευαισθησία του δέκτη. Η ευαισθησία του δέκτη είναι το σήμα ελάχιστης ισχύος που μπορεί να αποκωδικοποιηθεί από τον δέκτη. Όσο χαμηλότερη είναι η ευαισθησία του δέκτη λοιπόν τόσο μεγαλύτερη είναι η εμβέλεια του συστήματός μας.

Ενισχυτές

Οι ενισχυτές κάνουν τα σήματα μεγαλύτερα. Η ενίσχυση σήματος, η κέρδος μετράται σε decibels (dB). Οι ενισχυτές μπορούν να κατηγοριοποιηθούν σε τρείς κατηγορίες: χαμηλού θορύβου, υψηλής ισχύος, και όλοι οι υπόλοιποι.

Ενισχυτές χαμηλού θορύβου ή Low-noise amplifiers (LNAs)

Συνδέονται συνήθως σε κεραία για να δυναμώσουν το ληφθέν σήμα σε σημείο που να είναι αναγνωρίσιμο από τα ηλεκτρονικά στα οποία είναι συνδεδεμένο το σύστημα RF. Οι LNA βαθμολογούνται επίσης με το επίπεδο θορύβου που είναι μέτρο του πόσες εξωτερικές πληροφορίες εισάγει στην αναλογία σήματος προς θόρυβο (signal-to-noise ratio ή SNR). Μικρότερα επίπεδα θορύβου δίνουν την δυνατότητα στον δέκτη να "ακούει" μικρότερα σήματα και συνεπώς να έχει μεγαλύτερη εμβέλεια.

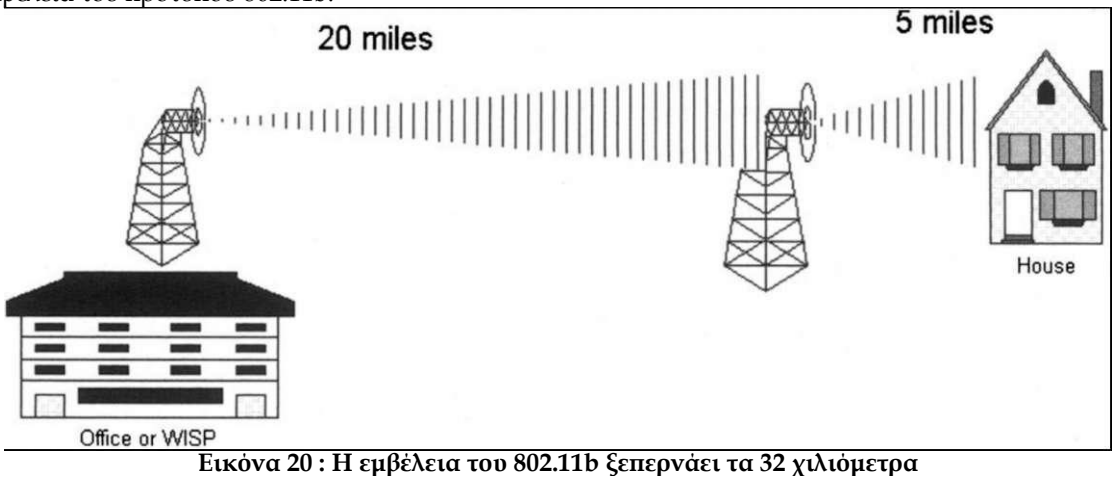
Ενισχυτές μεγάλης ισχύος High-power amplifiers (HPAs)

Χρησιμοποιούνται για να ενισχύσουν ένα σήμα στο μέγιστο δυνατό πριν την μετάδοση. Η ισχύς εξόδου μετράται σε dBm, που εκφράζει τον λόγο της ισχύος του σήματος προς το 1 mW. Στους ενισχυτές έχουν εφαρμογή οι νόμοι της θερμοδυναμικής. Εκπέμπουν θερμότητα ενισχύοντας ταυτόχρονα το σήμα. Ο αναμεταδότης σε μία 802.11 κάρτα για υπολογιστή είναι αναγκαστικά χαμηλής ισχύος γιατί πρέπει να λειτουργήσει από την μπαταρία αν είναι εγκατεστημένη σε laptop, αλλά είναι δυνατή η εγκατάσταση ενός εξωτερικού ενισχυτή. Ο ενισχυτής μπορεί να τροφοδοτηθεί από εξωτερική πηγή ρεύματος.

Εικόνα 19 : ενισχυτής WiFi

2.3. 802.11b από 32 εώς 115 χιλιόμετρα - Η λύση του μεγάλου δικτύου

Είναι πιθανό να έχουμε point-to-multipoint σε περισσότερο από 500 μέτρα με συνηθισμένο εξοπλισμό από την πλευρά του πελάτη. Με χρήση κεραιών μεγάλου κέρδους, ευαίσθητους δέκτες και ενισχυτές, αν είναι απαραίτητο, μπορούν να επιτευχθούν ταχύτητες επιπέδου Ethernet μέσω συνδέσμων σημείου-σημείου που ξεπερνούν τα 32 χιλιόμετρα. Ένα πείραμα απέδειξε ότι είναι θεωρητικά εφικτό να οδηγηθούν σήματα 802.11b για πολύ παραπάνω από 32 χιλιόμετρα χρησιμοποιώντας απλό εξοπλισμό. Για την ακρίβεια, ένας σύνδεσμος 115 χιλιομέτρων από το San Diego μέχρι το San Clemente έχει επιτευχθεί από τον Hans Werner- Braun με χρήση της ζώνης 2.4 GHz band. Στην εικόνα 20 φαίνεται η εμβέλεια του προτύπου 802.11b.



Εικόνα 20 : Η εμβέλεια του 802.11b ξεπερνάει τα 32 χιλιόμετρα

Συνοψίζοντας, το 802.11b από μόνο του δεν είναι περιορισμένο στην εμβέλεια των 100 μέτρων. Η μέγιστη εμβέλειά του ξεπερνάει τα 32 χιλιόμετρα.

2.3.1. *Metro Area Networks (MANs)*

Το WMAN χρησιμοποιεί τεχνολογίες βασισμένες σε ραδιοκύματα και laser που στοχεύουν στην παροχή ασύρματου δικτύου σε αποστάσεις που μπορεί να είναι από εκατοντάδες μέτρα ως και πολλά χιλιόμετρα. Οι ονομασίες Wireless broadband, broadband wireless access (BWA), wireless local loop

(WLL), fixed wireless, και wireless cable αναφέρονται όλες σε τεχνολογίες που μπορούν να χρησιμοποιηθούν για μετάδοση τηλεπικοινωνιακών υπηρεσιών στα τελευταία χιλιόμετρα ενός δικτύου. Οι Wireless broadband και BWA αναφέρονται σε ασύρματα δίκτυα μεγάλης ταχύτητας. Το WLL προέρχεται από τον όρο της ενσύρματης τηλεφωνίας local loop, που αναφέρεται στην σύνδεση μεταξύ ενός τοπικού τηλεφωνικού διακόπτη και του χρήστη. Το WLL και το fixed wiles γενικά αναφέρονται στην μετάδοση υπηρεσιών φωνής και δεδομένων σε ένα ασύρματο μέσο υψηλής ταχύτητας. Το Wireless cable συνήθως αναφέρεται σε συστήματα MMDS(Multichannel Multipoint Distribution Service) που χρησιμοποιούνται για μετάδοση τηλεοπτικών σημάτων.

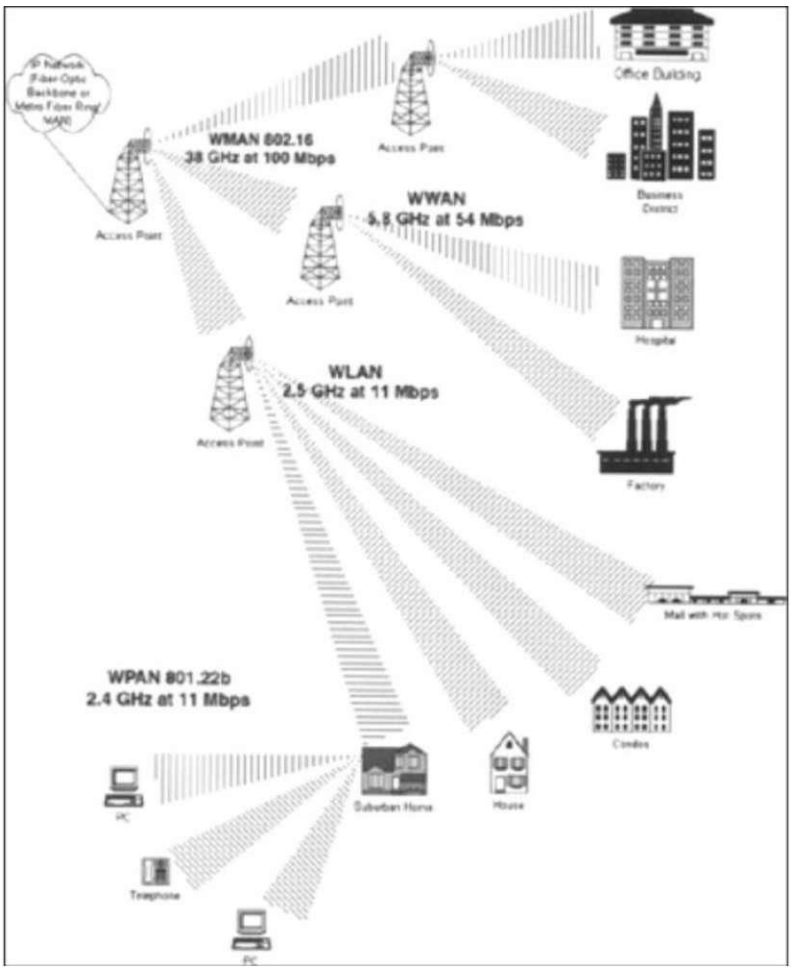
Δύο βασικές δικτυακές τοπολογίες υποστηρίζονται από αυτά τα συστήματα. Η απλούστερη είναι ένα σύστημα σημείου-σημείου που προσφέρει μία ασύρματη σύνδεση μεγάλης ταχύτητας μεταξύ δύο σταθερών τοποθεσιών. Το εύρος ζώνης δεν μοιράζεται, αλλά οι κεραίες των συνδέσμων πρέπει να έχουν οπτική επαφή. Η δεύτερη τοπολογία είναι ένα δίκτυο point- to-multipoint όπου το σήμα εκπέμπεται σε μία περιοχή μου ονομάζεται κελί και επικοινωνεί με σταθερές κεραίες χρηστών μέσα στο κελί. Επειδή το εύρος ζώνης στο κελί είναι πεπερασμένο και διαμοιράζεται σε πολλούς χρήστες, η απόδοση μπορεί να είναι μειωμένη μέσα σε κελιά με μεγάλη πυκνότητα κεραιών. Συστήματα διαφορετικών συχνοτήτων μπορούν να συνδυαστούν για την κάλυψη μιας περιοχής όπου υπάρχει παρεμπόδιση πλήρους κάλυψης.

Εκτός από την συχνότητα, κύρια διαφορά μεταξύ σταθερών ασύρματων συστημάτων, και δικτύων WLAN και WPAN (cellular networks) είναι η φορητότητα του εξοπλισμού των χρηστών. Υπάρχουν απόψεις για υποστήριξη φορητού εξοπλισμού των χρηστών στα σταθερά ασύρματα συστήματα. Αυτό θα επέτρεπε ίσως τα BWA συστήματα να λειτουργήσουν ως cellular networks τέταρτης γενιάς (4G), δίνοντας στους χρήστες ταχύτητες πολλών Mbits. Πολλά τεχνικά και εμπορικά εμπόδια καθώς και προβλήματα με κανονισμούς πρέπει να ξεπεραστούν πριν μπορέσει να γίνει αυτό πραγματικότητα, αλλά εταιρίες όπως η Wi-Fi έχουν ήδη αρχίσει να εξετάζουν προϊόντα που στοχεύουν σε αυτή την εφαρμογή.

Αν και η 802.11b σύνδεση σημείου-σημείου έχει εμβέλεια 32 χιλιομέτρων και μια point-to- multipoint σύνδεση έχει λίγο μικρότερη εμβέλεια, το να χτίσουμε ένα ασύρματο δίκτυο για να ανταγωνιστεί το PSTN είναι πολύ πιο πολύπλοκο. Ζητήματα όπως ο διαμοιρασμός του εύρους ζώνης και το ζήτημα των συχνοτήτων απαιτούν πολυμέτωπη στρατηγική για το χτίσιμο ενός WMAN για να αντικαταστήσει το PSTN σε μια οποιαδήποτε κοινότητα.

Ο περιορισμός στην εμβέλεια μπορεί να υπερνικηθεί μέσω σωστού σχεδιασμού της αρχιτεκτονικής ενός ασύρματου δικτύου. Τέσσερα αρχιτεκτονικά στοιχεία μπορούν να εφαρμοσθούν για αύξηση της μέγιστης εμβέλειας του 802.11b και των σχετικών πρωτοκόλλων.

Πρώτον, ένα WMAN τροφοδοτείται από ένα Internet Protocol (IP) σε μεγάλο εύρος ζώνης π.χ. , 100 Mbps. Ένα τέτοιο WMAN θα λειτουργούσε σε μια αδειοδοτημένη συχνότητα για να εξασφαλιστεί υψηλή ποιότητα μετάδοση χωρίς παρεμβολές. Οι κύριοι χρήστες του WMAN θα ήταν πάροχοι ασύρματου Internet(WISPs). Το WMAN τότε θα μπορούσε να τροφοδοτεί μικρότερα δίκτυα, όπως *wireless wide area networks* (WWANs). Τα WWANs θα μπορούσαν να λειτουργούν σε εύρος ζώνης του 802.11a, δηλαδή 54 Mbps, σε μια συχνότητα στην περιοχή των 5.9 GHz. Χρήστες του WWAN θα ήταν μεγάλες εταιρίες και μικρότεροι WISPs. Σο WWAN με τη σειρά του θα τροφοδοτούσε WLANs που θα τροφοδοτούσαν σπίτια και μικρές εταιρίες. Τα WPANs θα τροφοδοτούνταν από WLANs. Τελικά, το δίκτυο θα μπορούσε να επεκταθεί κι άλλο με μικρό κόστος με ένα δίκτυο ad-hoc που θα αποτελούνταν από συσκευές χρηστών, έξυπνων APs και ασύρματα routers.



Εικόνα 21 : Κάλυψη μεγάλης περιοχής με WMANs, WWANs, WLANs και WPANs

2.4. Διαφοροποιήσεις του 802.11

Το 1997, η IEEE υιοθέτησε το 802.11-1997, το πρότυπο WLAN. Αυτό το πρότυπο προσδιορίζει τα Medium access control (MAC) και PHY στρώματα για ένα LAN με ασύρματη συνδεσιμότητα. Αφορά LANs όπου οι συνδεδεμένες συσκευές επικοινωνούν μέσω του αέρα με άλλες συσκευές που είναι σε κοντινές αποστάσεις μεταξύ τους.

Ο βιομηχανικός όμιλος *Wireless Ethernet Compatibility Alliance* (WECA) πιστοποιεί τον εξοπλισμό των μελών του ως προς την συμβατότητα με το πρότυπο 802.11b και δίνει τη δυνατότητα σε συσκευές να πιστοποιηθούν ως συμβατές με Wi-Fi. Αυτό είναι μια προσπάθεια να υπάρχει εγγυημένη συμβατότητα μεταξύ των εκατοντάδων κατασκευαστών και των χιλιάδων συσκευών. Στη συνέχεια παρουσιάζουμε τις διαφοροποιήσεις του 802.11 Και την σχέση τους με το 802.11b.

i. IEEE 802.11

Το 802.11 θεωρείται το βασικό πρότυπο που ορίζει την λειτουργία σε MAC και PHY για δίκτυα δεδομένων όπως το TCP/IP. Τρία περιβάλλοντα PHY layer ορίζονται που δεν είναι συμβατά μεταξύ τους. Το ένα βασίζεται σε υπέρυθρες επικοινωνίες και τα άλλα δύο χρησιμοποιούν την μη-αδειοδοτημένη ζώνη των 2.4 GHz, που γενικά θεωρείται αρμονική σε όλες τις περιοχές του κόσμου. Η μία βασίζεται στο FHSS και η άλλη στο DSSS. Το 802.11 εκδόθηκε το 1997, και μια αναβαθμισμένη έκδοση έγινε διαθέσιμη το 1999. Το 2003, εκδόθηκαν τα υποπρότυπα 802.11a και 802.11b, με την ενσωμάτωσή τους στην οδηγία του 1999 (IEEE,2003a)

ii. IEEE 802.11a

Αυτό το υποπρότυπο ορίζει το PHY που επιτρέπει ρυθμούς ως 54 Mb/s λειτουργώντας στην μη-αδειοδοτημένη ζώνη των 5 GHz. Το IEEE 802.11a κάποιες φορές αναφέρεται ως Wi-Fi5 λόγω της λειτουργίας του στα 5 GHz.

iii. IEEE 802.11b

Ορίζει τον τρόπο μετάδοσης HR/DSSS με ταχύτητα κατακερματισμού 11 Mchip/s, απασχολώντας το ίδιο εύρος ζώνης καναλιού με το DSSS(IEEE,1999b). Ο μεγαλύτερος ρυθμός δεδομένων επιτυγχάνεται μέσω ενός τρόπου μετάδοσης που βασίζεται σε διαμόρφωση 8 κομματιών CCK. Το σύνολο κωδίκων των Complementary Codes είναι πλουσιότερο από το σύνολο των κωδίκων Walsh. Στα 11 Mbit/s, το μήκος του διευθύνοντος κώδικα είναι 8 και η διάρκεια συμβόλου είναι 8 αντί για 11 κομμάτια, που ήταν στο DSSS. Η διαμόρφωση των bit των δεδομένων είναι QPSK και DQPSK.

iv. IEEE 802.11c

Αυτό το πρότυπο δεν είναι ένα νέο ξεχωριστό υποπρότυπο του 802.11, αλλά προσέφερε αλλάγές στα υπόλοιπα υποπρότυπα. Η ομάδα του 802.11c προσδιόρισε πρωτόκολλα για αυτό που αναφέρεται ως AP bridging. Τα APs του 802.11 μπορούν να επικοινωνήσουν μεταξύ τους διαδικτυακά σε σχετικά μικρές αποστάσεις.

v. IEEE 802.11d

Αυτό το πρότυπο σχετίζεται με τον κανονισμό ραδιοκυμάτων σε διεθνές επίπεδο. Η χρήση του φάσματος συχνοτήτων κανονίζεται από έθνη και διαφέρει από το ένα έθνος στο άλλο. Το 802.11d προσφέρει διαδικασίες και πρωτόκολλα για να επιτραπεί στα δίκτυα 802.11 να λειτουργούν συμβατά σε σχέση με τους κανονισμούς, μέσω της χρήσης τομέων κανονισμών (regulatory domains). Αν ένας σταθμός δεν συμβαδίζει με τους κανόνες που ορίζει ένας συγκεκριμένος τομέας, δεν θα εκπέμπει και δεν θα συσχετίζεται με κάποιο δίκτυο. Οι τομείς ταυτοποιούνται μέσω πληροφοριών που στέλνει το AP.

vi. IEEE 802.11e

Η ομάδα του προτύπου αυτού ορίζει βελτιώσεις στο 802.11 για να επιτρέψει υποστήριξη του QoS. Λειτουργεί με οποιαδήποτε επέκταση PHY.

vii. IEEE 802.11f

Τα handovers μεταξύ Access Points υποστηρίζονται μέσω του πρωτοκόλλου Inter AP, που ορίζεται από το 802.11f. Συνεχής λειτουργία καθώς ο σταθμός κινείται υποστηρίζεται όταν χρησιμοποιείται το IAPP. Η λογική του handover είναι γνωστή από τα δίκτυα κελιών.

viii. IEEE 802.11g

Το πρότυπο αυτό συνδυάζει τα πλεονεκτήματα του 802.11b (σχετικά μεγάλη κάλυψη) και του 802.11a ορίζοντας την εφαρμογή του τρόπου μετάδοσης 802.11a OFDM στην ζώνη των 2.4 Ghz, όπου κανονικά λειτουργεί το 802.11b. Οπότε, το 802.11g προσφέρει ταχύτητας ως 54 Mbit/s.

ix. IEEE 802.11h

Η δυναμική επιλογή συχνότητας και ο έλεγχος ισχύος πομπού προσδιορίζονται από αυτό το πρότυπο, με περισσότερη βάση στο 802.11a και την ζώνη των 5 GHz. Ο λόγος για την εφαρμογή αυτών των σχεδίων είναι ο διαμοιρασμός φάσματος και η αποτελεσματικότητα, η υποστήριξη QoS και η κατανάλωση ενέργειας. Για επιλογή της συχνότητας λειτουργίας του σταθμού βάσης, ένα Access Point πρέπει να ξέρει την κατάσταση όλων των καναλιών συχνοτήτων. Η κατάσταση του παρόντος καναλιού είναι διαθέσιμη στο AP. Η συλλογή πληροφοριών για τα υπόλοιπα κανάλια γίνεται μέσω μετρήσεων από άλλους σταθμούς και από το ίδιο το AP.

x. IEEE 802.11i

Η ασφάλεια γίνεται όλο και πιο σημαντική με την αύξηση της δημοτικότητας του 802.11. Το 802.11i έχει την ευθύνη για την ανάπτυξη του Wired Equivalent Privacy (WEP) protocol (IEEE, 2004b).

xi. IEEE 802.11k

Ο σκοπός του προτύπου αυτού είναι να παρέχει κανόνες μετρήσεων και τρόπους με τους οποίους ένας ραδιοσταθμός μπορεί διαδράσει με τον περιβάλλοντα ραδιοχώρο.

xii. IEEE 802.11p

Το IEEE 802.11p πρωτόκολλο Ασύρματης Πρόσβασης σε Περιβάλλον Οχημάτων – WAVE – Wireless Access Vehicular Environment – ΚΥΜΑ που προβλέπεται για ασύρματη επικοινωνία μεταξύ οχήματος οχήματος και οχήματος καθοδόν υποδομής βρίσκεται πρόσφατα κάτω από το ενδιαφέρον της προτυποποίησης.

2.5. Ασφάλεια

Τα ασύρματα δίκτυα δεν είναι ασφαλή. Ως επί το πλείστον είναι επαρκώς ασφαλή, αλλά είναι αδύνατον να δημιουργηθεί ένα δίκτυο Wi-Fi απολύτως ιδιωτικό.

Ένα ασύρματο δίκτυο χρησιμοποιεί ραδιοσήματα με ένα καλά καθορισμένο σύνολο χαρακτηριστικών, έτσι κάποιος που θα αφιερώσει αρκετό χρόνο και προσπάθεια στο να τα παρακολουθεί μπορεί μάλλον να βρει τρόπο να υποκλέψει και να διαβάσει τα δεδομένα που περιέχονται σε αυτά. Αν στείλει κανείς απόρρητες πληροφορίες μέσω ενός ασύρματου συνδέσμου, μπορούν να υποκλαπούν.

Η κωδικοποίηση και άλλες μέθοδοι ασφάλειας μπορούν να κάνουν δυσκολότερη την υποκλοπή δεδομένων, αλλά δεν παρέχουν πλήρη προστασία. Ολόκληροι κατάλογοι από εργαλεία για "σπάσιμο" κωδικοποίησης WEP μπορούν εύκολα να βρεθούν στο Internet.

Τα πράγματα γίνονται ακόμη πιο επικίνδυνα από το γεγονός ότι πολλοί χρήστες και διαχειριστές δικτύων δεν χρησιμοποιούν τις κωδικοποιήσεις και λειτουργίες ασφαλείας που υπάρχουν ενσωματωμένες σε κάθε 802.11b σημείο πρόσβασης. Έτσι ιδιαίτερα σε αστικές περιοχές είναι συχνό το φαινόμενο της σύνδεσης αγνώστων σε λογαριασμούς άλλων χρηστών.

Από έρευνες που έχουν γίνει, διαπιστώθηκε ότι σε αστικές περιοχές των Η.Π.Α. ένας ειδικός ασφάλειας δικτύων μπορούσε να αποκτήσει πρόσβαση κατά μέσο όρο σε ασύρματα δίκτυα 6 χρηστών ανά τετράγωνο.
Ένα κοινό οικιακό ασύρματο δίκτυο έχει εμβέλεια περίπου 40 μέτρα προς κάθε κατεύθυνση. Είναι λογικό λοιπόν να εκτείνεται εκτός του σπιτιού του κάθε χρήστη. Αν λοιπόν δεν λάβει κανείς τα απαραίτητα μέτρα ασφαλείας που προσφέρουν τα σημεία πρόσβασης γείτονες ή ακόμα και περαστικοί με laptop μπορούν να εισέλθουν στο δίκτυο του, να υποκλέψουν αρχεία και στην πιο απλή περίπτωση να καθυστερούν την σύνδεσή του στο διαδίκτυο κατεβάζοντας δεδομένα οποιουδήποτε είδους.

Είναι σημαντικό να καταλάβουμε ότι μιλάμε για δύο διαφορετικής φύσης απειλές για την ασφάλεια ενός ασύρματου δικτύου. Η πρώτη είναι ο κίνδυνος σύνδεσης κάποιου μη εξουσιοδοτημένου υπολογιστή στο δίκτυο. Η δεύτερη είναι η υποκλοπή δεδομένων κατά την αποστολή ή την λήψη τους. Κάθε μια αντιπροσωπεύει ένα διαφορετικό πιθανό πρόβλημα που απαιτεί μια διαφορετική αντιμετώπιση για την πρόληψη του. Είναι σίγουρα αλήθεια πως κανένα από τα διαθέσιμα εργαλεία δεν μπορεί να προσφέρει απόλυτη προστασία, αλλά μπορούν να βάλουν πολλά εμπόδια στους περισσότερους επίδοξους εισβολείς.

Τα ασύρματα δίκτυα έχουν θετικά και αρνητικά. Τα προφανή πλεονεκτήματα μιας γρήγορης και εύκολης ασύρματης πρόσβασης έχουν το κόστος του συμβιβασμού της ασφάλειας.

2.5.1. Network Name (SSID)

Κάθε ασύρματο δίκτυο έχει ένα όνομα. Σε ένα δίκτυο με ένα μόνο σημείο πρόσβασης, το όνομα είναι το βασικό σύνολο υπηρεσιών ID (BSSID). Όταν το δίκτυο έχει περισσότερα σημεία πρόσβασης, το όνομα γίνεται Επεκταμένο σύνολο υπηρεσιών ID (ESSID). Το αρχικό καθορισμένο όνομα για όλα τα ονόματα δικτύων είναι το SSID και είναι ο πιο συχνά συναντώμενος όρος σε προγράμματα ρύθμισης σημείων πρόσβασης.

Όταν ρυθμίζεται το σημείο πρόσβασης ενός δικτύου πρέπει να καθοριστεί το SSID για αυτό το συγκεκριμένο δίκτυο. Κάθε σημείο πρόσβασης και πελάτης δικτύου πρέπει να χρησιμοποιούν το ίδιο SSID. Σε υπολογιστές που χρησιμοποιούν το λειτουργικό Windows το SSID πρέπει να είναι το ίδιο και με το όνομα της ομάδας εργασίας στην οποία ανήκει αυτός ο υπολογιστής.

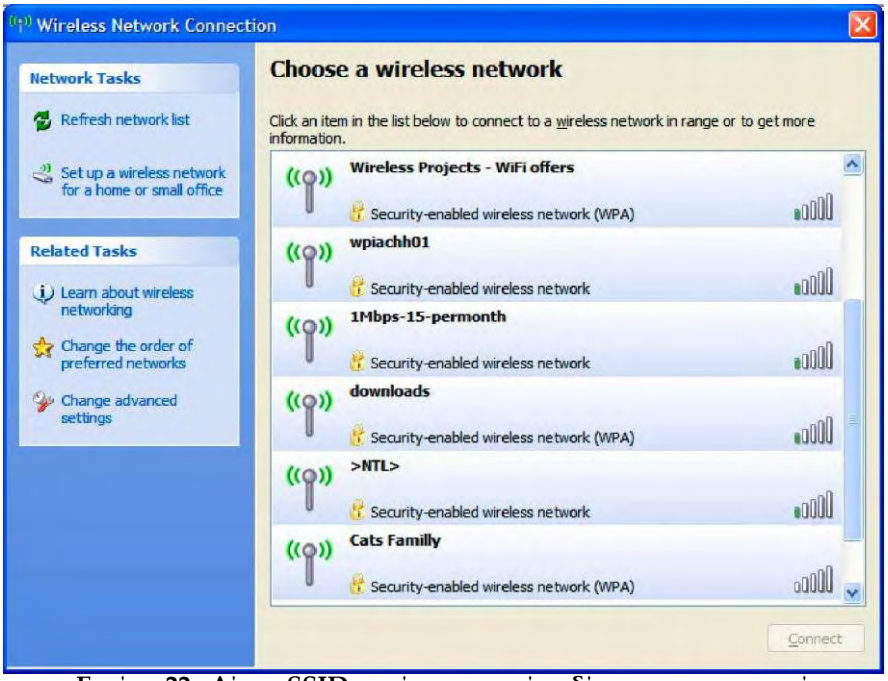
Όταν ένα δίκτυο ανιχνεύσει δύο ή περισσότερα σημεία πρόσβασης με το ίδιο SSID, υποθέτει ότι είναι και τα δύο μέρος του ίδιου δικτύου (ακόμη και αν τα σημεία πρόσβασης λειτουργούν σε διαφορετικά κανάλια), και πραγματοποιεί σύνδεση με το σημείο πρόσβασης που παρέχει το δυνατότερο ή καθαρότερο σήμα. Αν το σήμα αυτό ασθενήσει λόγω παρεμβολών, ο πελάτης θα προσπαθήσει να συνδεθεί σε άλλο σημείο πρόσβασης του δικτύου αυτού.

Αν δύο διαφορετικά δίκτυα με επικαλυπτόμενα σήματα έχουν το ίδιο όνομα, ένα πελάτης θα υποθέσει ότι ανήκουν στο ίδιο δίκτυο, και ίσως προσπαθήσει να πραγματοποιήσει ένα handoff από το ένα δίκτυο στο άλλο. Από την πλευρά του χρήστη, αυτό το λανθασμένο handoff θα φανεί σαν "πέσιμο" της σύνδεσης. Γι' αυτό, κάθε ασύρματο δίκτυο που θα μπορούσε να επικαλύπτεται από ένα άλλο πρέπει να έχει μοναδικό SSID.

Η εξαιρέσεις στον κανόνα του μοναδικού SSID είναι δημόσια και κοινοτικά δίκτυα που παρέχουν πρόσβαση μόνο στο διαδίκτυο, αλλά όχι σε άλλους υπολογιστές ή συσκευές σε ένα LAN. Αυτά τα δίκτυα συχνά έχουν ένα κοινό SSID, έτσι ώστε οι συνδρομητές να μπορούν να τα ανιχνεύουν και να συνδέονται σ' αυτά από διάφορες τοποθεσίες.

Κάποια σημεία πρόσβασης προσφέρουν την επιλογή μεταξύ ανοιχτής και κλειστής πρόσβασης. Όταν το σημείο πρόσβασης είναι σε λειτουργία ανοιχτής πρόσβασης, θα δεχτεί τη σύνδεση με ένα πελάτη που το SSID του είναι "ANY", αλλά και με συσκευές ρυθμισμένες στο SSID του σημείου πρόσβασης. Όταν είναι ρυθμισμένο σε λειτουργία κλειστής πρόσβασης, δέχεται συνδέσεις μόνο με συσκευές που το SSID τους είναι το ίδιο με το δικό του SSID. Αυτός είναι ένας καλός τρόπος για να κρατήσει κανείς κάποιους εισβολείς εκτός του δικτύου του, αλλά λειτουργεί μόνο αν κάθε συσκευή του δικτύου χρησιμοποιεί έναν αντάπτορα Orinoco. Αν ένας αντάπτορας φτιαγμένος από άλλο κατασκευαστή προσπαθήσει να συνδεθεί στο σημείο πρόσβασης, θα τον απορρίψει ακόμη και αν το SSID του είναι το σωστό.

Το SSID ενός δικτύου προσφέρει μια πολύ περιορισμένη μορφή ελέγχου πρόσβασης, γιατί είναι απραίτητος ο προσδιορισμός του SSID όταν στήνουμε μια ασύρματη σύνδεση. Η επιλογή SSID σε ένα σημείο πρόσβασης δέχεται οποιοδήποτε όνομα θελήσουμε να ορίσουμε, αλλά πολλά προγράμματα ρύθμισης δικτύου ανιχνεύουν αυτόματα τα SSID όλων των δικτύων της περιοχής τους(για παράδειγμα τα Windows εμφανίζουν μια λίστα της μορφής της εικόνας 22). Οπότε δεν είναι απαραίτητο συνήθως να ξέρουμε το SSID ενός δικτύου εκ των προτέρων για να προσπαθήσουμε να συνδεθούμε σ' αυτό.



Εικόνα 22 : Λίστα SSIDs από εντοπισμένα δίκτυα στην περιοχή

Κάθε σημείο πρόσβασης έχει ένα SSID εξαρχής το οποίο συνήθως είναι γνωστό και το ίδιο στα σημεία πρόσβασης που παράγει μια εταιρία. Οπότε δε θα πρέπει ποτέ να χρησιμοποιείται το εργοστασιακό SSID μιας συσκευής δικτύου.

Πολλά σημεία πρόσβασης έχουν την επιλογή το SSID να είναι κρυφό. Αυτό μπορεί να εμποδίσει πολλούς να ανιχνεύσουν το δίκτυο, αλλά και πάλι κάθε φορά που ένας νέος πελάτης συνδέεται στο δίκτυο εκπέμπεται το SSID του δικτύου με ασθενές σήμα το οποίο ανιχνεύεται όμως από λογισμικό όπως το Kismet. Οπότε η απόκρυψη του SSID μπορεί να δημιουργήσει μεγαλύτερη δυσκολία σε κάποιον που θέλει να μπει στο δίκτυο αλλά δεν προσφέρει τελικά ουσιαστική προστασία.

2.5.2. Κρυπτογράφηση WEP (Wired Equivalent Privacy)

Η κρυπτογράφηση WEP υπάρχει σε κάθε 802.11b σύστημα, οπότε είναι σημαντική η γνώση του πώς λειτουργεί. Όπως δηλώνει το όνομα, ο αρχικός προορισμός της WEP ήταν να παρέχει επίπεδα προστασίας εφάμιλλα ενός ενσύρματου δικτύου. Όμως έχει αποδειχτεί ότι ένα δίκτυο με κωδικοποίηση WEP είναι σχεδόν όσο τρωτό είναι ένα δίκτυο με καμία προστασία. Δεν αφήνει να εισβάλουν οι απλοί χρήστες, αλλά δεν έχει σχεδόν καμία αποτελεσματικότητα απέναντι σε έναν πεπειραμένο αποφασισμένο εισβολέα.

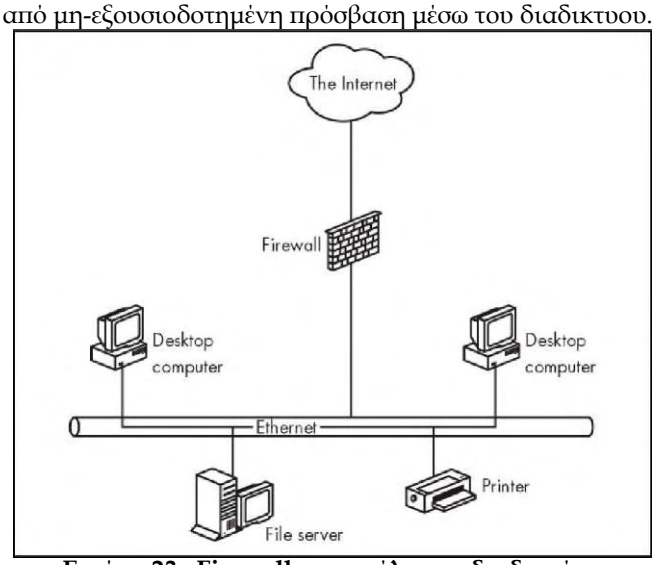
Η κωδικοποίηση WEP έχει σκοπό να επιτελέσει τρείς λειτουργίες : αποτρέπει μη- εξουσιοδοτημένη πρόσβαση στο δίκτυο, πραγματοποιεί έλεγχο πιστότητας σε κάθε μεταδιδόμενο πακέτο δεδομένων και προστατεύει τα δεδομένα από άτομα που "παρακολουθούν". Η WEP χρησιμοποιεί ένα μυστικό κλειδί κωδικοποίησης για να κωδικοποιήσει πακέτα δεδομένων πριν ένας πελάτης ή ένα σημείο πρόσβασης τα εκπέμψει, και χρησιμοποιεί το ίδιο κλειδί για την αποκωδικοποίηση των πακέτων αφού παραληφθούν.

Όταν ένας πελάτης προσπαθεί να ανταλλάξει δεδομένα με ένα δίκτυο με χρήση διαφορετικού κλειδιού, το αποτέλεσμα είναι διαστρεβλωμένο και αγνοείται. Οπότε, οι ρυθμίσεις WEP πρέπει να είναι ακριβώς οι ίδιες σε κάθε σημείο πρόσβασης και κάθε αντάπτορα πελάτη στο δίκτυο. Αυτό ακούγεται αρκετά απλό, αλλά μπορεί να γίνει περίπλοκο γιατί οι κατασκευαστές χρησιμοποιούν διαφορετικές μεθόδους για τον προσδιορισμό του μεγέθους και τον τύπο ενός κλειδιού WEP. Οι λειτουργίες δεν αλλάζουν από μια μάρκα στην άλλη, αλλά ίδιες ρυθμίσεις δεν έχουν πάντα ίδια περιγραφή.

2.5.3. Τείχος Προστασίας

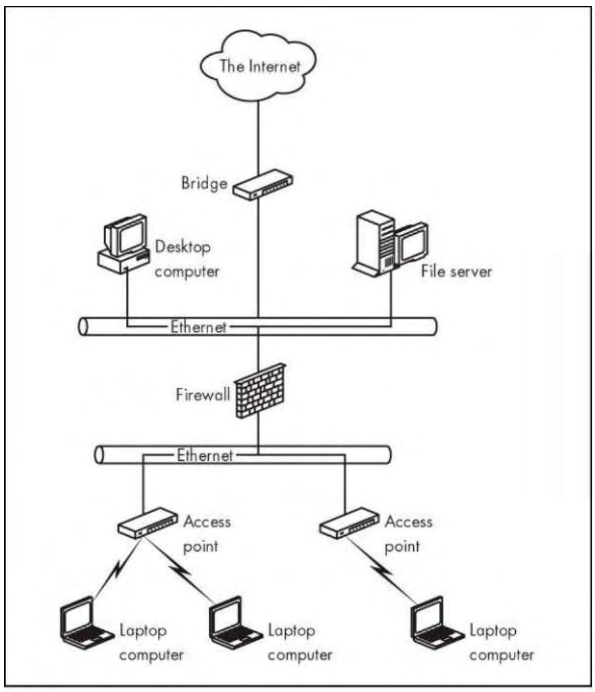
Αν δεχτούμε την ιδέα ότι η κωδικοποίηση WEP και το 802.1x δεν παρέχουν επαρκή προστασία για ένα ασύρματο LAN, το επόμενο λογικό βήμα είναι να βρούμε έναν άλλο τρόπο να κρατήσουμε τους εισβολείς εκτός του δικτύου μας. Χρειαζόμαστε ένα firewall.

Το Firewall είναι ένας proxy server που φιλτράρει όλα τα δεδομένα που περνάν μέσα από αυτόν στην πορεία από και πρός ένα δίκτυο, με βάση ένα σύνολο κανόνων που καθορίζονται από τον διαχειριστή του δικτύου. Για παράδειγμα ένα firewall μπορεί να απορρίψει δεδομένα που προέρχονται από άγνωστη πηγή ή αρχεία που αντιστοιχούν σε μία συγκεκριμένη πηγή, όπως ιούς. Ή μπορεί να επιτρέπει τη διέλευση όλων των δεδομένων προς το διαδίκτυο και να επιτρέπει τη διέλευση μόνο ορισμένων δεδομένων από το διαδίκτυο. Η πιο συνηθισμένη χρήση ενός firewall είναι στην πύλη για το διαδίκτυο όπως φαίνεται στην εικόνα 23. Το firewall παρακολουθεί όλα τα εξερχόμενα και εισερχόμενα δεδομένα μεταξύ του διαδικτύου και του τοπικού δικτύου. Αυτός ο τύπος firewall έχει σκοπό να προστατέψει τους υπολογιστές του LAN από μη-εξουσιοδοτημένη πρόσβαση μέσω του διαδικτυου.



Εικόνα 23 : Firewall στην πύλη του διαδικτύου

Σε ένα ασύρματο δίκτυο, ένα firewall μπορεί επίσης να τοποθετηθεί στην πύλη μεταξύ των ασύρματων σημείων πρόσβασης και του ενσύρματου δικτύου. Έτσι απομονώνει το ασύρματο κομμάτι από το ενσύρματο κομμάτι του LAN, έτσι ώστε εισβολείς που έχουν συνδέσει τον υπολογιστή τους στο δίκτυο χωρίς άδεια να μην μπορούν να χρησιμοποιήσουν την ασύρματη σύνδεση για να μπουν στο διαδίκτυο ή στο ενσύρματο κομμάτι του LAN. Αυτή η χρήση φαίνεται στην εικόνα 24.



Εικόνα 24 : firewall απομόνωσης ασύρματου και ενσύρματου LAN

2.5.4. Virtual Private Networks (VPN)

Αν τα εργαλεία στο 802.11 δεν είναι αρκετά υπάρχει και η εναλλακτική ενός εικονικού ιδιωτικού δικτύου (VPN). Το VPN μπορεί να προσθέσει μια άλλη μορφή αποτελεσματικής προστασίας στα δεδομένα.
Το VPN χρησιμοποιεί ένα "τούνελ δεδομένων" για να συνδέσει δυο σημεία σε ένα δίκτυο μέσω ενός κωδικοποιημένου καναλιού. Τα σημεία μπορεί να είναι ένας πελάτης δικτύου και ένας server, ένα ζεύγος πελατών ή οι πύλες σε ένα ζεύγος από LAN.

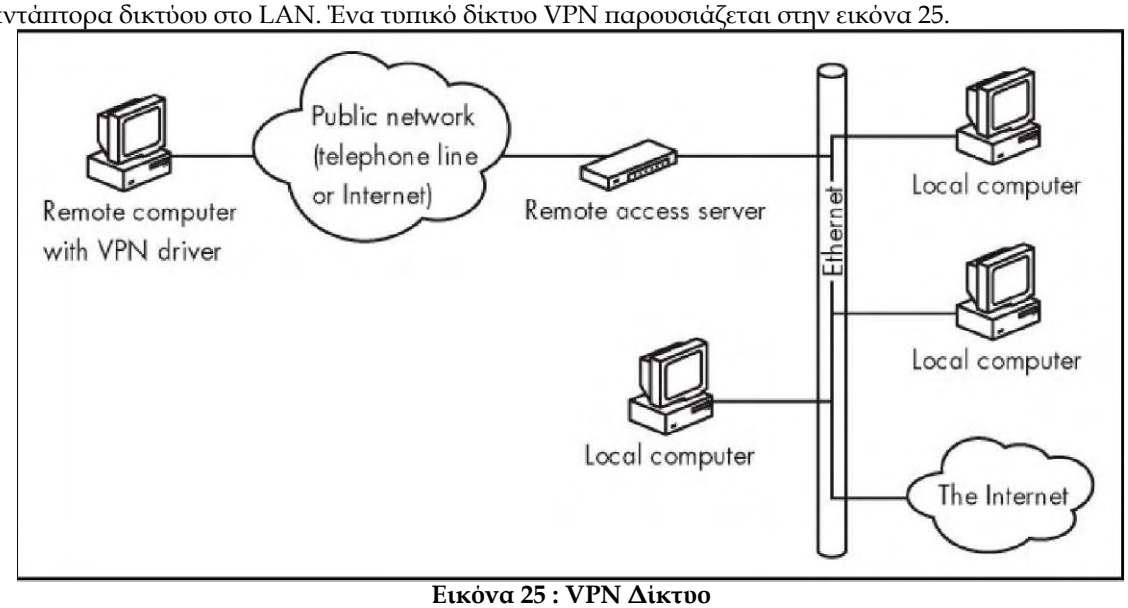
Δεδομένα που περνούν μέσω ενός δημόσιου δικτύου όπως το διαδίκτυο, είναι τελείως απομονωμένα από την υπόλοιπη κίνηση του δικτύου. Χρησιμοποιείται ταυτοποίηση μέσω κωδικού και ονόματος χρήστη και τα δεδομένα κωδικοποιούνται έτσι ώστε να είναι ακατανόητα σε εισβολείς. Επίσης χρησιμοποιεί πιστοποίηση των δεδομένων για να διατηρεί την πιστότητα κάθε πακέτου δεδομένων και να εξασφαλίζει ότι όλα τα δεδομένα προέρχονται από αξιόπιστους πελάτες δικτύου.

Το VPN δεν είναι απλά άλλη μια κωδικοποίηση. Απομονώνει το μονοπάτι δεδομένων από άλλους χρήστες του δικτύου, έτσι ώστε μη-εξουσιοδοτημένοι χρήστες να μην μπορούν να φτάσουν σε αυτό. Οι λειτουργίες του VPN γίνονται στο IP ή στο δικτυακό στρώμα του μοντέλου ISO. Οπότε, μπορούν να λειτουργήσουν πάνω από το 802.11b που λειτουργούν στο φυσικό στρώμα. Τα VPN μπορούν επίσης να περάσουν δεδομένα διαμέσου μιας σύνδεσης που περιλαμβάνει πάνω από ένα φυσικό μέσο (για παράδειγμα έναν ασύρματο σύνδεσμο που περνάει δεδομένα σε ένα ενσύρματο δίκτυο Ethernet). Με άλλα λόγια στο VPN δεν έχει σημασία αν χρησιμοποιούμε ασύρματο σύνδεσμο, καλώδιο Ethernet, μια απλή τηλεφωνική γραμμή, ή κάποιον συνδυασμό αυτών και άλλων μέσων μετάδοσης. Το VPN είναι ένα τούνελ που εκτείνεται από τη μια άκρη του δικτύου στην άλλη, άσχετα με το μέσο διάδοσης των δεδομένων. Αυτό προσθέτει ένα άλλο επίπεδο ασφάλειας (η προσφέρει μια εναλλακτική) στην κωδικοποίηση WEP.

Σε ένα τυπικό VPN, ένας απομακρυσμένος χρήστης μπορεί να μπει σε ένα μακρινό LAN και να χρησιμοποιήσει όλες τις υπηρεσίες δικτύου που είναι διαθέσιμες στους τοπικούς πελάτες. Τα VPN

χρησιμοποιούνται συχνά για να επεκταθούν εταιρικά δίκτυα σε θυγατρικά γραφεία αι να συνδέσουν χρήστες στον LAN από το σπίτι ή από εξωτερικές τοποθεσίες όπως το γραφείο ενός πελάτη.

Μια συσκευή συνδεδεμένη μέσω ενός server VPN παρουσιάζει την ίδια εμφάνιση στο υπόλοιπο δίκτυο όπως μια συσκευή στο ίδιο δωμάτιο ή κτίριο. Η μόνη διαφορά είναι ότι τα δεδομένα από το VPN περνούν μέσα από έναν VPN οδηγό και ένα δημόσιο δίκτυο αντί να πηγαίνουν κατευθείαν από τον αντάπτορα δικτύου στο LAN. Ένα τυπικό δίκτυο VPN παρουσιάζεται στην εικόνα 25.



Εικόνα 25 : VPN Δίκτυο

Όλα τα πλεονεκτήματα στην ασφάλεια ενός συνηθισμένου ενσύρματου VPN ισχύουν και για ένα μικρής εμβέλειας VPN που περνάει από ένα ασύρματο σύνδεσμο και ένα μεγαλύτερης εμβέλειας VPN που αρχίζει σε ένα ασύρματο δίκτυο και στέλνει τα δεδομένα σε έναν απομακρυσμένο server. Αυτές είναι δυο διαφορετικές χρήσεις για ένα VPN: ένα τοπικό VPN μπορεί να εκτείνεται μόνο στο ασύρματο κομμάτι ενός δικτύου μεταξύ των συσκευών πελατών και του σημείου πρόσβασης, ενώ ένα διευρυμένο δίκτυο μπορεί να μεταφέρει δεδομένα κωδικοποιημένα κατά VPN πέρα από τα σημεία πρόσβασης σε έναν server VPN μέσω ενός δημόσιου δικτύου όπως το διαδίκτυο.

Ένα διευρυμένο δίκτυο είναι ένα παραδοσιακό VPN που τυχαίνει να προέρχεται από έναν πελάτη ασύρματου δικτύου. Το ίδιο VPN μπορεί να υποστηρίξει επίσης συνδέσεις που δεν περιλαμβάνουν ασύρματο μέρος, μαζί με προσβάσεις από δημόσιες ασύρματες υπηρεσίες, όπως σε αεροδρόμια ή καφετέριες. Αυτός είναι ο συνηθισμένος τρόπος χρήσης ενός VPN.

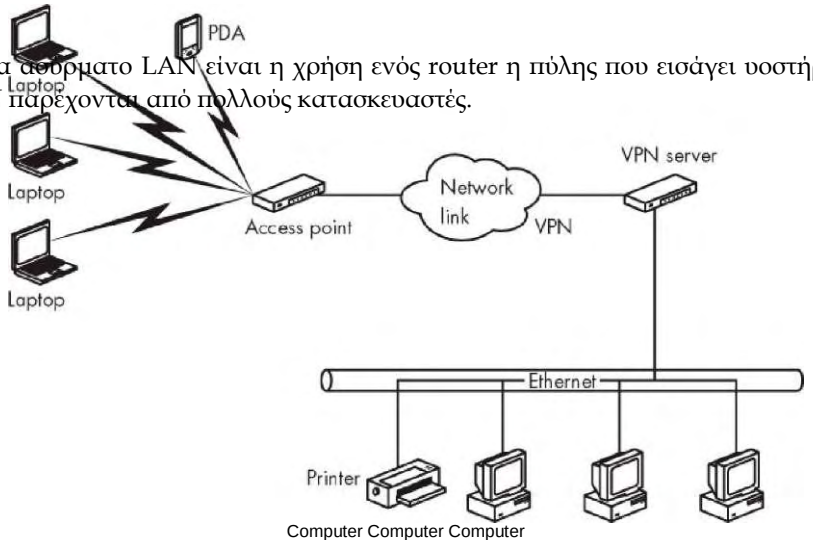
Τοπικά VPN μικρής εμβέλειας είναι πιο ενδιαφέροντα για ανθρώπους που διαχειρίζονται ασύρματα δίκτυα γιατί προσθέτουν ένα άλλο στρώμα ασφαλείας σε ασύρματους συνδέσμους. Επειδή τα δεδομένα που κινούνται μεταξύ ασύρματων πελατών και του σημείου πρόσβασης είναι κωδικοποιημένα (με χρήση ενός αλγορίθμου που είναι ασφαλέστερος της κωδικοποίησης WEP), είναι ακατανόητα για οποιονδήποτε τρίτο μπορεί να παρακολουθεί την ροή των δεδομένων. Επίσης, επειδή ο VPN server στο σημείο πρόσβασης δεν δέχεται συνδέσμους δεδομένων από ασύρματους πελάτες που δεν χρησιμοποιούν τους σωστούς οδηγούς και κωδικούς VPN, ένας εισβολέας δεν μπορεί να εισβάλει στο δίκτυο συσχετίζοντας έναν ψεύτικο πελάτη με το σημείο πρόσβασης.

Ο στόχος ενός ασύρματου VPN είναι να προστατεύει τον ασύρματο σύνδεσμο μεταξύ των πελατών και του σημείου πρόσβασης και να αποκλείει την σύνδεση μη εξουσιοδοτημένων χρηστών. Οπότε, τα απομονωμένα και κρυπτογραφημένα δεδομένα μπορούν να κινούνται σε κοντινή απόσταση αντί για εκατοντάδες ή χιλιάδες χιλιόμετρα. Φυσικά, το σημείο πρόσβασης μπορεί να μεταφέρει δεδομένα κωδικοποιημένα κατά VPN μέσω του διαδικτύου σε άλλη τοποθεσία.

Η εικόνα 26 δείχνει μια ασύρματη σύνδεση με ένα VPN. Ο VPN server βρίσκεται μεταξύ του ασύρματου σημείου πρόσβασης και του LAN, έτσι ώστε όλα τα πακέτα που κινούνται μέσω του ασύρματου μέρους

να είναι κρυπτογραφημένα. Το διάγραμμα δείχνει τον VPN server ως χωριστό στοιχείο, αλλά στην πράξη ο πιο πρακτικός τρόπος για να προσθέσουμε VPN

ασφάλεια σε ένα ασύρματο LAN είναι η χρήση ενός router η πύλης που εισάγει υοστήριξη VPN. Routers με VPN παρέχονται από πολλούς κατασκευαστές.



Εικόνα 26 : Το VPN παρέχει ασφαλή σύνδεση μεταξύ ασύρματου δικτύου και μιας διαδικτυακής πύλης

Μέθοδοι VPN

Ένα VPN μετακινεί δεδομένα μέσω ενός ή περισσότερων δικτύων σε έναν προορισμό ή σε ένα άλλο δίκτυο. Ο πελάτης του VPN "τυλίγει" τα πακέτα δεδομένων προσθέτοντας μία νέα επικεφαλίδα με πληροφορίες καθοδήγησης που λέει στα πακέτα πως θα φτάσουν στο τέλος του VPN. Το μονοπάτι μετάδοσης μέσω των δικτύων αυτών λέγεται τούνελ. Στην άλλη άκρη του τούνελ, ο VPN server αφαιρεί την επικεφαλίδα καθοδήγησης και προωθεί τα δεδομένα στον προορισμό που καθορίζεται από το επόμενο στρώμα επικεφαλίδων. Η ακριβής μορφή του τούνελ δεν παίζει ρόλο για τα δεδομένα, γιατί τα δεδομένα αντιμετωπίζουν το τούνελ σαν μια σύνδεση σημείου-σημείου.

Οι επικεφαλίδες τούνελ μπορούν να πάρουν διάφορες μορφές. Οι μέθοδοι που χρησιμοποιούνται ευρέως στα VPNs είναι :

1. Πρωτόκολλο τούνελ σημείου-σημείου (PPTP)
2. Πρωτόκολλο τούνελ δεύτερου στρώματος (L2TP)
3. IP Security (IPSec) mode

Τα δύο πρώτα μπορούν να μετακινήσουν δεδομένα μέσω IP, IPX Και NetBEUI δίκτυα. Η IPSec περιορίζεται σε IP δίκτυα. Ο πελάτης και ο server πρέπει να χρησιμοποιούν το ίδιο πρωτόκολλο.

Στα PPTP και L2TP, ο πελάτης και ο server πρέπει να ρυθμίσουν το τούνελ για κάθε μετάδοση πριν αρχίσουν να ανταλλάσουν δεδομένα. ΟΙ παράμετροι ρυθμίσεων περιλαμβάνουν την διαδρομή μέσω του δικτύου και τα χαρακτηριστικά και κρυπτογράφησης και συμπίεσης. Όταν η μετάδοση τελειώσει , ο πελάτης και ο server τερματίζουν τη σύνδεση και κλείνουν το τούνελ.

Κάθε ένα από τα πρωτόκολλα προσφέρει συγκεκριμένα πλεονεκτήματα και μειονεκτήματα, αλλά είναι όλα αρκούντως καλά για δημιουργία ενός ασφαλούς συνδέσμου μεταξύ ενός ασύρματου πελάτη και ενός σημείου πρόσβασης. Οι διαφορές μεταξύ τους είναι περισσότερο τεχνικές παρά πρακτικές.

3. ΚΑΤΑΣΚΕΥΗ ΔΙΚΤΥΩΝ 802.11

Η επιτυχημένη κατασκευή ενός δικτύου 802.11 απαιτεί προσεκτικό σχεδιασμό και μελέτη. Σ'αυτό το κεφάλαιο θα αναφερθούμε σε αυτά καθώς επίσης και την λειτουργία και τη συντήρηση που απαιτεί ένα τέτοιο δίκτυο για την ομαλή του λειτουργία.

3.1. Σχεδιασμός και Μελέτη

Οι εταιρίες όπως είδαμε παράγουν εξοπλισμό που χρησιμοποιεί διαφορετικά πρότυπα του 802.11. Κατά τον σχεδιασμό ενός δικτύου πρέπει να επιλεγεί το πρότυπο που θα χρησιμοποιηθεί. Το πιο κοινό πρότυπο σήμερα είναι το 802.11b. Αυτό όμως δεν σημαίνει πως είναι το σωστό για κάθε δίκτυο. Δύο νέα πρωτόκολλα εμφανίζονται : τα 802.11 g και 802.11a. Όμως το ποιο από όλα θα χρησιμοποιηθεί εξαρτάται από την εφαρμογή και τις απαιτήσεις τις.

Κάποιες από τα θέματα που αντιμετωπίζονται κατά την επιλογή του προτύπου, είναι ο συμβιβασμός ταχύτητας - εμβέλειας. Άλλα ερωτήματα είναι τα εξής : Ποια πρέπει να είναι η τοπολογία του δικτύου; Τι είδους σύνδεσμοι πρέπει να χρησιμοποιηθούν; Πως είναι το περιβάλλον του δικτύου; Ποια είναι η διαπερατότητα, η εμβέλεια και ο ρυθμός λαθών που χρειαζόμαστε; Ποιες ζώνες συχνοτήτων θα χρησιμοποιήσουμε με ποια πρωτόκολλα; Μπορεί η λύση να είναι κάποιο έτοιμο πρωτόκολλο, ένα από τα νέα ανερχόμενα πρότυπα ή μπορεί να χρειάζεται κάποια νέα παραμετροποιημένη λύση.

Τοπολογία δικτύου

Ένας από τους στόχους του σχεδιασμού είναι η σιγουριά ότι η δουλειά θα γίνει μέσα στα πλαίσια του προϋπολογισμού. Όλα τα σημεία σύνδεσης πρέπει να μπορούν να επικοινωνήσουν με άλλα σημεία σε οποιαδήποτε στιγμή. Τα σχέδια του δικτύου πρέπει να είναι τέτοια ώστε, αν ένα σημείο σύνδεσης αποτύχει, να μην επηρεάζεται κανένα άλλο σημείο. Αν η ασφάλεια είναι θέμα, τα ασφαλή σημεία του δικτύου πρέπει να είναι απομονωμένα από τα επισφαλή. Ένας από τους σημαντικότερους παράγοντες που καθορίζει την διαπερατότητα, αξιοπιστία, ασφάλεια, κόστος και "υγεία" του δικτύου είναι η γεωμετρική κατανομή του ή αλλιώς η τοπολογία του.

Πέντε κύριες τοπολογίες χρησιμοποιούνται σήμερα σε ενσύρματα δίκτυα : οι bus, star, tree, ring και mesh. Σε ένα WLAN, μόνο οι star και mesh έχουν τοπολογίες ανάλογες με τα ενσύρματα δίκτυα. Οι τοπολογίες αυτές μπορούν να πραγματοποιηθούν με χρήση τρόπων λειτουργίας που υποστηρίζονται από πρότυπα 802.11 της IEEE, το ad hoc και τον τρόπο λειτουργίας infrastructure. Αυτά θέτουν το ανεξάρτητο βασικό σύνολο υπηρεσιών(IBSS), το βασικό σύνολο υπηρεσιών(ESS) και το διευρυμένο σύνολο υπηρεσιών(ESS).

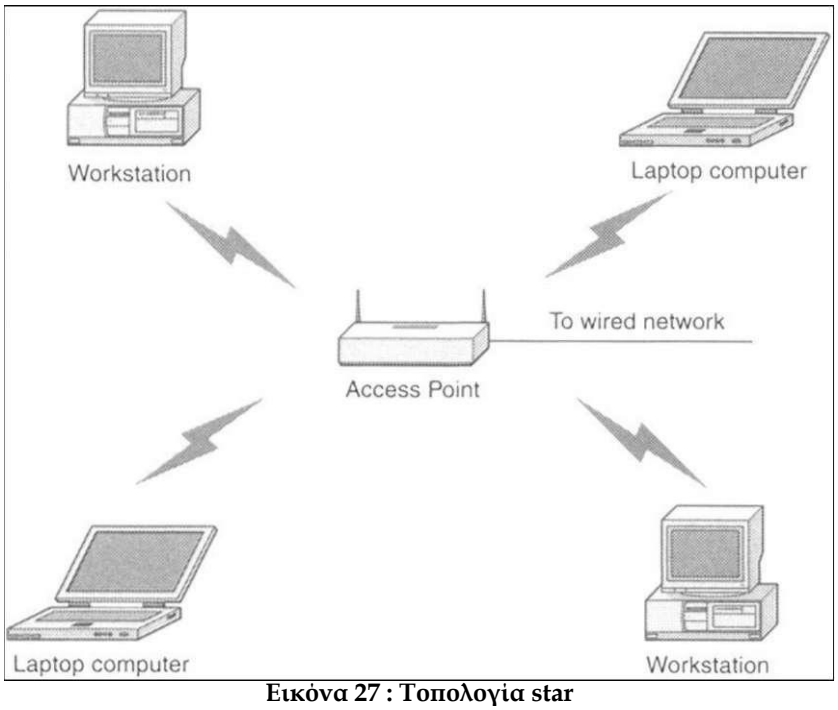
Ο πιο κοινός τρόπος λειτουργίας είναι το infrastructure. Σ' αυτόν τον τρόπο, οι ασύρματες συσκευές μπορούν να επικοινωνούν μεταξύ τους μέσω ενός ενσύρματου δικτύου. Όταν ένα σημείο πρόσβασης είναι συνδεδεμένο σε ένα ενσύρματο δίκτυο και ένα σύνολο ασύρματων σταθμών, αναφερόμαστε σ'αυτό ως BSS. Ένα BSS αποτελείται από τουλάχιστον ένα σημείο πρόσβασης συνδεδεμένο στο ενσύρματο δίκτυο και ένα σύνολο από ασύρματους τερματικούς σταθμούς. Έτσι, οι ρυθμίσεις του BSS βασίζονται σε ένα σημείο πρόσβασης που δρα ως διακόπτης για ένα κελί ή κανάλι ενός WLAN.

Ένα ESS είναι ένα σύνολο δύο ή περισσότερων BSS, που το καθένα περιλαμβάνει ένα σημείο πρόσβασης συνδεδεμένα μεταξύ τους μέσω ενός συστήματος διαμοιρασμού έτσι ώστε να σχηματίζουν ένα υποδίκτυο (subnet). Παρά το ότι το σύστημα διαμοιρασμού θα μπορούσε να είναι οποιοδήποτε είδος δικτύου, είναι συχνά ένα Ethernet LAN. Ένας κινητός χρήστης μπορεί να κινείται μεταξύ σημείων πρόσβασης και να επανασυσχετίζει με αυτό που του προσφέρει την καλύτερη κάλυψη. Με αυτό τον τρόπο, μια ενιαία κάλυψη είναι δυνατή μέσα στο υποδίκτυο. Τα περισσότερα WLANs λειτουργούν σε

τρόπο infrastructure γιατί απαιτούν πρόσβαση στο ενσύρματο LAN για υπηρεσίες όπως διακομιστές αρχείων, εκτυπωτές και πρόσβαση στο διαδίκτυο.

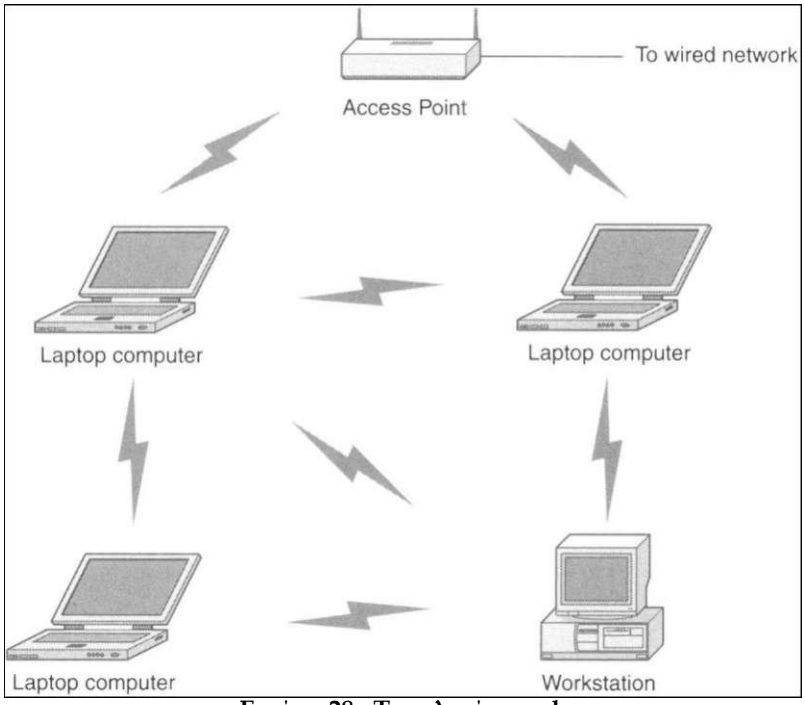
Στο ad hoc, οι συσκευές ή σταθμοί επικοινωνούν απευθείας ο ένας με τον άλλον, χωρίς την χρήση σημείων πρόσβασης. Εδώ χρησιμοποιείται το IBSS. Οι ρυθμίσεις του IBSS αναφέρονται επίσης ως ανεξάρτητες ρυθμίσεις ή δίκτυο ad hoc. Λογικά, μια ρύθμιση IBSS είναι ανάλογη με ένα δίκτυο peer-to-peer στο οποίο δεν χρειάζεται σύνδεσμος που να λειτουργεί ως διακόπτης ή router. Τα IBSS WLAN δίκτυα περιλαμβάνουν μερικούς ουνδέσμους ή ασύρματους σταθμούς που επικοινωνούν απ' ευθείας μεταξύ τους. Είναι χρήσιμα για το στήσιμο ενός ασύρματου δικτύου οπουδήποτε ένα ασύρματο Infrastructure είτε δεν υπάρχει είτε δεν είναι απαραίτητο για τις υπηρεσίες. Θα μπορούσε να είναι ένα δωμάτιο ξενοδοχείου, ένα αεροδρόμιο ή ένα συνεδριακό κέντρο όπου η πρόσβαση στο ενσύρματο δίκτυο είναι απαγορευμένη. Γενικά οι εφαρμογές του IBSS καλύπτουν μια περιορισμένη έκταση και δεν συνδέονται σε μεγαλύτερο δίκτυο.

Η τοπολογία star, που τυγχάνει ευρύτατης χρήσης, είναι ένα δίκτυο στο οποίο ένα κεντρικός σταθμός βάσης ή ένα σημείο πρόσβασης χρησιμοποιείται για επικοινωνία. Πακέτα επικοινωνίας εκπέμπονται από τον αρχικό σύνδεσμο και παραλαμβάνονται και καθοδηγούνται από το σημείο πρόσβασης στον σωστό ασύρματο προορισμό.



Εικόνα 27 : Τοπολογία star

Η τοπολογία mesh διαφέρει ελαφρώς από την τοπολογία star. Δεν έχει κεντρικό σταθμό βάσης. Κάθε σύνδεσμος που βρίσκεται μέσα στην εμβέλεια ενός άλλου μπορεί να επικοινωνεί ελεύθερα.



Εικόνα 28 : Τοπολογία mesh

Τα ασύρματα δίκτυα mesh είναι μία συναρπαστική νέα τοπολογία για δημιουργία χαμηλού κόστους, υψηλής αξιοπιστίας ασύρματα δίκτυα σε εσωτερικούς χώρους ή ακόμη και σε μητροπολιτικές περιοχές. Σε ένα τέτοιο δίκτυο, κάθε ασύρματος σύνδεσμος εξυπηρετεί σαν σημείο πρόσβασης και ταυτόχρονα σαν ασύρματο router, δημιουργώντας πολλαπλούς δρόμους για το σήμα. Έτσι αυτά τα δίκτυα δεν έχουν μοναδικό σημείο αποτυχίας και είναι αυτοιαζόμενα. Μπορούν να σχεδιαστούν ώστε να οδηγούν το σήμα γύρω από εμπόδια που θα δημιουργούσαν πρόβλημα σε άλλες τοπολογίες δικτύου. Παρόλα αυτά, ένα ασύρματο mesh χρειάζεται ειδικό λογισμικό που θα επιτελεί την λειτουργία οδήγησης και θα διαλέγει λειτουργία infrastructure ή ad hoc.

Είδος συνδέσμου (Link type)

Τα συστήματα 802.11 μπορούν να στηθούν είτε με συνδέσμους σημείου-σημείου είτε με συνδέσμους σημείου-πολλών σημείων.

Περιβάλλον

Στον σχεδιασμό πρέπει να ληφθούν υπόψη παράγοντες όπως αν ο χώρος είναι εξωτερικός ή εσωτερικός, αν υπάρχει οπτική επαφή μεταξύ των συνδέσμων και αν υπάρχουν στην περιοχή παράγοντες που μπορεί να προκαλέσουν παρεμβολές και παραμορφώσεις στο σήμα μας.

Διαπερατότητα, εμβέλεια και ρυθμός λαθών bit

Η διαπερατότητα σχετίζεται με την εμβέλεια και τον ρυθμό λαθών bit. Τα καλύτερα σχέδια δικτύων σταθμίζουν αυτούς τους παράγοντες περιορίζοντας των ρυθμό δεδομένων σε σχέση με τις απαιτήσεις σε ποσότητα δεδομένων και την χρονική καθυστέρηση.

Αν η κύρια χρήση του δικτύου θα είναι πρόσβαση στο διαδίκτυο με το σημείο πρόσβασης λιγότερο από 30 Μέτρα μακριά, τότε οποιοδήποτε από τα πρότυπα του 802.11 ταιριάζει. Η διαπερατότητα είναι περιορισμένη από το πρωτόκολλο και ο ρυθμός λαθών bit πρέπει να
είναι σχετικά μεγάλος για να έχουμε διαπερατότητα, οπότε η μόνη μεταβλητή που μένει είναι η εμβέλεια. Αυτή υπολογίζεται για δεδομένη διαπερατότητα με χρήση link budget.

Ανοχή απόσβεσης πολλών δρόμων(ΜηϊΗραiΗ Fading Tolerance)

Σε επικοινωνίες χωρίς οπτική επαφή πρέπει επιτρέπεται μεγάλο multipath fading. Το multipath δημιουργείται από ανακλάσεις που αποβαίνουν το κύριο σήμα. Η επιλογή ζώνης συχνοτήτων και πρωτοκόλλων θα εξαρτηθεί εν μέρει από το πόσο multipath είναι ανεκτό.

Link Budget

Μία βασική έννοια σε κάθε σύστημα επικοινωνιών είναι το link budget. Αυτό είναι το άθροισμα όλων των κερδών και των αποσβέσεων ενός συστήματος επικοινωνιών. Το αποτέλεσμα του link budget είναι η ισχύς εκπομπής που απαιτείται έτσι ώστε με δεδομένο λόγο σήματος προς θόρυβο, να παρουσιαστεί ένα σήμα στον δέκτη που να έχει τον επιθυμητό ρυθμό λαθών bit.

Για τα Wi-Fi αρκεί να λάβουμε υπόψη παράγοντες όπως απόσβεση, θόρυβο, ευαισθησία δέκτη, και κέρδη από κεραίες και καλώδια. Πριν υπολογίσουμε το Link budget πρέπει να ληφθεί υπόψη και η ζώνη συχνοτήτων.

Ζώνη συχνοτήτων

Οι τεχνολογίες του 802.11 μπορούν να εφαρμοστούν σε τέσσερις μη αδειοδοτημένες ζώνες συχνοτήτων, στι δύο ISM και U-NII ζώνες. Η ζώνη ISM των 2.4 GHz έχει δυνατότερο σήμα με μεγαλύτερη εμβέλεια και μπορεί να διαπερνάει τοίχους καλύτερα από τις ζώνες U-NII των 5 GHz. Παρόλα αυτά η ζώνη U-NII επιτρέπει σε περισσότερους χρήστες να βρίσκονται ταυτόχρονα στο ίδιο κανάλι. Η ζώνη ISM των 2.4 GHz έχει ένα μέγιστο τριών μη επικαλυπτόμενων καναλιών των 22 MHz, ενώ η ζώνη των 5 GHz έχει τέσσερα μη επικαλυπτόμενα κανάλια των 20 MHz σε κάθε μια από τις U-NII ζώνες.

ISM ζώνη

Οι ISM ζώνες αρχικά κρατήθηκαν διεθνώς για μη εμπορική χρήση. Δηλαδή για βιομηχανικές, επιστημονικές και ιατρικές χρήσεις. Πρόσφατα έχουν χρησιμοποιηθεί επίσης για επικοινωνίες που έχουν ανοχή στα λάθη όπως ασύρματα τηλέφωνα, Bluetooth και ασύρματο WLAN.

U-NII ζώνη

Οι ζώνες U-NII μπορούν να χρησιμοποιηθούν από συσκευές που παρέχουν ασύρματες ψηφιακές επικοινωνίες μικρού βεληνεκούς και υψηλής ταχύτητας. Αυτές οι συσκευές που δεν χρειάζονται αδειοδότηση, υποστηρίζουν την δημιουργία WLANs και την πρόσβαση στο διαδίκτυο. Το φάσμα του U-NII εντοπίζεται στα 5.15 έως 5.35 GHz και στα 5.725 έως 5.825 GHz.

Το φασματικό κομμάτι 5.15 έως 5.25 GHz προορίζεται χρήση σε εσωτερικούς χώρους και μικρό βεληνεκές. Η FCC υιοθέτησε ένα όριο ισοτροπικής εκπεμπόμενης ισχύος 200 milliwatt έτσι ώστε να επιτρέπει τις εφαρμογές WLAN μικρού βεληνεκούς σε αυτό το φάσμα χωρίς να έχουμε παρεμβολές σε κινητές δορυφορικές υπηρεσίες.

Συσκευές που λειτουργούν από τα 5.25 έως τα 5.35 GHz προορίζονται για παροχή επικοινωνιών μέσα σε κτίρια ή και μεταξύ κτιρίων. Οι συσκευές αυτές υπόκεινται στο όριο ισοτροπικής εκπεμπόμενης ισχύος του 1 watt.

Το δεύτερο φασματικό κομμάτι των 5.725 έως 5.825 GHz της ζώνης U-NII προορίζεται για δικτύωση σε μεγαλύτερες αποστάσεις. Η FCC επιτρέπει στις συσκευές αυτής της συχνοτικής περιοχής να λειτουργούν με όριο ισοτροπικής εκπεμπόμενης ισχύος τα 200 watt.

Κανονισμοί της FCC

Η χρήση αυτών των ζωνών είναι ρυθμισμένη βάσει των κανονισμών της FCC για την ισχύ και τα επιτρεπόμενα όρια αυτής.

Εύρος συχνοτήτων (MHz)	**Εύρος ζώνης(ΜΗζ)**	**Μέγιστη ισχύς στην κεραία**	**Όριο ισοτροπικής εκπεμπόμενης ισχύος**	**Σημειώσεις**
2400-2483.5	83.5	1 W (+30 *dB above 1 milliwatt* [dBm]), 1 W (+30 dBm)	4 W (+36 dBm)	
5150-5250	100	50 mW	200 mW (+23 dBm)	Εσωτερική χρήση.
5250-5350	100	250 mW (+24 dBm)	1 W (+30 dBm)	
5725-5825	100	1 W (+30 dBm)	200 W (+53 dBm)	

Πίνακας 3 : Όρια ισχύος για τις ζώνες συχνοτήτων που χρησιμοποιούν οι συσκευές Wi-Fi

Επιτρέπεται στις κεραίας να έχουν περισσότερα από 6 dB κέρδος αρκεί η ισχύς στην κεραία να μειώνεται ισόποσα στην ζώνη των 2.4 GHz. Αυτό υπονοεί ότι το όριο ισοτροπικής εκπεμπόμενης ισχύος είναι 4 watt ή 36 dBm. Αυτό φαίνεται στον πίνακα 4.

Ισχύς στην κεραία (mW)	**Ισχύς στην κεραία (dBm)**	**Μέγιστο κέρδος κεραίας (dBi)**	**Όριο ισοτροπικής εκπεμπόμενης ισχύος (watts)**	**Όριο ισοτροπικής εκπεμπόμενης ισχύος (dBm)**
1000	30	6	4	36
500	27	9	4	36
250	24	12	4	36
125	21	16	4	36
63	18	19	4	36
31	15	21	4	36
15	12	24	4	36
8	9	27	4	36
4	6	30	4	36

Πίνακας 4

Σύνδεσμοι σημείου-σημείου

Οι σύνδεσμοι σημείου-σημείου έχουν ένα μοναδικό σημείο εκπομπής και ένα μοναδικό σημείο λήψης. Τυπικά χρησιμοποιούνται σε εφαρμογές επικοινωνίας από οικοδομή σε οικοδομή. Επιτρέπεται στο όριο ισοτροπικής εκπεμπόμενης ισχύος να μεγαλώσει πέρα από το όριο των τεσσάρων watt που ισχύει στους συνδέσμους σημείου-πολλών σημείων, αρκεί για κάθε 3 dB κέρδους στην κεραία να πέφτει η ισχύς του εκπομπού 1 dB. Αυτός ο κανόνας 3 προς 1 παρουσιάζεται στον πίνακα 5.

Ισχύς στην κεραία (mW)	Ισχύς στην κεραία (dBm)	Μέγιστο κέρδος κεραίας (dBi)	Όριο ισοτροπικής εκπεμπόμενης ισχύος (watts)	Όριο ισοτροπικής εκπεμπόμενης ισχύος (dBm)
1000	30	6	4	36
794	29	9	6.3	38
631	28	12	10	40
500	27	15	16	42
398	26	18	25	44
316	25	21	39.8	46
250	24	24	63.1	48
200	23	27	100	50
157	22	30	157	52

Πίνακας 5 : Ο κανόνας 3 προς 1

Για την ζώνη των 5.8 GHz όπως φαίνεται στον πίνακα 6 ο περιορισμός του ορίου ισοτροπικής εκπεμπόμενης ισχύος είναι 53 dBm .

Ισχύς στην κεραία (mW)	Ισχύς στην κεραία (dBm)	Μέγιστο κέρδος κεραίας (dBi)	Όριο ισοτροπικής εκπεμπόμενης ισχύος (watts)	Όριο ισοτροπικής εκπεμπόμενης ισχύος (dBm)
1000	30	6	4	36
1000	30	9	8	39
1000	30	12	16	42
1000	30	15	316	45
1000	30	18	63.1	48
1000	30	21	125	51
1000	30	23	250	53

Πίνακας 6 : Όριο ισχύος στην ζώνη των 5.8 GHz

Τέσσερα βασικά πρωτόκολλα είναι διαθέσιμα σήμερα : 802.11, 802.11b, 802.11a, and 802.11g. Έχουμε αναφερθεί στα βασικά τους χαρακτηριστικά, αλλά θα ξαναδούμε κάποια από αυτά.

802.11

Ήταν το πρώτο πρότυπο που καθόρισε την λειτουργία ενός WLAN. Γίνεται χρήση FHSS, DSSS και υπερύθρων.

802.11b

Είναι το πιο ευρέως χρησιμοποιούμενο πρωτόκολλο και χρησιμοποιεί τεχνολογία DSSS, με μέγιστη ταχύτητα μεταφοράς μέσω του αέρα 11 Mbps. Χρησιμοποιεί την ζώνη των 2.4 GHz.

802.11a

Λειτουργεί στις τρεις ζώνες U-NII των 5 GHz οπότε δεν είναι συμβατό με το 802.11b. Οι ζώνες καθορίζονται ανάλογα με την εφαρμογή. Η ζώνη 5.1 GHz χρησιμοποιείται μόνο σε εσωτερικούς χώρους η 5.2 και εξωτερικούς και εσωτερικούς και η 5.7 GHz μόνο για εξωτερικούς.
Οι παρεμβολές είναι πολύ λιγότερο πιθανές λόγω του μικρότερου συνωστισμού της ζώνης των 5 GHz.

802.11g

Είναι προέκταση του 802.11b και λειτουργεί στην ίδια ζώνη συχνοτήτων. Αυξάνει τον ρυθμό μεταφοράς στα 54 Mbps με χρήση ορθογωνικής πολυπλεξίας με διαίρεση συχνότητας. Επίσης προσφέρει

μεγαλύτερη ανοχή multipath. Είναι πολλές φορές η καλύτερη επιλογή για συμβιβασμό εμβέλειας και εύρους ζώνης.

Επιλογή

Το ποιά είναι τελικά η καλύτερη επιλογή εξαρτάται από την εφαρμογή. Το FHSS προσφέρει αξιοπιστία ως προς τον θόρυβο και την ανοχή multipath. Το DSSS προσφέρει μεγαλύτερες ταχύτητες μεταφοράς. Το 802.11a είναι το καλύτερο για επίλυση προβλημάτων με παρεμβολές και έχει πολύ καλή διαπερατότητα. Η συνεργασία με συσκευές άλλων κατασκευαστών προϋποθέτει ένα στάνταρ πρωτόκολλο. Όμως, κάποιοι κατασκευαστές έχουν προϊόντα που προσφέρουν δυνατότητες που άλλα δεν προσφέρουν.

3.2 Υλοποίηση 3.2.1. Οικιακό δίκτυο

Είναι αρκετά απλό το στήσιμο ενός οικιακού δικτύου. Το πλεονέκτημα της ασύρματης δικτύωσης στο σπίτι είναι ή δυνατότητα χρήσης της σύνδεσης από οποιοδήποτε δωμάτιο του σπιτιού. Ενώ στην ενσύρματη δικτύωση η χρήση της σύνδεσης μπορεί να γίνει μόνο από το δωμάτιο στο οποίο φτάνει η παροχή της σύνδεσης.

Ως επί το πλείστον, δεν πειράζει η χρήση συσκευών από διαφορετικούς κατασκευαστές. Το στήσιμο έγκειται κυρίως στην σύνδεση του router(σημείο πρόσβασης) στην πρίζα παροχής DSL και στην πραγματοποίηση κάποιων ρυθμίσεων. Στη συνέχεια πρέπει να γίνει ρύθμιση της κάρτας δικτύου με το ίδιο SSID που έχει το router. Επίσης όπως αναλύσαμε στο κεφάλαιο για την ασφάλεια δικτύων, πρέπει να θέσουμε στις ρυθμίσεις του router έναν κωδικό WEP και τον ίδιο κωδικό να θέσουμε και στις ρυθμίσεις της κάρτας δικτύου μας ώστε να μπορεί να αποκωδικοποίηση τα πακέτα πληροφοριών που λαμβάνει από το router. Έτσι θα δυσκολέψουμε επίδοξους εισβολείς στο να χρησιμοποιήσουν την σύνδεση μας και να υποκλέψουν αρχεία.

Παρόλα αυτά ο τομέας του WEP μπορεί να έχει κάποια προβλήματα. Κάποια σημεία πρόσβασης υποστηρίζουν μόνο κλειδιά WEP 40 bit, ενώ τα νέα προϊόντα υποστηρίζουν 40 και 128 bit. Όμως οι ασυμβατότητες δε σταματούν εδώ. Ο τύπος(format) του κλειδιού μπορεί να διαφέρει από κατασκευαστή σε κατασκευαστή. Κάποιες συσκευές δέχονται χαρακτήρες ASCII. Ο κοινός παρονομαστής συνήθως είναι το κλειδί hex, οπότε πρέπει να χρησιμοποιήσουμε τον κωδικό για να παράγουμε ένα κλειδί hex και να το χρησιμοποιήσουμε παντού.

3.2.2. Μεγάλο δίκτυο επιχείρησης

Σε μια μεγάλη εταιρία υπάρχουν δύο προκλήσεις κατά το στήσιμο ενός δικτύου. Κατ' αρχάς χρειάζονται περισσότερα του ενός σημείου πρόσβασης. Αυτό σημαίνει ότι μία διερεύνηση του χώρου και των συχνοτήτων που θα χρησιμοποιηθούν είναι απαραίτητη. Δεύτερον, η ασφάλεια γίνεται πολύ πιο σημαντική γιατί στους υπολογιστές μπορεί να υπάρχουν ευαίσθητα δεδομένα της εταιρίας. Οπότε πλέον δεν αρκεί ένα απλό κλειδί WEP. Πρέπει να τεθούν σε λειτουργία άλλοι μέθοδοι ασφαλείας όπως τα VPN που αναλύσαμε στο κεφάλαιο της ασφάλειας.

3.3 Λειτουργία

Όταν ένα δίκτυο έχει στηθεί από κει και πέρα η μεγαλύτερη πρόκληση στην λειτουργία για τον διαχειριστή του δικτύου είναι οι δυναμικές παρεμβολές.

Σύμφωνα με την FCC όλοι οι χρήστες πρέπει να αποδέχονται παρεμβολές σαν μέρος της χρήσης των δημόσιων συχνοτήτων. Αλλά αυτό δε σημαίνει πως είναι κανείς υποχρεωμένος να δέχεται παρεμβολές τόσο μεγάλες που να δημιουργούν πρόβλημα σε άλλες τηλεπικοινωνιακές υπηρεσίες. Αυτό σημαίνει ότι φυσιολογικές παρεμβολές είναι αναπόφευκτες, έτσι πρέπει να υπολογίζονται εξαρχής και να αντιμετωπίζονται όταν εμφανίζονται.

Απλά το να ανεβάσουμε την ισχύ του δικτύου μας δεν είναι λύση γιατί προκαλούμε παρεμβολές. Οπότε πρέπει να βρεθούν πιο ήπιες λύσεις.

Υπάρχουν πολλές πηγές παρεμβολών στις ζώνες των 2.4 και 5 GHz. Κάποιες είναι τα ασύρματα τηλέφωνα, οι συσκευές Bluetooth, οι φούρνοπι μικροκυμάτων, ο φωτισμός με RF και άλλα WLANs. Προς το παρόν η ζώνη των 5 GHz έχει πολύ λίγες παρεμβολές, αλλά σιγά σιγά με την άνοδο των ασύρματων υπηρεσιών θα αποκτήσει κι αυτή περισσότερες.

Τα ασύρματα τηλέφωνα των 2.4 GHz δημιουργούν παρεμβολές στο 802.11b, γι' αυτό καλό είναι αν υπάρχει σε έναν χώρο 802.11b τα ασύρματα τηλέφωνα να είναι τύπου 900 MHz.

Το Bluetooth απ'την άλλη δημιουργεί παρεμβολές αλλά σε μικρή εμβέλεια λόγω της φύσης του που είναι μικρής εμβέλειας. Κατά τον σχεδιασμό ενός δικτύου δεν μπορεί να ληφθεί υπόψη γιατί η χρήση του γίνεται σε τυχαία σημεία του χώρου και σε τυχαίες στιγμές.

Οι φούρνοι μικροκυμάτων που έχουν διαρροές εκτός του ότι είναι επικύνδυνοι για την υγεία δημιουργούν και σημαντικές παρεμβολές αν βρίσκονται κοντά στο σημείο πρόσβασης. Είναι καλό λοιπόν να τοποθετούνται μακριά από αυτά. Αν για κάποιον λόγο πρέπει να είναι κοντά, τότε πρέπει να τεθεί το ως κανάλι λειτουργίας του σημείου πρόσβασης το 1 ή το 11, έτσι ώστε η συχνότητα λειτουργίας του να είναι όσο το δυνατόν πιο μακριά από την κεντρική συχνότητα των 2.45 GHz του φούρνου μικροκυμάτων.

Ο φωτισμός RF χρησιμοποιεί ένα μάγνητρο παρόμοιο με αυτό που χρησιμοποιείται στους φούρνους μικροκυμάτων. Έχει εγκριθεί από την FCC, αλλά υπάρχει περίπτωση να δημιουργήσει παρεμβολές στα Wi-Fi. Για παράδειγμα η χρήση του στην αεροπορική βάση Pope Air της Νότιας Καρολίνας στις Η.Π.Α. αποκλείει εντελώς την χρήση του 802.11b.

3.4 Συντήρηση

Μετά την εγκατάσταση ενός συστήματος Wi-Fi, χρειάζεται περιοδική συντήρηση. *Αρχεία*

ασφαλείας

Τα αρχεία ασφάλειας πρέπει να εξετάζονται για ασυνήθιστες δραστηριότητες. Η ασφάλεια ενός ασύρματου δικτύου είναι μια συνεχής διαδικασία.

Εντοπισμός "ψεύτικων" σημείων πρόσβασης

Για την εύρεσή τους μπορεί να χρησιμοποιηθεί ένα πρόγραμμα όπως τα Netstumbler και Airopeek με μία κάρτα πρόσβασης και μία κεραία Yagi. Τέτοιο λογισμικό και συσκευές μπορούν να εντοπίσουν όλα άγνωστα σημεία πρόσβασης και τις κάρτες πρόσβασης στην περιοχή. Μπορούν να βρουν στοιχεία, όπως χρήστες που χρησιμοποιούν ad hoc αντί για infrastructure, SSIDs που δεν ταιριάζουν και διευθύνσεις MAC που δεν ανήκουν στην ομάδα.

Θέματα κάλυψης

Είναι καλό να γίνεται ένας περιοδικός έλεγχος της κάλυψης. Η κεραία ενός σημείου πρόσβασης μπορεί να αποσυνδεθεί ή οι πομποδέκτες μπορεί να σταματήσουν να λειτουργούν. Οπότε κατά τον έλεγχο για ψεύτικα σημεία πρόσβασης μπορεί να γίνεται και ένας έλεγχος κάλυψης.

Αναβαθμίσεις

Οι αναβαθμίσεις είναι συχνά απαραίτητες καθώς προχωράει η τεχνολογία και αναπτύσσονται νέες μέθοδοι ασφαλείας. Αν μια νέα έκδοση λογισμικού για σημεία πρόσβασης εκδοθεί καλό είναι να γίνεται πρώτα δοκιμή της σε ένα σημείο πρόσβασης για ένα διάστημα πριν εγκατασταθεί σε όλα. Έτσι

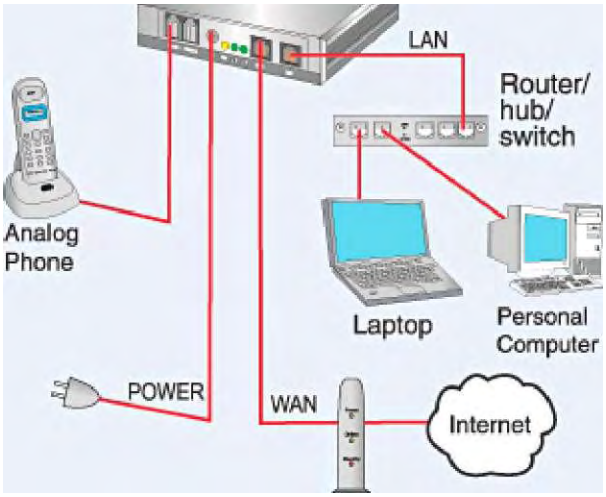
οποιοδήποτε πρόβλημα μπορεί να υπάρχει δε θα εξαπλωθεί σε όλο το δίκτυο και θα είναι εύκολη η επαναφορά στο αρχικό λογισμικό.

4. ΕΦΑΡΜΟΓΕΣ

4.1. Μετάδοση Φωνής με το 802.11

Τα ασύρματα συστήματα επικοινωνιών που είναι σταθερά σε μία θέση έχουν κατηγοριοποιηθεί ιστορικά σε δύο κατηγορίες με βάση την εφαρμογή τους. Η πρώτη εφαρμογή τους η απλή υπηρεσία τηλεφωνίας παρεχόταν από προϊόντα που λέγονται Wireless local loop (WLL). Η δεύτερη υπηρεσία, το διαδίκτυο, παρέχεται ως τώρα από ευρυζωνικά ασύρματα συστήματα. Επειδή τα WLL σχεδιάστηκαν για φωνή με χωρητικότητα κατά μεγιστο 64 Kbps δεν ήταν αρκετά για να μεταφέρουν δεδομένα με υψηλή ταχύτητα. Τα συστήματα Broadband wireless access (BWA) έχουν σχεδιαστεί για να παρέχουν υψηλής ταχύτητας πρόσβαση IP. Αλλά δεν σχεδιάστηκαν για με'τάδοση φωνής. Κανένα από αυτά τα συστήματα δεν είναι ευρέως χρησιμοποιούμενο. Μια ασύσματη ευρυζωνική τεχνολογία με δυνατότητα ποιοτικής μεταφοράς φωνής έχει την δυνατότητα να αντικαταστήσει την PSTN.

QroadVoice Router Ά. Phone fldaptsr
—t -



DSL or Cable Modem **Εικόνα 29 : τυπική συνδεσμολογία VoIP**

Η δημοτικότατα του Voice over IP μαζί με τα 802.11 LANs εγείρει τα εξής ερωτήματα: Μπορεί η φωνή να μεταφερθεί μέσω ενός δικτύου 802.11; Αν η φωνή μπορεί να ταξιδέψει μέσω ενός ενσύρματου IP δκτύου γιατί να μην μπορεί μέσω ενός ασύρματου δικτύου; Ποιοι είναι οι περιορισμοί σ'αυτήν τη μεταφορά και πως μπορούν να ξεπεραστούν;

4.1.2. VoIP

Το Voice over Internet Protocol είναι γενικός όρος για μια οικογένεια τεχνολογιών αναμετάδοσης φωνής μέσω δικτύων IP όπως είναι το Internet. Άλλοι όροι που συναντώνται και είναι συνώνυμοι με το VoIP είναι τηλεφωνία IP, τηλεφωνία Internet, Voice over Broadband και Ευρυζωνική τηλεφωνια.

4.1.2.1. Πως λειτουργεί το VoIP

Τα βασικά βήματα για την πραγματοποίηση μιας τηλεφωνικής κλήσης μέσω διαδικτύου είναι η μετατροπή του αναλογικού φωνητικού σήματος σε ψηφιακό και συμπίεση/μετάφραση του σήματος σε πακέτα IP για μετάδοση μέσω του διαδικτύου. Η διαδικασία αντιστρέφεται στον δέκτη.

Τα συστήματα VoIP χρησιμοποιούν πρωτόκολλα ελέγχου για και codecs ήχου, τα οποία κωδικοποιούν την ομιλία επιτρέποντας έτσι την αναμεταδοση της μέσω ενός δικτύου IP ως ψηφιακού ήχου. Τα codecs που χρησιμοποιούνται μπορεί να βασίζονται σε στενή ζώνη και συμπιεσμένη ομιλία, ενώ άλλα υποστηρίζουν υψηλής πιστότητας στερεοφωνικό ήχο.

4.1.2.2. Αντιρρήσεις και λύσεις

Τροφοδοσία

Τα παραδοσιακά αναλογικά τηλέφωνα συνδέονται συνήθως απευθείας στην τηλεφωνική γραμμή που παρέχει ρεύμα για την λειτουργία των περισσότερων απλών αναλογικών τηλεφωνικών συσκευών.
Τα τηλέφωνα VoIP συνδέονται σε routers ή modems που λειτουργούν με την βοήθεια πρίζας ρεύματος. Η λύση στο πρόβλημα αυτό δίνεται από κάποιες εταιρίες που προσφέρουν με τις συσκευές τους μπαταρίες με τις οποίες μπορεί να λειτουργήσει η συσκευή σε περίπτωση διακοπής ρεύματος.

Κλήσεις έκτακτης ανάγκης

Η φύση του IP κάνει δύσκολο τον γεωγραφικό εντοπισμό των χρηστών του. Οπότε οι κλήσεις έκτακτης ανάγκης δεν μπορούν εύκολα να οδηγηθούν σε κοντινό τηλεφωνικό κέντρο. Κάποιες φορές τα συστήματα VoIP μπορει να οδηγήσουν κλήσεις έκτακτης ανάγκης σε γραμμή που δεν είναι έκτακτης ανάγκης. Στις Η.Π.Α. τουλάχιστον ένα μεγάλο αστυνομικό τμήμα έχει αντιτεθεί στην χρήση αυτού του είδους τηλεφωνικών γραμμών για τον λόγο ότι θέτει τον κόσμο σε κίνδυνο.

Μια σταθερή τηλεφωνική γραμμή έχει μια άμεση σχέση μεταξύ ενός τηλεφωνικού αριθμού και μια φυσική τοποθεσία. Ο αριθμός αντιπροσωπεύει ένα ζεύγος καλωδίων που συνδέει μια τοποθεσία με το τηλεφωνικό κέντρο της εταιρίας. Όταν συνδεθεί μια γραμμή, η εταιρία αποθηκεύει τη διεύθυνση. Αν πραγματοποιηθεί μια κλήση ανάγκης είναι έτσι αμέσως γνωστή η φυσική τοποθεσία απτην οποία πραγματοποιήθηκε.

Στο IP δεν είναι όμως τόσο απλό. Ένας πάροχος μπορεί να ξέρει την τοποθεσία όπου σταματάν τα καλώδια, αλλά αυτό δεν επιτρέπει απαραίτητα τον προσδιορισμό μιας διεύθυνσης IP σε αυτήν την τοποθεσία. Οι διευθύνσεις IP συχνά αποδίδονται δυναμικά. Ο πάροχος αναγνωρίζει μεμονομένες διευθύνσεις αλλά δεν είναι απαραίτητο να ξέρει την φυσική διεύθυση στην οποία αντιστοιχεί η κάθε μία.

Υπάρχουν κι άλλα προβλήματα, λόγω του ότι το IP επιτρέπει μεγάλη φορητότητα. Για παράδειγμα, κατά την χρήση ενός κινητού με 3G ή ενός ευρυζωνικού αντάπτορα USB, η διεύθυνση IP δεν έχει καμία σχέση με κάποια φυσική τοποθεσία, αφού ένας χρήστης μπορεί να βρίσκεται οπουδήποτε στην εμβέλεια του δικτύου .
Συμπερασματικά δεν υπάρχει σχέση μεταξύ διεύθυνσης IP και φυσικής τοποθεσίας, οπότε η διεύθυνση δεν περιέχει χρήσιμες πληροφορίες για τις υπηρεσίες έκτακτης ανάγκης.

Έλλειψη αξιοπιστίας

Με τον διαχωρισμό διαδικτύου και PSTN, υπάρχει ένας βαθμός αξιοπιστίας. Μία διακοπή του διαδικτύου δεν σημαίνει διακοπή των φωνητικών επικοινωνιών ταυτόχρονα, επιτρέποντας στον κόσμο να πραγματοποιεί κλήσεις έκτακτης ανάγκης και σε εταιρίες και υπηρεσίες να συνεχίζουν να λειτουργούν. Σε περίπτωση που οι υπηρεσίες τηλεφωνίας γίνουν απόλυτα βασισμένες στο διαδίκτυο, μια διακοπή θα σήμαινε διακοπή επικοινωνιών σε ολόκληρες περιοχές.

4.1.2.3. Πλεονεκτήματα

Κόστος λειτουργίας

Το VoIP μπορεί να βοηθήσει στην ελάττωση του κόστους επικοινωνιών και αρχιτεκτονικής. Κάποια παραδείγματα για τρόπους μείωσης του κοστους είναι τα εξής :

i. Οδήγηση τηλεφωνικών κλήσεων μέσω υπαρχόντων δικτύων δεδομένων για αποφυγή χρήσης ξεχωριστών δικτύων φωνής και δεδομένων.
ii. Υπήρεσίες όπως τηλεφωνική συνδιάσκεψη, προώθηση κλήσεων και αναγνώριση ταυτότητας καλούντος που οι εταιρίες τηλεπικοινωνιών χρεώνουν επιπλέον, είναι διαθέσιμες δωρεάν στο VoIP.
iii. Η χρέωση της κλήσης γίνεται ανά megabyte και όχι ανά δευτερόλεπτο όπως στις απλές τηλεφωνικές κλήσεις. Στην πράξη η χρέωση είναι πολύ μικρότερη για τα δεδομένα που μεταφέρονται στον χρόνο που θα διαρκούσε μία αντίστοιχη αναλογική τηλεφωνική σύνδεση.

Πολυχρηστικότητα

Το VoIP μπορεί να επιτελέσει λειτουργίες και να προσφέρει υπηρεσίες που είναι πολύ δυσκολότερο να πραγματοποιηθούν μέσω PSTN.

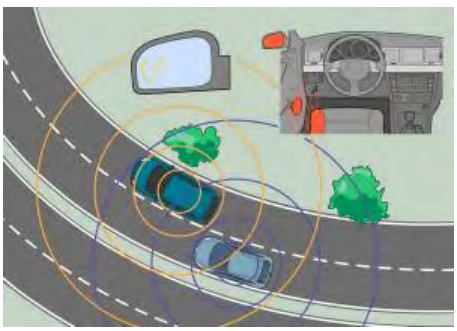
i. Η δυνατότητα μετάδοσης περισσότερων της μιας κλήσης μέσω μιας ευρυζωνικής σύνδεσης χωρίς ανάγκη για περισσότερες γραμμές.
ii. Ασφαλείς κλήσεις με χρήσης τυποποιημένων πρωτοκολλων. Οι περισσότερες δυσκολίες για δημιουργία ασφαλούς σύνδεσης μέσω απλής τηλεφωνικής γραμμής, όπως η ψηφιοποίηση, δεν υπάρχουν στο VoIP. Το μόνο που χρειάζεται είναι η κρυπτογράφηση και πιστοποίηση της υπάρχουσας ροής δεδομένων.
iii. Το μόνο που χρειάζεται για τη σύνδεση με τον παροχέα VoIP είναι μία αρκετά γρήγορη και σταθερή σύνδεση στο διαδίκτυο.

4.2. Vehicular ad hoc δίκτυα

Στα πλαίσια της ραγδαίας τεχνολογικής ανάπτυξης υπάρχει ιδιαίτερο ενδιαφέρον και πρόοδο στον τομέα των Δικτύων μεταξύ οχημάτων, γνωστά ως VANETs : Vehicular Ad Hoc Networks . Η ‘έκτη αίσθηση’ του αυτοκινήτου που προειδοποιεί τον οδηγό για κρίσιμες καταστάσεις. Τα οχήματα ‘μιλάνε μεταξύ τους’ μέσω δοκιμασμένης τεχνολογίας επικοινωνιών. Τα VANETs περιλαμβάνουν επικοινωνίες από όχημα σε όχημα και από όχημα σε καθ 'οδόν υποδομή που βασίζονται στις τεχνολογίες ασυρμάτου τοπικού δικτυού. Αυτό που καθιστά τα VANETs μια μοναδική τεχνολογία στο τομέα των ασύρματων επικοινωνιών είναι το σύνολο των θεμάτων που υποστηρίζουν.

Αυτά περιλαμβάνουν:

• Την παροχή μηνυμάτων για προειδοποίηση σύγκρουσης και την παροχή τοπικών πληροφοριών για την κυκλοφορία των οδηγών και των οχημάτων ,
• τους πόρους –άδεια φάσματος, επαναφορτιζόμενη πηγή ισχύος , καθώς και τη προστασία της ιδιωτικής ζωής.



Προειδοποίηση Αλλαγής Λωρίδας
(Lane Departure Warning LDW)

6.ΑΝΑΦΟΡΕΣ

6.1.Βιβλιογραφία

[1] Frank Ohrtman and Konrad Roeder , "Wi-Fi Handbook: Building 802.11b Wireless Networks", McGraw-Hill, April 2003

[2] John Ross, "The Book of Wi-Fi: Install, Configure, and Use 802.11b Wireless Networking", No Starch Pr, 2003

[3] Savo Glisic and Beatriz Lorenzo, "Advanced Wireless Networks", Wiley, July 13 2009

[4] Bernard H. Walke, Stefan Mangold, Lars Berlemann, "IEEE 802 Wireless Systems", John Wiley & Sons, 11 Jan 2007

6.2.Δικτυακές Πηγές

[1] http://wikipedia.com
[2] http://www.intel.com/standards /case/case 802 11 .htm
[3] http://openarchives.gr/view/460609