WiFi - 802.11b

Μια μελέτη του κραταιού πρωτοκόλλου ασύρματης δικτύωσης

Περιεχόμενα

1) Η Ασύρματη Πραγματικότητα

Κάνοντας μια έρευνα αγοράς στην αγορά πληροφορικής, κάποιος θα παρατηρούσε την μεγάλη αφθονία σε προϊόντα που υλοποιούν πρωτόκολλα, τα οποία υπόσχονται ασύρματες, εύκολες και κυρίως γρήγορες λύσεις για τις δικτυακές μας ανάγκες. Την τελευταία δεκαετία πολλά είναι τα πρότυπα που διεκδικούν ένα κομμάτι της αγοράς. Bluetooth, HiperLAN, HomeRF, 802.11a, 802.11b, 802.11g είναι κάποια από τα πολυδιαφημιζόμενα ονόματα προτύπων, αλλά και να μην ξεχνάμε το PACKET radio που έρχεται αρκετά χρόνια πριν. Στις παρακάτω παραγράφους θα περιγράψουμε το πιο διαδεδομένο μέλος της οικογένειας 802.11, το πρότυπο b. Αναλύοντας τα χαρακτηριστικά του, θα γίνει φανερό γιατί το wifi είναι από τα ελάχιστα success stories μιας αγοράς τηλεπικοινωνιών που χαρακτηρίζεται από γενική ύφεση.

2 - Το 802.11b

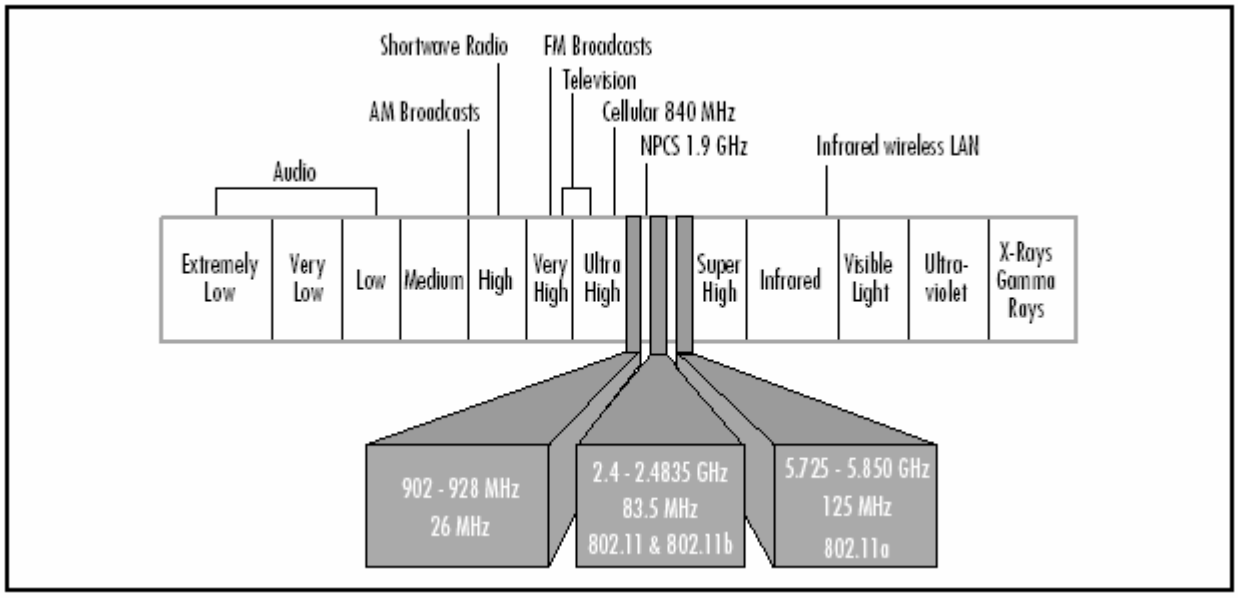
2.1 Κύρια χαρακτηριστικά του πρωτοκόλλου

Το 802.11b είναι το πρώτο wireless πρωτόκολλο που κατάφερε να μπει τόσο δυναμικά στον χώρο της δικτύωσης, έναν χώρο που γνωρίζει ελάχιστες επαναστάσεις και αλλαγές.

Το πρωτόκολλο 802.11, του οποίου το b αποτελεί επέκταση, και είναι ένας ορισμός του Media Access Control (MAC) Layer καθώς και τριών διαφορετικών και ασύμβατων Physical Layers στο υπάρχον δικτυακό μοντέλο OSI. Το πρωτόκολλο εγκρίθηκε από την ομάδα 802 της IEEE στις 26 Ιουνίου του 1997 και θέτει το πλαίσιο για μια προτυποποιημένη ασύρματη δικτυακή επικοινωνία ευρείας ζώνης. Στις παρακάτω σελίδες δίνουμε μια περιγραφή του 802.11 πρωτοκόλλου, και επεκτείνουμε την έρευνά μας στις επεκτάσεις και τροποποιήσεις που προσέθεσε το 802.11b.

2.2 Φάσμα εκπομπής

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



Εικόνα 1 - Οι ελεύθερες συχνότητες

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

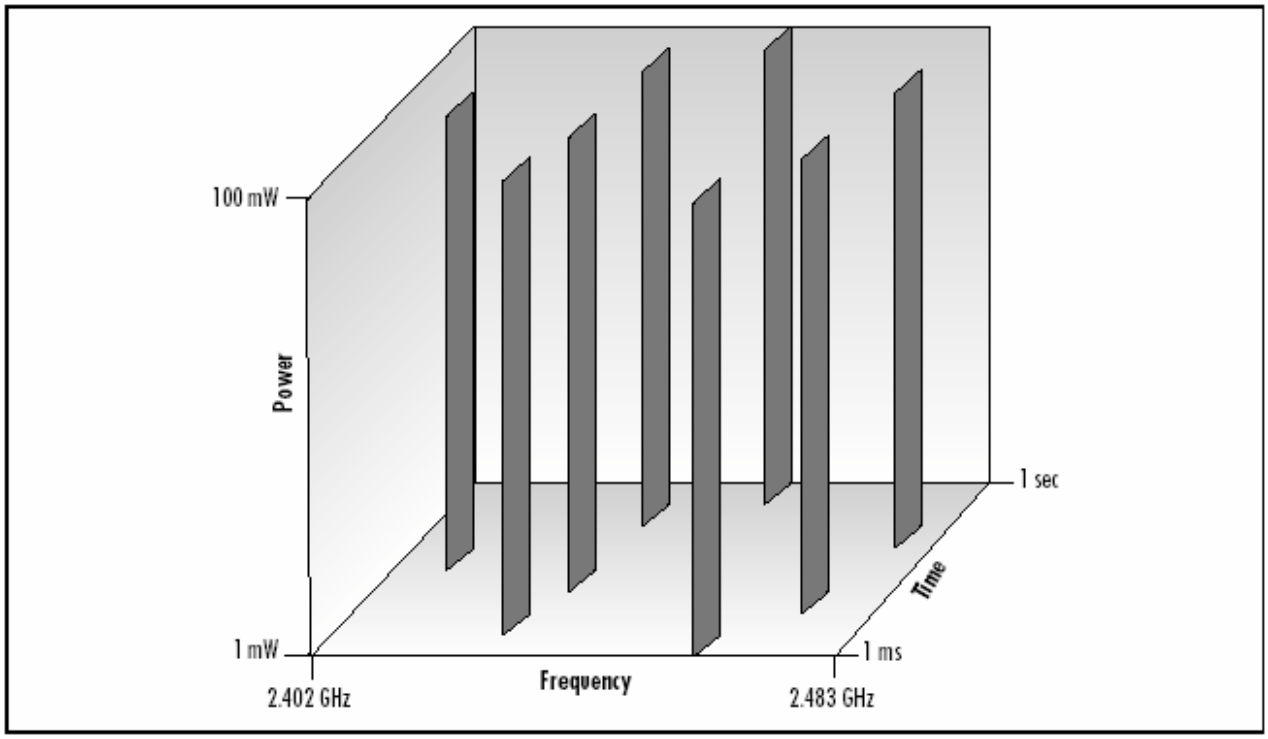
Δυστυχώς, το νομικό πλαίσιο που διέπει τις λεπτομέρειες χρήσης αυτής της μπάντας, εξαρτάται σε μεγάλο βαθμό από την νομοθεσία κάθε χώρας. Μεγάλα είναι τα νομικά κενά σε πολλές χώρες, όπως και στην Ελλάδα, που αφήνουν πολλά ερωτηματικά ως προς την μέγιστη νόμιμη εκπεμπόμενη ισχύ, την εμπορική ή όχι χρήση του ραδιοφωνικού φάσματος αυτού και πολλά άλλα.

Η ισχύς που ορίζει το στάνταρτ στις εξόδους κεραίας των εμπορικών συσκευών είναι τα 0.2mw, το οποίο με τις μικρές εργοστασιακές κεραίες που συνοδεύουν τις συσκευές WiFi, δίνει στο 802.11b εμβέλεια της τάξεως των 300μ σε ανοιχτό χώρο. Λόγω της φύσης των μικροκυματικών συχνοτήτων, η εμβέλεια συσκευών WiFi μειώνεται αισθητά όταν μεταξύ τους παρεμβάλλονται τσιμέντινοι τοίχοι, δέντρα(και γενικώς αντικείμενα που περιέχουν νερό) ή μεταλλικές πόρτες. Μείωση της ποιότητας σύνδεσης, σημαίνει αρχικά μειωμένο throughput του δικτύου με υψηλά error rates, και στην χειρότερη περίπτωση αδυναμία σύνδεσης των συσκευών. Για τον ίδιο λόγο, μακρινές συνδέσεις (>300μ) επιτυγχάνονται μόνο σε καταστάσεις όπου η μία συσκευή έχει οπτική επαφή με την άλλη (Line of Site), ένας κανόνας που ευτυχώς δεν είναι τόσο αυστηρός(καταστάσεις near-LOS). Αντανακλάσεις του σήματος μπορεί να επιτρέψουν σύνδεση χωρίς LOS. Βεβαίως, όπως είναι

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

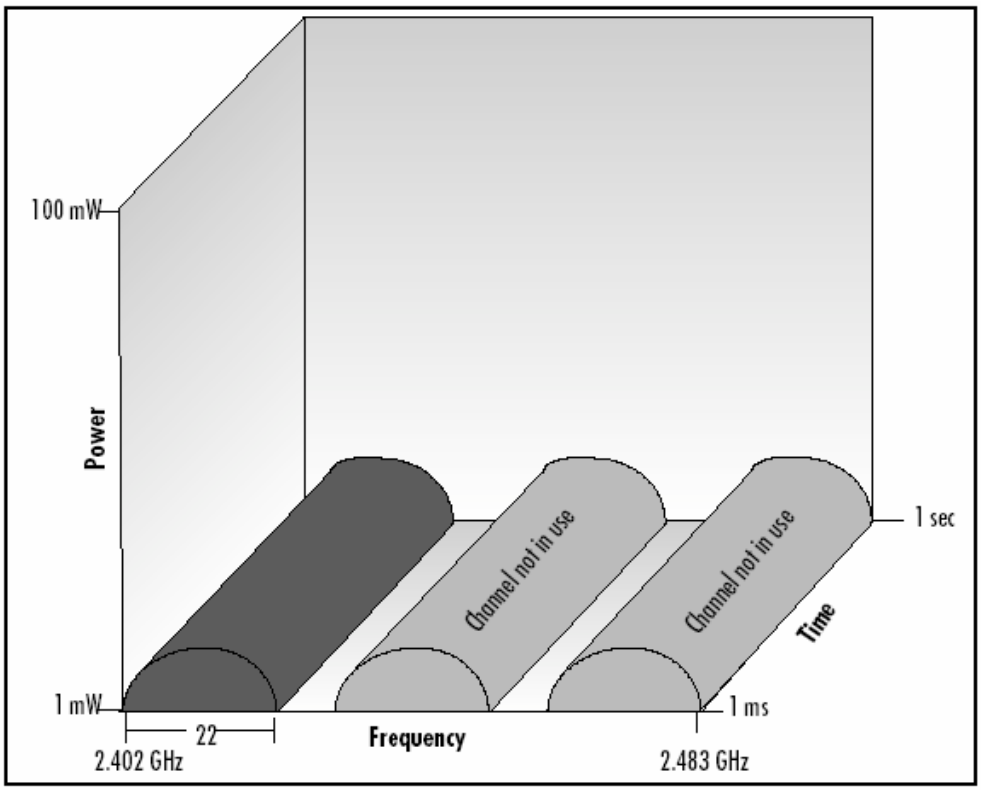
2.3 Διαμόρφωση

Στο αρχικό πρωτόκολλο 802.11, καθορίζονται δύο τρόποι κωδικοποίησης, ο FHSS (Frequency Hopping Spread Spectrum) και ο DSSS (Direct Sequence Spread Spectrum). Στον FHSS, η εκπομπή-λήψη μοιράζεται σε 75 κανάλια του ενός MHz και εναλλάσσεται συνεχώς σε ένα από αυτά. Χρησιμοποιώντας αυτή την τεχνική, ο εκπομπός στέλνει τα δεδομένα διαδοχικά σε μια ακολουθία από φαινομενικά τυχαίες συχνότητες(frequency hopping). Ο δέκτης ακολουθεί την ίδια ακολουθία εναλλαγής καναλιών συχνότητας με τον εκπομπό και λαμβάνει το μήνυμα. Το μήνυμα μπορεί να ληφθεί ακέραιο, μόνο όταν είναι γνωστή η ακολουθία της εναλλαγής συχνοτήτων. Καθώς μόνον ο δέκτης γνωρίζει την σωστή ακολουθία, το μήνυμα είναι αναγνώσιμο μόνο από τον πραγματικό του παραλήπτη. Με αυτή την τεχνική, ηλεκτρομαγνητικές παρεμβολές στον χώρο της λήψης θα επηρεάσουν μόνο ένα τμήμα του μηνύματος, έχοντας ως αποτέλεσμα την ανάγκη για επανεκπομπή μόνο μικρού όγκου μηνυμάτων. Ο συγκεκριμένος τρόπος κωδικοποίησης μπορεί να δώσει ταχύτητες μεταφοράς δεδομένων έως και 2mbit. Ακολουθεί γράφημα που δείχνει την τεχνική FHSS συναρτήσει της ισχύος και του χρόνου.



Εικόνα 2 – FSSS συναρτήσει ισχύος και χρόνου

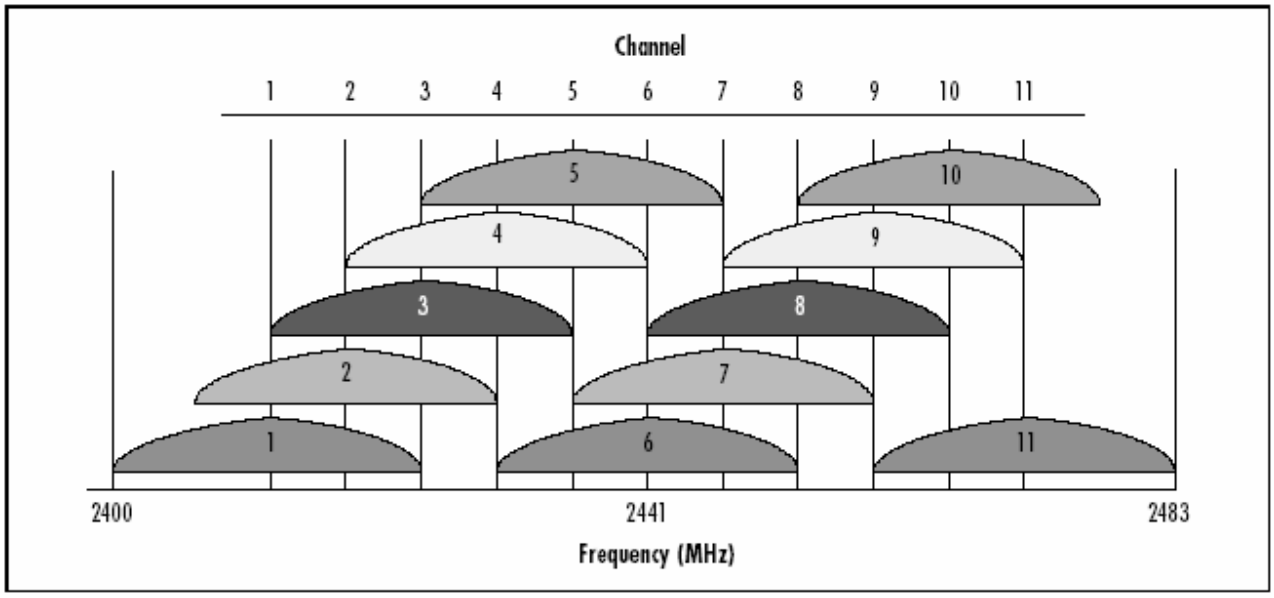
Στον DSSS το φάσμα χωρίζεται σε 14 μερικώς (ανά ~4) επικαλυπτόμενα κανάλια πλάτους 22MHz, και χρησιμοποιείται ένα κάθε φορά για επικοινωνία.



Εικόνα 3 – DSSS συναρτήσει ισχύος και χρόνου

Ένας εκπομπός direct sequence επικοινωνεί προσθέτοντας bits εφεδρείας που καλούνται chips, στα δεδομένα. Σε κάθε bit πληροφορίας προστίθενται τουλάχιστον

10 chips. Κατόπιν τα τμήματα των δεδομένων στέλνονται σε όσες περισσότερες συχνότητες είναι δυνατόν, εντός του καναλιού λειτουργίας, ταυτόχρονα. Η μέγιστη ταχύτητα φτάνει σε αυτόν τον τρόπο τα 11mbit. Στο ακόλουθο σχήμα βλέπουμε την κατανομή των καναλιών στο φάσμα των 2.4GHz, καθώς και τον τρόπο με τον οποίο επικαλύπτονται.



Εικόνα 4 – BSSS κανάλια

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

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

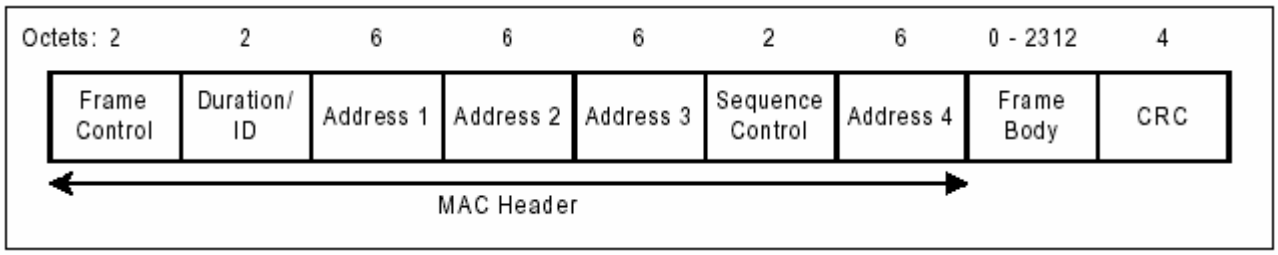
Εικόνα 4 –Κανάλια σε μερικες χώρες

Τελικά με την έλευση του 802.11b το Σεπτέμβρη του 1999, η επιτροπή αποφάσισε να αφήσει στο πρότυπο μόνο την κωδικοποίηση DSSS, παρόλο που το

FHSS αρχικά φαίνονταν σαν ευκολότερο αλλά και φθηνότερο στην υλοποίηση του. Με αυτό τον τρόπο το 802.11b απέκτησε ένα από τα μεγαλύτερά του πλεονεκτήματα, την υψηλή διαμεταγωγή δεδομένων.

2.4 Εύρος Ζώνης

Η ταχύτητα σύνδεσης που ορίζει το IEEE802.11b είναι τα 11mbps, και όπως εξηγήσαμε επιβάλλεται από την κωδικοποίηση BSSS που χρησιμοποιεί. Μιας και από την φύση τους οι ασύρματες συνδέσεις είναι επιρρεπής σε σφάλματα μετάδοσης, το overhead μετάδοσης πακέτων ελέγχου και διόρθωσης λαθών(βλ. εικόνα 1), μεταφράζεται σε πραγματική ταχύτητα μεταφοράς δεδομένων πολύ χαμηλότερη της ονομαστικής. Επίσης, λόγω του γεγονότος ότι όλες οι συσκευές WiFi έχουν ένα και μόνο ραδιοφωνικό πομποδέκτη, η λειτουργία τους σαν δικτυακές συσκευές είναι σε half-duplex mode, καθώς ο πομποδέκτης μπορεί να ακούει το δίκτυο ή να στέλνει σε αυτό, αλλά όχι και τα δύο ταυτόχρονα. Έτσι το πραγματικό όριο για το bandwidth μιας 802.11b σύνδεσης είναι διαμορφώνεται στα 5mbps. Πολλές εταιρίες υπόσχονται ονομαστικές διπλάσιες ή και περισσότερο ταχύτητες. Τέτοια χαρακτηριστικά είναι εκτός του στάνταρ, και λειτουργούν **μόνο** μεταξύ των προϊόντων της ίδιας εταιρίας. Από την στιγμή που επιτευχθεί σύνδεση με μια άλλη συσκευή WiFi, τότε ισχύουν όλοι οι κανόνες ενός κοινού Ethernet δικτύου.



Εικόνα 5 – Μορφή του 802.11 MAC πακέτου

2.5 Μέθοδος πρόσβασης στο μέσο (Access Method)

Η μέθοδος που υποστηρίζεται από το 802.11 πρωτόκολλο για την πρόσβαση στο φυσικό μέσο, είναι το PCF (Point Coordination Function) και DCF (Distributed Coordination Function) με Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) σε αναλογία με το Ethernet που υλοποιεί το CSMA/CD(Collision Detection). Το CSMA στο Ethernet λειτουργεί ως ακολούθως: όταν κάποιος επιθυμεί να στείλει δεδομένα, ελέγχει αν το κανάλι είναι κατειλημμένο από μια άλλη μεταφορά δεδομένων. Αν είναι, τότε περιμένει ένα τυχαίο χρονικό περιθώριο(μικρό) σύμφωνα με τον αλγόριθμο exponential random backoff. Ο τρόπος πρόσβασης αυτός δεν μπορεί να είναι αποδοτικός στο 802.11 για δύο λόγους:

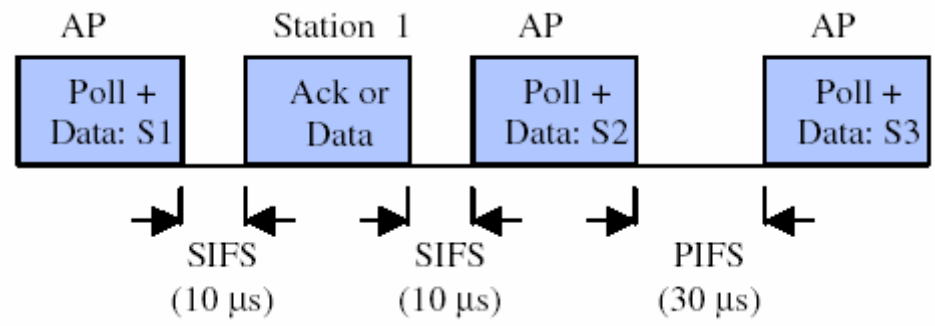
1. Η υλοποίηση αυτής της μεθόδου θα απαιτούσε ραδιοφωνικούς εκπομπούς που θα είχαν την δυνατότητα Full – Duplex επικοινωνίας (αποστολή και λήψη ταυτόχρονα), κάτι το οποίο θα αύξανε το κόστος.

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

Ας δούμε όμως πιο αναλυτικά από τι απαρτίζεται ο μηχανισμός. Το 802.11 ορίζει πέντε διαφορετικά χρονικά διαστήματα για συγχρονισμό στο MAC επίπεδο, το short interframe space (SIPS), το slot time, το priority interframe space (PIFS), το distributed interframe space (DIFS), και το extended interframe space (EIFS).Τα δύο από αυτά θεωρούνται βασικά και καθορίζονται από το MAC: το χρονικό διάστημα SIPS(short interframe space) και το slot time. Τα υπόλοιπα διαστήματα καθορίζονται βάσει των παραπάνω διαστημάτων. Το SIPS είναι το μικρότερο όλων των χρονικών αυτών διαστημάτων, ακολουθούμενο από το slot time, το οποίο μπορεί να ερμηνευθεί σαν η μονάδα χρόνου για το MAC του 802.11, παρόλο που το πρωτόκολλο δεν βασίζεται σε αρχιτεκτονική με χρονικές «θυρίδες» (time slots). Ειδικά στο 802.11b, οι χρόνοι SIFS και slot είναι 20μs, χρόνος που επιλέχθηκε έτσι ώστε να δώσει ένα λογικό σε διάρκεια διάστημα για τις καθυστερήσεις διάδοσης και επεξεργασίας από τις συσκευές. Ο χρόνος PIFS ισούται με τον χρόνο SIFS επαυξημένο κατά ένα slot και ο DIFS κατά δύο slots. Ο χρόνος EIFS είναι

μεγαλύτερος και από τους τέσσερις προηγούμενους, και χρησιμοποιείται για την επανεκπομπή πακέτων που ελήφθησαν λανθασμένα.

Το 802.11 υποστηρίζει δύο τρόπους λειτουργείας: τον PCF και τον DCF. Με την πρώτη μέθοδο λειτουργίας, το κεντρικό AP της κυψέλης(θα μιλήσουμε παρακάτω για αυτό) στέλνει μηνύματα στους σταθμούς πελάτες, κάνοντας Polling σε κάθε ένα από αυτούς, ρωτώντας στην ουσία για το αν έχει δεδομένα για αποστολή ή όχι. Αν ο σταθμός απαντήσει, μπορεί να στείλει την θετική του απάντηση (ACK) στο ίδιο πακέτο με τα δεδομένα προς αποστολή. Αν δεν απαντήσει εντός του χρονικού ορίου SIFS, τότε το Access Point προχωρά στον επόμενο σταθμό.

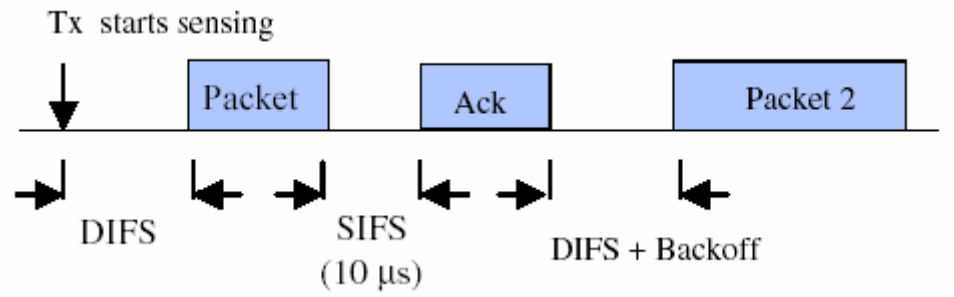


Εικόνα 6 – Μέθοδος PCF στο 802.11b MAC

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

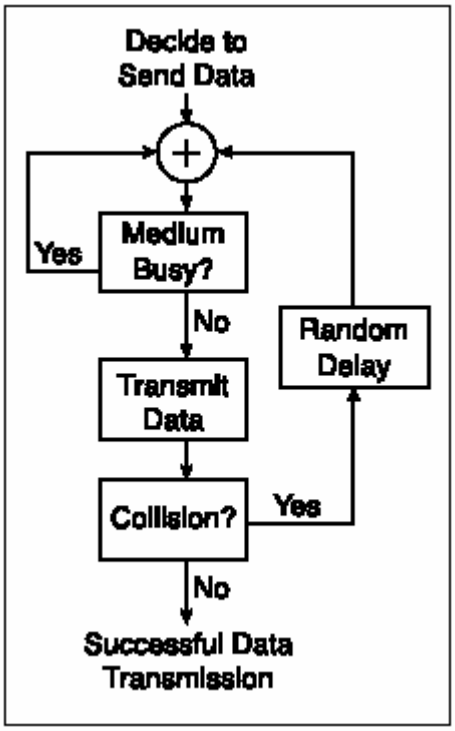
Στην μέθοδο λειτουργίας DCF, το 802.11 χρησιμοποιεί έναν μηχανισμό Αποφυγής Συγκρούσεων μαζί με αναγνώριση βεβαίωσης λήψης των πακέτων που στέλνονται. Αν ο εκπομπός, κατά την έναρξη διαδικασία αποστολής, δει ότι το μέσο είναι ελεύθερο(κανείς δεν χρησιμοποιεί το κανάλι) για χρόνο ίσο με DIFS, τότε αρχίζει

την εκπομπή. Σε αντίθετη περίπτωση, συνεχίζει να ελέγχει το κανάλι για να δει αν βρίσκεται σε κατάσταση busy ή idle. Εφόσον βρει το κανάλι ελεύθερο για χρόνο DIFS, τότε ξεκινά να μετράει τον χρόνο χρήσης του καναλίου σε μονάδες slot time, παράγει τυχαία χρονικά διαστήματα αναμονής σε μονάδες slot time, σύμφωνα με κατάλληλο αλγόριθμο, και συνεχίζει τον έλεγχο της κατάστασης του καναλιού. Κατά το τελευταίο βήμα, για κάθε time slot που ο εκπομπός βρίσκει ελεύθερο το κανάλι, ο τυχαίος χρόνος αναμονής μειώνεται κατά ένα time slot. Όταν ο χρόνος αυτός μηδενιστεί, τότε και μόνο ο εκπομπός μπορεί να εκκινήσει την διαδικασία μετάδοσης. Με αυτή τη μέθοδο αποφεύγονται οι συγκρούσεις πακέτων διαφορετικών εκπομπών, αλλά και αποκλείεται η μονοπώληση του καναλιού από έναν και μόνο σταθμό που θα ίσως να προσπαθούσε συνεχείς εκπομπές.



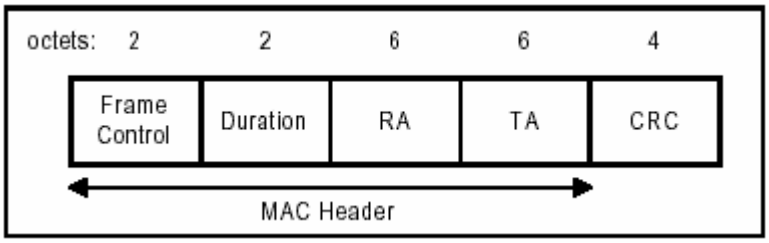
Εικόνα 7 – Μέθοδος DCF στο 802.11b MAC

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

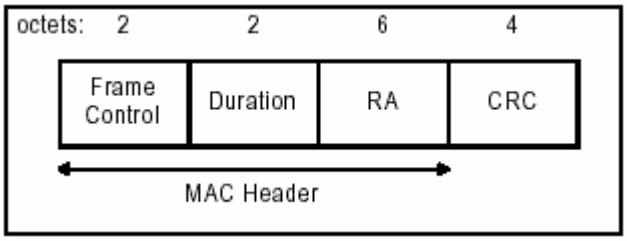


Εικόνα 8 – απλουστευμένος αλγόριθμος εκπομπής

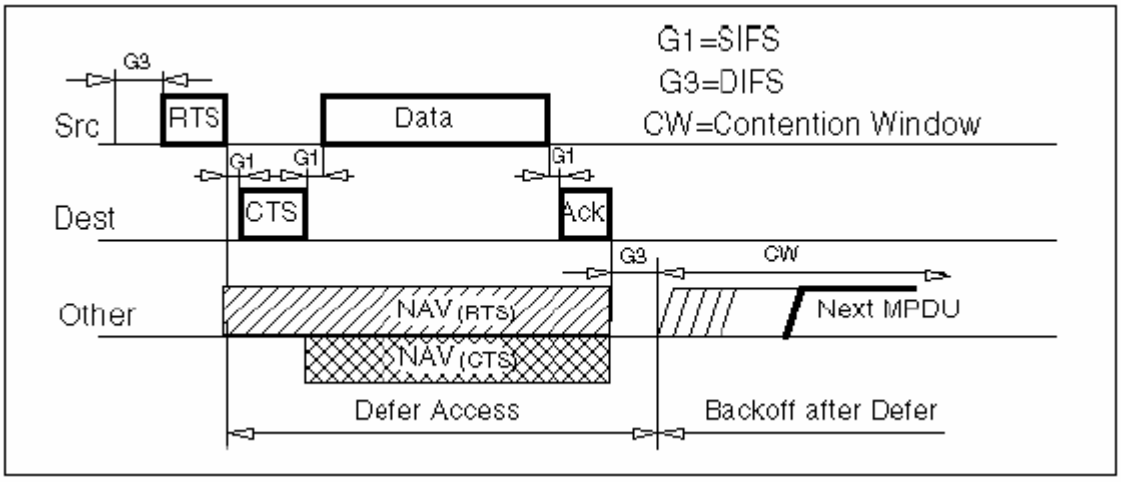
Η επιτροπή IEEE εισήγαγε έναν μηχανισμό Virtual Carrier Sense στο 802.11 για να αμβλύνει το φαινόμενο κατά το δύο σταθμοί δεν μπορούν να ακούσουν ο ένας τον άλλον και προκαλούνται συγκρούσεις. Ο μηχανισμός λέγεται CTS/RTS(clear to send/request to send). Όταν ενεργοποιείται, κάθε client πριν ξεκινήσει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



Εικόνα 9 - Το πλαίσιο RTS



Εικόνα 10 – Το πλαίσιο CTS

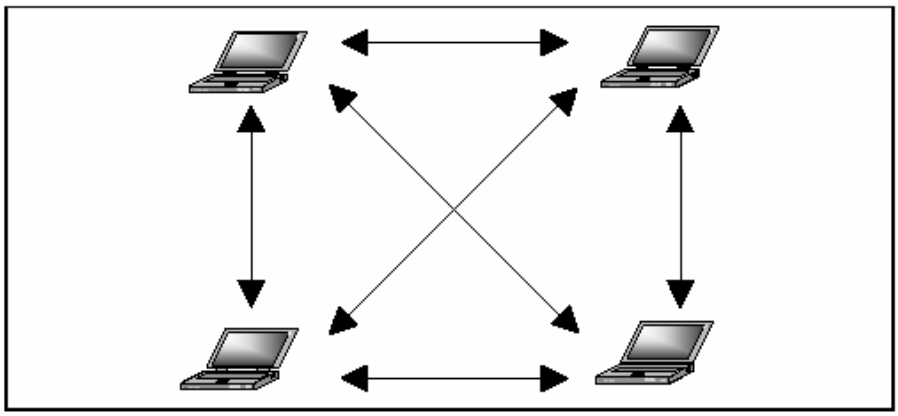


Εικόνα 11 – Η διαδικασία αποστολής των RTS-CTS

2.6 Τοπολογία ενός Wireless δικτύου

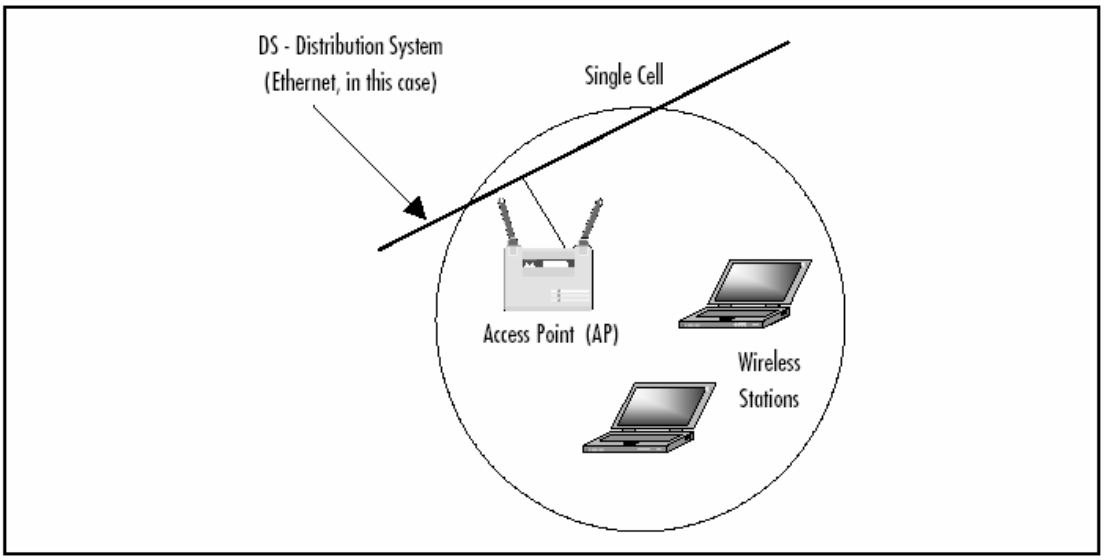
Το πρότυπο του wifi ορίζει τρεις τρόπους επικοινωνίας μεταξύ κόμβων ενός δικτύου, τον IBSS (Independent Basic Service Set) ή ad hoc ,τον BSS (Basic Service Set) ή infrastructure και τον ESS(Extended Service Set).

Με τον πρώτο τρόπο, 2 η περισσότερες συσκευές επικοινωνούν άμεσα η μία με την άλλη. Κάθε κόμβος θεωρείται ομότιμος(peer) και έτσι το δίκτυο απαρτίζεται από μονοπάτια. Συνήθως αυτός ο τρόπος χρησιμοποιείται για μικρά δίκτυα. Έχει παρόλαυτα μεγάλο ερευνητικό ενδιαφέρον, καθώς ένα ad hoc δίκτυο μπορεί να περιέχει πολλά μονοπάτια για επικοινωνία μεταξύ δύο κόμβων, και έτσι παρέχει μεγάλη αξιοπιστία λόγω εφεδρείας μονοπατιών, αλλά και αυξημένη ταχύτητα.



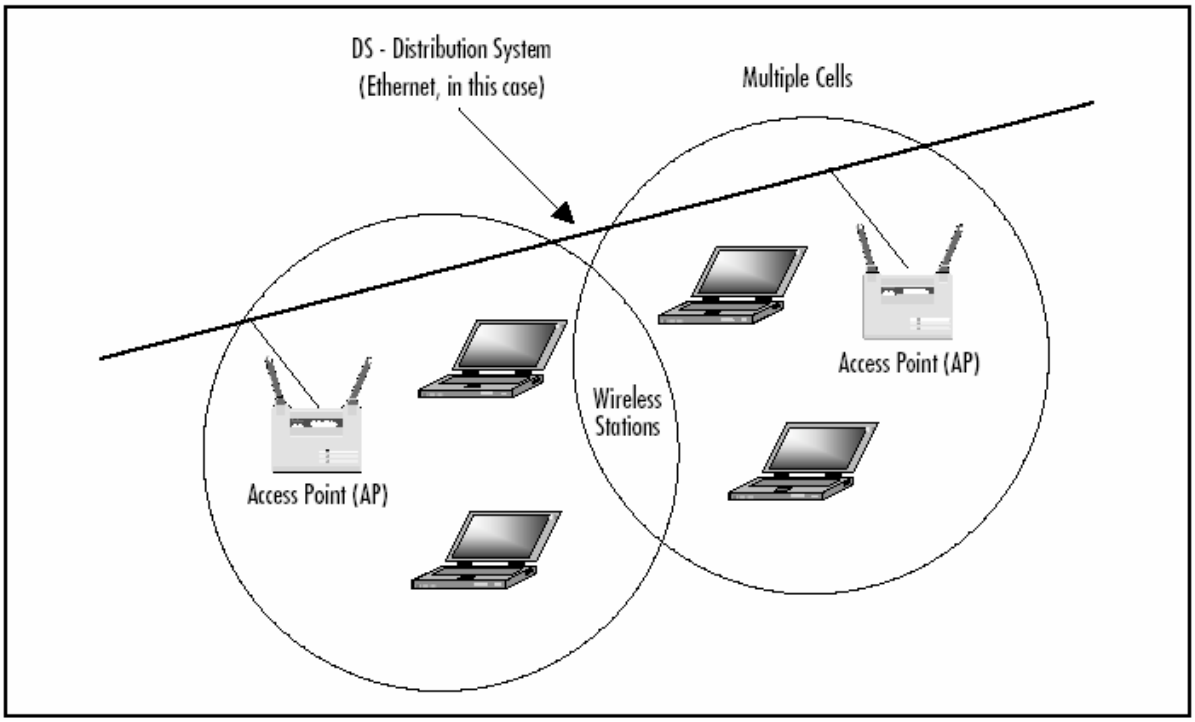
Εικόνα 12 - IBSS

Στην δεύτερη τοπολογία, το 802.11 δίκτυο αποτελεί ένα κυψελωτό δίκτυο, παρόμοιο των δικτύων κινητής τηλεφωνίας. Η κυψέλη στην ορολογία του 802.11 ονομάζεται Basic Service Set (BSS). Όλα μέλη του επικοινωνούν μεταξύ τους μέσω ενός κεντρικού διανομέα που ονομάζεται Base Station ή κοινώς Access Point, κατά το μοντέλο client – server. Σε αυτή την περίπτωση δεν χρειάζεται η άμεση οπτική επαφή ανάμεσα σε όλους τους κόμβους. Αρκεί όλοι να μπορούν να επικοινωνήσουν με το Access Point. Κάθε Access Point, έχει ένα όνομα που το αναγνωρίζει ανάμεσα σε άλλα που ίσως να βρίσκονται στον ίδιο χώρο, το SSID. Το SSID είναι πολλές φορές και αυτό που πρέπει να ξέρουμε, για να συνδεθούμε σε κάποιο ελεύθερο Access Point. Επίσης, κάθε Access Point εκπέμπει σε ένα από τα 14 κανάλια(λιγότερα ίσως σε κάποιες χώρες) εκπομπής που ορίζει το πρωτόκολλο. Για την μείωση των παρεμβολών μεταξύ των APs, είναι προτιμότερο να επιλέγονται κανάλια λειτουργίας που διαφέρουν κατά 4(ας πούμε τα 1-5-9-13 για τέσσερα APs στον ίδιο χώρο) έτσι ώστε να μην επικαλύπτονται οι εκπομπές τους. Ένα Access Point χρησιμοποιεί πολυκατευθυντική κεραία(Omnidirectional), καθώς πρόκειται για κεραίες που εκπέμπουν κυκλικά το σήμα τους, πράγμα που είναι και το ζητούμενο όταν θέλουμε να έχουμε την μέγιστη κάλυψη του περιβάλλοντος χώρου. Εν αντιθέσει, οι σταθμοί μπορούν να χρησιμοποιούν κατευθυντικές κεραίες για να επιτύχουν συνδέσεις με μακρινά(>300m) APs, κάτι βέβαια που εισάγει νέα προβλήματα στο δίκτυο(βλ. Κεφάλαιο hidden node). Για λειτουργία εντός της αποστάσεως των 300μ, είναι καλό να χρησιμοποιούνται πολυκατευθυντικές κεραίες πολύ μικρού κέρδους (<5dBi), καθώς επαρκούν για την επίτευξη σύνδεσης.



Εικόνα 13 – BSS

Ένα ασύρματο δίκτυο μπορεί να έχει την μορφή μίας και μόνο κυψέλης, όμως πολλές κυψέλες μπορούν να γεφυρωθούν μέσω ενός Συστήματος Διανομής (Distribution System). Το σύστημα διανομής μπορεί να είναι μια ενσύρματη εγκατάσταση, ή δεσμευμένοι ασύρματοι clients που αναλαμβάνουν την γεφύρωση των δύο υπό-δικτύων. Όλο το διασυνδεδεμένο δίκτυο, συμπεριλαμβανομένου του συστήματος διανομής και των Access Points, είναι ορατό στα ανώτερα επίπεδα του OSI μοντέλου σαν ένα μοναδικό 802 δίκτυο, το οποίο στο στάνταρτ περιγράφεται σαν Extended Service Set.



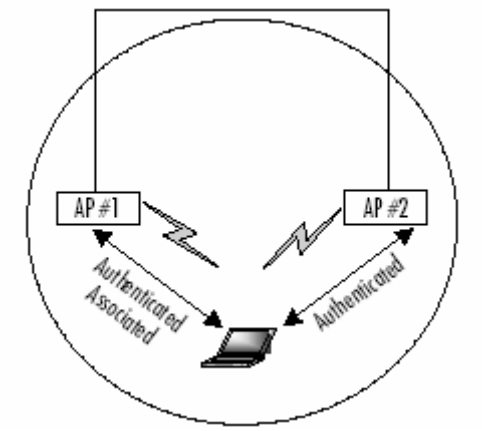
Εικόνα 14 – Τοπολογία Infrastructure

Ας μιλήσουμε όμως λίγο περισσότερο για τις υπηρεσίες που προσφέρει το ESS, καθώς δίνει στα δίκτυα 802.11 ένα τεράστιο πλεονέκτημα: το roaming χρηστών ανά τα διαθέσιμα Access Points. Ένας σταθμός ενός BSS, μπορεί να κινείται ελεύθερα αλλάζοντας BSSs(δηλαδή Access Points) χωρίς ούτε αυτός, ούτε και το δίκτυο να βλέπουν κάποια αλλαγή, ή να χρειάζονται νέες ρυθμίσεις. Κάθε BSS επικοινωνεί με τα υπόλοιπα BSSs για την διαμεταγωγή των πακέτων, αλλά και για την εναλλαγή των σταθμών, καθώς αυτοί αλλάζουν BSS, μέσω του Συστήματος Διανομής που περιγράψαμε ποιο πάνω. Την ευθύνη για αυτές τις λειτουργίες έχουν εννέα υπηρεσίες που προσφέρει το σχήμα ESS. Τέσσερις από αυτές ανήκουν στην ομάδα των υπηρεσιών σταθμού (station services) και οι υπόλοιπες ανήκουν στην ομάδα υπηρεσιών διανομής(distribution services).

Οι υπηρεσίες σταθμού απαρτίζονται από τις authentication, de-authentication, data delivery, και privacy, και παρέχουν στο ασύρματο δίκτυο λειτουργικότητα παρόμοια με αυτή ενός στάνταρ ενσύρματου δικτύου 802.3. Η πρώτη υπηρεσία παρέχει ένα είδος ταυτότητας σε κάθε σταθμό. Χωρίς αυτήν, ο σταθμός δεν έχει το δικαίωμα να συνδεθεί στο WLAN. Ένας σταθμός έχει την δυνατότητα να πιστοποιήσει την ύπαρξή του σε περισσότερα από ένα Access Points. Αυτού του είδους η προ-πιστοποίηση, παρέχει την δυνατότητα στα κοντινά του συγκεκριμένου σταθμού BSSs, να είναι έτοιμα για να δεχθούν το σταθμό αυτό καθώς αυτός θα κινηθεί στον χώρο του. Η υπηρεσία του de-authentication χρησιμοποιείται για να καταστραφεί η ταυτότητα ενός σταθμού που για οποιοδήποτε λόγο δεν μπορεί πλέον να υπάρχει στο τοπικό ασύρματο δίκτυο. Όταν η διαδικασία αυτή ξεκινήσει, ο σταθμός δεν μπορεί πλέον να έχει πρόσβαση στο δίκτυο, μέχρι να ξαναπεράσει από την φάση authentication. Με αυτό τον τρόπο ελευθερώνονται πόροι στο Access Point για άλλες συσκευές. Η υπηρεσία privacy χρησιμοποιεί έναν RC4 αλγόριθμο για να παρέχει κρυπτογράφηση στα δεδομένα που εκπέμπονται. Περισσότερα για αυτήν την υπηρεσία στο αντίστοιχο κεφάλαιο. Το data delivery στο επίπεδο του MAC, περιγράφεται πιο κάτω.

Πέντε διαδικασίες διανομής αναλαμβάνουν την αποστολή των δεδομένων καθώς ένας ασύρματος σταθμός κινείται μεταξύ πολλαπλών BSSs : association, reassociation, disassociation, integration, και distribution. Ένας σταθμός χρησιμοποιεί την διαδικασία association μόλις συνδεθεί στο AP. Αυτή η λειτουργία

δημιουργεί τα λογικά μονοπάτια για μεταξύ των συσκευών, και αποφασίζει για τον τρόπο με τον οποίο θα επικοινωνήσει το Σύστημα Διανομής με τον σταθμό. Αν δεν συμβεί αυτή η διαδικασία, τότε το ΣΔ δεν θα ξέρει που να στείλει τα πλαίσια δεδομένων. Όπως βλέπουμε στο σχήμα, ένας σταθμός μπορεί να είναι authenticated σε περισσότερα από ένα Access Point αλλά associated μόνο με ένα.



Εικόνα 13 – Authentication/Association

Η λειτουργία disassociation χρησιμοποιείται για να σταματήσει την «συνεργασία» ενός σταθμού και ενός BSS, λόγω του είτε αυτός σταμάτησε την λειτουργία του, ή κινήθηκε προς κάποιο άλλο BSS. Η λειτουργία distribution χρησιμοποιείται από τα APs για να αποφασίσει τον στόχο των πακέτων που εκπέμπονται, δηλαδή αν είναι για κάποια άλλη ασύρματη συσκευή ή προορίζονται για το ΣΔ. Τέλος, η υπηρεσία intergration είναι αυτή που «μεταφράζει» τα πακέτα που προέρχονται από ασύρματους σταθμούς (802.11b πακέτα) σε πακέτα για το ενσύρματο ΣΔ(πακέτα 802.3), αλλά και το αντίθετο.

Κάθε Access Point, πολυπλέκει στο χρόνο τις αιτήσεις από κάθε client και εξυπηρετεί το υποδίκτυο του. Καθώς το μέσο μετάδοσης είναι μοναδικό, όσους περισσότερους ταυτόχρονους clients έχουμε σε ένα AP, τόσο πέφτει και η απόδοση του δικτύου. Θεωρητικά η πτώση της απόδοσης είναι αντιστρόφως ανάλογη του αριθμού των μελών του δικτύου. Δυστυχώς λόγω πολλών άλλων παραγόντων(βλέπε κεφάλαιο Hidden Node), υπό συγκεκριμένες συνθήκες η μείωση της απόδοσης είναι δραματική.

Ένα ασύρματο δίκτυο είναι πιθανότητα ένα δίκτυο με μεγάλους ρυθμούς λαθών. Για τέτοιες περιπτώσεις που τα λάθη μετάδοσης είναι πραγματικότητα και όχι πιθανότητα, όπως εγκαταστάσεις με υψηλές παρεμβολές RF ή πολύ μακρινές

ζεύξεις, υπάρχει η παράμετρος του *fragmentation* που βοηθά στην εξομάλυνση του φαινομένου. Ο διαχειριστής του AP μπορεί να θέσει το πόσο μικρό ή μεγάλο θα είναι το μέγεθος των πακέτων που εκπέμπονται. Μικρότερα πακέτα έχουν μεγαλύτερη πιθανότητα να φτάσουν ανέπαφα στον προορισμό τους από μεγαλύτερα. Με αυτόν τον τρόπο μπορεί ο διαχειριστής να μειώσει το error rate του δικτύου, με το κόστος βεβαίως της μειωμένης απόδοσης, καθώς μεταδίδοντας πολλά μικρά πακέτα, έχουμε μετάδοση περισσότερου overhead και όχι χρήσιμης πληροφορίας.

2.7 Πρότυπα συμβατότητας και πιστοποίηση προτύπου WiFi

Το εμπόριο έχει κατακλυστεί πλέον από προϊόντα εταιριών που υλοποιούν με κάποιο τρόπο κάποιο μέρος του πρωτοκόλλου 802.11b(Access Points, clients, routers, VoIP terminals, cameras κτλ). Την λύση στην ερώτηση «τι εγγύηση έχει ο καταναλωτής για την συμβατότητα λειτουργίας όλων των 802.11b συσκευών;» έρχεται να δώσει η WECA(Wireless Ethernet Compatibility Alliance). Πρόκειται για μια οργάνωση που εξετάζει και πιστοποιεί την συμβατότητα των 802.11 συσκευών. Πρόκειται για μια πολύ σημαντική πρωτοβουλία, καθώς ένα wireless δίκτυο μπορεί να αποτελείται από συσκευές διαφορετικών εταιριών. Μια πιστοποιημένη από την weca συσκευή, έχει την εγγύηση ότι θα μπορεί να συνεργαστεί με άλλο ασύρματο ή όχι υλικό, που υποδεικνύεται από το πρωτόκολλο 802.11b για τον συγκεκριμένο τύπο συσκευής(π.χ. ένα Access Point πρέπει να μπορεί να συνδεθεί με οποιονδήποτε client, αλλά και να μπορεί να δεχτεί και μια Ethernet σύνδεση). Η WECA έχει θεσπίσει το Wireless Fidelity πρότυπο, και σε κάθε συσκευή που περνάει επιτυχώς όλες τις δοκιμές συμβατότητας, απονέμεται η «σφραγίδα συμβατότητας».

Εικόνα 14 – WiFi trademark

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

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

2.8 Εφαρμογές Wifi δικτύων στο σπίτι, το γραφείο, την βιομηχανία

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

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

Στο γραφείο, το wifi γίνεται συνώνυμο της ευελιξίας. Οι εργαζόμενοι μπορούν ελεύθερα να κινούνται με φορητούς υπολογιστές στους εργασιακούς τους χώρους, χωρίς να χάνουν ούτε λεπτό την σύνδεσή τους στο εταιρικό δίκτυο και το διαδίκτυο.

Με αυτό τον τρόπο αυξάνεται η παραγωγικότητά τους καθώς μπορούν να συνεργάζονται ευκολότερα και να έχουν συνεχή πρόσβαση σε κρίσιμες πληροφορίες. Πολλά τοπικά δίκτυα σε κάθε κτίριο μπορούν εύκολα να συνενωθούν με Links μεγάλων αποστάσεων, αποδοτικά και κυρίως οικονομικά. Δεν πρέπει βεβαίως να ξεχνάμε τους κινδύνους ασφάλειας που παρουσιάζονται, κινδύνους που θα αναλύσουμε στην αντίστοιχη παράγραφο.

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

3) 802.11b, τα προβλήματα

3.1 Ασφάλεια δικτύων 802.11b

Όσο οι συσκευές wifi εισέβαλλαν σε όλο και περισσότερα δίκτυα, τόσο οι χρήστες τους έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Αναρίθμητες μελέτες, τόσο από κοινούς χρήστες, όσο και από την επιστημονική κοινότητα, βοήθησαν στο να ξεσκεπαστούν πολλές θεμελιώδεις ατέλειες στο μοντέλο ασφάλειας του πρωτοκόλλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις.

Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP(wired equivalent prinvacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο. Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί από

όλους τους κατασκευαστές. Μια γρήγορη λύση για την υποκατάστασή του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το Access Point κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο Access Point. Αυτή είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών πελατών. Κάποιος εκτός λίστας, με αρκετά δικαιώματα σε ένα unix-like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται mac spoofing attacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (network sniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή WiFi κάρτα και ένα λάπτοπ να φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο Access Point-στόχο. Έτσι, αλλάζοντας την MAC διεύθυνσή του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά.

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα της κυβέρνησης των ΗΠΑ κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει ποσό τρωτό είναι ένα ανοιχτό δίκτυο, βιάστηκαν να υιοθετήσουν το πρότυπο αυτό.

Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης

κλειδιών, ενώ η εργασία του Maryland θίγει της αδυναμίες στους μηχανισμούς πρόσβασης, ακόμη και αυτούς που λειτουργούν με βάση το WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου, με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για το WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP:unsafe at any key length»).

Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης(RC4 της RCA), παρόλαυτα, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι Scott Fluhrer, Itsik Mantin, και Adi Shamir, ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως το AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου – στόχος.

Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα wifi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό Access Points που ανιχνεύτηκαν, έχουν πράγματι το WEP ενεργοποιημένο.

Το μεγαλύτερο ποσοστό των εταιρικών δικτύων, είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν web sites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών δικτύων. Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως το netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού τους υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως το SSID του Access Point, αν έχει ενεργοποιημένο το WEP, αλλά και την ποιότητα της εκπομπής της κεραίας – στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή wifi κάρτα και μια ακόμα φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», ενονόματι wardriving, επωφελούμενοι κυρίως από

την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο. Η επίθεση parking lot, συνεπάγεται την χρήση της εμβελείας ενός wifi δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας, για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος πάρκιν. Με μια δόση χιούμορ, πολλά άρθρα στο διαδίκτυο, για να ωθήσουν τους network administrators να αυξήσουν την ασφάλεια των ασύρματων δικτύων τους, ρωτούν: «μοιράζεστε την εταιρική σας σύνδεση στο ίντερνετ με εκείνο τον κύριο στο πάρκιν;».

Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη»(disassociation/deauthentication packets) προς το Access Point. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης, μπορεί να απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC-πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα, και θα αποσυνδέσει όσους σταθμούς του ζητηθούν, προκαλώντας έτσι την κατάρρευση του δικτύου.

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

3.2 Το πρόβλημα του Κρυμμένου Κόμβου(Hidden Node)

Στην παράγραφο αυτό θα ορίσουμε και θα περιγράψουμε ίσως ένα από τα μεγαλύτερα μειονεκτήματα του 802.11b, το πρόβλημα του κρυμμένου κόμβου, το οποίο είναι καθαρά εγγενές στο σχεδιασμό του πρωτοκόλλου και οφείλεται πιθανότατα στους ίδιους τους στόχους τους οποίους έθεσε η ομάδα εργασίας της IEEE για το WiFi σαν εναλλακτικό τρόπο δικτύωσης σε τοπικό επίπεδο. Είναι ένα πρόβλημα που εμφανίζεται μόνο σε infrastructure mode, όπως θα γίνει κατανοητό

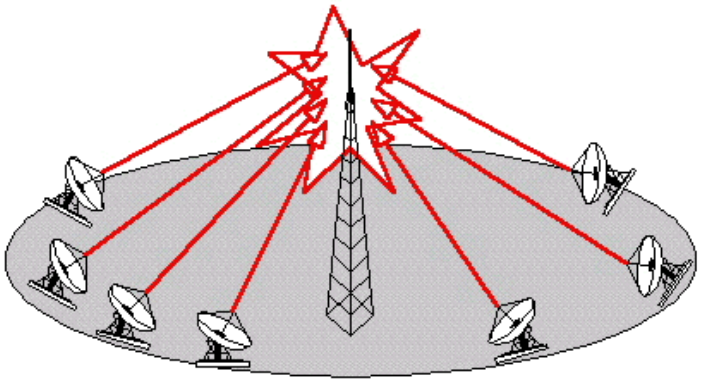
στις πιο κάτω γραμμές. Ας υποθέσουμε ότι έχουμε ένα κεντρικό Access Point και πολλούς clients σε διαφορετικές τοποθεσίες, έτσι ώστε όλοι οι clients να έχουν οπτική επαφή με το AP, αλλά όχι και καθένας με τον άλλο. Μιλάμε δηλαδή για μια αρκετά τυπική περίπτωση ενός π.χ., ενδοπανεπιστημιακού δικτύου.

Από τον ορισμό του το 802.11b προορίζονταν για ένα κλειστό περιβάλλον γραφείου. Σε αυτό το περιβάλλον, η επιτροπή της IEEE θεώρησε λογικό το ότι όλοι οι client κόμβοι που είναι συνδεδεμένοι σε ένα Access Point θα μπορούν «ακούν» το τι στέλνει ο γείτονάς τους. Χωρίς δηλαδή στην πραγματικότητα να λαμβάνουν τα δεδομένα που εκπέμπει ο διπλανός client προς το AP, έχουν την πληροφορία ότι αυτή την στιγμή κάποιος χρησιμοποιεί το κανάλι, στέλνοντας δεδομένα.

Η κύρια μέθοδος αποφυγής συγκρούσεων στο 802.11 είναι το CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Η λειτουργία Carrier Sense πραγματοποιείται με παρακολούθηση του καναλιού πριν της έναρξη εκπομπής. Αν κάποιος άλλος client εκείνη την ώρα τύχει να εκπέμπει, τότε ο πρώτος περιμένει, έως ότου να βρεθεί στιγμή που το κανάλι να είναι ελεύθερο. Όπως καταλαβαίνουμε, για να επιτευχθεί ένα καλό ποσοστό συγχρονισμού, που θα εξασφαλίσει την εύρυθμη λειτουργία του δικτύου, πρέπει οι περισσότεροι client να βρίσκονται σε θέση να ακούν τις εκπομπές όλων των άλλων. Όταν δηλαδή ένας σταθμός ελέγχει το μέσο για να δει αν είναι σε χρήση, μπορεί εσφαλμένα να αποφασίσει ότι είναι ελεύθερο, μιας και δεν είναι σε θέση να λαμβάνει τις εκπομπές όλων των άλλων σταθμών του Access Point. Σε αυτήν την περίπτωση, το αποτέλεσμα θα είναι συνεχείς συγκρούσεις. Σε περίπτωση σύγκρουσης, το αποτέλεσμα είναι όμως δεν είναι τυχαίο, κάτι που αν συνέβαινε θα οδηγούσε ίσως σε ισορροπία. Συνήθως το Access Point τείνει να ευνοεί τον εκπομπό με το καλύτερο σήμα, καθώς λαμβάνει το σήμα του ασθενέστερου σαν θόρυβο και απορρίπτοντάς το. Δεδομένων λοιπόν των συνθηκών, μια και μόνο συσκευή μπορεί να μονοπωλήσει ολόκληρο το εύρος ζώνης του AP.

Ευνοϊκές συνθήκες για την εμφάνιση προβλήματος κρυμμένου κόμβου δεν είναι όμως μόνο οι περιπτώσεις που υπάρχουν εμπόδια μεταξύ δύο ή περισσότερων σταθμών. Η επικοινωνία τύπου «όλοι ακούν όλους», μπορεί να είναι εφικτή μόνο όταν χρησιμοποιούμε μη κατευθυντικές(omni directional) κεραίες, οι οποίες εκπέμπουν κυκλικά το σήμα τους. Πολλές φορές όμως, η χρήση κατευθυντικών κεραιών(yagi, parabolic grid) υψηλού κέρδους σήματος, είναι μονόδρομος για να

επιτευχθεί σύνδεσή (βλέπε εικόνα 7). Κάτω από αυτές τις συνθήκες, μια και μόνο client συσκευή είναι δυνατόν να μονοπωλήσει όλο το εύρος ζώνης του Access Point, προκαλώντας έτσι τεράστια συμφόρηση στις διακινήσεις δεδομένων των υπόλοιπων κόμβων.



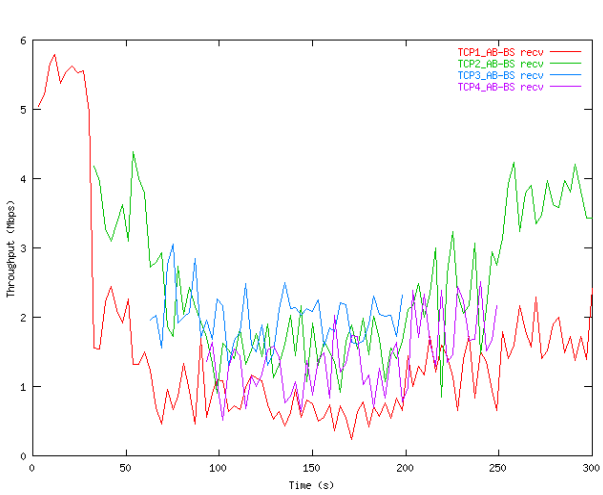
Εικόνα 15 – Wlan με πελάτες κατευθυντικής εκπομπής

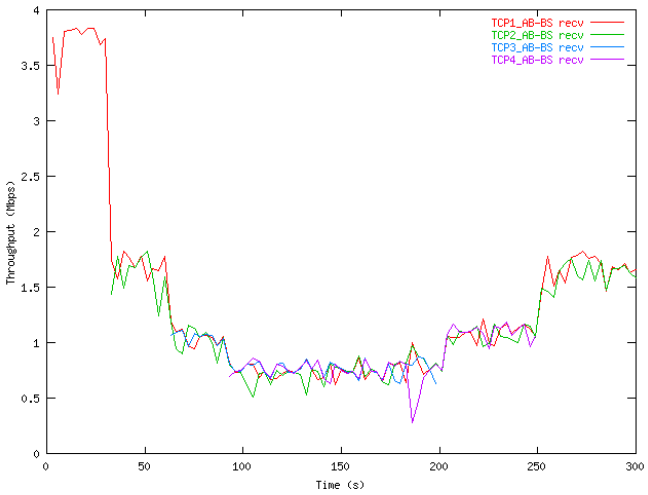
Η εισαγωγή του μηχανισμού RTS/CTS έδωσε κάποια ελπιδοφόρα μηνύματα στην κοινότητα χρηστών του 802.11b. Η υλοποίηση βέβαια του μηχανισμού αυτού δεν είναι υποχρεωτική, και υπάρχουν πάρα πολλές συσκευές που δεν το υποστηρίζουν. Τελικά όμως ο μηχανισμός αυτός αποτυγχάνει πλήρως να αμβλύνει το φαινόμενο του Hidden Node, εν μέρει λόγω συγκρούσεων στα ίδια τα πακέτα RTS (περνάνε μόνο τα RTS του δυνατότερου). Παρόλο τον σχεδιασμό του, με πακέτα μικρού μεγέθους και ως εκ τούτου μικρότερη πιθανότητα σύγκρουσης, αλλά και γρηγορότερη διόρθωση των συγκρούσεων, η πραγματική χρήση τους σε δίκτυα εξωτερικού χώρου δεν φαίνεται να έχει αποτέλεσμα.

Λύσεις υπάρχουν, και διαφέρουν σε προσέγγιση αλλά και κόστος. Υπάρχουν ειδικές συσκευές (ή firmware για συσκευές) οι οποίες εφαρμόζουν ένα είδος polling στο δίκτυο. Τέτοιες λύσεις έχουν θεωρικά αλλά και πρακτικά μεγάλη επιτυχία στην σωστή χρήση του εύρους ζώνης, αλλά έχουν μεγάλο κόστος, καθώς είναι παντελώς ασύμβατες με τα κλασσικά wifi προϊόντα, μιας και βγαίνουν εκτός του προτύπου. Λύσεις για bandwidth control σε υψηλότερο επίπεδο ερευνούνται, μα και πάλι δεν παρέχουν καμία εγγύηση για την εξάλειψη συγκρούσεων. Ίσως η καλύτερη λύση στο πρόβλημα έχει να προσφέρει η κοινότητα ανοιχτού κώδικα, και για την ακρίβεια, η ομάδα του Patras Wireless.

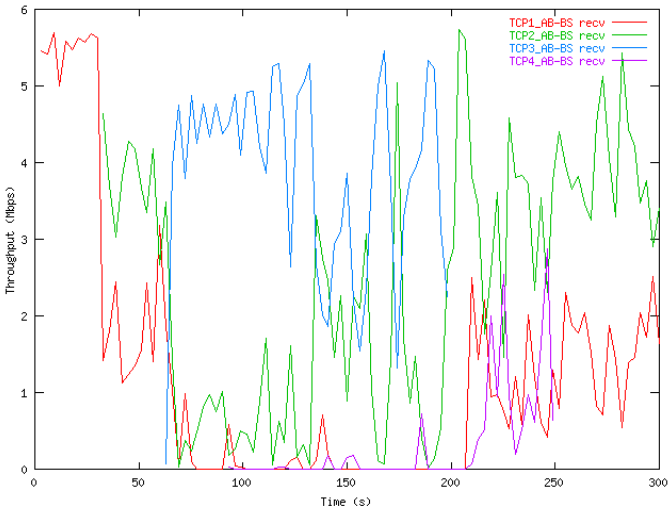
Μια ελπιδοφόρος λύση είναι το πρωτόκολλο WiCCP(Wireless Central Coordination Protocol), το οποίο γράφτηκε και υλοποιήθηκε από δύο μέλη του PWN. Το πρωτόκολλο υλοποιείται σε δύο κομμάτια λογισμικού, ένα master και ένα client network driver. Το πρώτο μπαίνει σε έναν υπολογιστή με wired σύνδεση στο AP και το client κομμάτι στο network driver stack κάθε υπολογιστή-χρήστη του AP. Στο πρωτόκολλο υπάρχει η ιδέα του token. Ο master δίνει το token σε κάθε client για ένα συγκεκριμένο χρονικό περιθώριο (timeslice). Μόνο ένας client μπορεί να έχει το token κάθε φορά. Όταν ο client θέλει να στείλει κάποιο πακέτο, κοιτάει αν το master τμήμα(στο access point) του έχει δώσει το token. Αν ναι, τότε προχωρά στην αποστολή, που θα κρατήσει όσο χρόνο του αφήνει το token. Αν δεν το έχει, τότε ο driver κρατά τα πακέτα που στέλνει ο χρήστης σε προσωρινή ουρά, και περιμένει να ξαναπάρει το token, αδειάζοντας την ουρά. Στην ουσία δημιουργεί ένα είδος token-ring στο standard Ethernet που χρησιμοποιεί το δίκτυο, τελείως transparent στις εφαρμογές χρήστη. Έτσι εγγυημένα αποφεύγονται όλες οι συγκρούσεις, καθώς μόνο ένας μιλάει κάθε φορά στο Access Point. Δείτε το patraswireless.net για περισσότερες πληροφορίες πάνω στο πρωτόκολλο, το οποίο ονομάζεται WiCCP(Wireless Central Coordinated Protocol), και βρίσκεται αισίως στην έκδοση 0.5. Η ανάπτυξη του driver γίνεται σε συνεργασία με άλλες μεγάλες ασύρματες κοινότητες, όπως το Perth Wireless της Αυστραλίας.

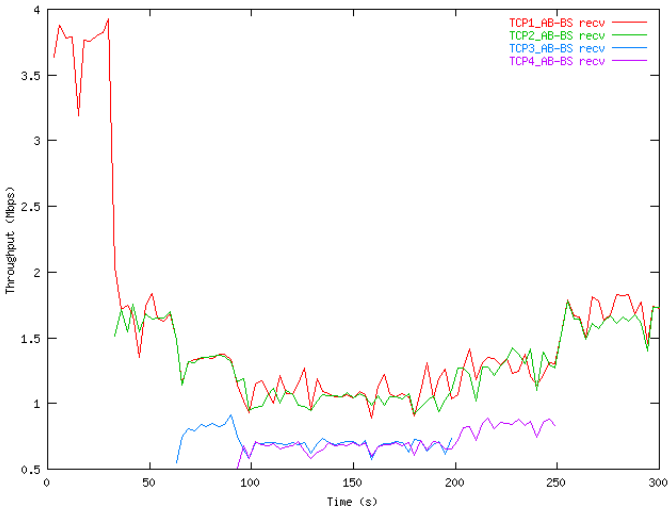
Ας δούμε μερικές χαρακτηριστικές συναρτήσεις χρόνου(ms)/διαμεταγωγής(Mbps) που δημιουργήθηκαν χρησιμοποιώντας αληθινά πειραματικά δεδομένα, ενός δικτύου με τέσσερις σταθμούς και ένα Access Point, με διάφορα σενάρια διακίνησης δεδομένων μεταξύ όλων των κόμβων. Συγκρίνονται οι δύο τρόποι πρόσβασης στο μέσο, ο CSMA/CA και ο τρόπος του polling. Δεν μας ενδιαφέρει η ακριβής υλοποίηση του polling, καθώς με σωστή υλοποίηση του σε κάποιο δικτυακό επίπεδο, θα έδινε τα ίδια περίπου αποτελέσματα, απλά μετατοπισμένα στον Υ άξονα λόγω της διαφορετικής υλοποίησης (και διαφορετικής ποσότητας overhead). Ξεκινάμε με την βέλτιστη περίπτωση για την μέθοδο CSMA. Το Access Point στέλνει μία ροή σε κάθε ένα σταθμό. Όλοι οι πελάτες ακούν εξ ορισμού το AP, και έτσι η σωστή λειτουργία του CSMA είναι εφικτή.





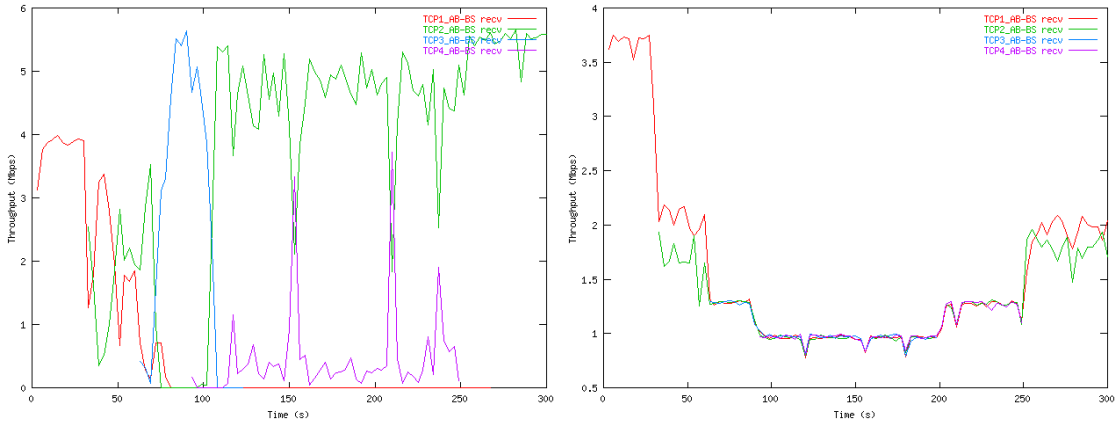
Παρατηρούμε ότι ακόμη και στην βέλτιστη περίπτωση, η διακύμανση της διαμεταγωγής είναι πολύ μεγάλη με την μεθοδο CSMA(δεξιά εικόνα). Αντίθετα η λύση του polling δείχνει την υπεροχή της. Η μέση περίπτωση είναι αυτή κατά την οποία 2 σταθμοί στέλνουν στο Access Point και το AP στέλνει στους υπόλοιπους 2 σταθμούς.





Οι συγκρούσεις στα πακέτα δεδομένων είναι μαζικές με το CSMA(δεξιά εικόνα). Μία και μόνο σύνδεση μονοπωλεί σχεδόν το εύρος ζώνης, ενώ άλλες ακυρώνονται πλήρως. Αντίθετα το polling δίνει και πάλι ανεκτά αποτελέσματα.

Μπορούμε εύκολα να φανταστούμε την γραφική παράσταση που θα παρουσιάζει μια μετάδοση από τους τέσσερις σταθμούς προς το AP. Οι συγκρούσεις είναι τρομακτικές, και οι διακυμάνσεις δείχνουν δραματικά την πλήρη κατάρρευση της κυψέλης.



Τα παραπάνω πειραματικά δεδομένα δείχνουν με τον πιο πειστικό τρόπο την ανεπάρκεια του CSMA/CA - RTS/CTS μηχανισμού. Μια ασύρματη δικτυακή εγκατάσταση μπορεί δεδομένων κάποιων συνθηκών να καταρρεύσει πλήρως. Θα μπορούσαμε να περιγράψουμε κάτι τέτοιο σαν μια (distributed) denial of service attack, που μπορεί να προκληθεί είτε από κακοπροαίρετους παρείσακτους κόμβους, είτε από απλούς χρήστες που θέλουν να κάνουν την δουλειά τους. Οι σχεδιαστές δικτύου πρέπει να είναι καλά ενημερωμένοι για το πρόβλημα, και να προσπαθούν να κατασκευάζουν δίκτυα που θα επηρεάζονται από hidden node σε μικρές κλίμακες. Η επιλογή point to point ad hoc των συνδέσεων ραχοκοκαλιάς(backbone) του δικτύου είναι προτιμότερη από αρχιτεκτονικές AP-client.

4) Συμπερασματικά

4.1 Άλλα πρωτόκολλα ασύρματης δικτύωσης

Το 802.11 και η οικογένεια πρωτοκόλλων του b,a και g δεν είναι βεβαίως οι μοναδικοί παίκτες στο παιχνίδι της ασύρματης δικτύωσης. Ας κάνουμε μια αναφορά στα υπόλοιπα πρωτόκολλα, απαριθμώντας κάποια σύντομα χαρακτηριστικά.

Το HiperLAN είναι μια πρωτοβουλία της ευρωπαϊκής οργάνωσης ETSI(European Telecommunications Standards Institute) που ξεκίνησε το 1996. Η πρώτη έκδοση του πρωτοκόλλου υποστηρίζει λειτουργία στο φάσμα των 5GHz και εύρος ζώνης στα 22Mbps. Χρησιμοποιεί connectionless τρόπο πρόσβασης στο

ασύρματο δίκτυο για τους χρήστες του, όπως το Ethernet. Υποστηρίζει QoS για ανάγκες όπως το streaming video, VoIP κτλ. Η δεύτερη έκδοση του πρωτοκόλλου που είναι υπό κατασκευή (HiperLAN2) θα λειτουργεί και πάλι στα 5GHz με ταχύτητα της τάξης των 54Mbps, θα έχει connection-oriented τρόπο πρόσβασης και θα είναι ικανό να μεταφέρει πακέτα Ethernet, ATM και IP.

Το HomeRF ξεκίνησε από την HomeRF Working Group η οποία προσέφερε στην αγορά μια ανοιχτή βιομηχανική προδιαγραφή με το όνομα SWAP(Shared Access Wireless Protocol), με προορισμό την ασύρματη ψηφιακή επικοινωνία μεταξύ ηλεκτρονικών υπολογιστών και ηλεκτρονικών συσκευών στο οικιακό περιβάλλον. Υποστηρίζει διαμόρφωση Frequency Hopping spread spectrum με ταχύτητα του 1Mbps. Αναμένεται νέα δημοσίευση του πρωτοκόλλου με ταχύτητα στα 10Mbps.

Περνώντας στο πεδίο των προσωπικών δικτύων (Personal Area Networks, εν αντιθέσει με τα LANs), πρέπει να αναφερθούμε στο Bluetooth, ένα πρωτόκολλο με μεγάλη αποδοχή από τους μεγαλύτερους κατασκευαστές στον χώρο. Λειτουργεί και αυτό στους 2.4 μεγάκυκλους και έχει μέγιστη ταχύτητα το 1mbps. Έχει σκοπό την δημιουργία ενός δικτύου μικρής εμβέλειας γύρω από τον χρήστη του, το οποίο μπορεί να αλληλεπιδρά με αντίστοιχες Bluetooth-enabled συσκευές.

4.2 Συμπέρασμα

Η τεχνολογία 802.11(b) ήταν η πρώτη εδώ και αρκετά χρόνια πρωτοβουλία, για την εισαγωγή ενός πρωτοκόλλου ασύρματης τοπικής δικτύωσης μεγάλου εύρους ζώνης. Τα πλεονεκτήματα που περιγράψαμε ποιο πάνω, σε συνδυασμό με το γεγονός ότι δεν είναι αναγκαία η απόκτηση ειδικής άδειας χρήσης αυτής της ραδιοφωνικής συχνότητας, έκανε την αποδοχή του από τους καταναλωτές και τις εταιρίες ταχύτατη. Μάλιστα οι δυνατότητες της οικογένειας πρωτοκόλλων 802.11, είναι τέτοιες που το καθιστούν μια καλή λύση του προβλήματος του τελευταίου χιλιομέτρου(last mile problem), δηλαδή την παροχή broadband υπηρεσιών στον τελικό χρήστη από το δίκτυο μεταφοράς δεδομένων του ήδη εγκατεστημένου τηλεφωνικού δικτύου. Στο εξωτερικό ανθεί η αγορά των wISPs(wireless Internet service provider), που προσφέρουν ευρυζωνικό internet μέσω της ασύρματης υποδομής που κατασκευάζουν οι ίδιοι, και μισθώνοντας γρήγορες συνδέσεις στο

διαδίκτυο, τις οποίες και παρέχουν στους τελικούς πελάτες. Στην Ελλάδα κάτι τέτοιο είναι ανέφικτο για την ώρα, λόγω του ασαφούς νομικού πλαισίου περί της εμπορικής χρήσης της συχνότητας των 2,4GHz. Είναι επιτακτική λοιπόν η ανάγκη για νομοθετικές αλλαγές, που θα βοηθήσουν να αρθεί το μονοπώλιο των κρατικών τηλεπικοινωνιακών φορέων, και θα δώσει νέες ανταγωνιστικές δυνατότητες σε μικρότερες επιχειρήσεις.

Παρατηρώντας την μεγάλη αποδοχή του 802.11b, σε σχέση με το πόσο πρόσφατα έγινε η προτυποποίηση, είναι ξεκάθαρη η επιτυχία του σαν standard. Επιπλέον, δεν μπορούμε παρά να αναγνωρίσουμε πως αυτός ο νέος τρόπος ασύρματης επικοινωνίας και ανταλλαγής δεδομένων, είναι μια νέα και σχετικά ανεξερεύνητη περιοχή, που ίσως μας επιφυλάσσει μεγάλες αλλαγές στην ποιότητα, την αποδοτικότητα αλλά και την αντίληψη που έχουμε για τις ψηφιακές τηλεπικοινωνίες.

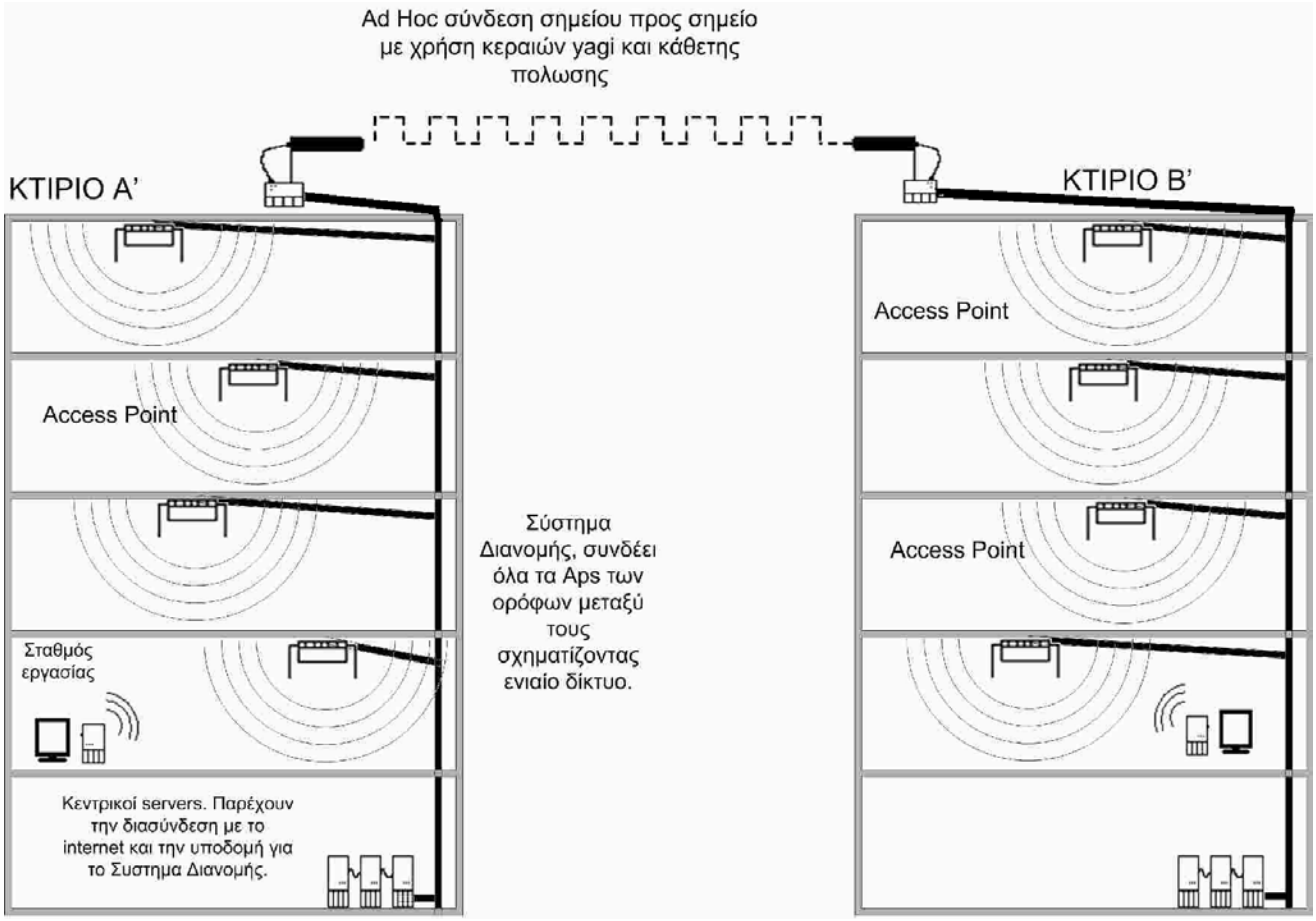
4.3 Παράδειγμα ασύρματου δικτυακής εγκατάστασης: Η εταιρία Χ

Η εταιρία Χ δραστηριοποιείται στον χώρο των web services. Σε κάθε όροφο του τετραώροφου κτιριακού της συγκροτήματος πρέπει να παρέχεται σύνδεση στο εταιρικό LAN στους υπαλλήλους, καθώς και διασύνδεση με το internet. Access Points στημένα σε κάθε όροφο, συνδεδεμένα στον ενσύρματο «κορμό» του εταιρικού δικτύου, θα δίνουν αυτή τη δυνατότητα στους υπαλλήλους. Οι εργαζόμενοι μπορούν είτε να εργάζονται στους σταθμούς εργασίας τους, είτε να κινούνται με φορητούς υπολογιστές ανά τους ορόφους χωρίς να χάνουν την σύνδεση με το δίκτυο. Ένα προφανές πρόβλημα, είναι ότι η επιχείρηση έχει κτίρια και στις δύο μεριές μιας λεωφόρου. Θα ξεπεράσουμε αυτό το εμπόδιο, εγκαθιστώντας μια ad hoc σύνδεση μεταξύ των δύο κτιρίων, χρησιμοποιώντας μια συσκευή σταθμό σε κάθε ταράτσα, εφοδιασμένη με κατευθυντικές yagi κεραίες μικρού σχετικά κέρδους, μιας και η απόσταση που πρέπει να καλυφθεί είναι μικρή. Η χρήση αυτού του τύπου κεραίας(ιδιαίτερα κατευθυντικής εκπομπής) γίνεται για δύο σημαντικούς λόγους.

Α) Χρειαζόμαστε ένα απόλυτα κατευθυντικό Link. Δεν θέλουμε να συνδεθούμε η να παρέχουμε κάποια υπηρεσία σε κανέναν άλλον εκτός από το απέναντι κτίριο. Με αυτό το δεδομένο, οποιαδήποτε ποσότητα ενέργειας της εκπομπής μας γίνεται σε

χώρο εκτός της απέναντι κεραίας, θεωρείται σπατάλη, καθώς επιζητούμε την μέγιστη ποιότητα σύνδεσης που μπορούμε να έχουμε με μία δεδομένη ισχύ. Η ισχύς της κεραίας πρέπει πάντα να κρατηθεί εντός νομικών ορίων.

Β) Κατευθυντική εκπομπή στην ελάχιστη δυνατή ισχύ, σε αυτή την περίπτωση, σημαίνει αυξημένη ασφάλεια. Ένας υποθετικός εισβολέας, για να μπορέσει να εκμεταλλευτεί όλα τα μειονεκτήματα ασφαλείας του 802.11b που αναφέραμε ποιο πάνω, πρέπει αρχικά να έχει πρόσβαση στην ίδια την μικροκυματική εκπομπή της κεραίας μας. Σε ένα ιδανικά και απόλυτα κατευθυντικό link, κάποιος θα μπορούσε να υποκλέψει την πληροφορία που διακινείτο στον αέρα, μόνο αν ήταν πάνω στην νοητή ευθεία των δύο κεραιών. Εφόσον η πρόσβαση στις ταράτσες των κτιρίων είναι απαγορευμένη, είναι πολύ μικρή η πιθανότητα να καταφέρει κάποιος την κακοπροαίρετη λήψη πακέτων χωρίς να αποθαρρυνθεί από την κακή ποιότητα σήματος που θα έχει από παραδείγματος χάριν, τον δρόμο.



Εικόνα 16 – Η εταιρία Χ

Σε όλα τα Access Points μπορούμε να εφαρμόσουμε ρυθμίσεις ασφαλείας αναλόγως τις απαιτήσεις μας. Συνίσταται η ενεργοποίηση του WEP, όσο ανασφαλές και αν

είναι, καθώς αποτελεί ένα πρώτο «φράκτη» για οποιονδήποτε εισβολέα. Μπορούμε επίσης να κρατάμε βάση δεδομένων με τις επιτρεπόμενες hardware διευθύνσεις(MAC address) και απαγορέψουμε όλες τις άλλες. Αυτό βέβαια χρειάζεται την επίπονη δουλειά της συνεχούς ενημέρωσης μιας βάσης δεδομένων με τα επιτρεπόμενα MACs, και κάτι πέτοιο μπορεί να είναι απαγορευτικό σε ένα δυναμικό περιβάλλον. Για να αυξήσουμε ακόμη περισσότερο την ασφάλεια του εξωτερικού link μεταξύ των κτιρίων, μπορούμε να εφαρμόσουμε κάποια μέθοδο κρυπτογράφησης των δεδομένων σε υψηλότερο δικτυακό επίπεδο ακριβώς πριν και μετά την έξοδό τους από αυτό, όπως IPsec ή κάποιο είδος secure tunnel.

ΠΑΡΑΡΤΗΜΑ

Η οικογένεια πρωτοκόλλων 802.11

Η νέες γενιές πρωτοκόλλων στην οικογένεια 802.11 αρχίζουν να κάνουν τα βήματά τους. Ένας αρκετά μεγάλος αριθμός ομάδος εργασίας της IEEE συνεργάζονται για να φέρουν σε πέρας την προτυποποίηση αυτών προσπαθειών. Ας δούμε όμως αναλυτικά, ανά κωδικό ομάδας εργασίας, τι είναι αυτό που υπόσχονται τα «παιδιά» της οικογένειας 802.11.

Ομάδα εργασίας G(802.11g)

Το πρωτόκολλο αυτό είναι προς τα πίσω συμβατό με το 802.11b. Η ομάδα αυτή επικεντρώνεται στην αναζήτηση υψηλότερης(22mbps ή και περισσότερο) διαμεταγωγής δεδομένων στην μπάντα των 2,4GHz, χωρίς όμως να χάνεται η δυνατότητα λειτουργίας με υπάρχοντα b δίκτυα. Αρχικά για τον τρόπο διαμόρφωσης η εταιρία intersil πρότεινε την χρησιμοποίηση του OFDM (Orthogonal Frequency Division Multiplexing), μια μέθοδο που αναπτύχθηκε για το 802.11a(βλ. πιο κάτω). Αυτή η πρόταση βρήκε αντίπαλες πολλές εταιρίες, όπως η Texas Instruments, που πρότεινε την χρήση της δικής της τεχνολογίας PBCC (Packet Binary Convolution Coding) για το πρωτόκολλο. Τελικά η προτυποποίηση του πρωτοκόλλου 802.11g, έφερε και την λύση. Το πρωτόκολλο χρησιμοποιεί υποχρεωτικά όλους τους τρόπους κωδικοποίησης του 802.11b για εγγυημένη προς τα πίσω συμβατότητα. Επίσης υποχρεωτική είναι η υλοποίηση του OFDM σαν τρόπο κωδικοποίησης στο g πρωτόκολλο. Προαιρετικά μπορεί ο κάθε κατασκευαστής να υλοποιήσει και μια τροποποιημένη έκδοση του OFDM ή τον PBCC, αν επιθυμεί συσκευές με καλύτερες επιδόσεις.

Ομάδα εργασίας A(802.11a)

Το πρωτόκολλο a χρησιμοποιεί την ραδιοφωνική μπάντα των 5GHz. Αυτό το γεγονός, του δίνει ένα (κάπως σύντομο χρονικά) πλεονέκτημα κατά των υπολοίπων προτύπων : η μπάντα των 5GHz δεν χρησιμοποιείται από σχεδόν κανέναν, όντας ελεύθερη παρεμβολών. Η ομάδα της IEEE εγγυάται την συμβατότητα όλων των μερών εκτός του ραδιοφωνικού πομπού μιας συσκευής με τα άλλα πρωτόκολλα b,g. Έτσι ένας κατασκευαστής μπορεί να χρησιμοποιεί κοινό HW και διαφορετικούς εκπομπούς, για να παράγει συσκευές που θα είναι συμβατές με μια πλειάδα πρωτοκόλλων.

Ομάδα εργασίας H(802.11h)

Η ομάδα αυτή θα προσπαθήσει να εισάγει στο 802.11a την δυνατότητα για καλύτερο έλεγχο συγκρούσεων, καθώς και την λειτουργία Transmit Power Control(TPC) και Dynamic Frequency Selection ή DFS. Μια συσκευή θα επιλέγει αυτόματα την ελάχιστη αναγκαία ισχύ εκπομπής, πριν ξεκινήσει οποιαδήποτε ανταλλαγή δεδομένων. Επίσης θα επιλέγει αυτόματα σε ποια συχνότητα θα λειτουργήσει, αναλόγως την χρήση της κάθε συχνότητας στον περιβάλλοντα χώρο.

Ομάδα εργασίας E(802.11E)

Η ομάδα αυτή προσανατολίζεται στην εισαγωγή λειτουργιών Quality of Service με εισαγωγή προτεραιοτήτων στα πακέτα των 802.11 δικτύων, για μεταδώσεις VoIP και streaming media. Η πραγματοποίηση αυτού του στόχου θα απαιτήσει συνεννόηση μεταξύ σταθμών πελατών και Access Points, αλλά και από τον διαχειριστή του δικτύου.

Ομάδα εργασίας I(802.11I)

Η ομάδα αυτή είναι συνώνυμη της ασφάλειας. Θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου (;)πρωτοκόλλου ασφαλείας προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του. Η αρχική προσέγγιση προσανατολίζεται στην αύξηση του μήκους κλειδιού, έτσι ώστε brute force επιθέσεις σε αυτόν να έχουν απαγορευτικούς χρόνους επιτυχίας με την υπάρχουσα τεχνολογία. Δυστυχώς και πάλι μπορούν να χρησιμοποιηθούν σχεδιαστικές ατέλειες που θα καταστήσουν έναν τέτοιο αλγόριθμο ανασφαλή.

Wireless Communities

Με την έλευση των πρώτων εμπορικών δικτυακών συσκευών που υλοποιούσαν το 802.11b, ξεκίνησε και ο πειραματισμός από ιδιώτες που ενδιαφέρονταν να επαληθεύσουν της υποσχέσεις για ένα νέο, ασύρματο, αλλά και γρήγορο τρόπο δικτύωσης. Πολλοί οραματίστηκαν κοινότητες που θα σιγά σιγά θα δημιουργούσαν μια υποδομή από ομότιμους κόμβους, υποδομή προσβάσιμη σε όλους που θέλουν να την χρησιμοποιήσουν χωρίς εμπορικό σκοπό.

Αυτά τα οράματα άρχισαν να υλοποιούνται, καθώς η wifi τεχνολογία γινόταν φθηνότερη και καλύτερη. Πολλές πόλεις, αλλά και ολόκληρες μη αστικές περιοχές απέκτησαν το δικό τους Wireless Network. Στην πόλη της Αθήνας, η προσπάθεια ξεκίνησε το 2000 μέσω ηλεκτρονικών τόπων συνάντησης ατόμων που γνώριζαν και ατόμων που ήθελαν να μάθουν. Σε πολλές πόλεις, όπως και στην Πάτρα, η προσπάθεια ενός ή δύο ατόμων αποτέλεσε την υποδομή και το σπόρο για το ξεκίνημα της δημιουργίας κοινότητας. Τα wireless networks είναι πραγματικότητα σε πάνω από 5 πόλεις της Ελλάδας. Μάλιστα το Μετροπολιτικό Δίκτυο της Αθήνας έχει τους περισσότερους κόμβους σε ολόκληρη την Ευρώπη, ενώ το web site της κοινότητας (www.awmn.gr) μετρά πάνω από 1000 μέλη! Οι κοινότητες αυτές είναι που βοηθούν στην βελτίωση της τεχνολογία ασύρματης δικτύωσης, καθώς είναι εκείνες που πιέζουν στα άκρα τις δυνατότητές της. Καθαρά για εντυπωσιασμό θα αναφέρουμε το γεγονός ότι μέλη του Ασυρμάτου Δικτύου της Πάτρας έχουν καταφέρει να κάνουν σύνδεση σε infrastructure mode από το Αντίρριο με την περιοχή της Αρόης Πατρών, δηλαδή link δεκάδες φορές μακρύτερο της εργοστασιακής δυνατότητας των συσκευών. Είναι συνήθως οι πρώτοι που ανακαλύπτουν προβλήματα σε wifi συσκευές, βοηθώντας την γρηγορότερη αντιμετώπιση των προβλημάτων από της εταιρίες. Επίσης εμπλουτίζουν τα εργαλεία λογισμικού που έχει στα χέρια του ο μηχανικός αλλά και ο απλός χρήστης με προγράμματα ανοιχτού κώδικα. Τα ίδια τα δίκτυα βέβαια είναι τις περισσότερες φορές καλά δομημένα intranets, με υπηρεσίες όπως DNS, irc servers, web servers, voice and video conference υπηρεσίες κτλ, όπως άλλωστε είναι το Patras Wireless Network. Τα WNs της Ελλάδος έχουν αρκετές φορές γίνει φορέας πίεσης για νομικές αλλαγές που αφορούν την ραδιοφωνική μπάντα των 2.4 μεγάκυκλων, αλλά και γενικότερης δράσης υπέρ της (πραγματικής)ένταξης της Ελλάδας στην κοινωνία της πληροφορίας.

Βιβλιογραφία

802.11 Wireless Networks - Definitive Guide, O'Reilly Press

Broadband Telecommunications Handbook 2nd edition, McGraw – Hill

Building Wireless Community Networks, O'Reilly Press

Wireless LANs – Second Edition, SAMS publishing

Hack Proofing Your Wireless Network, Syngress

Designing a Wireless Network, Syngress

IEEE P802.11 Wireless LANs, Unsafe at any key size; An analysis of the WEP encapsulation

Final draft ETSI EN 300 328 V1.4.1 (2002-11) Candidate Harmonized European Standard (Telecommunications series)

http://aqua.comptek.ru/test/HiddenNode/hidden_node_en.html