ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ασύρματα τοπικά δίκτυα Wi-Fi

Πτυχιακή εργασία της **Τσίτσα Αγγελικής**

Επιβλέπων καθηγητής: **Βίτσας Βασίλειος**

ΘΕΣΣΑΛΟΝΙΚΗ, ΜΑΡΤΙΟΣ 2010

Πρόλογος

Ολοκληρώνοντας τις σπουδές μου, με τη συγγραφή της παρούσας πτυχιακής, θα ήθελα να ευχαριστήσω τους καθηγητές μου για τις γνώσεις που απέκτησα κατά τη διάρκεια της φοίτησης μου στο Τ.Ε.Ι Θεσσαλονίκης. Ιδιαίτερα θα ήθελα να ευχαριστήσω τον επιβλέποντα της πτυχιακής μου εργασίας, κ. Βίτσα Βασίλη αλλά και τον κ. Ηλιούδη Χρήστο για τη πολύτιμη καθοδήγησή τους κατά τη διάρκεια συγγραφής της εργασίας.

Θα ήθελα επίσης να ευχαριστήσω και να αφιερώσω την εργασία στους γονείς μου που ήταν πάντα δίπλα μου και ακούραστα με στήριζαν, ηθικά και οικονομικά. Τέλος, θέλω να ευχαριστήσω όλους τους φίλους και φίλες που ήταν στο πλευρό μου και με εμψύχωναν.

Περίληψη

Σκοπός της παρούσας πτυχιακής είναι η παρουσίαση και περιγραφή του τρόπου λειτουργίας του προτύπου IEEE 802.11, γνωστό ως Wi-Fi. Το πρώτο κεφάλαιο αποτελεί μία εισαγωγή στα ασύρματα δίκτυα αναλύοντας τα πλεονεκτήματα και μειονεκτήματα των ασύρματων δικτύων έναντι των ενσύρματων, παρουσιάζοντας τα διάφορα 802.11 πρότυπα που έχουν αναπτυχθεί, περιγράφοντας τα συστατικά ενός ασύρματου δικτύου, τις υπηρεσίες του και την αρχιτεκτονική του. Στο δεύτερο κεφάλαιο γίνεται μία ανάλυση του επιπέδου MAC. Συγκεκριμένα γίνεται αναφορά στον μηχανισμό διαχείρισης συγκρούσεων, CSMA/CA, στο πρόβλημα του κρυφού κόμβου, στις δύο βασικές τεχνικές πρόσβασης στο μέσο, DCF και PCF, στον τρόπο διαχείρισης της ενέργειας και το καφάλαιο ολοκληρώνεται με την περιγραφή των πλαισίων του 802.11. Στο τρίτο κεφάλαιο αναλύονται οι τεχνολογίες φυσικού επιπέδου FHSS, DSSS, HR/DSSS, OFDM και ERP-OFDM. Ακολουθεί το τέταρτο κεφάλαιο το οποίο πραγματεύεται το θέμα ασφάλεια στα ασύρματα δίκτυα. Αρχικά γίνεται μια αναφορά στις επιθέσεις που μπορεί να δεχτεί ένα ασύρματο δίκτυο και κατόπιν αναλύονται οι τεχνικές και τα πρωτόκολλα που αναπτύχθηκαν για να αντιμετωπιστούν οι επιθέσεις αυτές. Τέλος, στο πέμπτο κεφάλαιο παρουσιάζονται απόψεις διάφορων διεθνών επιστημονικών οργανισμών για το αν τα ασύρματα δίκτυα αποτελούν απειλή για την ανθρώπινη υγεία.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΑΡΑΡΤΗΜΑΤΑ

Κεφάλαιο 1 Ασύρματα Δίκτυα

1.1 Εισαγωγή

Τα ασύρματα δίκτυα επιτρέπουν στους ανθρώπους να επικοινωνούν και να έχουν πρόσβαση σε εφαρμογές χωρίς τη χρήση καλωδίων. Αυτό το χαρακτηριστικό δίνει στους χρήστες τη δυνατότητα να μετακινούνται χωρίς να χάνουν τη σύνδεση με το δίκτυο.

Ανάλογα με το μέγεθος και τη φυσική περιοχή που μπορεί να καλύψει ένα ασύρματο δίκτυο ανήκει σε μία από τις ακόλουθες κατηγορίες:

- Wireless Personal-Area Network (PAN)
- Wireless Local-Area Network (LAN)
- Wireless Metropolitan-Area Network (MAN)
- Wireless Wide-Area Network (WAN)

Τα τελευταία χρόνια όλο και περισσότερα WLANs εγκαθίστανται σε γραφεία, πανεπιστήμια, σπίτια και επιχειρήσεις επεκτείνοντας ή αντικαθιστώντας τα ενσύρματα τοπικά δίκτυα. Ένα WLAN περιλαμβάνει συσκευές όπως προσωπικούς ψηφιακούς βοηθούς (personal digital assistants ή PDAs), φορητούς υπολογιστές (laptops), προσωπικούς υπολογιστές (personal computers ή PCs), εξυπηρετητές και εκτυπωτές. Κάθε μία από αυτές τις συσκευές διαθέτει έναν ασύρματο πομποδέκτη ο οποίος χρησιμοποιείται για τη μετάδοση των δεδομένων. Τα δεδομένα αυτά μεταφέρονται μέσω του αέρα με χρήση ραδιοκυμάτων. Οι ζώνες συχνοτήτων στις οποίες λειτουργούν τα WLANs είναι οι ISM (Industrial, Scientific and Medical) ζώνες συχνοτήτων των 900MHz, 2.4GHz και 5GHz, οι οποίες είναι ελεύθερες για χρήση χωρίς άδεια.

Το πιο γνωστό κι επικρατέστερο πρότυπο για WLANs είναι το IEEE 802.11. Το πρότυπο αυτό ορίζει δύο αρχιτεκτονικές ασύρματων τοπικών δικτύων. Στην πρώτη αρχιτεκτονική, η οποία ονομάζεται Infrastructure BSS, οι σταθμοί μπορούν να επικοινωνούν μεταξύ τους αλλά και να συνδέονται σε ένα δίκτυο κορμού μέσω ενός κεντρικού σημείου πρόσβασης, του Access

Point (AP). Στη δεύτερη αρχιτεκτονική, γνωστή ως Independent BSS (IBSS), δεν υπάρχει κάποιο κεντρικό σημείο πρόσβασης αλλά όλοι οι σταθμοί αυτορυθμίζονται σε ένα δίκτυο [22]. Υπάρχουν διάφορες εκδόσεις και τροποποιήσεις του 802.11 προτύπου ανάλογα με τις οποίες ένα 802.11 δίκτυο μπορεί να επιτύχει ρυθμούς μετάδοσης της τάξης των 1, 2, 11 ή 54Mbps.

Τα ασύρματα δίκτυα υπερέχουν σε αρκετά σημεία των ενσύρματων δικτύων αλλά έχουν και κάποια σημεία στα οποία μειονεκτούν. Στις επόμενες παραγράφους αναπτύσσονται τα θέματα αυτά.

1.2 Πλεονεκτήματα ασύρματων δικτύων

Ένα από τα πιο βασικά και εμφανή πλεονεκτήματα είναι η δυνατότητα κίνησης (mobility). Οι χρήστες μπορούν να έχουν πρόσβαση σε δεδομένα, που είναι αποθηκευμένα κεντρικά, ενώ κινούνται ή αλλάζουν θέσεις (αρκεί βέβαια να παραμένουν εντός της περιοχής που καλύπτει το ασύρματο δίκτυο). Για παράδειγμα, οι πελάτες-επισκέπτες μιας εταιρείας μπορούν με έναν φορητό υπολογιστή να συνδέονται άμεσα και να έχουν πρόσβαση στο δίκτυο της εταιρείας αλλά και στο διαδίκτυο, οι φοιτητές ενός πανεπιστημίου να έχουν σύνδεση στο δίκτυο του από όλους τους χώρους του ή ένας χρήστης γενικά να μπορεί να βλέπει τα e-mail του από οποιοδήποτε δωμάτιο του σπιτιού του.

Ένα άλλο σημείο υπεροχής των ασύρματων δικτύων είναι η ευκολία και η ταχύτητα ανάπτυξής τους. Τα ασύρματα δίκτυα δεν χρειάζονται καλώδια κι αυτό είναι ιδιαίτερα ωφέλιμο όταν θέλουμε να εγκαταστήσουμε ένα δίκτυο σε ένα παλιό κτίριο. Αλλά ακόμα και σε νέες εγκαταστάσεις η εγκατάσταση καλωδίων μπορεί να είναι δύσκολη και χρονοβόρα.

Τα ασύρματα δίκτυα είναι επίσης πολύ ευέλικτα σε σχέση με τα ενσύρματα. Καθώς το μέσο μετάδοσης υπάρχει παντού, είναι πολύ εύκολο να προστεθούν νέοι χρήστες σε ένα τέτοιο δίκτυο επεκτείνοντάς το. Επιπλέον, ένα WLAN είναι η λύση όταν υπάρχει άμεση ανάγκη για δημιουργία ενός δικτύου για προσωρινή χρήση, για παράδειγμα στα πλαίσια μιας σύσκεψης.

Όσον αφορά το κόστος, γενικά ο ασύρματος εξοπλισμός είναι ακριβότερος από τον ενσύρματο. Σε κάποιες περιπτώσεις όμως, τα ασύρματα δίκτυα αποδεικνύονται πιο συμφέρουσα λύση. Για παράδειγμα, δεν περιλαμβάνουν καθόλου κόστος για την εγκατάσταση καλωδίων όταν αρχικά στήνεται το δίκτυο αλλά και όταν συμβαίνουν αλλαγές ή προσθήκες σε αυτό. Επίσης, για τη σύνδεση των τοπικών δικτύων δύο διαφορετικών κτιρίων μπορούν να χρησιμοποιηθούν εξωτερικές ασύρματες γέφυρες. Μία τέτοια λύση είναι πιο οικονομική από την αγορά και την εγκατάσταση οπτικών ινών, ειδικά αν ανάμεσα στα δύο κτίρια υπάρχουν φυσικά εμπόδια όπως αυτοκινητόδρομοι ή ποτάμια [20]. Ακόμα, ένα βασικό σημείο είναι ότι όταν μία εταιρεία θέλει να μετακομίσει σε ένα νέο κτίριο μπορεί να μεταφέρει και το ασύρματο δίκτυο που είχε, χωρίς καμία απώλεια στην αρχική της επένδυση.

1.3 Μειονεκτήματα ασύρματων δικτύων

Ένα σημείο στο οποίο τα WLANs υστερούν σε σχέση με τα ενσύρματα δίκτυα είναι αυτό της αξιοπιστίας. Η ενσύρματη δικτύωση είναι πλέον μια ώριμη τεχνολογία που έχει δεχθεί πολλές βελτιώσεις. Αντίθετα, τα ασύρματα δίκτυα αντιμετωπίζουν ακόμα αρκετά προβλήματα που σχετίζονται με τις παρεμβολές από άλλες ασύρματες συσκευές οι οποίες λειτουργούν στις ίδιες συχνότητες με αυτά. Τέτοιες συσκευές είναι οι φούρνοι μικροκυμάτων, τα ασύρματα τηλέφωνα κ.α. Ένα άλλο φαινόμενο που δημιουργεί προβλήματα στη μετάδοση των ραδιοκυμάτων είναι εξασθένηση πολλαπλών διαδρομών(multipath fading). Καθώς τα ραδιοκύματα διασχίζουν το χώρο αντανακλώνται πάνω στα φυσικά αντικείμενα με αποτέλεσμα το σήμα να φτάνει στον αποστολέα πολλές φορές από διαφορετικές διαδρομές.

Επίσης, η απόδοση ενός ασύρματου δικτύου είναι αρκετά μικρότερη από ενός ενσύρματου δικτύου. Το 802.11b προσφέρει ρυθμούς μετάδοσης μέχρι 11Mbps και τα 802.11a/g προσφέρουν 54Mbps τη στιγμή που το Fast Ethernet υποστηρίζει μέχρι 100Mbps. Επιπλέον, η απόδοση μειώνεται καθώς μεγαλώνει η απόσταση των σταθμών από το AP αλλά και όσο αυξάνεται ο αριθμός των χρηστών του WLAN.

Ένα άλλο μειονέκτημα των ασύρματων δικτύων είναι το ότι, λόγω της φύσης του μέσου, δεν είναι πολύ ασφαλή. Τα δεδομένα μεταδίδονται μέσω του αέρα και μπορούν εύκολα να υποκλαπούν.

Τέλος, μπορεί τα ασύρματα δίκτυα να προσφέρουν ελευθερία κίνησης, επειδή όμως οι ασύρματες συσκευές λειτουργούν με μπαταρία, μετά από κάποιο χρονικό διάστημα χρήσης θα πρέπει αναγκαστικά να συνδεθούν σε κάποιο καλώδιο προκειμένου να φορτιστούν.

1.4 Τα πρότυπα του 802.11

802.11

Το αρχικό 802.11 πρότυπο επικυρώθηκε το 1997. Πρόκειται για άλλο ένα επίπεδο συνδέσμου που μπορεί να χρησιμοποιεί την 802.2/LLC ενθυλάκωση [1]. Η 802.11 περιλαμβάνει ένα επίπεδο MAC και τρεις διαφορετικές τεχνολογίες φυσικού επιπέδου, τις:

- Direct sequence spread spectrum radio (DSSS) in the 2.4 GHz band
- Frequency hopping spread spectrum radio (FHSS) in the 2.4 GHz band
- Infrared light (IR)

Παρόλο που το 802.11 ορίζει την IR τεχνολογία, ουσιαστικά αυτή δεν χρησιμοποιήθηκε ποτέ και θεωρείται απαρχαιωμένη [19].

Συσκευές 802.11 μπορούσαν να επικοινωνούν μεταξύ τους ή με ένα access point, το οποίο με τη σειρά του συνδεόταν σε ένα ενσύρματο τοπικό δίκτυο, με ρυθμούς μετάδοσης 1Mbps και, προαιρετικά, 2Mbps.

Για την αντιμετώπιση ζητημάτων ασφάλειας χρησιμοποιήθηκε το Wired Equivalent Privacy (WEP).

802.11a

Το 802.11a δημοσιεύθηκε το 1999 και ήταν το δεύτερο πρότυπο της οικογένειας 802.11. Όμως, προϊόντα 802.11a δεν κυκλοφόρησαν στην αγορά πριν από τα τέλη του 2001 [1].

Λειτουργεί στα 5GHz και παρέχει ρυθμούς μετάδοσης 6, 12, 24Mbps, υποχρεωτικά, και 9, 18, 36, 48, 54Mbps, προαιρετικά [10]. Η τεχνολογία φυσικού επιπέδου που περιγράφει είναι η Orthogonal Frequency Division Multiplexing (OFDM). Προσφέρει 12 μη αλληλεπικαλυπτόμενα κανάλια με 20MHz εύρος το καθένα. Έτσι παρέχει μεγαλύτερη χωρητικότητα και αποτελεί καλύτερη επιλογή από το 802.11b/g για ένα περιβάλλον με πολλούς χρήστες και εφαρμογές με υψηλές απαιτήσεις [7]. Επίσης, οι χρήστες ενός 802.11a δικτύου θα έχουν υψηλότερα επίπεδα απόδοσης καθώς η ζώνη των 5GHz δεν είναι τόσο φορτωμένη όσο αυτή των 2.4Ghz, που χρησιμοποιεί το 802.11b. Πολλές συσκευές, όπως ασύρματα τηλέφωνα και φούρνοι μικροκυμάτων, λειτουργούν στα 2.4Ghz με αποτέλεσμα να παρεμβάλλονται στα 802.11b δίκτυα, που βρίσκονται στον ίδιο χώρο, ελαττώνοντας έτσι την απόδοση των τελευταίων.

Ένα μειονέκτημα του 802.11a είναι το ότι δεν είναι συμβατό με το αρχικό 802.11 και με το 802.11b. Αυτό συμβαίνει γιατί λειτουργούν σε διαφορετικές συχνότητες αλλά και γιατί χρησιμοποιούν διαφορετικές τεχνολογίες. Ωστόσο, αυτό το πρόβλημα αντιμετωπίζεται πλέον με τη χρήση καρτών πολλαπλών καταστάσεων (multimode radio cards) που υλοποιούν και το 802.11a και το 802.11b. Το καλό βέβαια είναι ότι 802.11a κάρτες μπορούν να συνυπάρχουν στον ίδιο φυσικό χώρο με 802.11 ή 802.11b/g κάρτες λόγω του ότι χρησιμοποιούν διαφορετικές συχνότητες [19].

Ένα άλλο μειονέκτημα του 802.11a είναι το περιορισμένο εύρος που προσφέρει, καθώς αυτό δεν ξεπερνά τα 30 μέτρα, στις περισσότερες περιπτώσεις. Αυτό οφείλεται στις υψηλές συχνότητες στις οποίες μεταδίδει [7].

802.11b

Το 802.11b πρότυπο δημοσιεύθηκε το 1999 με στόχο να ξεπεράσει τους μειονεκτικούς ρυθμούς μετάδοσης του αρχικού 802.11. Λειτουργεί στα 2.4GHz και χρησιμοποιεί την τεχνολογία Direct Sequence Spread Spectrum (DSSS). Εκδόθηκε την ίδια χρονική περίοδο με το 802.11a αλλά λόγω της εξέλιξης που υπήρχε ήδη στα 2.4GHz τα προϊόντα βγήκαν στην αγορά πριν από αυτά του 802.11a. Εξαιτίας αυτού, αλλά και λόγω συμβατότητας με το 802.11 αποτελεί το πιο δημοφιλές πρότυπο ασύρματων τοπικών δικτύων.

Υποστηρίζει ταχύτητες 1, 2, 5.5 και 11Mbps και μπορεί να καλύψει περίπου 90 μέτρα στις περισσότερες εσωτερικές εγκαταστάσεις [7]. Οι ρυθμοί μετάδοσης 5.5 και 11Mbps είναι γνωστοί ως High-Rate DSSS (HR-DSSS) [19].

Ένα μειονέκτημα του 802.11b είναι ότι διαθέτει μόνο τρία μη επικαλυπτόμενα κανάλια στα 2.4GHz. Το 802.11 πρότυπο ορίζει 14 κανάλια για τη ρύθμιση σημείων πρόσβασης (access points, APs) αλλά οι περισσότερες εταιρίες χρησιμοποιούν μόνο τα κανάλια 1, 6 και 11 για να είναι σίγουρες ότι τα APs δεν θα παρεμβάλλονται το ένα στο άλλο. Αυτό περιορίζει τη συνολική χωρητικότητα του 802.11b και το κάνει κατάλληλο μόνο για εφαρμογές μέτριων απαιτήσεων, όπως η ηλεκτρονική αλληλογραφία και η περιήγηση στο διαδίκτυο [7]. Ωστόσο, μπορούν να χρησιμοποιηθούν και τα άλλα κανάλια αλλά θα υπάρχουν επικαλύψεις που θα επηρεάζουν την απόδοση.

Ένα άλλο μειονέκτημα του 802.11b είναι ότι δέχεται παρεμβολές από άλλες συσκευές που λειτουργούν στη συχνότητα των 2.4GHz, όπως τα ασύρματα τηλέφωνα και οι φούρνοι μικροκυμάτων.

802.11g

Το 802.11g προτυποποιήθηκε το 2003. Προσφέρει ταχύτητες μέχρι 54Mbps χρησιμοποιώντας την τεχνολογία OFDM και λειτουργεί στα 2.4GHz. Εκτός από την OFDM τεχνολογία, υποστηρίζει και την DSSS [19]. Το γεγονός ότι εκπέμπει στη συγκεκριμένη ζώνη συχνοτήτων αλλά και το ότι υποστηρίζει

και την DSSS τεχνολογία, το κάνει απόλυτα συμβατό με το 802.11b και το 802.11 DSSS [1].

Η συμβατότητα του 802.11g με το 802.11b αποτελεί το μεγαλύτερο πλεονέκτημά του καθώς η αναβάθμιση ενός 802.11b δικτύου σε 802.11g είναι απλή αλλά και μία εταιρεία που έχει εγκατεστημένα 802.11b APs μπορεί να φιλοξενήσει και 802.11g χρήστες (ισχύει και το αντίστροφο). Ωστόσο, οι 802.11g χρήστες θα περιοριστούν στους χαμηλότερους ρυθμούς μετάδοσης του 802.11b. Επιπλέον, οι παρεμβολές που εμφανίζονται στο 802.11b από άλλες συσκευές παρουσιάζονται και στο 802.11g λόγω του ότι εκπέμπουν στα 2.4GHz.

802.11e

Το 802.11e ανακοινώθηκε το 2005 και ορίζει βελτιωμένες μεθόδους πρόσβασης στο μέσο για να υποστηρίξει απαιτήσεις Quality-of-Service (QoS). Βελτιώνει την αποδοτικότητα, έτσι ώστε να είναι δυνατή η εκτέλεση χρονικά ευαίσθητων εφαρμογών, όπως VoIP και βίντεο, σε ένα 802.11 δίκτυο.

Ο Wi-Fi Alliance έχει και ένα πιστοποιητικό γνωστό ως Wi-Fi Multimedia (WMM), το οποίο αποτέλεσε ένα προσωρινό πρότυπο προτού ολοκληρωθεί το 802.11e. Το WMM ορίζει την προτεραιότητα της κίνησης σε τέσσερις κατηγορίες πρόσβασης με διαφορετικούς βαθμούς σπουδαιότητας [19].

802.11d

Το αρχικό 802.11 πρότυπο ήταν συμβατό με τις ρυθμιστικές αρχές των Ηνωμένων Πολιτειών, του Καναδά και της Ευρώπης. Οι κανονισμοί άλλων χωρών μπορεί να ορίζουν διαφορετικά όρια στις επιτρεπόμενες συχνότητες και την ισχύ μετάδοσης. Η 802.11d τροποποίηση, που δημοσιεύθηκε το 2001, προσέθεσε τις απαραίτητες απαιτήσεις και ορισμούς έτσι ώστε να επιτρέπει σε 802.11 εξοπλισμό να λειτουργεί σε περιοχές που δεν καλύπτονταν από το αρχικό 802.11 πρότυπο [19].

802.11F

Το 802.11F αποτελεί μια προσπάθεια προτυποποίησης του τρόπου μετάβασης των σταθμών από ένα AP σε ένα άλλο. Προτείνει τη χρήση του Inter-Access Point Protocol (IAPP) το οποίο παρέχει τις δυνατότητες για επικοινωνία ανάμεσα σε APs διαφορετικών κατασκευαστών σε ένα κατανεμημένο σύστημα (distribution system). Το κεφαλαίο F δηλώνει ότι δεν πρόκειται για ένα πρότυπο αλλά για μία συνιστώμενη πρακτική.

802.11i

Αρχικά, το 802.11 χρησιμοποιούσε για κρυπτογράφηση το WEP, το οποίο αρκετά γρήγορα παραβιάστηκε. Το 802.11i, που επικυρώθηκε και δημοσιεύθηκε το 2004, βελτιώνει κι ενισχύει τους μηχανισμούς ασφάλειας ορίζοντας ισχυρότερες και καλύτερες μεθόδους κρυπτογράφησης και πιστοποίησης. Μέχρι την ολοκλήρωση του 802.11i, ο Wi-Fi Alliance είχε ανακοινώσει μία πιστοποίηση γνωστή ως Wi-Fi Protected Access (WPA), η οποία ήταν ένα υποσύνολο του 802.11i. Τώρα υπάρχει πλέον και το WAP2 το οποίο είναι απόλυτα συμβατό με το 802.11i [19].

802.11h

Σκοπός αυτού του προτύπου, η δημοσίευση του οποίου έγινε το 2003, είναι η αποδοχή του 802.11a από τις ρυθμιστικές αρχές της Ευρώπης, όπου η ζώνη συχνοτήτων των 5GHz χρησιμοποιείται από τα ραντάρ.

Το 802.11h ορίζει έναν μηχανισμό δυναμικής επιλογής συχνότητας (dynamic frequency selection, DFS) και έναν μηχανισμό ελέγχου της ισχύος μετάδοσης (transmit power control, TPC) [19].

Αν και η τροποποίηση 802.11h αρχικά επικυρώθηκε για να διευθετήσει τη συμβατότητα με τις ευρωπαϊκές ρυθμιστικές αρχές στα 5GHz, πολλοί κατασκευαστές εφαρμόζουν υπηρεσίες TPC και DFS ακόμα και σε κάρτες που λειτουργούν στα 2.4GHz [19].

802.11j

Το 802.11j παρέχει κάποιες βελτιώσεις στο 802.11 MAC και στο φυσικό επίπεδο του 802.11a για να συμβαδίζει με τις Ιαπωνικές ρυθμιστικές αρχές και να μπορεί να λειτουργεί στις ζώνες των 4.9GHz και 5GHz αυτής της χώρας. Η δημοσίευσή του έγινε το 2005 [15].

802.11k

Είναι ένα πρότυπο που επιτρέπει στους σταθμούς να συλλέγουν πληροφορίες για το μέσο και να τις μεταδίδουν στα APs για επεξεργασία. Σε κάποιες περιπτώσεις βέβαια μπορεί και οι σταθμοί να ζητήσουν τις επεξεργασμένες πληροφορίες από τα APs. Μερικές από τις μετρήσεις που ορίζει το 802.11k είναι οι εξής: Transmit power control (TPC), πληροφορίες φυσικού επιπέδου όπως λόγος σήματος προς θόρυβο, ισχύς του σήματος, ρυθμοί μετάδοσης, πληροφορίες του MAC επιπέδου όπως μετάδοση πλαισίων, επαναλήψεις προσπάθειας μετάδοσης, σφάλματα κ.ά. Το 802.11k δημοσιεύθηκε το 2008 και σε συνδυασμό με το 802.11r “fast roaming” έχει τη δυνατότητα να βελτιώσει την περιήγηση σε ένα 802.11 ασύρματο δίκτυο [19].

802.11n

Στις 11 Σεπτεμβρίου 2009 η IEEE ανακοίνωσε την επικύρωση του 802.11n προτύπου. Το πρότυπο αυτό λειτουργεί και στα 2.4GHz και στα 5GHz. Χρησιμοποιεί την τεχνολογία πολλαπλών εισόδων-πολλαπλών εξόδων (multiple-input-multiple-output, MIMO) σε συνδυασμό με την OFDM για να επιτύχει ρυθμούς μετάδοσης έως και 450Mbps [19][46].

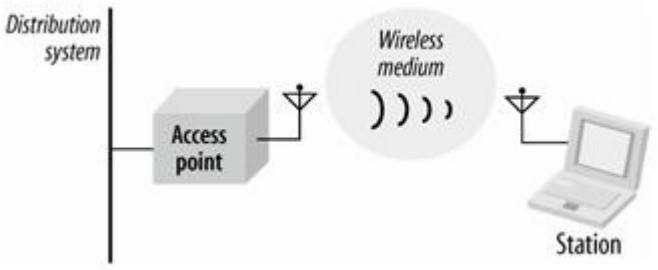
802.11r

Όταν ένας σταθμός κινείται από ένα AP σε ένα άλλο χρειάζεται κάποιος χρόνος προκειμένου να λάβει χώρα η διαδικασία πιστοποίησης με το νέο AP. Το 802.11r παρέχει βελτιώσεις που μειώνουν αυτό το χρονικό διάστημα κι έτσι μπορούν να υποστηριχθούν εφαρμογές με QoS απαιτήσεις, όπως το VoIP. Η προδιαγραφή αυτή, που είναι γνωστή και ως “fast roaming” (γρήγορη περιήγηση), δημοσιεύθηκε το 2008 [34].

Πέρα από τα πρότυπα που περιγράφηκαν παραπάνω, υπάρχουν και άλλα σε ανάπτυξη τα οποία αναμένεται να δημοσιευθούν σύντομα. Μερικά από αυτά είναι τα εξής: 802.11s (φιλοδοξεί να παρέχει ασύρματη πρόσβαση στο διαδίκτυο σε ολόκληρες πόλεις), 802.11p (θα καλύπτει την ανάγκη για γρήγορη περιήγηση των οχημάτων από κυψέλη σε κυψέλη), 802.11T (για τη μέτρηση της απόδοσης 802.11 ασύρματου δικτυακού εξοπλισμού), 802.11u (δυνατότητα συνεργασίας του 802.11 με άλλες τεχνολογίες δικτύων όπως τα δίκτυα WiMAX) κ.ά.

1.5 Συστατικά ενός 802.11 δικτύου

Τα 802.11 δίκτυα αποτελούνται από τέσσερα βασικά συστατικά, τους ασύρματους σταθμούς, τους σταθμούς βάσης, το ασύρματο μέσο μετάδοσης και το σύστημα διανομής. Η εικόνα 1.1 δείχνει τη σχέση ανάμεσα σε αυτά τα συστατικά.



Εικόνα 1.1 Συστατικά ενός ασύρματου δικτύου [1]

1.5.1 Ασύρματοι σταθμοί

Οι ασύρματοι σταθμοί είναι υπολογιστικές συσκευές που διαθέτουν μία ασύρματη κάρτα δικτύου (WNIC). Συνήθως πρόκειται για φορητούς υπολογιστές (laptops) ή για PDAs. Πέρα όμως από τα laptops και τα PDAs, σε ένα ασύρματο δίκτυο μπορεί να συνδεθεί και οποιαδήποτε άλλη υπολογιστική μηχανή, όπως ένας επιτραπέζιος υπολογιστής ή ένας εκτυπωτής, αρκεί, όπως αναφέρθηκε και παραπάνω, να διαθέτουν μία ασύρματη κάρτα δικτύου.

Επίσης κάθε συσκευή χρειάζεται λογισμικό για ν' αντιλαμβάνεται την ύπαρξη του ασύρματου δικτύου. Σε κάποιες περιπτώσεις, το λειτουργικό σύστημα έχει ενσωματωμένα χαρακτηριστικά που βελτιώνουν τα ασύρματα δίκτυα. Για παράδειγμα, τα Windows XP έχουν την ικανότητα να αναγνωρίζουν και να συσχετίζονται αυτόματα με WLANs [7].

1.5.2 Σταθμοί βάσης (Access Points, APs)

Ένα AP αποτελεί το κεντρικό σημείο σύνδεσης σε ένα WLAN τύπου infrastructure. Είναι η συσκευή που δίνει τη δυνατότητα στους ασύρματους σταθμούς να επικοινωνήσουν μεταξύ τους. Κάθε επικοινωνία σε ένα Infrastructure BSS γίνεται υποχρεωτικά μέσω ενός AP. Επιπλέον, τα APs συνήθως συνδέονται σε ένα δίκτυο κορμού – σε ένα Ethernet κατά κύριο λόγο – και λειτουργούν ως γέφυρες ανάμεσα στο ενσύρματο και το ασύρματο δίκτυο. Έτσι, οι ασύρματοι σταθμοί μπορούν να έχουν πρόσβαση σε ένα πλήθος από δικτυακές υπηρεσίες όπως είναι ο παγκόσμιος ιστός, η ηλεκτρονική αλληλογραφία και εφαρμογές βάσεων δεδομένων. Ένα AP μπορεί να επικοινωνεί με πολλούς σταθμούς αλλά κάθε σταθμός μπορεί να είναι συνδεδεμένος με ένα AP κάθε φορά. Πολλά APs μπορούν να συνδεθούν μαζί επεκτείνοντας έτσι το WLAN και επιτρέποντας την περιαγωγή (roaming) σε ένα μεγάλο συγκρότημα, για παράδειγμα σε ένα πανεπιστήμιο. Αυτό επιτυγχάνεται χάρη στη δυνατότητα που έχουν τα APs να παρακολουθούν τις μετακινήσεις των σταθμών και να επικοινωνούν μεταξύ τους ανταλλάσσοντας πληροφορίες για τη θέση των ασύρματων σταθμών σε κάθε χρονική στιγμή.

Κάθε AP διαθέτει μία NIC για να συνδεθεί στο ενσύρματο δίκτυο κορμού και μία WNIC για να επικοινωνεί με τους χρήστες του ασύρματου δικτύου. Για να είναι δυνατή αυτή η τελευταία επικοινωνία πρέπει η WNIC του AP και αυτές των ασύρματων σταθμών να υλοποιούν το ίδιο πρότυπο. Υπάρχουν βέβαια και dual-mode APs που υποστηρίζουν δύο ή και περισσότερα πρότυπα [23].

1.5.3 Ασύρματο μέσο μετάδοσης

Το μέσο που χρησιμοποιείται για τη μετάδοση πακέτων στα ασύρματα δίκτυα είναι ο αέρας. Το 802.11 έχει ορίσει διάφορες τεχνολογίες φυσικού επιπέδου. Αρχικά είχαν προτυποποιηθεί δύο τεχνολογίες ραδιοκυμάτων, οι

DSSS και FHSS, στα 2.4GHz και μία τεχνολογία υπέρυθρων (IR). Μετά ακολούθησε και μία τεχνολογία που μπορούσε να μεταδώσει στα 5GHz και να επιτύχει υψηλότερους ρυθμούς μετάδοσης, η OFDM.

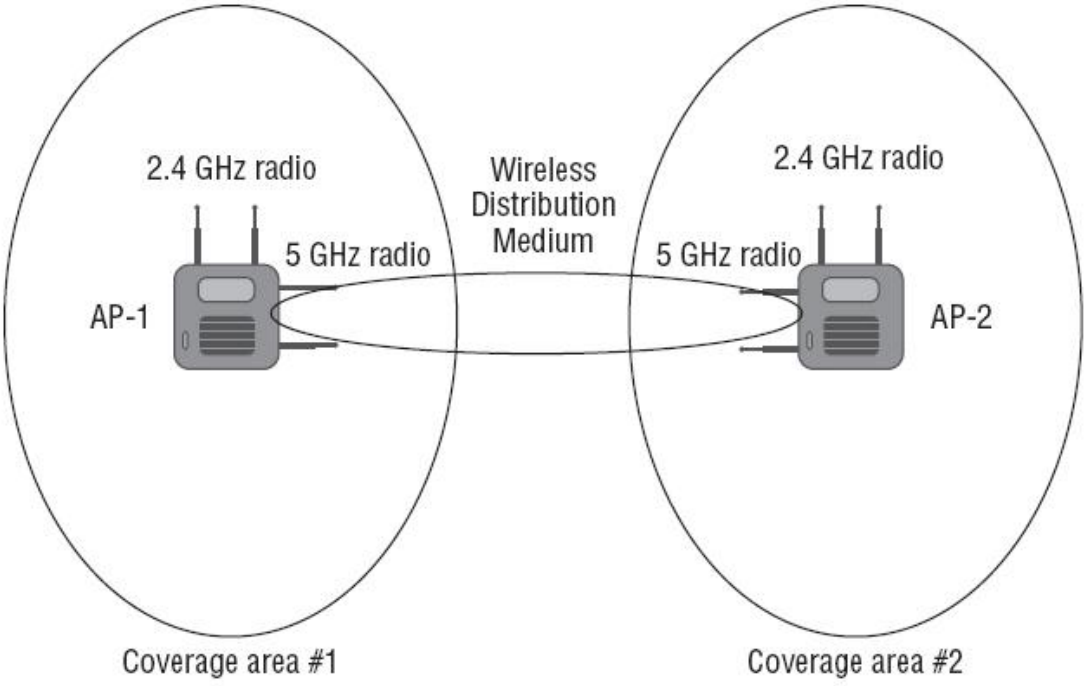
Η ποιότητα της μετάδοσης εξαρτάται από τα εμπόδια που βρίσκονται στο περιβάλλον ενός ασύρματου δικτύου και τα οποία είτε ελαττώνουν την ισχύ του σήματος είτε του προκαλούν διασπορά [7].

1.5.4 Σύστημα διανομής (Distribution System, DS)

Σε μία τοπολογία Infrastructure BSS, πολλά APs μπορούν να συνδεθούν σε ένα κοινό DS για να καλύψουν μία ευρεία περιοχή, δίνοντας στους ασύρματους σταθμούς τη δυνατότητα να μετακινούνται από το ένα BSS στο άλλο χωρίς να χάνουν τη συνδεσιμότητά τους. Το DS είναι το συστατικό του 802.11 που χρησιμοποιείται για την προώθηση των πλαισίων στον προορισμό τους. Το DS αποτελείται από μία γέφυρα, η οποία βρίσκεται εντός του AP και από ένα δίκτυο κορμού (backbone network), που χρησιμοποιείται για τη μετάδοση των πλαισίων ανάμεσα στα APs. Το 802.11 δεν ορίζει κάποια συγκεκριμένη τεχνολογία για το δίκτυο κορμού αλλά αυτό που χρησιμοποιείται συνήθως είναι ένα 802.3 Ethernet. Όταν ένα πλαίσιο φτάνει στο DS, παραδίδεται στο σωστό AP και κατόπιν μεταδίδεται από το AP στον σταθμό παραλήπτη. Για να γίνει αυτό, το DS πρέπει να γνωρίζει τη φυσική θέση κάθε ασύρματου σταθμού. Αυτή η γνώση βρίσκεται μέσα στα APs χάρη στη λειτουργία γεφύρωσης που υλοποιούν. Όλα τα APs πρέπει να γνωρίζουν ποιοι σταθμοί συσχετίζονται με ποιο AP για να μπορούν να προωθούν κατάλληλα τα πλαίσια που λαμβάνουν. Σε ένα ασύρματο δίκτυο όπου οι σταθμοί μετακινούνται συνεχώς, αλλάζοντας συσχετίσεις, τα APs πρέπει να ενημερώνονται μεταξύ τους για τις νέες θέσεις των σταθμών. Αυτό γίνεται με τη βοήθεια ενός Inter Access Point Protocol (IAPP). Το IAPP πρότυπο της IEEE είναι το 802.11F.

Όπως αναφέρθηκε και παραπάνω, το 802.11 δεν περιορίζεται σε μία συγκεκριμένη τεχνολογία δικτύου κορμού. Έτσι, εκτός από ένα ενσύρματο δίκτυο μπορεί να χρησιμοποιηθεί και ένα ασύρματο DS (WDS) για τη σύνδεση των APs. Ένα WDS μπορεί να λειτουργήσει με APs τα οποία μπορεί να

χρησιμοποιούν ένα ή δύο 802.11 κανάλια. Στην πρώτη περίπτωση η επικοινωνία των APs με τους σταθμούς αλλά και η μεταξύ τους επικοινωνία γίνεται μέσω της ίδιας συχνότητας. Ένα μειονέκτημα αυτής της επιλογής είναι η μείωση της απόδοσης καθώς, λόγω της half-duplex φύσης του μέσου, ένα AP δεν μπορεί να επικοινωνεί με ένα σταθμό και ένα άλλο AP την ίδια στιγμή. Στην περίπτωση όμως των APs διπλής κατάστασης, μπορεί να χρησιμοποιηθεί μία συχνότητα για την επικοινωνία με τους σταθμούς και μία διαφορετική για την επικοινωνία μεταξύ των APs, όπως φαίνεται και στην εικόνα 1.2. Έτσι, οι δύο αυτές επικοινωνίες μπορούν να λαμβάνουν χώρα την ίδια χρονική στιγμή χωρίς να επηρεάζουν την απόδοση του δικτύου [19].



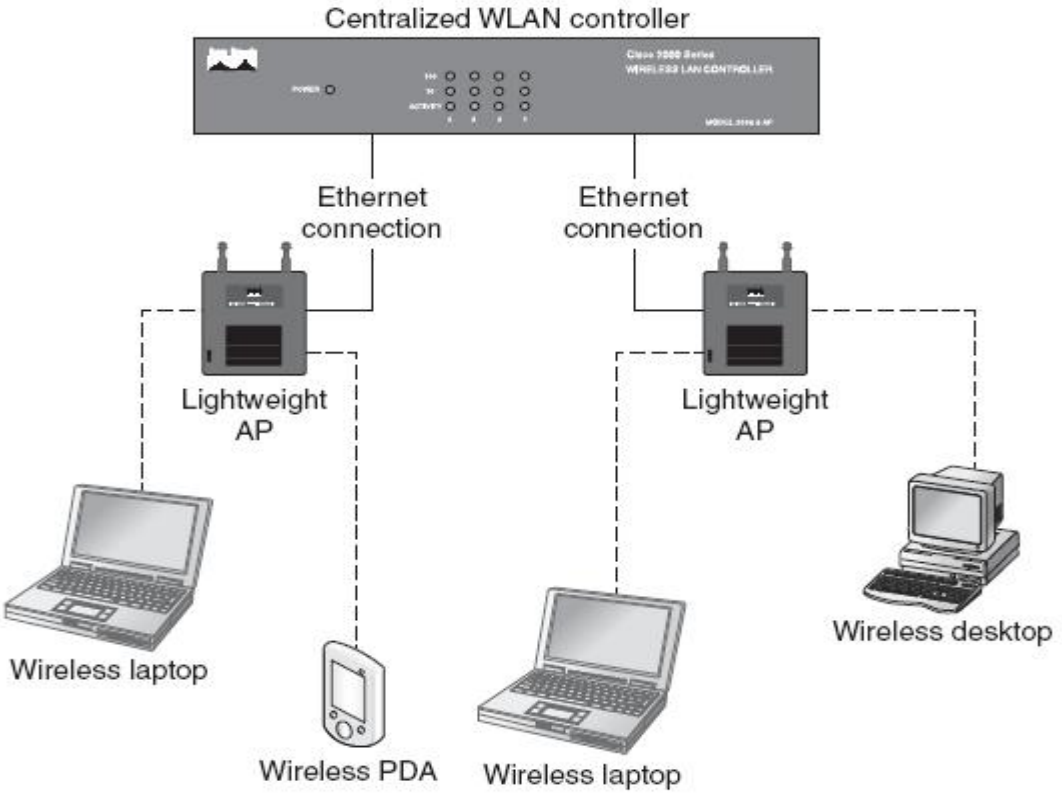
Εικόνα 1.2 Ασύρματο μέσο διανομής [19]

1.5.5 Άλλες συσκευές

Πέρα από τα βασικά συστατικά που περιγράφηκαν παραπάνω υπάρχουν και κάποιες συσκευές οι οποίες ενισχύουν τη λειτουργία των ασύρματων LANs.

Μία από τις συσκευές αυτές είναι οι ασύρματοι ελεγκτές πρόσβασης (WLAN access controllers). Οι συσκευές αυτές βελτιώνουν τα WLANs σε θέματα ασφάλειας, QoS και περιαγωγής. Συνήθως, είναι υλικό το οποίο

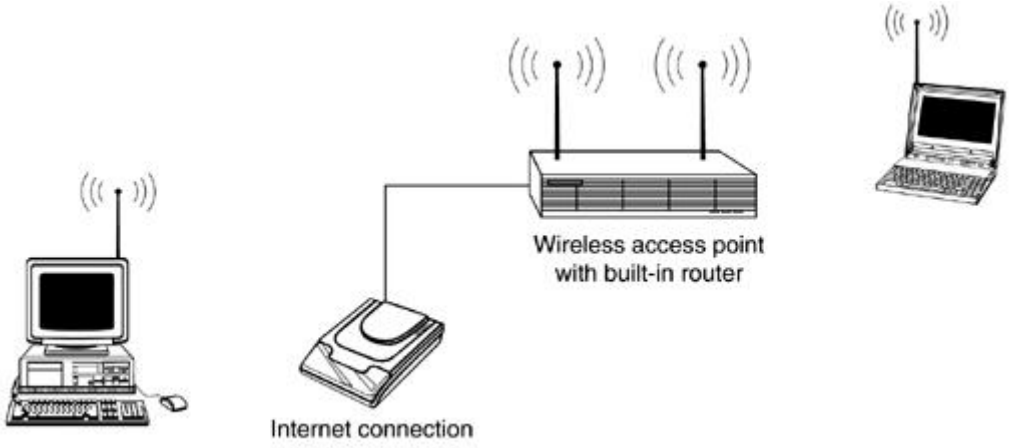
βρίσκεται ανάμεσα στο AP και στην προστατευόμενη ενσύρματη πλευρά του δικτύου και ρυθμίζει την κίνηση ανάμεσα στο ασύρματο δίκτυο και σε σημαντικούς πόρους. Σε κάποιες περιπτώσεις όμως, η λειτουργία ελέγχου πρόσβασης βρίσκεται μέσα στο ίδιο το AP. Όμως, αυτά τα έξυπνα APs είναι πιο ακριβά από αυτά που απλά υλοποιούν το 802.11 πρότυπο και τίποτε παραπάνω (αυτά τα τελευταία APs είναι γνωστά ως “thin” APs). Έτσι, πολλοί προτιμούν να χρησιμοποιούν έναν access controller, ο οποίος συγκεντρώνει όλες τις λειτουργίες ελέγχου πρόσβασης, σε συνδυασμό με οικονομικά thin APs. Οι λειτουργίες που υλοποιούν οι access controllers είναι: πιστοποίηση, κρυπτογράφηση, διαχείριση του εύρους ζώνης και περιαγωγή [7]. Στην εικόνα 1.3 φαίνεται ένα δίκτυο που χρησιμοποιεί έναν κεντρικό ελεγκτή και δύο thin APs.



Εικόνα 1.3 WLAN access controller [15]

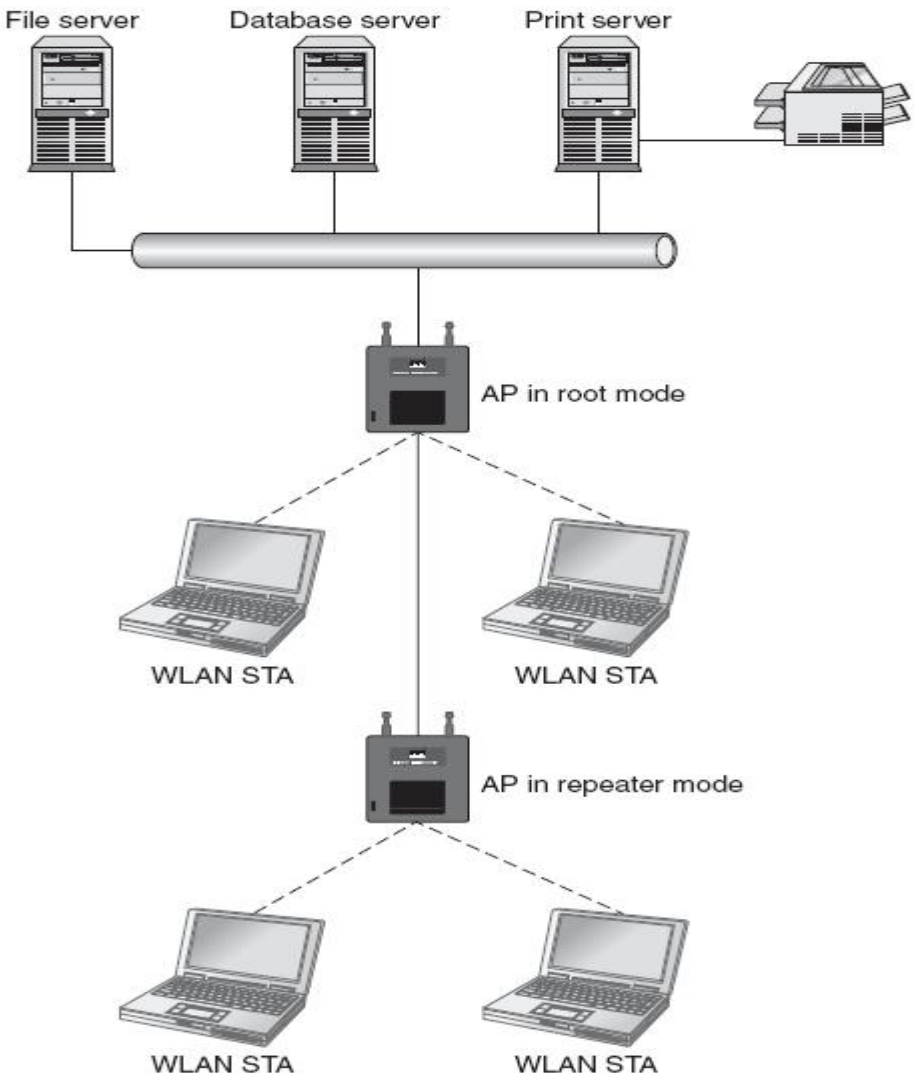
Μία άλλη συσκευή που χρησιμοποιείται σε WLANs είναι ο ασύρματος δρομολογητής (WLAN router). Ένας WLAN router ενσωματώνει μία λειτουργία

access point σε έναν Ethernet δρομολογητή. Αποτελούν μια καλή λύση για ένα WLAN ενός σπιτιού ή μικρού γραφείου όπου πολλές δικτυακές συσκευές μοιράζονται μία IP διεύθυνση. Αντί να υπάρχει μία συσκευή για τον δρομολογητή και μία άλλη για το AP μπορεί να χρησιμοποιηθεί ένας ασύρματος δρομολογητής που περιλαμβάνει και τις δύο λειτουργίες, όπως αυτός της εικόνας 1.4.



Εικόνα 1.4 Χρήση ενός AP/router για σύνδεση στο internet [24]

Επίσης, οι ασύρματοι επαναλήπτες (WLAN repeaters) μπορούν να χρησιμοποιηθούν εναλλακτικά για να επεκτείνουν ένα WLAN αντί να προστεθούν επιπλέον APs. Υπάρχουν αρκετοί αυτόνομοι WLAN repeaters αλλά συνήθως τα APs έχουν ενσωματωμένη μία κατάσταση επαναλήπτη. Όταν όμως τεθούν σε αυτή την κατάσταση, λειτουργούν ως επαναλήπτες και όχι ως APs. Το δίκτυο της εικόνας 1.5 χρησιμοποιεί ένα AP το οποίο λειτουργεί κανονικά ως AP και ένα άλλο το οποίο λειτουργεί ως επαναλήπτης. Με τη χρήση αυτόνομων ασύρματων επαναληπτών τα οφέλη είναι οικονομικά καθώς είναι πιο φθηνοί από τα APs. Το μειονέκτημα από την χρήση επαναληπτών γενικά είναι η μείωση της απόδοσης, αφού κάθε σήμα που λαμβάνουν θα πρέπει να το αναμεταδώσουν με αποτέλεσμα να διπλασιάζεται η κίνηση στο μέσο. Γι’ αυτό καλό είναι να αποφεύγεται η χρήση πολλών επαναληπτών σε ένα WLAN.



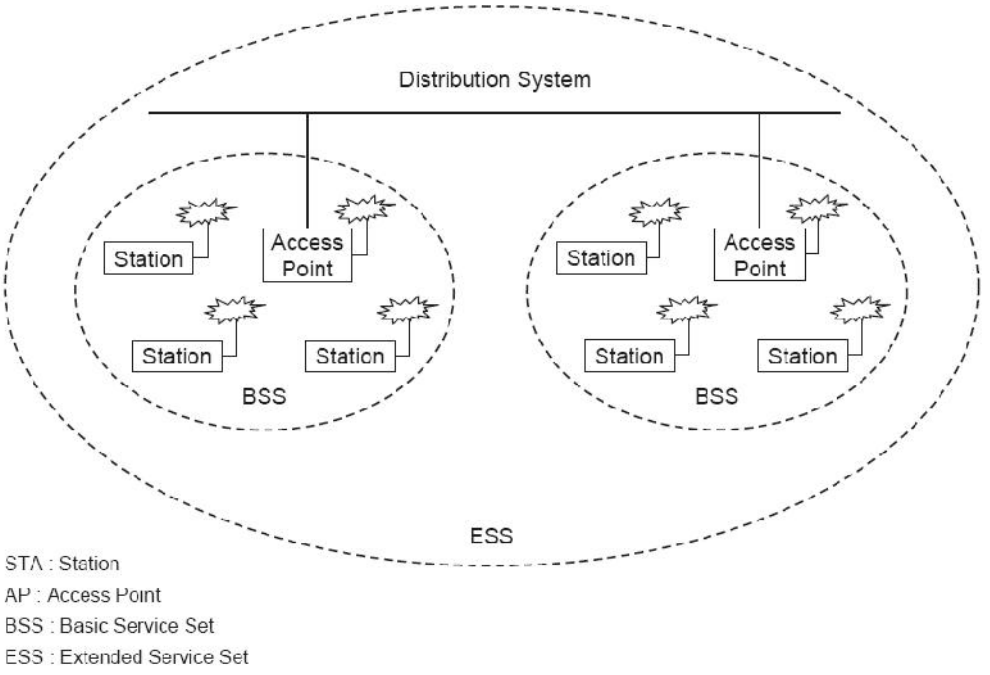
Εικόνα 1.5 Χρήση ενός AP ως επαναλήπτη [15]

Τέλος, για τη σύνδεση δύο διαφορετικών δικτύων μία λύση είναι να χρησιμοποιηθούν ασύρματες γέφυρες (wireless bridges). Ένα AP συνδέει πολλούς σταθμούς σε ένα δίκτυο αλλά όχι ένα δίκτυο σε ένα άλλο. Αντίθετα οι γέφυρες συνδέουν δίκτυα και συχνά είναι πιο φθηνές από τα APs. Μία συσκευή, στην οποία δεν γίνεται να προστεθεί μία WNIC, μπορεί να συνδεθεί σε ένα WLAN, μέσω μιας θύρας Ethernet, με μία Ethernet-to-Wireless γέφυρα. Υπάρχουν επίσης ασύρματες γέφυρες τύπου workgroup οι οποίες συνδέουν ασύρματα δίκτυα σε μεγαλύτερα Ethernet δίκτυα. Ουσιαστικά μια workgroup γέφυρα ενεργεί ως ασύρματος πελάτης στο ασύρματο LAN και διασυνδέεται μετά σε ένα ενσύρματο δίκτυο. Η ενσύρματη πλευρά της μπορεί να συνδεθεί άμεσα με μια συσκευή ή με ένα Ethernet hub ή switch που

συνδέουν πολλές συσκευές. Τέλος, κάποιοι κατασκευαστές προσφέρουν APs που μπορούν να ρυθμιστούν ώστε να λειτουργούν ως γέφυρες (δεν μπορούν όμως παράλληλα να λειτουργούν και ως APs) [37].

1.6 Αρχιτεκτονική 802.11 δικτύων

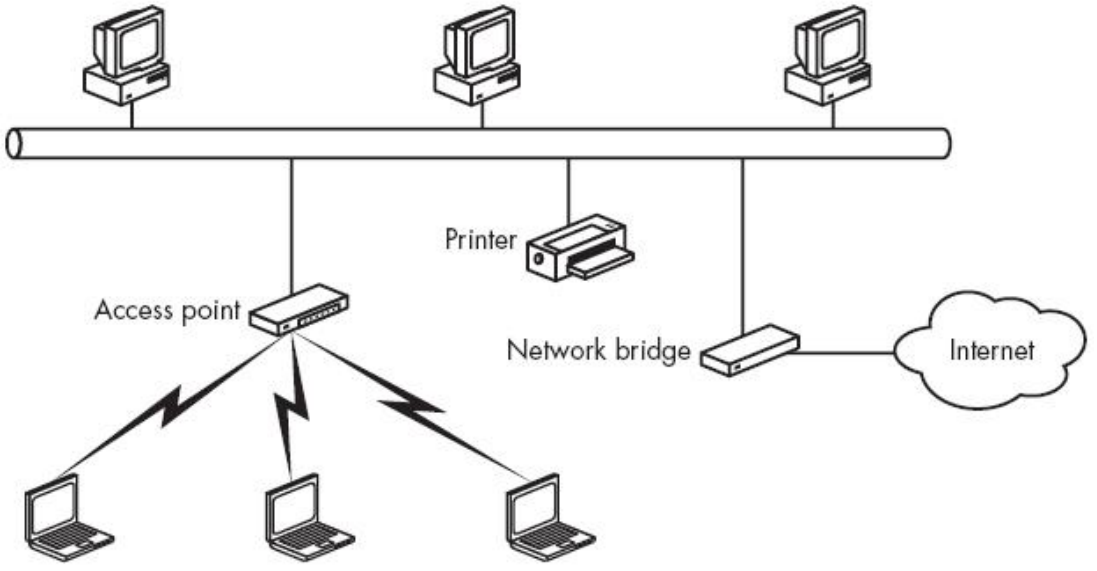
Στα 802.11 δίκτυα ένα σύνολο από, τουλάχιστον, δύο σταθμούς που επικοινωνούν ονομάζεται Basic Service Set (BSS). Η έκταση που καλύπτει το BSS, δηλαδή η φυσική περιοχή στην οποία λαμβάνουν χώρα οι επικοινωνίες, είναι γνωστή ως Basic Service Area (BSA). Το μέγεθος και το σχήμα μίας BSA εξαρτάται από πολλές συνιστώσες όπως η ισχύς με την οποία μεταδίδει το AP και ο φυσικός περιβάλλοντας χώρος. Επειδή ο περιβάλλοντας χώρος αλλάζει συχνά, η BSA είναι ευμετάβλητη [19]. Το 802.11 ορίζει δύο διαφορετικές BSS τοπολογίες, την Independent BSS (IBSS) και την Infrastructure BSS. Με τη σύνδεση πολλών Infrastructure BSSs σε ένα δίκτυο κορμού προκύπτει άλλη μία τοπολογία, η Extended Service Set (ESS). Στην εικόνα 1.6 δύο APs σχηματίζουν δύο ξεχωριστά BSS και συνδεόμενα σε ένα δίκτυο κορμού σχηματίζουν μαζί ένα ESS.



Εικόνα 1.6 BSS και ESS τοπολογίες [20]

1.6.1 Infrastructure BSS

Το βασικό χαρακτηριστικό αυτής της τοπολογίας είναι η χρήση ενός κεντρικού κόμβου που ονομάζεται Access Point (AP). Σε ένα τέτοιο δίκτυο, όλες οι επικοινωνίες γίνονται μέσω του AP. Όταν ένας σταθμός θέλει να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, το πλαίσιο αρχικά θα σταλεί στο AP και από το AP στο σταθμό παραλήπτη. Αυτό ισχύει και για την επικοινωνία μεταξύ σταθμών που ανήκουν στο ίδιο BSS. Έτσι, η BSA, σ' αυτά τα δίκτυα, ορίζεται από το εύρος που μπορεί να καλύψει το AP. Οι σταθμοί πρέπει να συσχετίζονται με ένα AP προκειμένου να αποκτήσουν δικτυακές υπηρεσίες. Ένας ασύρματος σταθμός μπορεί να συσχετιστεί μόνο με ένα AP ενώ ένα AP μπορεί να εξυπηρετεί πολλούς ασύρματους σταθμούς, ανάλογα με την επιθυμητή απόδοση. Τυπικά, το AP σε ένα Infrastructure BSS συνδέεται σε ένα σύστημα διανομής, το Distribution System (DS), χωρίς όμως αυτό να είναι απαραίτητο. Στην εικόνα 1.7 ένα AP συνδέει ασύρματα τρεις σταθμούς ενώ παράλληλα ο ίδιος συνδέεται σε ένα δίκτυο κορμού με μια ενσύρματη γραμμή. Οι ασύρματοι σταθμοί μπορούν να έχουν πρόσβαση στους πόρους του ενσύρματου δικτύου καθώς επίσης και στο internet, μέσω του AP.



Εικόνα 1.7 Infrastructure BSS [16]

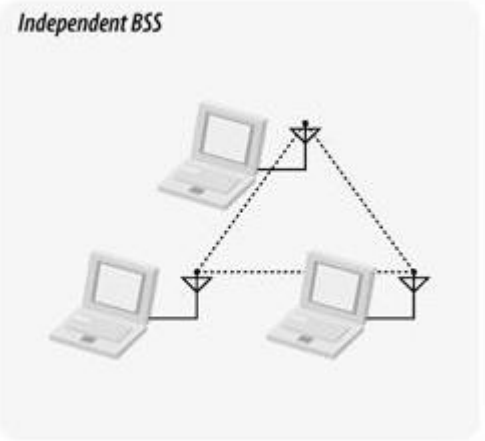
Ένα μεγάλο πλεονέκτημα αυτής της τοπολογίας είναι το ότι το AP συνεργάζεται με τους σταθμούς για την εξοικονόμηση ενέργειας σε αυτούς. Όταν ένα AP διαπιστώνει ότι ένας σταθμός έχει εισέλθει σε κατάσταση εξοικονόμησης ενέργειας, αποθηκεύει τα πλαίσια που προορίζονταν για το

σταθμό αυτό για να του τα στείλει όταν ο τελευταίος ενεργοποιήσει πάλι τον πομποδέκτη του.

Κάθε Infrastructure BSS έχει ένα BSSID το οποίο είναι η MAC διεύθυνση του AP. Το BSSID αποτελεί ένα μοναδικό αναγνωριστικό του Infrastructure BSS και χρησιμοποιείται για λόγους ταυτοποίησης, για δρομολόγηση της κίνησης εντός του BSS αλλά και μεταξύ διαφορετικών BSSs που ανήκουν στο ίδιο ESS. Όταν συνυπάρχουν πολλά BSSs, κάθε ασύρματος σταθμός χρησιμοποιεί το BSSID για να συνδεθεί σε ένα συγκεκριμένο BSS.

1.6.2 Independent BSS (IBSS)

Σε αυτή την τοπολογία οι σταθμοί επικοινωνούν άμεσα μεταξύ τους, χωρίς την μεσολάβηση ενός AP, όπως φαίνεται στην ακόλουθη εικόνα.



Εικόνα 1.8 Independent BSS [1]

Τέτοιου είδους δίκτυα είναι γνωστά και ως ad-hoc ή peer-to-peer δίκτυα. Ένα βασικό τους πλεονέκτημα είναι ότι δεν υπάρχει ένα κεντρικό σημείο αποτυχίας. Αν ένας σταθμός τεθεί εκτός λειτουργίας οι υπόλοιποι δεν επηρεάζονται και συνεχίζουν να επικοινωνούν κανονικά. Χρησιμοποιούνται κυρίως όταν υπάρχει ανάγκη για γρήγορη και εύκολη δημιουργία ενός ασύρματου δικτύου χωρίς να είναι απαραίτητη η πρόσβαση σε πόρους ενός μεγαλύτερου δικτύου κορμού. Το πιο απλό παράδειγμα ενός IBSS δικτύου είναι δύο φορητοί υπολογιστές που θέλουν απλά ν' ανταλλάξουν δεδομένα. Έτσι, στις περισσότερες των περιπτώσεων, ένα IBSS αποτελείται από λίγους

σταθμούς, καλύπτει μία περιορισμένη έκταση και έχει μικρή διάρκεια ζωής. Αν ένας από τους σταθμούς συνδέεται ενσύρματα σε ένα άλλο δίκτυο, μπορεί να παρέχει πρόσβαση στο δίκτυο αυτό και στους υπόλοιπους σταθμούς [27].

Όλοι οι σταθμοί που ανήκουν σε ένα IBSS μοιράζονται το ίδιο SSID ως όνομα δικτύου. Υπάρχει επίσης ένα BSSID το οποίο χρησιμοποιείται για ταυτοποίηση των σταθμών εντός του IBSS. Αυτό το BSSID παράγεται, με τυχαίο τρόπο, από τον πρώτο σταθμό που ξεκινάει το IBSS και έχει τη μορφή μίας διεύθυνσης MAC [19].

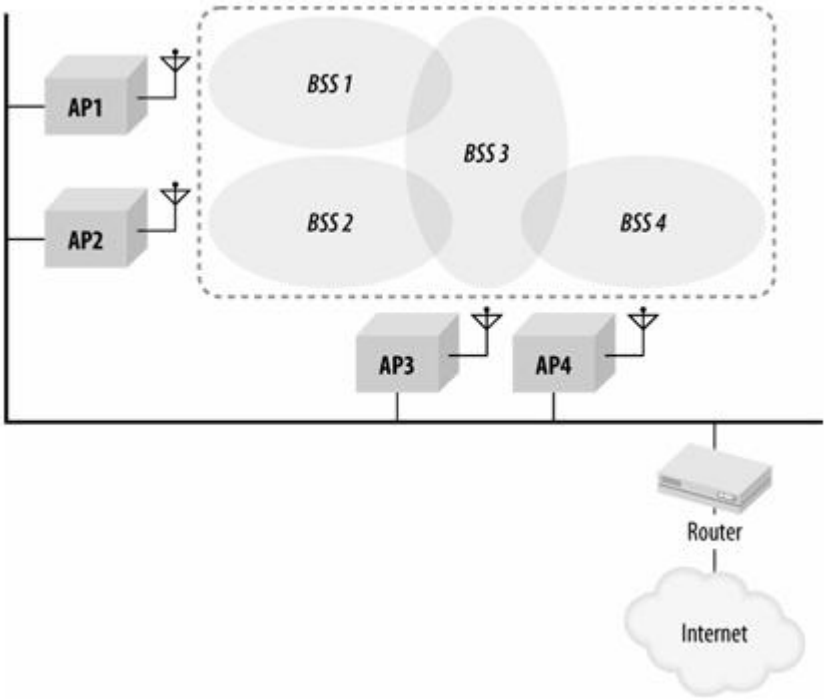
1.6.3 Extended Service Set (ESS)

Πολλά Infrastructure BSSs μπορούν να συνδεθούν σε ένα δίκτυο κορμού σχηματίζοντας ένα ESS. Έτσι δίνεται η δυνατότητα κάλυψης μιας ευρύτερης περιοχής. Παρόλο που το 802.11 δεν ορίζει κάποιο συγκεκριμένο δίκτυο κορμού, στις περισσότερες περιπτώσεις πρόκειται για ένα IEEE 802.3 LAN. Οι σταθμοί που βρίσκονται στα όρια του ίδιου ESS μπορούν να επικοινωνούν μεταξύ τους, ακόμα κι αν ανήκουν σε διαφορετικά BSSs, αλλά και να κινούνται μεταξύ των BSSs αυτών χωρίς να χάνουν τη σύνδεση με το δίκτυο. Κάθε φορά όμως που ένας σταθμός αλλάζει BSS θα πρέπει να αλλάζει και τις συσχετίσεις. Θα πρέπει να συσχετίζεται με το νέο AP του νέου BSS και να διακόπτει τη συσχέτιση με το προηγούμενο AP.

Τα BSSs που ανήκουν σε ένα ESS σχηματίζουν ένα ενιαίο υποδίκτυο. Όλα τα APs σε ένα ESS έχουν το ίδιο Service Set Identifier (SSID), το οποίο χρησιμεύει ως όνομα του δικτύου, και όλοι οι σταθμοί είναι ρυθμισμένοι να χρησιμοποιούν αυτό το SSID όταν συνδέονται στο ασύρματο δίκτυο [1]. Όπως αναφέρθηκε και στην προηγούμενη παράγραφο, κάθε BSS έχει ένα μοναδικό BSSID. Κάθε ασύρματος σταθμός χρησιμοποιεί το BSSID για να συνδεθεί σε ένα συγκεκριμένο BSS. Έτσι, τα APs γνωρίζουν ποιος σταθμός είναι συσχετισμένος με ποιο AP ούτως ώστε να μπορούν να προωθούν κατάλληλα τα δεδομένα από το ένα BSS στο άλλο, εντός του ίδιου ESS.

Συνήθως, σε ένα ESS υπάρχει μερική επικάλυψη των κελιών των APs. Αυτό σημαίνει ότι υπάρχει συνεχής συνδεσιμότητα καθώς οι σταθμοί

μετακινούνται από το ένα BSS στο άλλο. Μπορεί όμως να μην υπάρχει καθόλου επικάλυψη των κελιών. Σε αυτή την περίπτωση, όταν ένας σταθμός αφήνει την περιοχή κάλυψης ενός AP θα χάσει τη σύνδεση με το δίκτυο μέχρι να βρεθεί εντός εμβέλειας ενός άλλου AP όπου θα μπορέσει να επανεγκαθιδρύσει τη σύνδεση. Αυτό το είδος περιαγωγής είναι γνωστό ως “νομαδική περιαγωγή”. Για παράδειγμα, στην εικόνα 1.9, ένας σταθμός από το BSS1 μπορεί να μετακινείται μέσω του BSS3 χωρίς να χάνει τη σύνδεση. Αν όμως μεταβεί κατευθείαν στο BSS1 η σύνδεση του με το δίκτυο θα διακοπεί και θα πρέπει να την αποκαταστήσει. Τέλος, οι περιοχές κάλυψης των APs μπορεί να έχουν απόλυτη επικάλυψη. Αυτή η τοπολογία λέγεται συν-τοποθέτηση (co-location) κι έχει σαν στόχο την αύξηση της χωρητικότητας χρηστών [19].



Εικόνα 1.9 ESS με μερικώς επικαλυπτόμενα BSS [1]

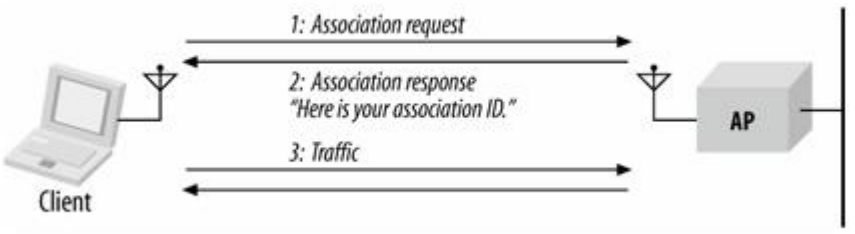
1.7 Υπηρεσίες 802.11 δικτύων

Το 802.11 πρότυπο ορίζει εννιά υπηρεσίες που θα πρέπει να παρέχει ένα WLAN. Οι πέντε από αυτές τις υπηρεσίες είναι υπηρεσίες διανομής και οι υπόλοιπες τέσσερις υπηρεσίες σταθμών. Οι πέντε υπηρεσίες διανομής

παρέχονται από τα APs και δίνουν τη δυνατότητα στο δίκτυο να γνωρίζει τη θέση των ασύρματων σταθμών ούτως ώστε να παραδίδουν τα πλαίσια αναλόγως. Οι υπηρεσίες αυτές είναι οι ακόλουθες.

1.7.1 Συσχέτιση (Association)

Αυτή η υπηρεσία χρησιμοποιείται από τους σταθμούς για να συνδεθούν με ένα AP και ουσιαστικά συμβαίνει τη στιγμή που ο σταθμός θα βρεθεί εντός της εμβέλειας ενός AP. Έτσι, το δίκτυο διανομής αποκτά γνώση σχετικά με τη φυσική θέση των σταθμών μέσα στο δίκτυο, γνώση απαραίτητη για τη σωστή προώθηση και παράδοση των πλαισίων. Τη διαδικασία της συσχέτισης την ξεκινάει πάντα ο σταθμός στέλνοντας ένα πλαίσιο το οποίο περιλαμβάνει στοιχεία όπως υποστηριζόμενοι ρυθμοί μετάδοσης και επιθυμητό SSID. Το AP στη συνέχεια απαντάει με ένα πλαίσιο επιβεβαιώνοντας ή απορρίπτοντας τη συσχέτιση. Η διαδικασία φαίνεται στην εικόνα 1.10. Τέλος, ένας σταθμός μπορεί να είναι συσχετισμένος μόνο με ένα AP κάθε στιγμή, ενώ ένα AP μπορεί να εξυπηρετεί πολλούς σταθμούς.

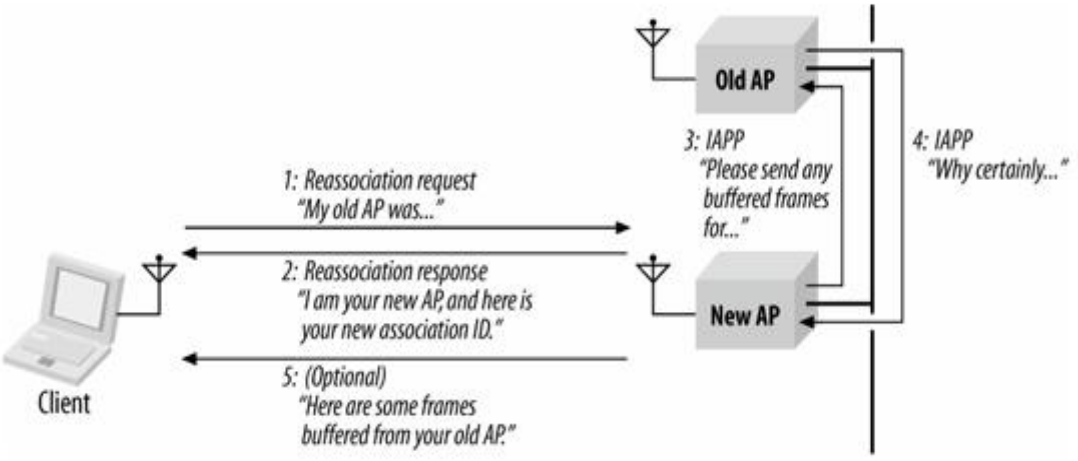


Εικόνα 1.10 διαδικασία συσχέτισης [1]

1.7.2 Επανασυσχέτιση (Reassociation)

Όταν ένας σταθμός μετακινείται από το ένα BSS στο άλλο, μέσα σε ένα ESS, χάνει την επαφή με το AP που ήταν συνδεδεμένο και πρέπει να συνδεθεί με ένα νέο AP. Αυτό γίνεται μέσω της διαδικασίας της επανασυσχέτισης. Πρόκειται για μια υπηρεσία παρόμοια με αυτή της συσχέτισης μόνο που τώρα επιπλέον ο σταθμός παρέχει στο νέο AP πληροφορίες για το AP με το οποίο ήταν συσχετισμένο προηγουμένως. Έτσι, το νέο AP μπορεί να επικοινωνήσει με το προηγούμενο για να μετακινήσει την παλιά συσχέτιση και να ζητήσει πλαίσια που πιθανόν είχαν αποθηκευθεί εκεί

και προορίζονταν για το σταθμό. Επίσης, το DS ενημερώνεται για τις νέες συσχετίσεις. Τα βήματα της διαδικασίας επανασυσχέτισης ακολουθούν τη σειρά που φαίνεται στην εικόνα 1.11. Η υπηρεσία αυτή λέγεται επανασυσχέτιση όχι επειδή ο σταθμός επανασυσχετίζεται με το AP αλλά με το SSID του ασύρματου δικτύου [19].



Εικόνα 1.11 Επανασυσχέτιση [1]

1.7.3 Αποσυσχέτιση (Disassociation)

Με αυτή τη λειτουργία διακόπτεται μία συσχέτιση. Μπορεί να προκληθεί είτε από το AP είτε από τον σταθμό. Ένα AP μπορεί να χρησιμοποιήσει αυτή την υπηρεσία πριν απενεργοποιηθεί για λόγους συντήρησης και ένας σταθμός μπορεί να διακόψει τη σύνδεση με ένα AP όταν πάψει να χρειάζεται τις υπηρεσίες του. Επίσης, όταν ένας σταθμός πρόκειται να αφήσει το δίκτυο θα πρέπει να εκτελεί αυτή τη διαδικασία. Ωστόσο, το MAC είναι σχεδιασμένο να φιλοξενεί σταθμούς οι οποίοι θα εγκαταλείψουν το δίκτυο χωρίς να τερματίσουν επίσημα τη σύνδεση [1]. Η υπηρεσία αυτή είναι μια ειδοποίηση, όχι μία αίτηση, και κανένα από τα δύο μέρη της σχέσης δεν μπορεί να αρνηθεί τον τερματισμό μιας συσχέτισης. Η όλη διαδικασία γίνεται με την αποστολή ενός πλαισίου αποσυσχέτισης από το μέρος που θέλει να τερματίσει τη συσχέτιση.

1.7.4 Διανομή (Distribution)

Πρόκειται για τη βασική υπηρεσία που χρησιμοποιείται από τους 802.11 σταθμούς σε ένα infrastructure δίκτυο. Κάθε φορά που ένας σταθμός στέλνει ένα πλαίσιο η υπηρεσία διανομής εκτελείται. Συγκεκριμένα, όταν ένα AP λάβει ένα πλαίσιο το παραδίδει στο σύστημα διανομής. Κατόπιν εκτελείται η υπηρεσία διανομής προκειμένου να επιλεγεί το σωστό AP εξόδου με το οποίο είναι συσχετισμένος ο τελικός παραλήπτης. Αυτή η διαδικασία εκτελείται τόσο για την ανταλλαγή πλαισίων μεταξύ σταθμών που είναι συσχετισμένοι με διαφορετικά APs όσο και για σταθμούς συσχετισμένους με το ίδιο AP.

Η προδιαγραφή δεν ορίζει πώς διανέμεται το μήνυμα μέσα στο σύστημα διανομής. Αυτό που πρέπει να κάνει το IEEE 802.11 είναι να παρέχει την απαραίτητη πληροφορία στο σύστημα διανομής ώστε αυτό να μπορεί να καθορίσει το σημείο εξόδου το οποίο συνδέεται με τον παραλήπτη. Η πληροφορία αυτή παρέχεται μέσω των τριών υπηρεσιών συσχέτισης (association, reassociation και disassociation) [10].

1.7.5 Ενοποίηση (Integration)

Η υπηρεσία της ενοποίησης επιτρέπει τη σύνδεση του συστήματος διανομής σε ένα μη 802.11 δίκτυο. Όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου που δεν είναι της μορφής 802.11 και χρησιμοποιεί διαφορετική μέθοδο διευθυνσιοδότησης ή μορφή πλαισίων, η υπηρεσία αυτή διαχειρίζεται τη μετατροπή από τη μορφή του 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού [25]. Οι λεπτομέρειες της υπηρεσίας αυτής εξαρτώνται από το σύστημα διανομής που χρησιμοποιείται και δεν ορίζονται από το 802.11 [10]. Το 802.11 ορίζει μόνο ότι η υπηρεσία της ενοποίησης πρέπει να παρέχεται από το σύστημα διανομής.

Οι υπόλοιπες τέσσερις υπηρεσίες που παρέχονται από τους σταθμούς είναι οι εξής:

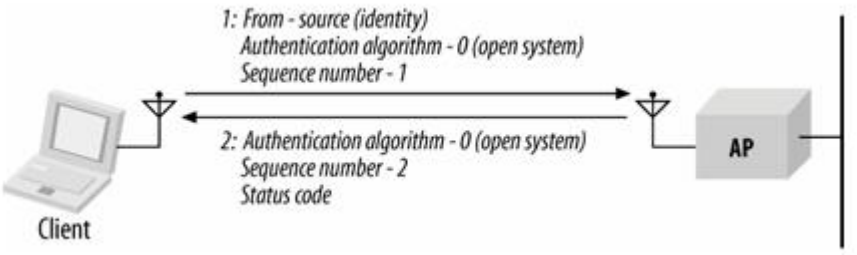
1.7.6 Πιστοποίηση ταυτότητας (Authentication)

Τα ασύρματα δίκτυα, σε σχέση με τα ενσύρματα, υστερούν στο θέμα της ασφάλειας λόγω της φύσης του μέσου. Έτσι, πρέπει να βασιστούν σε

επιπρόσθετες διαδικασίες πιστοποίησης για να μην έχουν πρόσβαση στο δίκτυο ανεπιθύμητοι χρήστες. Η υπηρεσία της πιστοποίησης είναι μία βασική λειτουργία που ελέγχει την πρόσβαση σε ένα WLAN. Για να μπορέσει ένας σταθμός να συσχετιστεί και να έχει πρόσβαση στο δίκτυο θα πρέπει πρώτα να πιστοποιηθεί. Πρόκειται για μία διαδικασία η οποία είναι υποχρεωτική τόσο στα Infrastructure BSSs όσο και στα IBSSs. Χρησιμοποιείται από όλους τους σταθμούς για να εξακριβώσει ο ένας την ταυτότητα του άλλου προκειμένου να επικοινωνήσουν. Το 802.11 ορίζει δύο μεθόδους πιστοποίησης: Open System Authentication και Shared Key Authentication.

1.7.6.1 Open System Authentication

Είναι η προκαθορισμένη και πιο απλή μέθοδος πιστοποίησης. Όπως φαίνεται και στην εικόνα 1.12, περιλαμβάνει δύο στάδια: αρχικά ο σταθμός που θέλει να συνδεθεί στο δίκτυο στέλνει στο AP ένα πλαίσιο πιστοποίησης που περιλαμβάνει την ταυτότητά του, η οποία ουσιαστικά είναι η MAC διεύθυνσή του [1]. Κατόπιν το AP απαντάει επίσης με ένα πλαίσιο πιστοποίησης που περιλαμβάνει την έγκριση ή όχι της πιστοποίησης. Λόγω του ότι πρόκειται για μια απλή μέθοδο πιστοποίησης, η Open System Authentication χρησιμοποιείται όταν παράλληλα υλοποιούνται πιο εξελιγμένες μέθοδοι πιστοποίησης όπως οι 802.11i, 802.1X/EAP και WAP [19].



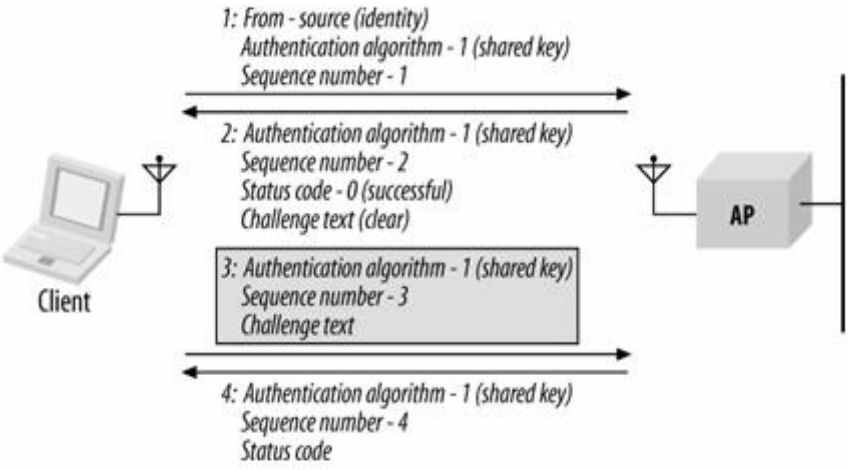
Εικόνα 1.12 Open system authentication [1]

1.7.6.2 Shared Key Authentication

Αυτή η μέθοδος πιστοποίησης χρησιμοποιεί το Wired Equivalent Privacy (WEP) και στηρίζεται στη χρήση ενός κοινού διαμοιραζόμενου κλειδιού. Τα APs και οι σταθμοί έχουν λάβει ένα κρυφό κλειδί μέσα από ένα ασφαλές

κανάλι ανεξάρτητο του 802.11 δικτύου. Ένα AP μπορεί να είναι ρυθμισμένο με πολλά κλειδιά έτσι ώστε κάποιοι σταθμοί να επικοινωνούν μαζί του χρησιμοποιώντας ένα κλειδί και κάποιοι άλλοι χρησιμοποιώντας άλλο κλειδί.

Η διαδικασία περιλαμβάνει τα τέσσερα βήματα, όπως φαίνεται στην εικόνα 1.13 και έχει ως εξής: ο σταθμός που επιθυμεί να πιστοποιηθεί στέλνει ένα πλαίσιο πιστοποίησης στο AP. Κατόπιν, το AP απαντάει με ένα πλαίσιο στο οποίο έχει προσθέσει ένα κείμενο πρόκλησης (challenge text). Ο σταθμός χρησιμοποιεί το WEP κλειδί για να κρυπτογραφήσει αυτό το κείμενο και το στέλνει πίσω στο AP με ένα άλλο πλαίσιο πιστοποίησης. Το AP αποκρυπτογραφεί το κείμενο και το συγκρίνει με το αρχικό. Αν τα δύο κείμενα είναι ίδια, το AP θεωρεί ότι ο σταθμός έχει το σωστό κλειδί και τερματίζει τη διαδικασία στέλνοντας του ένα πλαίσιο εγκρίνοντας την πιστοποίηση [7].



Εικόνα 1.13 Shared key authentication [1]

1.7.7 Ακύρωση πιστοποίησης ταυτότητας (Deauthentication)

Με αυτή την υπηρεσία διακόπτεται μια τρέχουσα (υπάρχουσα) πιστοποίηση. Μπορούν να την προκαλέσουν και τα δύο μέρη της σχέσης. Όταν ένας σταθμός θέλει να εγκαταλείψει το δίκτυο μπορεί να στείλει ένα πλαίσιο ακύρωσης πιστοποίησης στο AP αλλά και ένα AP μπορεί να στείλει ένα τέτοιο πλαίσιο σε ένα σταθμό. Όπως και στην περίπτωση της αποσυσχέτισης, έτσι κι εδώ πρόκειται για μία ενημέρωση την οποία δεν μπορεί να την αρνηθεί κανένα από τα δύο μέρη. Επειδή η διαδικασία της

πιστοποίησης προηγείται της συσχέτισης, μια διαδικασία ακύρωσης πιστοποίησης θα προκαλέσει και μια αποσυσχέτιση.

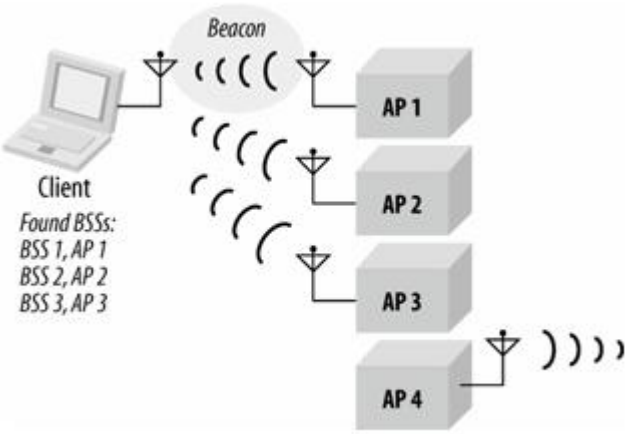
1.7.8 Προστασία απορρήτου (Privacy)

Καθώς τα δεδομένα διασχίζουν το ασύρματο μέσο μετάδοσης, μπορούν εύκολα να υποκλαπούν. Για να αντιμετωπίσει αυτό το πρόβλημα, το 802.11 επιτρέπει την κρυπτογράφηση των περιεχομένων των μηνυμάτων μέσω της υπηρεσίας προστασίας απορρήτου. Η υπηρεσία αυτή εφαρμόζεται σε όλα τα πλαίσια δεδομένων και σε μερικά πλαίσια πιστοποίησης [10]. Αρχικά για την υποστήριξη αυτής της υπηρεσίας γινόταν χρήση του αλγόριθμου WEP. Επειδή όμως το WEP παραβιάστηκε, το 802.11 έχει ορίσει νέες μεθόδους για την προστασία των δεδομένων όπως το 802.11i πρότυπο [1].

1.7.9 Παράδοση δεδομένων (Data delivery)

Το 802.11 παρέχει αυτή την υπηρεσία για τη μετάδοση και τη λήψη δεδομένων. Επειδή το 802.11 ακολουθεί το μοντέλο του Ethernet και η μετάδοση στο Ethernet δεν είναι εγγυημένα αξιόπιστη κατά 100%, ούτε η μετάδοση στο 802.11 είναι εγγυημένα αξιόπιστη. Τα ανώτερα επίπεδα θα πρέπει να ασχοληθούν με την ανίχνευση και την επιδιόρθωση των σφαλμάτων [25].

Προτού όμως ένας σταθμός συνδεθεί σε ένα δίκτυο θα πρέπει πρώτα να το έχει εντοπίσει. Το 802.11 ορίζει δύο μεθόδους ανίχνευσης, την παθητική ανίχνευση (passive scanning) και την ενεργητική ανίχνευση (active scanning). Στην πρώτη περίπτωση, όπως φαίνεται στην εικόνα 1.14, ο σταθμός απλά “ακούει” το μέσο ενώ τα APs στέλνουν περιοδικά ένα πλαίσιο που περιέχει πληροφορίες γι’ αυτά, όπως το SSID και οι υποστηριζόμενοι ρυθμοί μετάδοσης. Τα πλαίσια αυτά είναι γνωστά ως beacons. Ο σταθμός χρησιμοποιεί αυτές τις πληροφορίες σε συνδυασμό με την ισχύ του σήματος του κάθε AP για να αποφασίσει με ποιο θα συσχετιστεί.



Εικόνα 1.14 Passive scanning [1]

Στην περίπτωση της ενεργούς ανίχνευσης ο σταθμός είναι αυτός που ξεκινάει τη διαδικασία στέλνοντας μία αίτηση ανίχνευσης (probe request). Τα APs που λαμβάνουν αυτά τα πλαίσια στέλνουν μία απάντηση ανίχνευσης (probe response) η οποία περιλαμβάνει τις ίδιες πληροφορίες με ένα πλαίσιο beacon. Και πάλι ο σταθμός θα επιλέξει να συσχετιστεί με το AP που ανταποκρίνεται στις απαιτήσεις του. Ο σταθμός θα συνεχίσει να στέλνει περιοδικά αιτήσεις ανίχνευσης. Έτσι μπορεί να διατηρεί μία λίστα με τα APs και όταν θελήσει να αλλάξει BSS αυτό θα γίνει πιο γρήγορα και αποτελεσματικά [19]. Επίσης, θα πρέπει να σημειωθεί ότι και στα IBSSs δίκτυα οι σταθμοί στέλνουν εκ περιτροπής πλαίσια beacon για να ενημερώνονται οι νέοι σταθμοί για την ύπαρξη του δικτύου [7].

1.8 Wi-Fi Alliance

Ο Wi-Fi Alliance (WFA) (αρχικά το όνομά του ήταν Wireless Ethernet Compatibility Alliance (WECA), μέχρι το 2003 που μετονομάστηκε σε Wi-Fi Alliance) είναι ένας διεθνής μη κερδοσκοπικός οργανισμός ο οποίος δημιουργήθηκε το 1999 με σκοπό την πιστοποίηση συμβατότητας ανάμεσα σε 802.11 συσκευές διαφορετικών κατασκευαστών. Σήμερα μετρά 300 μέλη σε περισσότερες από 20 χώρες και έχει πιστοποιήσει πάνω από 5000 προϊόντα [29].

Ο WFA διαχειρίζεται την πιστοποίηση Wi-Fi ασύρματων συσκευών που υλοποιούν τη διεθνή προδιαγραφή 802.11, εκτελώντας αυστηρούς ελέγχους. Τα προϊόντα δοκιμάζονται ως προς τη συμβατότητα τους με άλλα Wi-Fi πιστοποιημένα προϊόντα και όσα περάσουν αυτόν τον έλεγχο λαμβάνουν το δικαίωμα να χρησιμοποιούν την ένδειξη Wi-Fi.

Wi-Fi, συντομογραφία του wireless fidelity (ασύρματη πιστότητα), είναι ένα πιο φιλικό προς τους καταναλωτές όνομα που χρησιμοποιεί ο WFA για να περιγράψει προϊόντα ασύρματων τοπικών δικτύων, που βασίζονται στην οικογένεια προτύπων 802.11, του Institute of Electrical and Electronics Engineers (IEEE).

Ο WFA βεβαιώνει ότι κάθε Wi-Fi συσκευή θα επικοινωνήσει με κάθε άλλη Wi-Fi συσκευή, ανεξάρτητα από τον κατασκευαστή. Έτσι οι καταναλωτές είναι σίγουροι ότι αγοράζοντας προϊόντα με πιστοποίηση Wi-Fi αυτά θα λειτουργήσουν επιτυχώς με προϊόντα άλλων κατασκευαστών που φέρουν την ίδια πιστοποίηση.

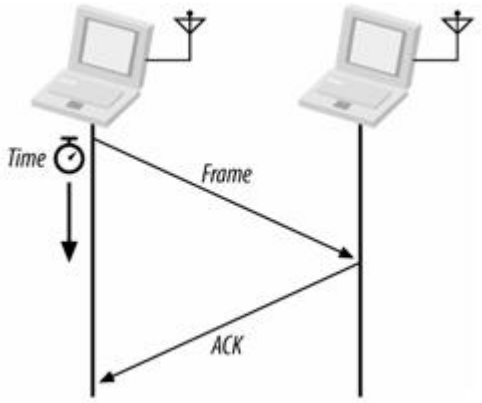
Κεφάλαιο 2 Επίπεδο MAC

2.1 Εισαγωγή

Το επίπεδο MAC του 802.11 είναι κοινό για όλες τις 802.11 τεχνολογίες φυσικού επιπέδου. Ελέγχει την πρόσβαση στο μέσο και διαχειρίζεται τη μεταφορά των δεδομένων από τα ανώτερα επίπεδα προς το φυσικό επίπεδο. Επίσης, όταν ένα ασύρματο δίκτυο συνδέεται με ένα ενσύρματο δίκτυο, το επίπεδο MAC παρέχει τη διεπαφή ανάμεσα στα δύο αυτά δίκτυα. Ανάμεσα στο 802.11 και τα υπόλοιπα IEEE 802 πρότυπα χρησιμοποιείται ένα κοινό LLC επίπεδο το οποίο δημιουργεί μία γέφυρα ανάμεσα στα ενσύρματα και τα ασύρματα τοπικά δίκτυα [14].

2.2 Carrier Sense Multiple Access/ Collision Avoidance (CSMA/CA)

Οι κυριότερες διαφορές μεταξύ 802.11 και Ethernet προκύπτουν από το μέσο που χρησιμοποιούν. Ανάμεσα στα δύο πρωτόκολλα όμως υπάρχουν και κάποια κοινά σημεία. Όπως στο Ethernet, έτσι και στο 802.11 η πρόσβαση στο μέσο είναι κατανεμημένη χωρίς να υπάρχει ένας κεντρικός ελεγκτής. Άλλη μία ομοιότητα με το Ethernet είναι ότι και το 802.11 χρησιμοποιεί ένα σχήμα πολλαπλής πρόσβασης με ανίχνευση φέροντος (CSMA- Carrier Sense Multiple Access) για τον έλεγχο της πρόσβασης στο μέσο. Όμως, επειδή οι ασύρματοι σταθμοί δεν μπορούν να εκπέμπουν και να λαμβάνουν την ίδια στιγμή, στο 802.11 δεν γίνεται ανίχνευση συγκρούσεων (CD- Collision Detection) αλλά αποφυγή συγκρούσεων (CA- Collision Avoidance) με το σταθμό παραλήπτη να στέλνει μια επιβεβαίωση για κάθε πλαίσιο που λαμβάνει επιτυχώς. Στην εικόνα 2.1 φαίνεται η διαδικασία αποστολής ενός πλαισίου και της επιβεβαίωσής του. Η ακολουθία αυτή είναι μία ατομική λειτουργία, δηλαδή μία αδιαίρετη λειτουργία η οποία δεν μπορεί να διακοπεί. Αν ο αποστολέας του πλαισίου δε λάβει επιβεβαίωση θεωρεί ότι το πλαίσιο χάθηκε κι έτσι πρέπει να το ξαναστείλει.



Εικόνα 2.1 Επιβεβαίωση πλαισίων [1]

Οι επιβεβαιώσεις χρησιμοποιούνται μόνο για τα πλαίσια που απευθύνονται σε έναν παραλήπτη (unicast) ενώ για τα πλαίσια που απευθύνονται σε πολλούς (multicast) ή όλους (broadcast) τους σταθμούς δεν στέλνονται επιβεβαιώσεις [1].

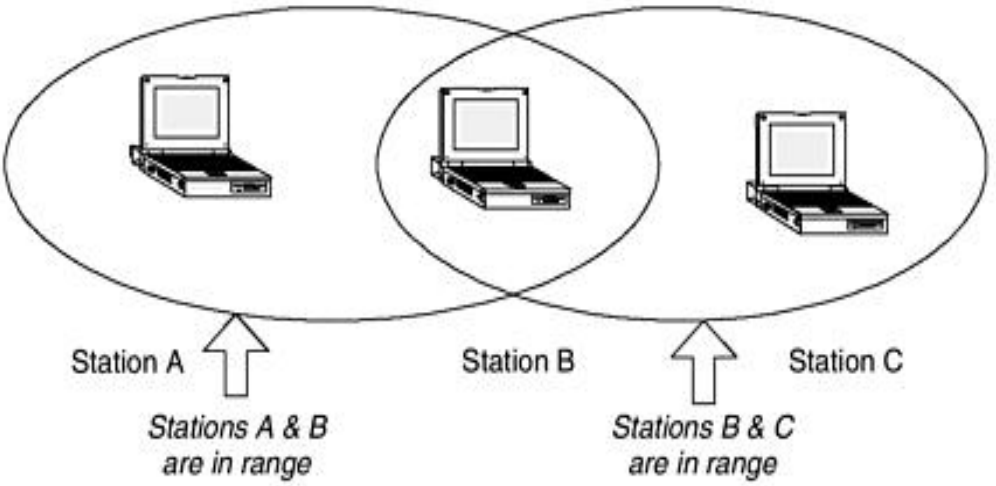
Ο μηχανισμός CSMA/CA είναι ο βασικός μηχανισμός πρόσβασης στο μέσο και επίσημα αναφέρεται ως Distributed Coordination Function (DCF). Υπάρχει και ένας δεύτερος μηχανισμός πρόσβασης, ο Point Coordination Function (PCF) ο οποίος όμως είναι προαιρετικός και δεν χρησιμοποιείται ιδιαίτερα. Και οι δύο μηχανισμοί αναλύονται σε ακόλουθες παραγράφους.

Ένα από τα προβλήματα που σχετίζονται με τον βασικό μηχανισμό πρόσβασης είναι ότι θεωρείται πως ο σταθμός αποστολέας μπορεί να ακούσει όλους τους άλλους σταθμούς και να ανιχνεύσει ένα σήμα φορέα. Όμως, λόγω φυσικών εμποδίων αλλά και του γεγονότος ότι κάποιο σταθμοί μπορεί να βρίσκονται έξω από το εύρος κάποιων άλλων, δεν είναι σίγουρο ότι όλοι οι σταθμοί μπορούν να ακούσουν τους άλλους. Αυτή η κατάσταση είναι γνωστή ως πρόβλημα του κρυμμένου κόμβου (hidden node problem) [14].

2.3 Hidden node problem

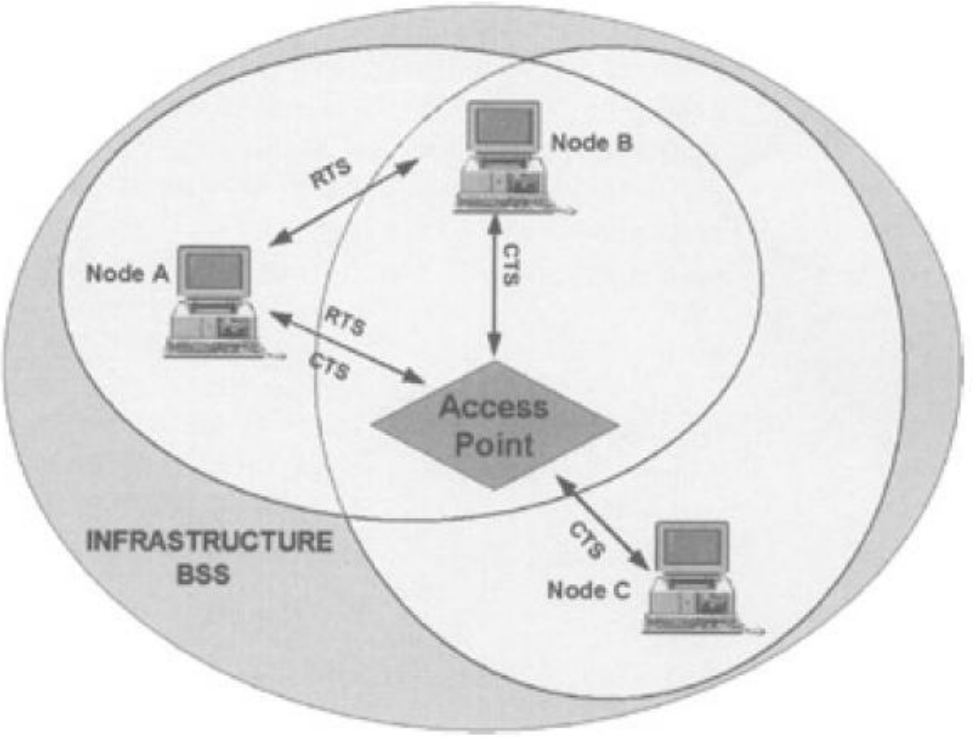
Το πρόβλημα του κρυφού κόμβου, όπως αναφέρθηκε και πιο πάνω, προκύπτει όταν δύο κόμβοι που ανήκουν στο ίδιο δίκτυο είναι εκτός εύρους ο

ένας με τον άλλον. Στην εικόνα 2.2 ο σταθμός Β μπορεί να επικοινωνήσει και με τον Α και με τον C. Όμως, οι δύο τελευταίοι δεν μπορούν να επικοινωνήσουν μεταξύ τους γιατί βρίσκονται πολύ μακριά ο ένας από τον άλλον. Ο σταθμός C είναι κρυφός κόμβος για τον Α και αντίστροφα. Αν ο σταθμός Α επιχειρήσει να εκπέμψει, ενώ ήδη εκπέμπει ο C, ή και αντίστροφα, τότε θα προκληθεί σύγκρουση κοντά στον σταθμό Β. Αυτό θα έχει σαν αποτέλεσμα ο μεν Β να μην μπορέσει να καταλάβει καμία από τις μεταδόσεις, οι δε Α και C να μείνουν ανυποψίαστοι για τη σύγκρουση καθώς αυτή ήταν τοπική στο σταθμό Β.



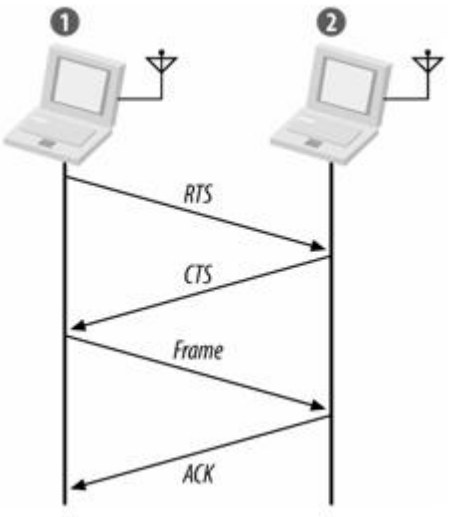
Εικόνα 2.2 Το πρόβλημα του κρυφού κόμβου [14]

Για την αποφυγή των συγκρούσεων σε μία τέτοια περίπτωση οι σταθμοί έχουν τη δυνατότητα να δεσμεύσουν το κανάλι με την ανταλλαγή Request to Send (RTS) και Clear to Send (CTS) πλαισίων. Η εικόνα 2.3 περιγράφει τη διαδικασία.



Εικόνα 2.3 RTS/CTS μέθοδος σε IBSS τοπολογία [2]

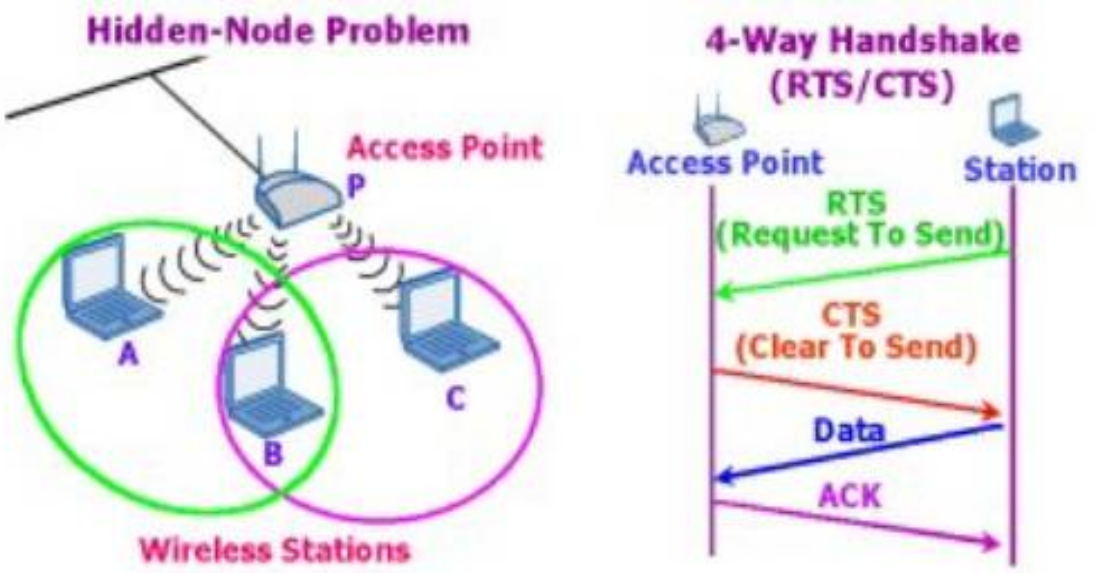
Όταν ο σταθμός Α θέλει να στείλει ένα πλαίσιο, ξεκινά τη διαδικασία στέλνοντας ένα RTS πλαίσιο στο AP. Με αυτό το πλαίσιο όχι μόνο δεσμεύει το κανάλι αλλά επιπλέον όλοι οι σταθμοί, που βρίσκονται στο εύρος του σταθμού Α, θα ακούσουν αυτό το πλαίσιο και θα σιωπήσουν. Κατόπιν, το AP απαντά με ένα CTS πλαίσιο, το οποίο με τη σειρά του θα σιωπήσει κάθε σταθμό που βρίσκεται στο εύρος του AP. Έπειτα ο σταθμός Α μπορεί να στείλει τα δεδομένα χωρίς τον κίνδυνο παρεμβολής από κρυφούς κόμβους. Και αφού το κανάλι έχει δεσμευτεί με τη χρήση των RTS/CTS πλαισίων, στέλνετε θετική επιβεβαίωση από το AP και η διαδικασία ολοκληρώνεται. Τα RTS/CTS πλαίσια, το πλαίσιο δεδομένων και η επιβεβαίωση αποτελούν μέρη μίας ατομικής ενέργειας (εικόνα 2.4).



Εικόνα 2.4 Δέσμευση καναλιού με RTS/CTS πλαίσια [2]

Επειδή όμως η μετάδοση των πλαισίων RTS/CTS καταναλώνει μέρος της χωρητικότητας, κυρίως λόγω της πρόσθετης καθυστέρησης που παρουσιάζεται πριν τη μετάδοση των δεδομένων, η διαδικασία αυτή χρησιμοποιείται μόνο σε περιβάλλοντα με μεγάλη χωρητικότητα και σε περιβάλλοντα με μεγάλο ανταγωνισμό για μετάδοση. Η RTS/CTS διαδικασία μπορεί να ελεγχθεί, αν το επιτρέπει ο οδηγός συσκευής της 802.11 κάρτας, θέτοντας ένα RTS κατώφλι. Για πλαίσια μεγαλύτερα από αυτό το κατώφλι προηγείται μία RTS/CTS ανταλλαγή για δέσμευση του καναλιού ενώ μικρότερα πλαίσια απλά μεταδίδονται [1].

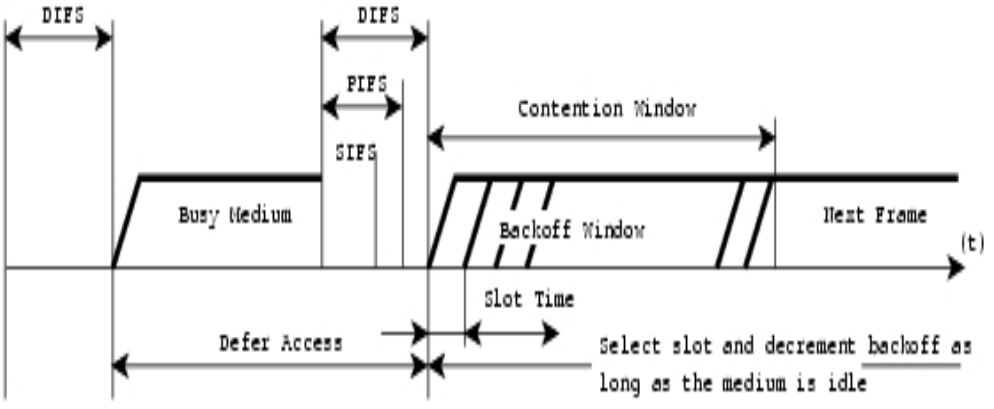
Η διαδικασία RTS/CTS λειτουργεί και σε BSS και σε IBSS δίκτυα. Σε ένα IBSS δίκτυο η ανταλλαγή των πλαισίων RTS/CTS γίνεται μεταξύ των σταθμών που θέλουν να επικοινωνήσουν ενώ σε ένα infrastructure BSS δίκτυο η ανταλλαγή των πλαισίων RTS/CTS γίνεται μεταξύ των σταθμών και του access point [15]. Η εικόνα 2.5 δείχνει την τελευταία διαδικασία.



Εικόνα 2.5 RTS/CTS μέθοδος σε infrastructure BSS τοπολογία [43]

2.4 Interframe Spacing

Για τη ρύθμιση της πρόσβασης στο μέσο και την απόδοση προτεραιοτήτων το 802.11 ορίζει τέσσερα χρονικά διαστήματα (interframe spaces) που διαχωρίζουν τα μεταδιδόμενα πλαίσια. Στην εικόνα 2.6 φαίνεται η σχέση αυτών των διαστημάτων.



Εικόνα 2.6 Interframe spaces [44]

Τα διαστήματα αυτά διαφέρουν ανάλογα με τον τύπο των πλαισίων και είναι τα εξής:

Short interframe space (SIFS)

Το διάστημα αυτό έχει τη μικρότερη χρονική διάρκεια από όλα τα υπόλοιπα και χρησιμοποιείται για τη μετάδοση των πλαισίων με την υψηλότερη προτεραιότητα. Τέτοια πλαίσια είναι τα CTS πλαίσια σε μία RTS/CTS ακολουθία, οι θετικές επιβεβαιώσεις (ACKs), πλαίσια που ακολουθούν ένα CTS πλαίσιο και τα πλαίσια που αποτελούν κομμάτια ενός μεγαλύτερου πλαισίου που υπέστη τμηματοποίηση (fragmentation). Εξαίρεση στην τελευταία περίπτωση αποτελεί το πρώτο τμήμα (fragment) της ακολουθίας το οποίο στέλνεται μετά από ένα DIFS. Οι χρόνοι που ορίζονται για κάθε τεχνολογία φυσικού επιπέδου είναι : FHSS – 28 μs, DSSS – 10 μs, OFDM – 16 μs, HR/DSSS 10 μs, ERP OFDM – 10 μs [15].

PCF interframe space (PIFS)

Το διάστημα PIFS χρησιμοποιείται από την PCF κατά τη διάρκεια της λειτουργίας χωρίς ανταγωνισμό. Σε αυτή την περίπτωση οι σταθμοί μεταδίδουν αμέσως μόλις ολοκληρωθεί το PIFS και πριν προλάβει να αρχίσει η περίοδος ανταγωνισμού. Η διάρκεια ενός PIFS είναι ίση με τη διάρκεια ενός SIFS συν τη διάρκεια μίας χρονοθυρίδας. Για παράδειγμα, το DSSS έχει 20 μs χρονοθυρίδα και 10 μs SIFS. Επομένως το PIFS για το DSSS θα είναι 30 μs [15].

DCF interframe space (DIFS)

Όταν χρησιμοποιείται η λειτουργία ανταγωνισμού (DCF), το κανάλι πρέπει να παραμείνει ανενεργό τουλάχιστον για ένα χρονικό διάστημα ίσο με το DIFS προτού οι σταθμοί αρχίσουν ν’ ανταγωνίζονται για την πρόσβαση σε αυτό. Ένα DIFS έχει διάρκεια ίση με τη διάρκεια ενός SIFS συν τη διάρκεια δύο χρονοθυρίδων [15].

Extended interframe space (EIFS)

Το διάστημα αυτό χρησιμοποιείται μόνο όταν παρουσιαστεί κάποιο λάθος στη μετάδοση, όταν για παράδειγμα ένα πλαίσιο φτάσει στον παραλήπτη αλλά διαπιστωθεί ότι είναι κατεστραμμένο βάσει της τιμής του Frame Check Sequence (FCS). Ο υπολογισμός του γίνεται ως εξής: EIFS = SIFS + (8*ACK size) + Preamble length + PLCP Header length + DIFS [15].

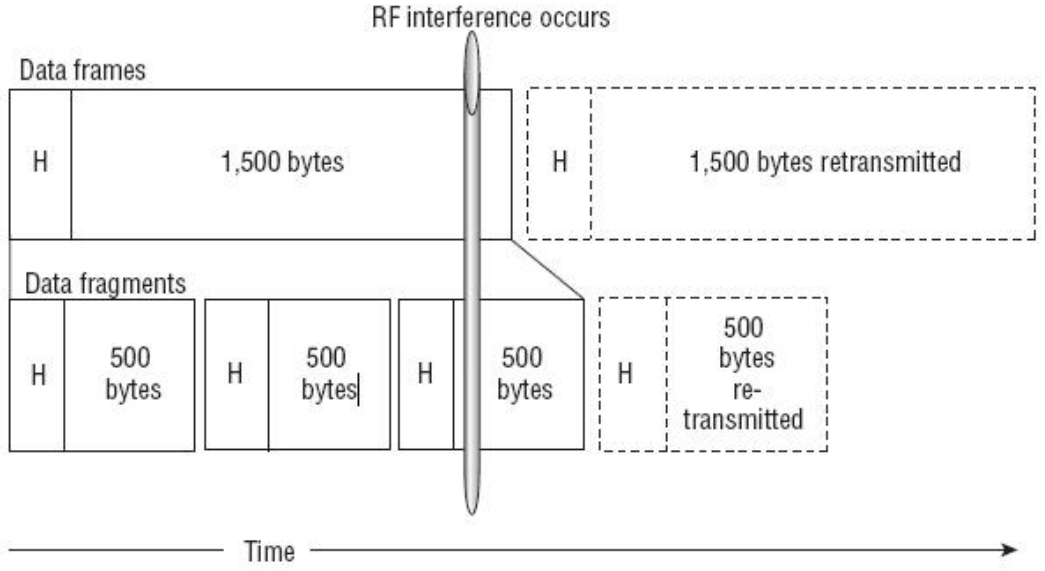
2.5 Τμηματοποίηση (fragmentation)

Η τμηματοποίηση είναι μια γνωστή λειτουργία στα δίκτυα υπολογιστών. Το TCP/IP έχει μια μέγιστη μονάδα μετάδοσης (maximum transmission unit, MTU) IP πακέτων ίση με 1.500 bytes. Αυτό σημαίνει ότι το TCP/IP χωρίζει τα προς μετάδοση δεδομένα σε τμήματα που δεν ξεπερνούν τα 1.500 bytes. Όταν το IP περνά ένα πακέτο στο DLL επίπεδο για να μεταδοθεί από το 802.11, το μέγεθος αυτού του πακέτου των 1.500 bytes δεν είναι πρόβλημα, καθώς το 802.11 έχει δυνατότητα μεταφοράς ωφέλιμου φορτίου μέχρι 2.304 bytes [19].

Κάθε 802.11 πλαίσιο αποτελείται όχι μόνο από το ωφέλιμο φορτίο, αλλά και από την κεφαλίδα που προσθέτει το MAC. Για να μπορεί ένα δίκτυο να παρέχει την καλύτερη απόδοση, πρέπει να μεταδίδει αρκετά μεγάλα πλαίσια για να ελαχιστοποιεί την ποσότητα της επιπλέον πληροφορίας που προσθέτουν οι κεφαλίδες, ενώ παράλληλα πρέπει να εξασφαλίζεται ότι τα πλαίσια δεν θα είναι τόσο μεγάλα ώστε να περιορίζουν την πρόσβαση στο μέσο από άλλους σταθμούς. Σε ένα ιδανικό περιβάλλον όταν όλα λειτουργούν σωστά, το 802.11 δίκτυο θα λειτουργήσει καλά μεταδίδοντας τα πλαίσια. Δυστυχώς όμως, οι 802.11 μεταδόσεις είναι ευαίσθητες στις παρεμβολές και κάποιες από αυτές τις μεταδόσεις μπορεί να αποτύχουν. Αν ο αποστολέας δε λάβει επιβεβαίωση για ένα πλαίσιο, θεωρεί ότι η μετάδοση ήταν ανεπιτυχής οπότε πρέπει να ξαναστείλει το πλαίσιο.

Η 802.11 τμηματοποίηση σπάζει τα πλαίσια σε μικρότερα κομμάτια γνωστά ως τμήματα, προσθέτει τις πληροφορίες κεφαλίδων σε κάθε ένα από αυτά και τα μεταδίδει χωριστά. Αν και η ποσότητα των πραγματικών δεδομένων που μεταδίδεται είναι η ίδια, κάθε τμήμα απαιτεί τη δική του κεφαλίδα και η μετάδοση κάθε τμήματος ακολουθείται από ένα SIFS και μία επιβεβαίωση. Σε ένα 802.11 δίκτυο που λειτουργεί καλά, τα μικρότερα τμήματα θα μειώσουν την απόδοση λόγω των πρόσθετων κεφαλίδων, του SIFS και της επιβεβαίωσης του κάθε τμήματος. Απ' την άλλη μεριά όμως, εάν η ποσότητα των δεδομένων που καταστρέφονται είναι μεγάλη, η χρήση μικρών τμημάτων μπορεί να βελτιώσει την απόδοση.

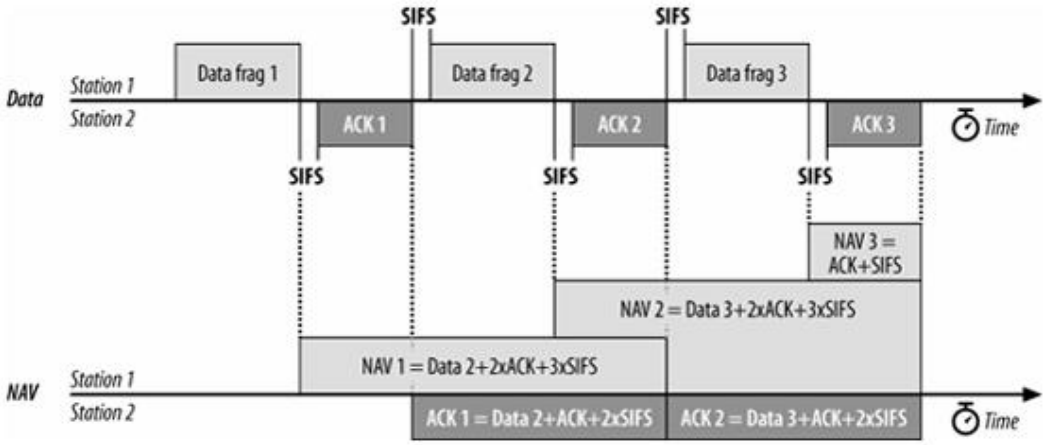
Όπως φαίνεται και στην εικόνα 2.7, εάν ένα πλαίσιο καταστραφεί και πρέπει να αναμεταδοθεί, ολόκληρο το πλαίσιο πρέπει να ξανασταλθεί. Όταν όμως το πλαίσιο έχει σπάσει σε πολλαπλά τμήματα, οι παρεμβολές θα επηρεάσουν μόνο ένα ή μερικά από τα μικρά τμήματα. Έτσι αντί ενός ολόκληρου μεγάλου πλαισίου θα πρέπει να αναμεταδοθούν μόνο μερικά μικρά τμήματα. Η αναμετάδοση ενός μικρού τμήματος θα χρειαστεί πολύ λιγότερο χρόνο από την αναμετάδοση ενός μεγαλύτερου πλαισίου.



Εικόνα 2.7 Τμηματοποίηση πλαισίων [19]

Τα τμήματα έχουν έναν αριθμό ακολουθίας και έναν αριθμό τμήματος που βοηθούν στην συναρμολόγηση του πλαισίου στη μεριά του δέκτη. Ο αριθμός

ακολουθίας είναι ίδιος για όλα τα τμήματα του ίδιου πλαισίου ενώ ο αριθμός τμήματος αλλάζει καθώς αυξάνεται κατά ένα για κάθε ακόλουθο τμήμα. Η διαδικασία αποστολής μιας ακολουθίας τμημάτων φαίνεται στην εικόνα 2.8.



Εικόνα 2.8 Μετάδοση μιας ακολουθίας τμημάτων [1]

Τα τμήματα και οι επιβεβαιώσεις τους χωρίζονται με SIFS, έτσι ώστε να έχουν μεγαλύτερη προτεραιότητα και ο σταθμός αποστολέας να έχει τον έλεγχο του καναλιού καθ' όλη τη διάρκεια της μετάδοσης των τμημάτων. Όλα τα τμήματα σχηματίζουν μια αλυσίδα και καθ' ένα από αυτά δεσμεύει το κανάλι, θέτοντας έναν μετρητή, τον NAV, μέχρι το τέλος της επιβεβαίωσης του επόμενου τμήματος. Όταν σταλεί και το τελευταίο τμήμα με την επιβεβαίωσή του, ο NAV μηδενίζεται υποδεικνύοντας ότι το μέσο θα είναι πλέον ελεύθερο [1].

Η τμηματοποίηση ελέγχεται από ένα ρυθμιζόμενο κατώφλι. Πλαίσια μεγαλύτερα από το κατώφλι τμηματοποίησης σπάνε σε μικρότερα τμήματα. Μεγαλύτερο κατώφλι τμηματοποίησης συνεπάγεται λιγότερο φόρτο (overhead) αλλά περισσότερα δεδομένα μπορεί να καταστραφούν και να χρειαστεί να ξανασταλθούν. Μικρότερο κατώφλι τμηματοποίησης προσθέτει περισσότερο φόρτο αλλά προσφέρει μεγαλύτερη αντοχή στις παρεμβολές [1].

2.6 Τεχνικές πρόσβασης στο μέσο

Το 802.11 ορίζει τρεις τεχνικές για την πρόσβαση στο μέσο. Η ανταγωνιστική μέθοδος CSMA/CA παρέχεται από την Distributed Coordination Function (DCF). Μία άλλη τεχνική, η Point Coordination Function (PCF), χρησιμοποιείται για μη ανταγωνιστική πρόσβαση στο μέσο. Τέλος, υπάρχει και μία ενδιάμεση τεχνική, η Hybrid Coordination Function (HCF), που παρέχει υπηρεσίες QoS. Ωστόσο, προτού λάβει χώρα οποιαδήποτε από τις τρεις προαναφερθείσες μεθόδους πρέπει να γίνει ανίχνευση του μέσου για να διαπιστωθεί εάν είναι ελεύθερο.

2.6.1 Μέθοδοι ανίχνευσης καναλιού

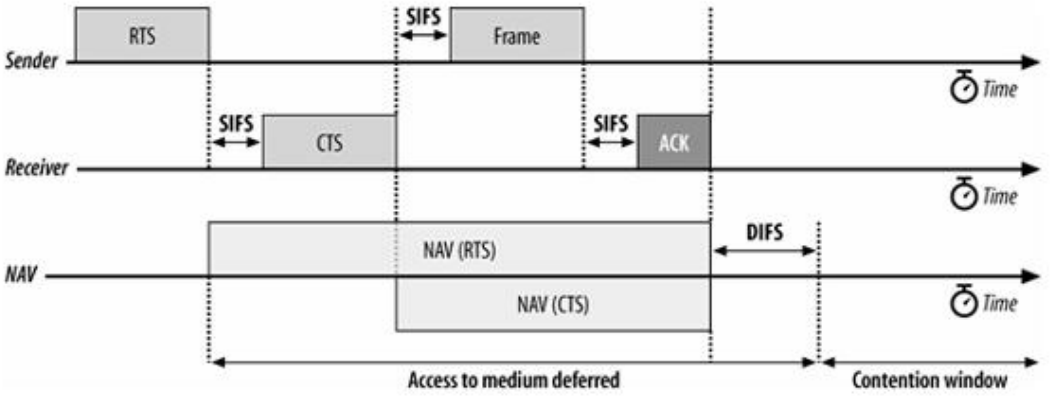
Στο 802.11 υπάρχουν δύο τρόποι ανίχνευσης του καναλιού: φυσική ανίχνευση φέροντος (physical carrier-sensing) και νοητή ανίχνευση φέροντος (virtual carrier-sensing). Εκτελούνται πάντα και οι δύο αυτοί μηχανισμοί, ο μεν physical carrier-sensing στο φυσικό επίπεδο ο δε virtual carrier-sensing στο επίπεδο MAC [19]. Έστω και μία από τις δύο λειτουργίες να υποδείξει ότι το κανάλι είναι απασχολημένο, οι σταθμοί αναβάλλουν τις μεταδόσεις τους.

Στην περίπτωση της ανίχνευσης από το φυσικό επίπεδο χρησιμοποιείται η μέθοδος Clear Channel Assessment (CCA). Η CCA υλοποιείται με την παρακολούθηση του μέσου για να διαπιστωθεί αν η ποσότητα της ηλεκτρομαγνητικής ενέργειας ξεπερνά ένα συγκεκριμένο κατώφλι [15]. Ωστόσο, λόγω της πιθανής ύπαρξης κρυφών κόμβων, η φυσική ανίχνευση φέροντος δεν παρέχει όλες τις απαραίτητες πληροφορίες [1]. Έτσι, την τεχνική αυτή συμπληρώνει η νοητή ανίχνευση φέροντος.

Η νοητή ανίχνευση φέροντος επιτυγχάνεται με τη χρήση ενός μετρητή, του Network Allocation Vector (NAV). Τα περισσότερα 802.11 πλαίσια έχουν ένα πεδίο χρονικής διάρκειας (Duration/ID field), το οποίο περιέχει μία τιμή από 0 έως 32,767 και που μπορεί να χρησιμοποιηθεί για τη δέσμευση του καναλιού [19]. Ο NAV είναι ένας μετρητής που δείχνει το χρόνο για τον οποίο το κανάλι θα μείνει δεσμευμένο, σε εκατομμυριοστά του δευτερολέπτου. Ο σταθμός που μεταδίδει θέτει τον NAV ανάλογα με το χρόνο που θα χρειαστεί το κανάλι,

υπολογίζοντας κάθε απαραίτητο πλαίσιο για την ολοκλήρωση της τρέχουσας μετάδοσης. Οι υπόλοιποι σταθμοί ρυθμίζουν το δικό τους NAV σύμφωνα με αυτόν που υπάρχει στο πλαίσιο που μεταδίδεται και μετρούν αντίστροφα από τον NAV μέχρι το 0. Όσο ο NAV έχει μη μηδενική τιμή, το κανάλι θεωρείται απασχολημένο. Όταν ο NAV φτάσει στο 0 η λειτουργία της νοητής ανίχνευσης υποδεικνύει ότι το κανάλι είναι ανενεργό και οι σταθμοί μπορούν να ανταγωνιστούν για την πρόσβαση στο μέσο.

Για να εξασφαλιστεί ότι η ακολουθία των πλαισίων δε θα διακοπεί, ο σταθμός αποστολέας θέτει τον NAV μέσα στο RTS πλαίσιο που στέλνει για να δεσμεύσει το κανάλι. Όλοι οι σταθμοί που ακούνε το RTS πλαίσιο αναβάλλουν τις δικές τους μεταδόσεις μέχρι τη λήξη του NAV. Επειδή το RTS πλαίσιο μπορεί να μην ανιχνευθεί από όλους τους σταθμούς, ο παραλήπτης απαντά με ένα CTS πλαίσιο το οποίο χρησιμοποιείται επίσης για την ενημέρωση του NAV, για την τρέχουσα μετάδοση. Έτσι όλοι οι σταθμοί, είτε ακούσουν το RTS είτε το CTS, θα ενημερώσουν σωστά τον NAV και δε θα επιχειρήσουν να μεταδώσουν μέχρι τη λήξη του. Με το τέλος της μετάδοσης και αφού περάσει ένα διάστημα DIFS, το κανάλι είναι ελεύθερο για χρήση από οποιονδήποτε σταθμό. Στη εικόνα 2.9 φαίνεται η χρήση του NAV.



Εικόνα 2.9 Χρήση του NAV για ανίχνευση και δέσμευση του καναλιού [1]

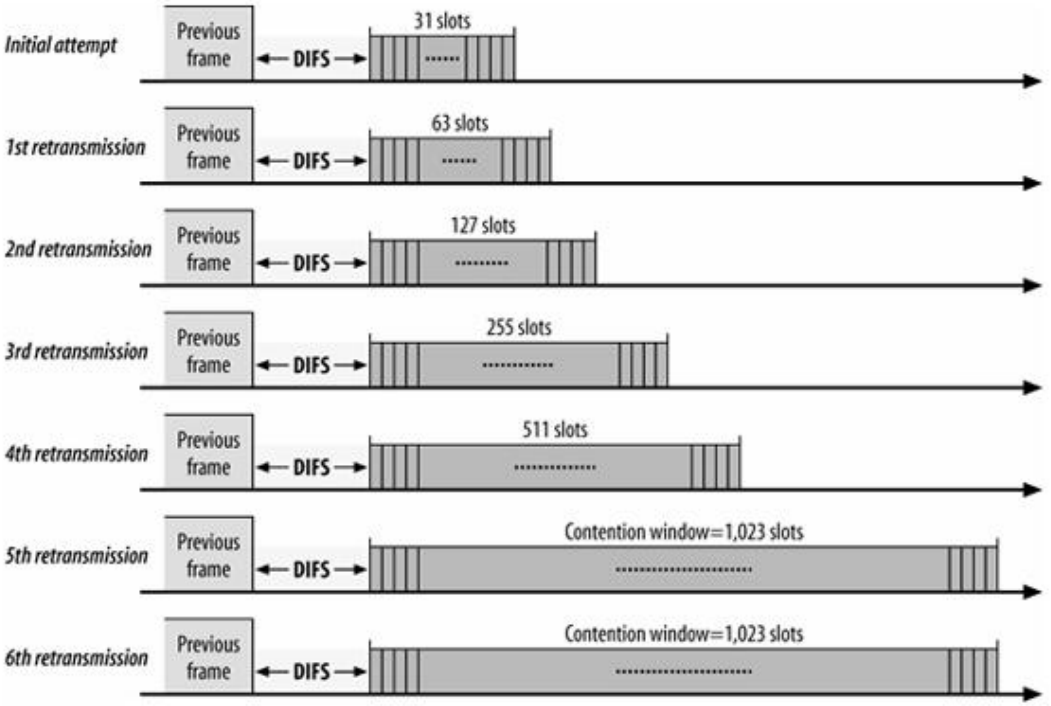
2.6.2 Distributed Coordination Function (DCF)

Ο DCF είναι ο βασικός μηχανισμός πρόσβασης του 802.11 προτύπου. Επιτρέπει σε πολλαπλούς ανεξάρτητους σταθμούς να αλληλεπιδρούν χωρίς τη χρήση κεντρικού ελέγχου κι έτσι μπορεί να χρησιμοποιηθεί και σε BSS και σε IBSS δίκτυα. Όπως στο Ethernet, έτσι κι εδώ όταν ένας σταθμός θέλει να μεταδώσει ελέγχει πρώτα αν το κανάλι είναι ελεύθερο. Αν ναι, τότε ο σταθμός μπορεί να το δεσμεύσει και να μεταδώσει το πλαίσιό του. Αν όμως το κανάλι είναι απασχολημένο, ο σταθμός θα πρέπει να περιμένει μέχρι να ολοκληρωθεί η τρέχουσα μετάδοση. Μετά την ολοκλήρωση αυτής της μετάδοσης ο σταθμός περιμένει για ένα χρονικό διάστημα γνωστό ως DIFS (Distributed Interframe Spacing). Μετά τη λήξη του DIFS, για να μειωθεί ακόμα περισσότερο η πιθανότητα συγκρούσεων μεταξύ σταθμών που προσπαθούν να εκπέμψουν την ίδια στιγμή, κάθε σταθμός ανταγωνίζεται για το κανάλι κατά τη διάρκεια ενός χρονικού παραθύρου γνωστό ως παράθυρο ανταγωνισμού (contention window). Το παράθυρο ανταγωνισμού χωρίζεται σε χρονοθυρίδες. Μία χρονοθυρίδα είναι ίση με το χρόνο που χρειάζεται κάθε σταθμός για να ανιχνεύσει τη μετάδοση ενός πλαισίου από κάθε άλλο σταθμό. Σε αυτό το σημείο ο σταθμός επιλέγει μία τυχαία τιμή οπισθοχώρησης, η οποία δεν είναι τίποτε άλλο από μια χρονοθυρίδα. Το εύρος που μπορεί να έχει αυτή η τιμή είναι από το 0 έως το μέγεθος του αρχικού παραθύρου. Έπειτα, αυτή η τιμή πολλαπλασιάζεται με το μέγεθος της χρονοθυρίδας και το αποτέλεσμα ορίζει έναν μετρητή οπισθοχώρησης. Όση ώρα το κανάλι μένει ανενεργό ο σταθμός μειώνει τον μετρητή. Όταν ο μετρητής πάρει την τιμή 0, ο σταθμός μπορεί να δεσμεύσει το κανάλι για μετάδοση.

Αν κάποιος άλλος σταθμός προλάβει και δεσμεύσει το κανάλι προτού ο μετρητής οπισθοχώρησης φτάσει στο 0, τότε ο σταθμός ξεκινά τη διαδικασία από την αρχή αλλά κρατάει τον τρέχοντα μετρητή. Έτσι μετά το επόμενο DIFS ο σταθμός δεν υπολογίζει καινούριο μετρητή αλλά αρχίζει να μετρά αντίστροφα από το σημείο που είχε μείνει ο προηγούμενος [19].

Αν η μετάδοση αποτύχει, ο σταθμός θα ξαναπροσπαθήσει να στείλει το πλαίσιο αφού όμως πρώτα διπλασιάσει το παράθυρο ανταγωνισμού. Αυτό θα

συμβαίνει για κάθε αποτυχημένη προσπάθεια και μέχρι το παράθυρο να πάρει μια μέγιστη τιμή η οποία διαφέρει ανάλογα με το φυσικό επίπεδο. Η εικόνα 2.10 δείχνει πώς αυξάνεται το παράθυρο ανταγωνισμού καθώς αυξάνει ο αριθμός των προσπαθειών μετάδοσης, χρησιμοποιώντας τους αριθμούς του DSSS PHY.

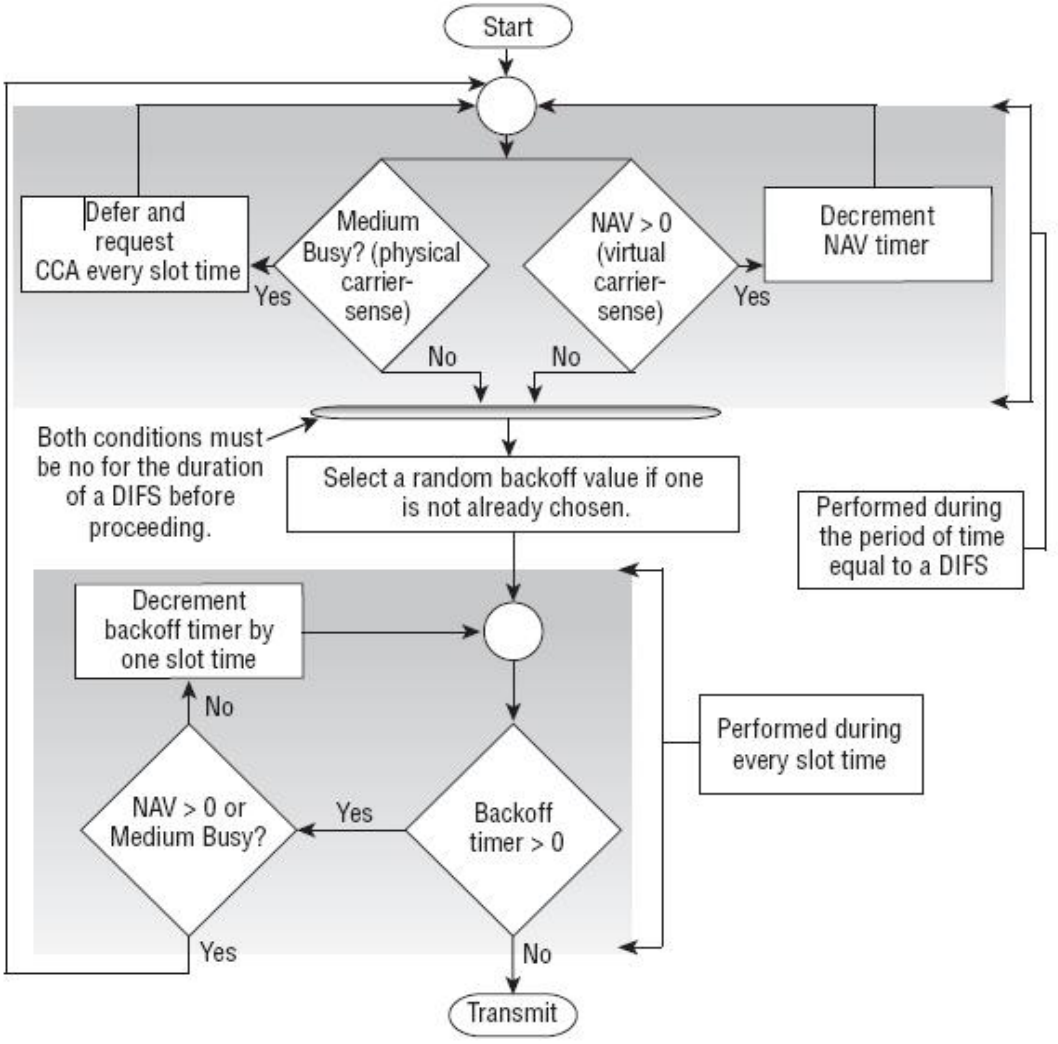


Εικόνα 2.10 Παράθυρο ανταγωνισμού του DSSS PHY [1]

Άλλη μία παράμετρος που ορίζει τον αριθμό των επαναμεταδόσεων ενός πλαισίου είναι ένας μετρητής γνωστός ως *retry counter.* Ο μετρητής αυτός ξεκινάει από το 0 και αυξάνεται κάθε φορά που η αποστολή ενός πλαισίου αποτυγχάνει. Κάθε φορά που ο retry counter αυξάνεται, το παράθυρο ανταγωνισμού διπλασιάζεται. Όταν το παράθυρο ανταγωνισμού πάρει τη μέγιστη δυνατή τιμή, σταματά να διπλασιάζεται. Το παράθυρο θα ρυθμιστεί εκ νέου στο μικρότερο μέγεθός του όταν το πλαίσιο μεταδοθεί επιτυχώς ή όταν ο σχετικός retry counter φτάσει στη μέγιστη τιμή, οπότε το πλαίσιο απορρίπτεται.

Όταν, μετά από μια επιτυχημένη μετάδοση, ο ίδιος σταθμός επιθυμεί να στείλει κι άλλο πλαίσιο θα πρέπει πάλι να ανταγωνιστεί για το μέσο

επαναλαμβάνοντας όλη την προηγούμενη διαδικασία. Το διάγραμμα ροής στην εικόνα 2.11 αναπαριστά την DCF διαδικασία.



Εικόνα 2.11 Διάγραμμα ροής της DCF διαδικασίας [19]

Διάρκεια χρονοθυρίδας

Η διάρκεια μιας χρονοθυρίδας είναι σταθερή για κάθε τεχνολογία φυσικού επιπέδου. Οι χρόνοι όπως ορίζονται για το κάθε PHY είναι οι ακόλουθοι [15]:

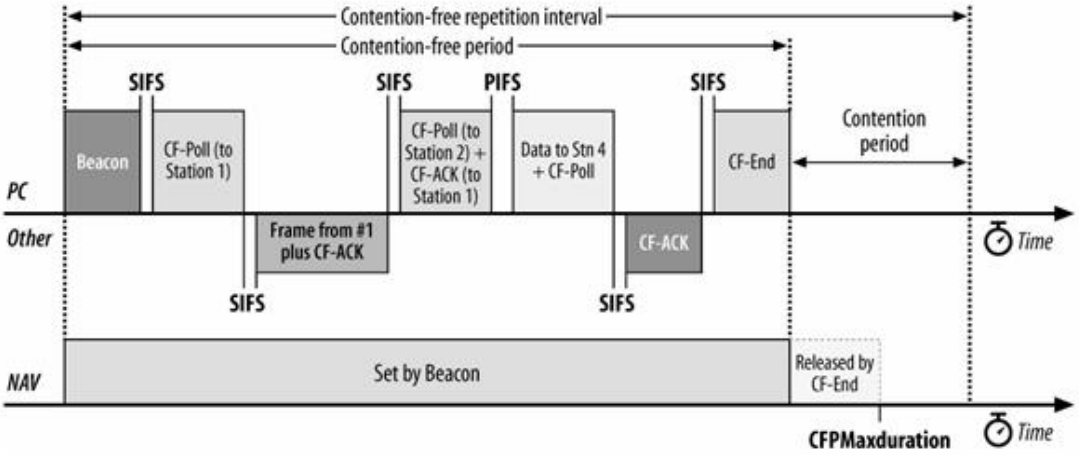
- FHSS - 50 μs
- DSSS - 20 μs
- OFDM - 9 μs
- HR/DSSS - 20 μs
- ERP-OFDM Long Slot Time - 20 μs

- ERP-OFDM Short Slot Time - 9 μs

2.6.3 Point Coordination Function (PCF)

Η PCF είναι μία προαιρετική τεχνική πρόσβασης του 802.11 MAC. Παρέχει υπηρεσίες χωρίς ανταγωνισμό χρησιμοποιώντας ένα κεντρικό σημείο για να ορίζει την πρόσβαση στο μέσο. Η περίοδος κατά την οποία λειτουργεί η PCF λέγεται Contention-free Period (CFP). Η λειτουργία που ελέγχει την πρόσβαση λέγεται point coordinator (PC) και υλοποιείται μέσα στα access points (AP). Επομένως η χρήση της PCF περιορίζεται μόνο σε infrastructure BSS δίκτυα. Όταν χρησιμοποιείται η PCF τεχνική, οι σταθμοί μπορούν να δεσμεύσουν το κανάλι μετά από ένα PCF interframe space (PIFS) και που είναι μικρότερο από το DIFS. Έτσι, έχουν μεγαλύτερη προτεραιότητα σε σχέση με τους σταθμούς που ανταγωνίζονται για την πρόσβαση στο μέσο στα πλαίσια της περιόδου ανταγωνισμού (Contention Period, CP) που ορίζει η DCF.

Όταν ένα AP είναι ρυθμισμένο να χρησιμοποιήσει PCF, ουσιαστικά χρησιμοποιεί και την PCF και την DCF τεχνική με τον χρόνο να μοιράζεται στην CFP και την CP περίοδο [15]. Η εικόνα 2.12 περιγράφει τον τρόπο λειτουργίας της PCF.



Εικόνα 2.12 Τεχνική PCF [1]

Στην αρχή της CFP περιόδου το AP μεταδίδει ένα beacon πλαίσιο με το οποίο ανακοινώνει τη μέγιστη διάρκεια της CFP περιόδου, CFPMaxDuration. Όλοι οι σταθμοί που λαμβάνουν το beacon πλαίσιο θέτουν τον NAV σύμφωνα με τη μέγιστη αυτή διάρκεια αποτρέποντας κάθε DCF πρόσβαση στο μέσο. Κατόπιν, αφού περάσει ένα SIFS, το AP στέλνει Contention Free-Poll (CF-Poll) πλαίσια σε κάθε σταθμό, έναν κάθε φορά, για να τους δώσει το δικαίωμα να μεταδώσουν τα πλαίσιά τους. Ο πρώτος σταθμός που λαμβάνει ένα CF-Poll πλαίσιο θα απαντήσει στο AP μόλις περάσει ένα SIFS. Το AP συνεχίζει στέλνοντας ένα CF-Poll πλαίσιο στο δεύτερο σταθμό αλλά δε λαμβάνει απάντηση. Περιμένοντας για ένα PIFS, το AP συνεχίζει με τον επόμενο σταθμό. Αυτό θα συνεχιστεί μέχρι να ολοκληρωθεί η λίστα με τους σταθμούς που έχει το AP, έχοντας δώσει σε όλους την ευκαιρία για μετάδοση σε μία μη ανταγωνιστική περίοδο. Στο τέλος το AP στέλνει ένα CF-END πλαίσιο και η περίοδος ανταγωνισμού (Contention Period, CP) ξεκινά με την DCF να χρησιμοποιείται πλέον για την πρόσβαση στο μέσο. Επειδή ο χρόνος στην CFP περίοδο είναι πολύτιμος, ένα πλαίσιο μπορεί να συνδυάζει και να μεταφέρει παράλληλα δεδομένα, επιβεβαιώσεις και CF-Polls αυξάνοντας την αποδοτικότητα. Ωστόσο, η PCF δεν χρησιμοποιείται ιδιαίτερα [1].

2.6.4 Hybrid Coordination Function (HCF)

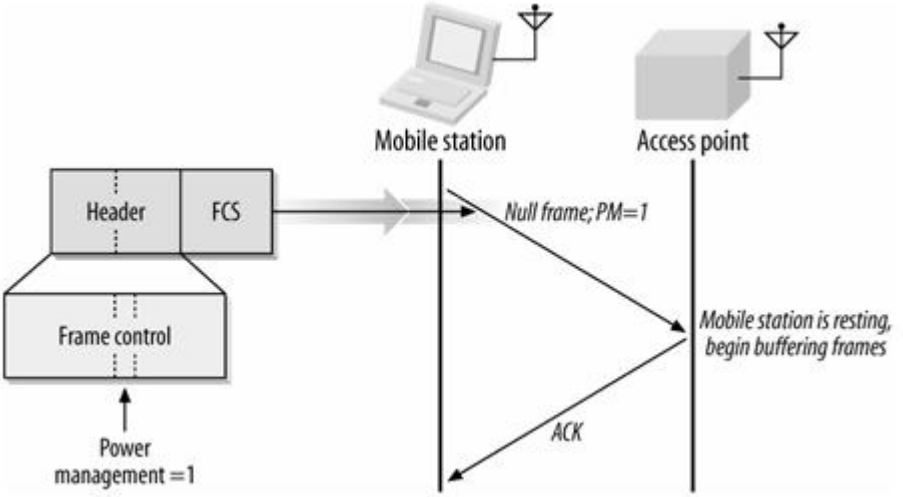
Η HCF συνδυάζει τις λειτουργίες της DCF και της PCF αλλά με κάποιες βελτιώσεις για να παρέχει υπηρεσίες Quality of Service. Η HCF υλοποιείται ως κομμάτι της 802.11e προδιαγραφής [1].

2.7 Διαχείριση ενέργειας

Ένα από τα βασικά πλεονεκτήματα των ασύρματων δικτύων είναι το ότι παρέχουν τη δυνατότητα κίνησης στους χρήστες. Αυτό συνεπάγεται ότι οι συσκευές που διαχειρίζονται οι εν κινήσει χρήστες λειτουργούν με μπαταρία. Το βασικότερο θέμα που αφορά τέτοιες συσκευές είναι πόσο μπορεί να διαρκέσει η μπαταρία μέχρι να χρειαστεί να επαναφορτιστεί. Για να αυξηθεί η διάρκεια της μπαταρίας των ασύρματων σταθμών, το 802.11 τους επιτρέπει

να εισέρχονται σε κατάσταση εξοικονόμησης ενέργειας (Power Save Mode, PS-mode) .

Όταν ένας σταθμός εισέρχεται σε αυτήν την κατάσταση κλείνει τον πομποδέκτη του για κάποιο χρονικό διάστημα αφού πρώτα ενημερώσει το AP, με το οποίο είναι συσχετισμένος, στέλνοντας ένα Null πλαίσιο με την τιμή του Power Management bit ίση με 1. Η χρήση των Null πλαισίων φαίνεται στην εικόνα 2.13.



Εικόνα 2.13 Χρήση Null πλαισίων [1]

Στο εξής, κάθε πλαίσιο που λαμβάνει το AP για τον συγκεκριμένο σταθμό θα το αποθηκεύει σε μία προσωρινή μνήμη (buffer). Το AP διατηρεί μία λίστα, γνωστή ως Traffic Indication Map (TIM), με τα association identifier (AID) όλων των σταθμών για τους οποίους αποθηκεύει πλαίσια. Με το επόμενο beacon πλαίσιο που θα στείλει το AP θα ενημερώσει όλους τους σταθμούς που βρίσκονται στον TIM ότι έχει αποθηκευμένα πλαίσια γι' αυτούς. Τα beacon πλαίσια στέλνονται σε προκαθορισμένα χρονικά διαστήματα, γνωστά ως target beacon transmission time (TBTT), οπότε οι σταθμοί ξέρουν πότε να εξέλθουν από την κατάσταση εξοικονόμησης ενέργειας για να λάβουν κάποιο από τα πλαίσια αυτά. Όταν ο σταθμός λάβει ένα beacon πλαίσιο ελέγχει αν το AID του περιλαμβάνεται στον TIM, υποδεικνύοντας ότι υπάρχουν πλαίσια γι' αυτόν αποθηκευμένα στο AP. Αν ναι, τότε παραμένει ενεργός και στέλνει ένα PS-Poll πλαίσιο στο AP. Όταν το AP λάβει το PS-Poll πλαίσιο θα αρχίσει να στέλνει όλα τα αποθηκευμένα πλαίσια στο σταθμό. Εφόσον λάβει όλα τα

πλαίσια, ο σταθμός μπορεί να εισέλθει και πάλι σε κατάσταση εξοικονόμησης ενέργειας [19].

Αντίστοιχα, όταν το AP έχει αποθηκευμένα πλαίσια τα οποία προορίζονται για πολλούς ή για όλους τους σταθμούς (multicast or broadcast frames) και θέλει να εξασφαλίσει ότι αυτοί οι σταθμοί είναι σε ενεργή κατάσταση, στέλνει ένα Delivery Traffic Indication Message (DTIM) ως μέρος ενός beacon πλαισίου και αρχίζει αμέσως να μεταδίδει τα δεδομένα. Αν το AID ενός σταθμού βρισκόταν στο DTIM, ο σταθμός αυτός παραμένει ενεργός για να λάβει τα αποθηκευμένα πλαίσια από το AP [19].

Οι δύο παραπάνω διαδικασίες συμβαίνουν σε infrastructure BSS. Στα IBSS, που δεν υπάρχει ένας κεντρικός σταθμός, όταν ένας σταθμός περιέρχεται σε κατάσταση εξοικονόμησης ενέργειας ενημερώνει όλους τους άλλους σταθμούς, οι οποίοι στο εξής θα αποθηκεύουν κάθε πλαίσιο που προοριζόταν για το σταθμό αυτό. Περιοδικά όλοι οι σταθμοί ξυπνούν και ενημερώνουν ο ένας τον άλλον για τα αποθηκευμένα πλαίσια. Αυτή η επαναλαμβανόμενη χρονική περίοδος είναι γνωστή ως announcement traffic indication message (ATIM) window. Κατά τη διάρκεια του ATIM παραθύρου, αν ένας σταθμός έχει αποθηκευμένα δεδομένα για κάποιον άλλο σταθμό, θα στείλει ένα ATIM πλαίσιο στο σταθμό αυτό για να του υποδείξει ότι πρέπει να μείνει ενεργός μέχρι το επόμενο ATIM παράθυρο για να παραλάβει τα αποθηκευμένα δεδομένα. Όταν το ATIM παράθυρο λήξει, οι σταθμοί που έχουν ενεργοποιηθεί θα χρησιμοποιήσουν τη CSMA/CA διαδικασία για την ανταλλαγή των δεδομένων. Αν ένας σταθμός δεν καταφέρει να μεταδώσει την πρώτη φορά, απλά θα στείλει ένα άλλο ATIM πλαίσιο στο επόμενο ATIM παράθυρο και θα προσπαθήσει πάλι να στείλει τα δεδομένα στην ακόλουθη CSMA/CA περίοδο [19].

2.8 Πλαίσια του 802.11

Τα 802.11 πλαίσια είναι πιο πολύπλοκα καθώς το ασύρματο μέσο απαιτεί διάφορα χαρακτηριστικά διαχείρισης και αντίστοιχους τύπους πλαισίων που δεν συναντούνται στα ενσύρματα δίκτυα.

2.8.1 Μορφή του 802.11 MAC πλαισίου

Τα 802.11 πλαίσια μοιράζονται κάποια κοινά χαρακτηριστικά με όλα τα IEEE 802 πλαίσια. Ωστόσο, ένα ξεχωριστό χαρακτηριστικό των 802.11 πλαισίων είναι το μέγεθός τους. Μπορούν να μεταφέρουν μέχρι 2,304 bytes δεδομένων ενώ το μέγεθος ενός 802.3 πλαισίου είναι 1,518 bytes [19]. Επίσης, τα 802.11 MAC πλαίσια έχουν τέσσερα πεδία διευθύνσεων έναντι δύο πεδίων που συναντάμε στο 802.3. Η εικόνα 2.14 αναπαριστά τη γενική μορφή ενός 802.11 MAC πλαισίου.

Εικόνα 2.14 Γενική μορφή ενός 802.11 MAC πλαισίου [1]

2.8.1.1 Frame control

Κάθε πλαίσιο ξεκινάει με το πεδίο Frame Control το οποίο έχει μήκος 2 byte. Τα συστατικά αυτού του πεδίου φαίνονται στην εικόνα 2.15 και είναι τα εξής:

Protocol version

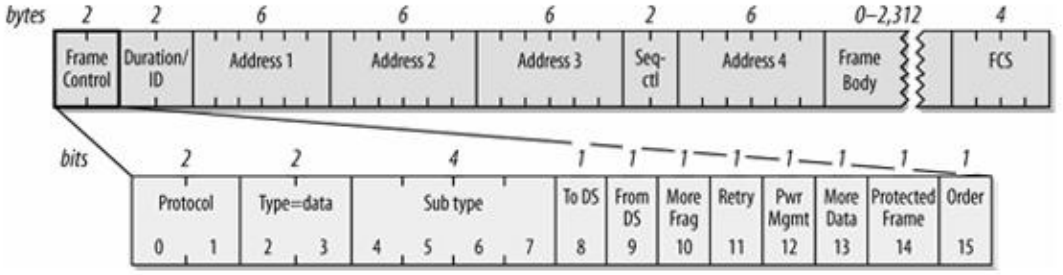
Δύο bits υποδεικνύουν την έκδοση του 802.11 MAC. Ωστόσο, μέχρι στιγμής μόνο μία έκδοση του 802.11 MAC υπάρχει κι έτσι η τιμή αυτού του πεδίου έχει οριστεί να είναι 0 [1].

Type και subtype

Τα δύο αυτά πεδία συνδυάζονται για να προσδιορίσουν τον τύπο του πλαισίου. Το υποπεδίο type μπορεί να έχει τιμή 00 προσδιορίζοντας ένα πλαίσιο διαχείρισης, 01 για τα πλαίσια ελέγχου ή 10 για πλαίσια δεδομένων [15].

ToDS και FromDS bits

Αυτά τα δύο bits δείχνουν αν το πλαίσιο προορίζεται ή προέρχεται, αντίστοιχα, από το σύστημα διανομής. Η ερμηνεία των πεδίων διεύθυνσης εξαρτάται από αυτά τα bits.



Εικόνα 2.15 Το πεδίο Frame Control [1]

More fragments bit

Όταν σε ένα πακέτο έχει γίνει τμηματοποίηση (fragmentation) από το MAC, όλα τα τμήματα εκτός από το τελικό θέτουν σ' αυτό το bit την τιμή 1 για να υποδείξουν ότι ακολουθούν κι άλλα τμήματα για το ίδιο πακέτο.

Retry bit

Κάποιες φορές κάποια πλαίσια μπορεί να χρειαστεί να ξανασταλθούν. Κάθε τέτοιο πλαίσιο έχει τιμή 1 στο retry bit έτσι ώστε ο παραλήπτης να μην τα λάβει εις διπλούν.

Power management bit

Αυτό το bit υποδεικνύει αν ο αποστολέας θα είναι σε κατάσταση εξοικονόμησης ενέργειας (PS-mode) μετά την ολοκλήρωση της τρέχουσας μετάδοσης. Η τιμή 1 δείχνει ότι ο σταθμός θα μπει σε αυτή την κατάσταση ενώ η τιμή 0 δείχνει ότι ο σταθμός θα είναι ενεργός. Επειδή τα APs εκτελούν πολλές λειτουργίες διαχείρισης δεν μπορούν να εισέλθουν σε PS-mode και γι' αυτό η τιμή αυτού του bit είναι πάντα 0 στα πλαίσια που μεταδίδουν τα APs.

More data bit

Ένα AP θέτει αυτό το bit για να υποδείξει σε ένα σταθμό που βρίσκεται σε PS-mode ότι υπάρχει τουλάχιστον ένα πλαίσιο αποθηκευμένο γι' αυτόν.

Protected Frame bit

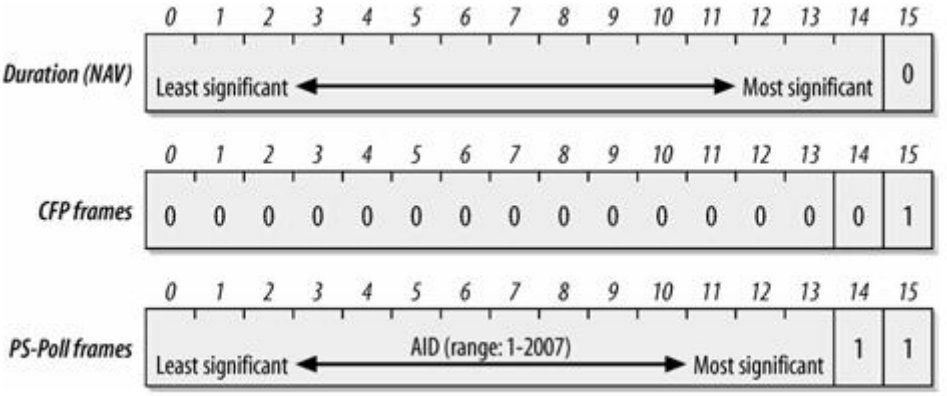
Αυτό το bit παίρνει την τιμή 1 αν το πλαίσιο προστατεύεται από πρωτόκολλα ασφάλειας. Αυτό το bit πρώτα λεγόταν WEP bit.

Order bit

Όταν το bit αυτό έχει τιμή 1 τότε τα πλαίσια και τα τμήματα (fragments) πρέπει να μεταδίδονται και να λαμβάνονται με τη σειρά.

2.8.1.2 Duration/ID Field

Το πεδίο αυτό έχει διάφορες χρήσεις και μπορεί να πάρει μία από τις μορφές που φαίνονται στην εικόνα 2.16.



Εικόνα 2.16 Duration/ID Field [1]

Duration (NAV)

Όταν το bit 15 είναι 0, το πεδίο αυτό χρησιμοποιείται για τη ρύθμιση του NAV.

CFP frames

Κατά τη διάρκεια της CFP περιόδου το bit 14 είναι 0 και το bit 15 είναι 1, ενώ όλα τα υπόλοιπα bits έχουν τιμή 0. Έτσι, το Duration/ID πεδίο

έχει τιμή 32,768. Η τιμή αυτή ερμηνεύεται ως NAV και επιτρέπει στους σταθμούς, που δεν έλαβαν το πλαίσιο φάρο (beacon) που ανακοίνωσε την έναρξη της CFP περιόδου, να ενημερώσουν τον NAV με μία τιμή αρκετά μεγάλη ώστε να μην παρεμβληθούν σε μία CFP μετάδοση.

PS-Poll frames

Όταν τα bits 14 και 15 έχουν και τα δύο τιμή 1, πρόκειται για ένα PS-Poll frame που στέλνει ένας σταθμός στο AP όταν εξέρχεται από PS-mode για να λάβει τυχόν αποθηκευμένα πλαίσια που προορίζονται γι' αυτόν.

2.8.1.3 Address fields

Υπάρχουν τέσσερα πεδία διεύθυνσης τα οποία περιέχουν κάποιους από τους παρακάτω τύπους MAC διευθύνσεων: διεύθυνση πηγής (source address), διεύθυνση προορισμού (destination address), διεύθυνση αποστολέα (transmitter address), διεύθυνση παραλήπτη (receiver address) και BSSID. Κάποια πλαίσια δεν περιλαμβάνουν και τα τέσσερα αυτά πεδία. Όπως στο 802.3 πρότυπο έτσι και στο 802.11 οι MAC διευθύνσεις έχουν μήκος 48bits και μπορεί να περιγράφουν τη διεύθυνση ενός συγκεκριμένου σταθμού (individual address) ή μιας ομάδας σταθμών (multicast address) ή όλους τους σταθμούς (broadcast address).

Destination address (DA)

Είναι η διεύθυνση του τελικού παραλήπτη που θα λάβει το πλαίσιο και θα το μεταφέρει στα ανώτερα επίπεδα για επεξεργασία.

Source address (SA)

Αυτή είναι η διεύθυνση του αποστολέα.

Receiver address (RA)

Αυτή η διεύθυνση υποδεικνύει το σταθμό που θα λάβει το πλαίσιο από το ασύρματο μέσο. Αν ο σταθμός αυτός είναι ο τελικός παραλήπτης τότε η RA είναι ίδια με την DA. Πολλές φορές όμως ο παραλήπτης είναι

ένας ενδιάμεσος σταθμός οπότε οι δύο αυτές διευθύνσεις είναι διαφορετικές.

Transmitter address (TA)

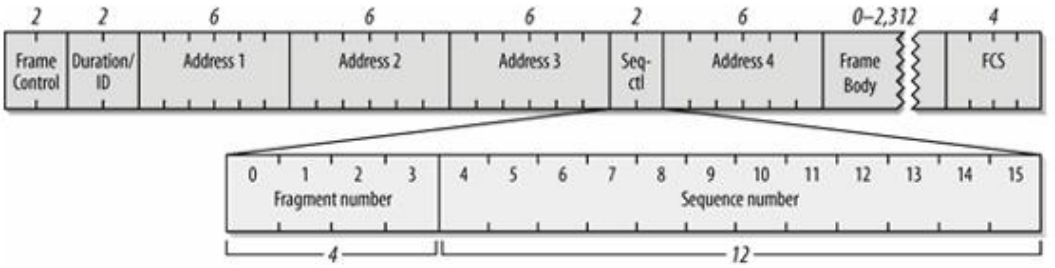
Η διεύθυνση αυτή υποδεικνύει την ασύρματη διεπαφή που μετέδωσε το πλαίσιο στο ασύρματο μέσο.

Basic Service Set ID (BSSID)

Σε κάθε σταθμό που συνδέεται σε ένα ασύρματο δίκτυο εκχωρείται το αναγνωριστικό (BSSID) του συγκεκριμένου δικτύου. Στα BSS δίκτυα το BSSID είναι η διεύθυνση MAC του AP ενώ τα IBSS δίκτυα παράγουν τυχαία BSSID.

2.8.1.4 Sequence Control Field

Αυτό το πεδίο χρησιμοποιείται για τη συναρμολόγηση των τμημάτων (defragmentation) και για απόρριψη διπλότυπων πλαισίων. Τέσσερα από τα 16 bits χρησιμοποιούνται για να προσδιορίσουν τον αριθμό του τμήματος (fragment number) και τα υπόλοιπα 12bits αποτελούν τον αριθμό ακολουθίας.



Εικόνα 2.17 Sequence Control Field [1]

Σε κάθε πακέτο που περνάει στο επίπεδο MAC για μετάδοση, δίνεται ένας αριθμός ακολουθίας. Αν ένα πακέτο τμηματοποιηθεί, όλα τα τμήματα θα έχουν τον ίδιο αριθμό ακολουθίας. Αυτό που αλλάζει σε κάθε τμήμα είναι ο αριθμός τμήματος. Το πρώτο τμήμα έχει αριθμό τμήματος 0 και κάθε επόμενο τμήμα αυξάνει τον αριθμό αυτό κατά ένα. Τμήματα που ξαναμεταδίδονται, διατηρούν τον ίδιο αριθμό τμήματος [20].

2.8.1.5 Frame body

Αυτό το πεδίο μεταφέρει τα δεδομένα. Το μέγιστο ωφέλιμο φορτίο για το 802.11 είναι 2,304 bytes χωρίς κρυπτογράφηση ή 2,312 όταν το σώμα του πλαισίου είναι κρυπτογραφημένο [20].

2.8.1.6 Frame Check Sequence

Όπως και το Ethernet, το 802.11 πλαίσιο κλείνει με ένα πεδίο ελέγχου ορθότητας ολόκληρου του πλαισίου. Το FCS επιτρέπει στους σταθμούς να ελέγχουν την ακεραιότητα των ληφθέντων πλαισίων.

2.8.2 Τύποι πλαισίων του 802.11

Το 802.11 έχει τρεις τύπους πλαισίων. Υπάρχουν τα πλαίσια δεδομένων (data frames), τα πλαίσια ελέγχου (control frames) και τα πλαίσια διαχείρισης (management frames).

2.8.2.1 Πλαίσια δεδομένων

Τα πλαίσια δεδομένων μεταφέρουν δεδομένα των ανώτερων επιπέδων. Η μορφή των πλαισίων αυτών ποικίλει ανάλογα με τη λειτουργία που επιτελούν. Οι δύο βασικότεροι υποτύποι, που χρησιμοποιούνται μόνο από τη DCF, είναι τα πλαίσια δεδομένων (subtype=Data) και τα Null πλαίσια (subtype=Null). Τα πλαίσια Data χρησιμοποιούνται για τη μεταφορά των δεδομένων από σταθμό σε σταθμό ενώ τα Null πλαίσια στέλνονται από τους σταθμούς στα APs όταν πρόκειται να εισέλθουν σε PS-mode.

2.8.2.2 Control frames

Τα πλαίσια αυτά βοηθούν στην παράδοση των πλαισίων δεδομένων. Χρησιμοποιούνται για τη δέσμευση του καναλιού και την αποστολή επιβεβαιώσεων. Αποτελούνται μόνο από την κεφαλή και το πεδίο FCS. Τα πλαίσια ελέγχου είναι τα ακόλουθα:

- Request To Send (RTS)
- Clear To Send (CTS)

- Acknowledgement (ACK)
- Power Save (PS)-Poll
- Contention-Free (CF)-End (PCF-Only)
- CF-End + CF-ACK (PCF-Only)

2.8.2.3 Management frames

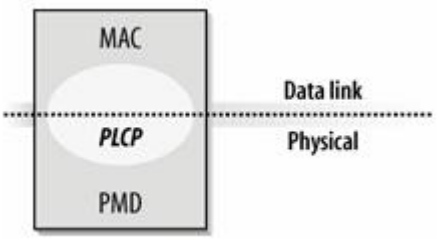
Τα πλαίσια διαχείρισης είναι αυτά που δίνουν τη δυνατότητα στους σταθμούς να εγκαθιδρύουν και να διατηρούν τις επικοινωνίες. Τα πλαίσια διαχείρισης είναι τα εξής:

- Πλαίσια πιστοποίησης ταυτότητας (authentication frames)
- Πλαίσια ακύρωσης της πιστοποίησης ταυτότητας (deauthentication frames)
- Πλαίσια αίτησης για συσχέτιση (association request frames)
- Πλαίσια απάντησης για συσχέτιση (association response frames)
- Πλαίσια αίτησης επανασυσχέτισης (reassociation request frames)
- Πλαίσια απάντησης επανασυσχέτισης (reassociation response frames)
- Πλαίσια αποσυσχέτισης (disassociation frames)
- Πλαίσια φάροι (beacon frames)
- Πλαίσια αίτησης διερεύνησης (Probe request frames)
- Πλαίσια απάντησης διερεύνησης (Probe response frames)

Κεφάλαιο 3 Φυσικό επίπεδο (PHY layer)

3.1 Φυσικό επίπεδο

Το 802.11 πρότυπο εστιάζει στα δύο χαμηλότερα επίπεδα του μοντέλου OSI, στο υποεπίπεδο MAC του DLL επιπέδου και στο φυσικό επίπεδο (PHY). Το φυσικό επίπεδο χωρίζεται σε δύο επιμέρους επίπεδα: το Physical Layer Convergence Procedure (PLCP) και το Physical Medium Dependent (PMD), όπως φαίνεται και στην εικόνα 3.1.



Εικόνα 3.1 Αρχιτεκτονική φυσικού επιπέδου [1]

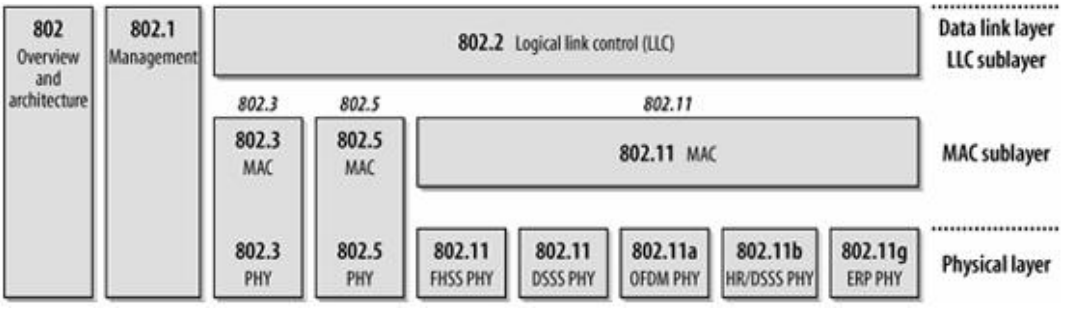
Το υποεπίπεδο PLCP βρίσκεται ανάμεσα στο επίπεδο MAC και το υποεπίπεδο PMD. Η λειτουργία που επιτελεί είναι να μετατρέπει τα πλαίσια που λαμβάνει από το MAC σε μία μορφή κατάλληλη για μετάδοση από το PMD. Σε κάθε πλαίσιο MAC, το PLCP προσθέτει τη δική του κεφαλίδα. Το υποεπίπεδο PMD είναι αυτό που έρχεται σε επαφή με το μέσο και είναι υπεύθυνο για τη μετάδοση και την παραλαβή των δεδομένων. Η διαμόρφωση και αποδιαμόρφωση των σημάτων είναι δουλειά του υποεπιπέδου αυτού. Το φυσικό επίπεδο περιλαμβάνει και μία λειτουργία εκτίμησης του καναλιού (clear channel assessment, CCA) για την ανίχνευση μεταδόσεων [1].

3.1.1 Τεχνολογίες φυσικού επιπέδου

Το αρχικό 802.11 πρότυπο όριζε τρεις τεχνολογίες φυσικού επιπέδου: Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας ή FHSS (Frequency Hopping Spread Spectrum), Εξάπλωση Φάσματος Άμεσης Ακολουθίας ή DSSS (Direct Sequence Spread Spectrum) και μία τεχνολογία υπέρυθρης ακτινοβολίας (Infrared, IR). Και οι τρεις τεχνολογίες υποστηρίζουν ρυθμούς μετάδοσης 1 και 2Mbps. Η IR τεχνολογία δεν έγινε ποτέ δημοφιλής καθώς τα

IR σήματα δεν μπορούν να διαπεράσουν συμπαγή αντικείμενα και σε περιβάλλοντα με πολύ φως τα IR εξασθενούν εύκολα [20].

Αργότερα, η ανάγκη για υψηλότερους ρυθμούς μετάδοσης οδήγησε στην υλοποίηση νέων τεχνολογιών φυσικού επιπέδου. Ρυθμοί μετάδοσης έως 11Mbps έγιναν πραγματικότητα με το High-Rate Direct Sequence (HR/DSSS) PHY που ορίζεται στο 802.11b ενώ τα 54Mbps ήταν ο στόχος του 802.11a, χρησιμοποιώντας Orthogonal Frequency Division Multiplexing (OFDM) PHY και αργότερα του 802.11g χρησιμοποιώντας το Extended Rate OFDM PHY (ERP- OFDM). Στην εικόνα φαίνεται η σχέση του 802.11 με το μοντέλο OSI καθώς και οι διάφορες τεχνολογίες φυσικού επιπέδου που χρησιμοποιεί.



Εικόνα 3.2 Τεχνολογίες φυσικού επιπέδου [1]

3.1.2 Εξάπλωση φάσματος (Spread Spectrum, SS)

Μία από τις βασικότερες τεχνολογίες που χρησιμοποιεί το 802.11 είναι η εξάπλωση φάσματος. Η SS τεχνική χρησιμοποιεί περισσότερο εύρος από αυτό που είναι απαραίτητο για τη μετάδοση της πληροφορίας εξαπλώνοντας την ισχύ του σήματος σε ένα μεγάλο φάσμα συχνοτήτων. Με αυτόν τον τρόπο καταναλώνεται μεγάλο τμήμα του εύρους ζώνης αλλά ταυτόχρονα ενισχύεται η αξιοπιστία, η ακεραιότητα και η ασφάλεια των μεταδόσεων.

Η εξάπλωση των σημάτων σε ένα ευρύ φάσμα συχνοτήτων, τα κάνει να φαίνονται σαν τυχαίος θόρυβος κι έτσι είναι δύσκολο να ανιχνευθούν ή να υποκλαπούν από έναν δέκτη που χρησιμοποιεί μια στενή ζώνη συχνοτήτων (narrowband receiver). Επίσης, τα SS συστήματα είναι αρκετά ευέλικτα όσον

αφορά το πρόβλημα των πολλαπλών διαδρομών (multipath) και των επακόλουθων παρεμβολών μεταξύ των σημάτων (inter-symbol interference, ISI). Αυτό συμβαίνει γιατί χρησιμοποιούνται πολλές συχνότητες για τη μεταφορά του σήματος, κάποιες από τις οποίες μπορεί να επηρεαστούν από αυτά τα φαινόμενα ενώ κάποιες άλλες όχι [20]. Τέλος, επειδή η ισχύς των SS σημάτων εξαπλώνεται σε ένα μεγάλο εύρος, τα σήματα αυτά μπορούν να συνυπάρχουν με σήματα στενών συχνοτήτων χωρίς να παρουσιάζονται παρεμβολές.

Οι δύο βασικές SS τεχνικές που χρησιμοποιεί το 802.11 είναι οι Direct Sequence (DS) και Frequency Hopping (FH). Η DSSS διασκορπίζει το σήμα χρησιμοποιώντας επιπλέον bits για κάθε bit που μεταδίδει. Όσα περισσότερα bits χρησιμοποιούνται για την κωδικοποίηση τόσο πιο εύκολη γίνεται η ανάκτηση των δεδομένων. Στα FHSS συστήματα το σήμα αλλάζει συνεχώς συχνότητα βάσει μίας ακολουθίας, γνωστής και στον πομπό και στον δέκτη.

Στα FH συστήματα πρέπει να υπάρχει καλός συγχρονισμός πομπού και δέκτη, καθώς πρέπει να εναλλάσσονται ταυτόχρονα, αλλά γενικά είναι πιο απλά και οικονομικά στην υλοποίηση και καταναλώνουν λιγότερη ενέργεια από τα DSSS συστήματα, τα οποία πρέπει να λειτουργήσουν σε υψηλότερο ρυθμό για να μεταδώσουν τα πλεονάζοντα bits. Επιπλέον, η FHSS τεχνική είναι πιο ανεκτική στο θόρυβο από την DSSS τεχνική. Ωστόσο, η DS τεχνική έχει τη δυνατότητα για υψηλότερους ρυθμούς μετάδοσης από την FH τεχνική [1].

3.2 Εξάπλωση Φάσματος με συνεχή Αλλαγή Συχνότητας (Frequency Hopping Spread Spectrum, FHSS)

Αλλαγή συχνότητας είναι μία από τις τεχνικές εξάπλωσης φάσματος που χρησιμοποιεί το 802.11 πρότυπο με ρυθμούς μετάδοσης 1 και 2 Mbps στα 2.4GHz της ISM ζώνης συχνοτήτων. Αρχικά, ένα από τα βασικά πλεονεκτήματα της χρήσης FH δικτύων ήταν ότι ένας μεγαλύτερος αριθμός δικτύων μπορούσαν να συνυπάρχουν και η συνολική απόδοση όλων των

δικτύων σε μια συγκεκριμένη περιοχή ήταν υψηλή [1]. Ωστόσο, με 1MHz εύρος διαθέσιμο κάθε στιγμή, ο ρυθμός μετάδοσης δεν ξεπερνά τα 2Mbps κι έτσι η τεχνική αυτή δε χρησιμοποιείται ιδιαίτερα, με εξαίρεση τις Bluetooth συσκευές που είναι ιδιαίτερα δημοφιλείς [15].

3.2.1 Μετάδοση με αλλαγή συχνοτήτων

Σε ένα ασύρματο δίκτυο που χρησιμοποιεί τεχνολογία μετάδοσης FHSS η συχνότητα μετάδοσης αλλάζει συνεχώς βάσει μιας προκαθορισμένης ψευδοτυχαίας ακολουθίας (hopping sequence). Κάθε χώρα έχει ορίσει για χρήση έναν αριθμό καναλιών με 1MHz εύρος το καθένα. Στη Βόρεια Αμερική και στις περισσότερες ευρωπαϊκές χώρες χρησιμοποιούνται 79 από αυτά τα κανάλια του 1MHz, ξεκινώντας από τα 2.402GHz ως τα 2.480 GHz. Άλλες χώρες ορίζουν διαφορετικό αριθμό καναλιών. Στον πίνακα 3.1 φαίνονται τα κανάλια που χρησιμοποιεί η FHSS τεχνική, όπως αυτά ορίζονται από τις διάφορες ρυθμιστικές αρχές.

Regulatory domain	Allowed channels
U.S. (FCC)	2 to 79 (2.402-2.479 GHz)
Canada (IC)	2 to 79 (2.402-2.479 GHz)
Europe (excluding France and Spain) (ETSI)	2 to 79 (2.402-2.479 GHz)
France	48 to 82 (2.448-2.482 GHz)
Spain	47 to 73 (2.447-2.473 GHz)
Japan (MKK)	73 to 95 (2.473-2.495 GHz)

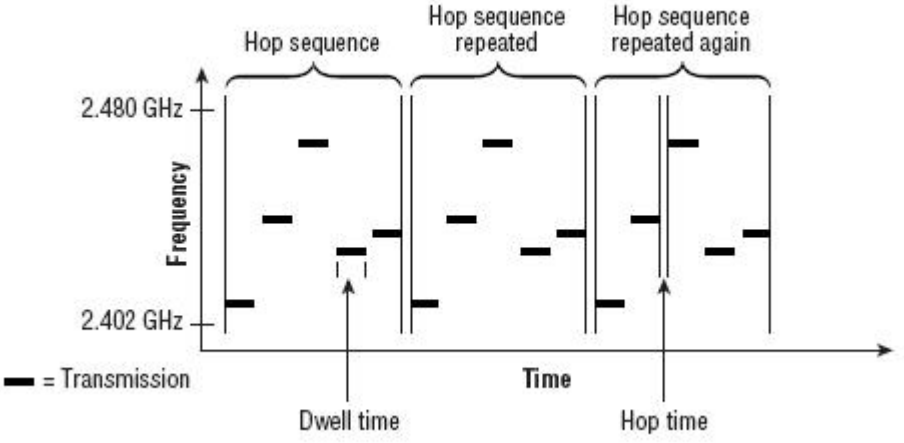
Πίνακας 3.1 FHSS χρησιμοποιούμενα κανάλια [1]

Επίσης, κάθε χώρα ορίζει συγκεκριμένες ακολουθίες συχνοτήτων. Για παράδειγμα, στην Ευρώπη και τη Βόρεια Αμερική υπάρχουν τρία σετ ακολουθιών με 26 κανάλια η κάθε μία. Σε άλλες περιοχές που οι ρυθμιστικές αρχές ορίζουν μικρότερο αριθμό καναλιών τα σετ των ακολουθιών έχουν διαφορετικό αριθμό μελών (πίνακας 3.2) [1][14][20].

Regulatory domain	Hop set size
U.S. (FCC)	26
Canada (IC)	26
Europe (excluding France and Spain) (ETSI)	26
France	27
Spain	35
Japan (MIC)	23

Πίνακας 3.2 Μέγεθος ομάδων των ακολουθιών ανά ρυθμιστική περιοχή [1]

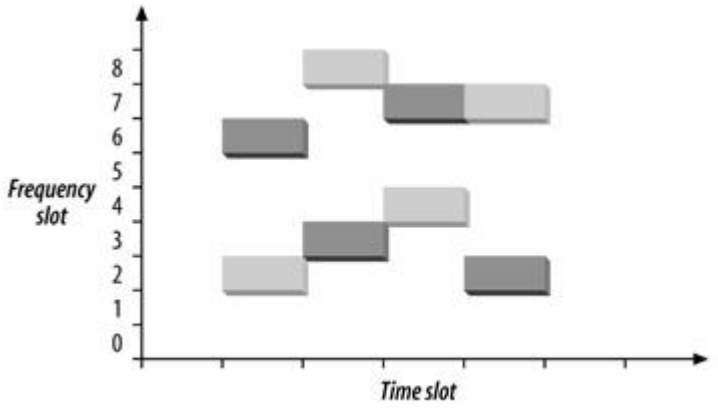
Η χρονική διάρκεια χρήσης κάθε καναλιού ονομάζεται χρόνος παραμονής (dwell time) και δεν πρέπει να υπερβαίνει τα 400ms. Όταν η ακολουθία ολοκληρωθεί, επαναλαμβάνεται και η διαδικασία αυτή συνεχίζει μέχρι να τελειώσει η μετάδοση [15]. Ο χρόνος που χρειάζεται για τη μετάβαση από τη μία συχνότητα στην άλλη ονομάζεται χρόνος μετάβασης (hop time) και πρέπει να είναι μέχρι 224μs [19]. Η εικόνα 3.3 δείχνει τους χρόνους που χρησιμοποιεί η FH και τον τρόπο που μια ακολουθία επαναλαμβάνεται.



Εικόνα 3.3 Συστατικά της FHSS τεχνικής [19]

Για να μπορέσουν δύο FH συστήματα να συνυπάρξουν, θα πρέπει να ρυθμιστούν με μία διαφορετική ακολουθία για να μην παρεμβάλλεται το ένα στο άλλο. Σε κάθε χρονική περίοδο (time slot) τα δύο συστήματα θα πρέπει να βρίσκονται σε διαφορετικό κανάλι της ακολουθίας (frequency slot). Οι ακολουθίες που δεν επικαλύπτονται ονομάζονται ορθογώνιες. Όπως φαίνεται

στην εικόνα 3.4, ένα σύστημα χρησιμοποιεί την ακολουθία {2,8,4,7} και ένα άλλο την {6,3,7,2}, η οποία είναι ορθογώνια στην πρώτη κι έτσι δεν υπάρχουν επικαλύψεις.



Εικόνα 3.4 Ορθογώνιες ακολουθίες συχνοτήτων [1]

Η εναλλαγή της συχνότητας μπορεί να είναι γρήγορη (fast FH), γεγονός που σημαίνει ότι η συχνότητα αλλάζει για κάθε μεταδιδόμενο σύμβολο, ή αργή (slow FH) όταν δύο ή περισσότερα σύμβολα μεταδίδονται σε κάθε συχνότητα [20].

3.2.2 Σύνδεση σε ένα FH δίκτυο

Όταν ένας σταθμός θέλει να συνδεθεί σε ένα FHSS δίκτυο, βρίσκει όλη την απαραίτητη πληροφορία στα πλαίσια φάρους (beacon frames) που εκπέμπουν τα APs. Τα πλαίσια αυτά περιέχουν μία χρονοσφραγίδα (timestamp) και το στοιχείο FH Parameter Set. Η χρονοσφραγίδα ορίζει πότε θα συμβαίνει μία μετάβαση. Το FH Parameter Set περιλαμβάνει τον αριθμό ακολουθίας που χρησιμοποιείται και έναν δείκτη ο οποίος υποδεικνύει τη συγκεκριμένη συχνότητα της ακολουθίας που βρίσκεται τη συγκεκριμένη στιγμή το δίκτυο. Έτσι ο σταθμός μπορεί να συγχρονίσει και τη δική του ακολουθία [1].

3.2.3 Τεχνικές διαμόρφωσης

Η FHSS τεχνολογία χρησιμοποιεί τη διαμόρφωση Two-level Gaussian Frequency Shift Key (2GFSK) για μετάδοση στο 1Mbps και την Four-level

Gaussian Frequency Shift Key (4GFSK) διαμόρφωση για μετάδοση στα 2Mbps. Η 2GFSK κωδικοποιεί ένα bit σε κάθε σύμβολο. Έτσι με εύρος 1MHz μπορούν να μεταδοθούν ένα εκατομμύριο σύμβολα το δευτερόλεπτο. Η 4GFSK κωδικοποιεί δύο bits σε κάθε σύμβολο. Έτσι με ένα εκατομμύριο σύμβολα ανά δευτερόλεπτο προκύπτουν τα 2Mbps . Αυτό όμως ισχύει μόνο για το σώμα του πλαισίου καθώς η κεφαλή του PLCP διαμορφώνεται με 2GFSK και μεταδίδεται με 1Mbps [1]. Επίσης, για να μοιάζουν τα δεδομένα περισσότερο με τυχαίο θόρυβο, το PMD κωδικοποιεί τις τυχόν μακριές σειρές από αλλεπάλληλα 0 ή 1 εφαρμόζοντας έναν whitening αλγόριθμο στα πλαίσια. Ο αλγόριθμος αυτός εφαρμόζεται μόνο στα δεδομένα και όχι στην PLCP κεφαλή. Οι δέκτες αντιστρέφουν τη διαδικασία για να ανακτήσουν τα δεδομένα [20].

3.2.4 Πλεονεκτήματα

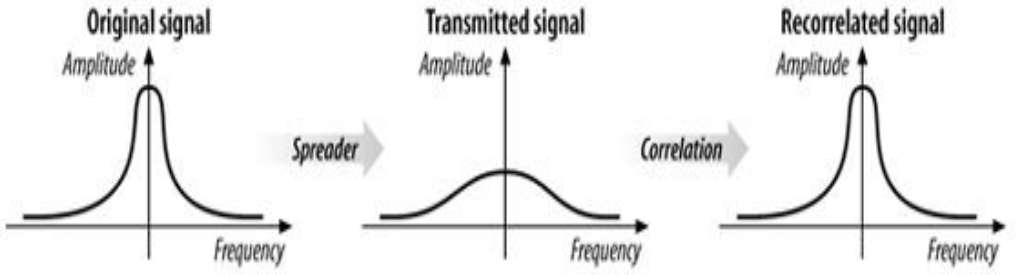
Η FHSS είναι αρκετά ανθεκτική στις ραδιοκυματικές παρεμβολές και στο πρόβλημα της εξασθένησης πολλαπλών διαδρομών, καθώς το σύστημα αλλάζει συνεχώς συχνότητα. Αν ένα από τα παραπάνω φαινόμενα εμφανιστεί σε ένα κανάλι, θα επηρεάσει το συγκεκριμένο μόνο κανάλι αφήνοντας, πιθανότατα, ανεπηρέαστα τα υπόλοιπα. Για παράδειγμα, αν ένα πλαίσιο που μεταφέρεται με μία συγκεκριμένη συχνότητα, δεν μπορέσει να παραληφθεί λόγω εμφάνισης παρεμβολών, απλά ξαναστέλνεται όταν ο πομπός μεταβεί στην επόμενη συχνότητα [15]. Επίσης, η FH τεχνική παρέχει κάποια περιορισμένη ασφάλεια, αφού ένας εισβολέας που δε γνωρίζει την ακολουθία συχνοτήτων ή το χρόνο παραμονής δεν μπορεί να υποκλέψει τις μεταδόσεις. [25]. Τέλος, η συνολική απόδοση όλων των FH δικτύων σε μια περιοχή μπορεί να είναι αρκετά υψηλή. Για παράδειγμα στην Αμερική μπορούν να ρυθμιστούν 26 FH δίκτυα, ανά σετ, σε μία περιοχή. Αν κάθε ένα από αυτά τα δίκτυα λειτουργεί στα 2Mbps και το μισό του χρόνου χρησιμοποιείται για μεταφορά δεδομένων, η συνολική απόδοση στην περιοχή αυτή θα είναι 26Mbps [1].

3.3 Εξάπλωση φάσματος άμεσης ακολουθίας (Direct Sequence Spread Spectrum, DSSS)

Η DSSS τεχνική έχει οριστεί στο αρχικό 802.11 πρότυπο, χρησιμοποιεί την 2.4GHz ISM ζώνη συχνοτήτων και παρέχει ρυθμούς μετάδοσης 1 και 2 Mbps. Η DSSS ορίζεται αργότερα και στην 802.11b προδιαγραφή παρέχοντας ρυθμούς μετάδοσης 5.5 και 11 Mbps χρησιμοποιώντας την ίδια ζώνη συχνοτήτων. Αυτή η βελτιωμένη έκδοση του 802.11 είναι γνωστή ως High-Rate DSSS (HR-DSSS).

3.3.1 Direct Sequence

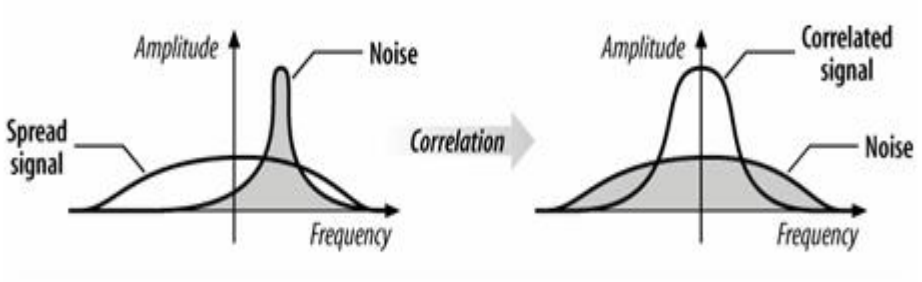
Η κεντρική ιδέα σε ένα DS σύστημα είναι η εξάπλωση της ηλεκτρομαγνητικής ενέργειας σε μία ευρύτερη ζώνη συχνοτήτων. Αυτό επιτυγχάνεται με τη χρήση θραυσμάτων για τη διαμόρφωση των προς μετάδοση δεδομένων. Τα θραύσματα αυτά είναι δυαδικά ψηφία, γνωστά και ως ψευδοτυχαίοι κωδικοί θορύβου (Pseudorandom Noise codes, PN) και αποτελούν μέρος της διαδικασίας κωδικοποίησης και μεταφοράς αλλά τα ίδια δεν μεταφέρουν (αποτελούν) πληροφορία. Η αναλογία ανάμεσα στον αριθμό των θραυσμάτων και τα δεδομένα είναι γνωστή ως processing gain. Όσο μεγαλύτερη είναι αυτή η αναλογία τόσο βελτιώνεται η δυνατότητα ανάκτησης των δεδομένων αλλά ταυτόχρονα απαιτείται και μεγαλύτερο εύρος [1]. Για τους PN codes το 802.11 χρησιμοποιεί μία λέξη Barker των 11 bit που έχει την εξής μορφή: {+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1}. Τα +1 αντιστοιχούν σε 1 και τα -1 σε 0, έτσι η ακολουθία γίνεται: 10110111000. Η ακολουθία αυτή εφαρμόζεται σε κάθε bit δεδομένων με έναν modulo-2 προσθέτη. Έτσι, όταν κωδικοποιείται ένα 1 όλα τα bit αλλάζουν ενώ για το 0 μένουν ως έχουν [1]. Κάθε ακολουθία θραυσμάτων που παράγεται, μεταδίδεται στο μέσο και στο δέκτη συγκρίνεται με μία πανομοιότυπη ακολουθία για να αποκαλυφθούν τα πραγματικά δεδομένα. Εκτελείται δηλαδή μία συνάρτηση συσχετισμού (correlation function), η οποία ουσιαστικά αντιστρέφει τη διαδικασία εξάπλωσης του σήματος και τα σήματα παίρνουν την αρχική τους μορφή. Στην εικόνα 3.5 φαίνεται η βασική λειτουργία της DSSS τεχνικής.



Εικόνα 3.5 Βασική περιγραφή της DSSS τεχνικής [1]

Αριστερά είναι ένα συνηθισμένο σήμα στενής συχνότητας. Στη συνέχεια, μέσω μαθηματικών μετασχηματισμών που εφαρμόζονται από έναν μηχανισμό εξάπλωσης (spreader), το πλάτος του σήματος απλώνεται σε ένα ευρύ φάσμα συχνοτήτων. Τέλος, στο δέκτη εκτελείται η διαδικασία συσχετισμού και το σήμα παίρνει την αρχική του μορφή.

Επίσης, με τη διαδικασία συσχετισμού το σήμα μπορεί να απαλλαγεί από τυχών θόρυβο που παρεμβλήθηκε στη μετάδοση. Όπως φαίνεται στην εικόνα 3.6, ο θόρυβος συνήθως έχει τη μορφή στενών παλμών οι οποίοι επηρεάζουν μόνο ένα μικρό κομμάτι των χρησιμοποιούμενων συχνοτήτων. Σε αυτήν την περίπτωση, η διαδικασία συσχετισμού εξαπλώνει το θόρυβο σε όλο το εύρος των συχνοτήτων ενώ παράλληλα το συσχετισμένο σήμα παίρνει την αρχική του μορφή και διακρίνεται ξεκάθαρα.



Εικόνα 3.6 Εξάπλωση του θορύβου μέσω της διαδικασίας συσχετισμού [1]

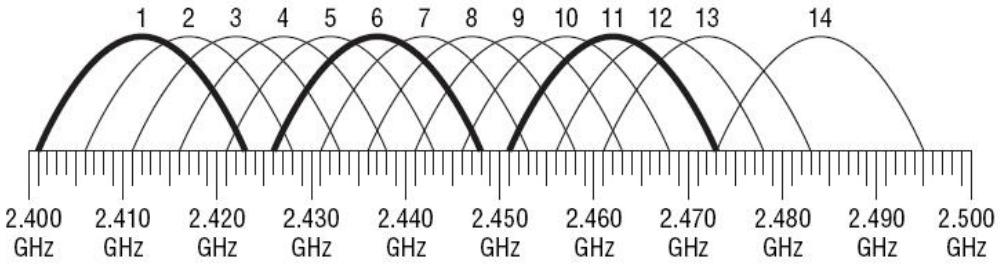
3.3.2 Τεχνικές διαμόρφωσης

Πριν τη μετάδοση, τα κωδικοποιημένα δεδομένα πρέπει να διαμορφωθούν. Για μετάδοση στο 1 Mbps, το 802.11 DS PHY χρησιμοποιεί την Differential Binary Phase-Shift Keying (DBPSK) τεχνική διαμόρφωσης.

Στα 2 Mbps χρησιμοποιείται η DBPSK για το προοίμιο και την κεφαλή και η Differential Quadrature Phase-Shift Keying (DQPSK) για τη διαμόρφωση των δεδομένων. Όπως στην FHSS τεχνική, έτσι κι εδώ εφαρμόζεται ένας μηχανισμός, που ονομάζεται scrambler, για την απομάκρυνση αλλεπάλληλων άσσων ή μηδενικών, ο οποίος όμως εφαρμόζεται σε ολόκληρο το πλαίσιο συμπεριλαμβανομένου του προοιμίου και της κεφαλής [1].

3.3.3 Κανάλια λειτουργίας

Η τεχνολογία DS χρησιμοποιεί 14 κανάλια στη ζώνη των 2.4GHz με 22MHz εύρος το καθένα και με 5MHz απόσταση το ένα από το άλλο. Συνεπώς, τα κανάλια είναι μερικώς επικαλυπτόμενα (Εικόνα 3.7).



Εικόνα 3.7 Κανάλια λειτουργίας του 802.11 [19]

Στις Ηνωμένες Πολιτείες και τον Καναδά τα μόνα μη επικαλυπτόμενα κανάλια είναι τα 1, 6 και 11 και γι' αυτό μπορούν να χρησιμοποιηθούν στον ίδιο χώρο χωρίς τον κίνδυνο παρεμβολών. Σε περιοχές που επιτρέπεται η χρήση των καναλιών 1-13 (Ευρώπη) ή 1-14 (Ιαπωνία) μπορούν να υπάρξουν κι άλλοι συνδυασμοί μη επικαλυπτόμενων καναλιών. Ωστόσο, αυτά που επιλέγονται συνήθως είναι τα 1, 6 και 11 [19]. Ο πίνακας 3.3 δείχνει τα επιτρεπόμενα κανάλια των διάφορων ρυθμιστικών περιοχών.

Regulatory domain	Allowed channels
U.S. (FCC)/Canada (IC)	1 to 11 (2.412-2.462 GHz)
Europe, excluding Spain (ETSI)	1 to 13 (2.412-2.472 GHz)
Spain	10 to 11 (2.457-2.462 GHz)
Japan (MIC)	1 to 13 (2.412-2.462 GHz) and 14 (2.484 GHz)

Πίνακας 3.3 Κανάλια λειτουργίας DSSS [1]

3.3.4 Πλεονεκτήματα

Τα DS συστήματα είναι αρκετά ανθεκτικά στις παρεμβολές. Με 11chips/bit μπορούν να καταστραφούν αρκετά chips για να θεωρηθεί ότι χάθηκε ένα bit δεδομένων. Επιπλέον, λόγω του ότι η ισχύς των DS σημάτων εξαπλώνεται σε ένα μεγαλύτερο εύρος, τα σήματα αυτά φαίνονται σαν τυχαίος θόρυβος στους δέκτες στενών συχνοτήτων. Επίσης, DS συστήματα μπορούν να λειτουργούν καλά σε περιβάλλοντα με πηγές θορύβου στενής ζώνης καθώς η συνάρτηση συσχετισμού αντιμετωπίζει αποτελεσματικά τέτοιες παρεμβολές. Τέλος, η DS τεχνική μπορεί να επιτύχει και μεγαλύτερους ρυθμούς μετάδοσης.

3.4 802.11b High-Rate/DSSS (HR/DSSS)

Το αρχικό DSSS PHY των 1 και 2 Mbps φαινόταν ότι είχε τη δυνατότητα να επιτύχει πιο υψηλούς ρυθμούς. Έτσι, το 1999 ένα φυσικό επίπεδο με ρυθμούς μετάδοσης 5.5Mbps και 11Mbps προτυποποιήθηκε στο 802.11b. Το νέο φυσικό επίπεδο ονομάζεται High-Rate/DSSS (HR/DSSS) και όμοια με το αρχικό DSSS λειτουργεί στα 2.4GHz και χρησιμοποιεί τα ίδια κανάλια. Η παλαιότερη 1 και 2 Mbps και η νεότερη 5.5 και 11Mbps τεχνολογίες φυσικού επιπέδου συχνά συνδυάζονται σε μία διεπαφή παρόλο που περιγράφονται από διαφορετικές προδιαγραφές [1].

3.4.1 Complementary Code Keying (CCK)

Τα 802.11 DS συστήματα χρησιμοποιούν 11 εκατομμύρια chips το δευτερόλεπτο. Το αρχικό DSSS διαιρούσε την ακολουθία των chips σε λέξεις Barker των 11bit και μετέδιδε 1 εκατομμύριο τέτοιες λέξεις το δευτερόλεπτο.

Κάθε λέξη Barker κωδικοποιούσε 1 ή 2 bit και οι ρυθμοί μετάδοσης ήταν 1 ή 2Mbps, αντίστοιχα. Για να αυξηθεί ο ρυθμός μετάδοσης, με τη χρήση της ίδιας τεχνικής, θα πρέπει κάθε σύμβολο να κωδικοποιεί περισσότερα από 2 bit. Αυτό όμως σημαίνει ότι οι δέκτες θα πρέπει να μπορούν να ανιχνεύσουν μικρότερες αλλαγές φάσης, κάτι που είναι αρκετά δύσκολο παρουσία παρεμβολών (multipath interference) και που απαιτεί πιο εξειδικευμένη και, ως εκ τούτου, ακριβή τεχνολογία [1].

Έτσι, ήταν απαραίτητη μία άλλη μέθοδος διαμόρφωσης. Η μέθοδος που χρησιμοποιήθηκε ήταν η Complementary Code Keying (CCK). Η CCK διαιρεί την ακολουθία θραυσμάτων σε κωδικοσύμβολα των 8 bit. Αυτό έχει σαν αποτέλεσμα να μεταδίδονται 1.375 εκατομμύρια σύμβολα το δευτερόλεπτο έναντι ενός εκατομμυρίου που μεταδίδονται στο DSSS. Αυτές οι ακολουθίες των 8 bit, με τη χρήση κατάλληλων μαθηματικών μετασχηματισμών, μπορούν να κωδικοποιήσουν 4 ή ακόμα και 8 bit πετυχαίνοντας τα 5.5 και 11 Mbps αντίστοιχα. Η διαδικασία μοιάζει αρκετά με αυτήν που χρησιμοποιείται στο DSSS. Η διαφορά είναι ότι δεν χρησιμοποιείται πλέον μία στατική ακολουθία, όπως η λέξη Barker, αλλά 64 κωδικολέξεις των 8 bit, οι οποίες παράγονται μερικώς από τα δεδομένα και χρησιμοποιούνται τόσο για να εξαπλώσουν το σήμα αλλά και για να μεταφέρουν πληροφορία [1] [20].

3.4.2 Τύποι πλαισίων και πρόσθετα χαρακτηριστικά

Στο HR/DSSS ορίζονται δύο τύποι πλαισίων: το βασικό μακρύ πλαίσιο (long frame) με 192 bits στο προοίμιο, το οποίο είναι συμβατό με τις αρχικές 1Mbps και 2Mbps προδιαγραφές και ένα προαιρετικό μικρό πλαίσιο (short frame) που μειώνει το μήκος του προοιμίου στα 72 bits αυξάνοντας την αποδοτικότητα. Πλαίσια με μικρό προοίμιο χρησιμοποιούνται μόνο όταν όλοι οι σταθμοί ενός δικτύου τα υποστηρίζουν [1] [10].

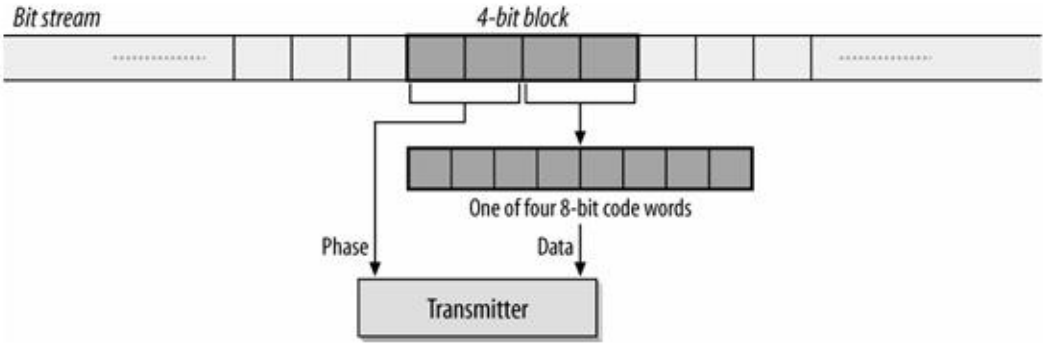
Επίσης, το 802.11b περιλαμβάνει και δύο πρόσθετα χαρακτηριστικά φυσικού επιπέδου. Το πρώτο λέγεται Packet Binary Convolutional Coding (HR/DSSS/PBCC) και έχει στόχο την επίτευξη των 11Mbps. Το άλλο προαιρετικό χαρακτηριστικό ονομάζεται Channel Agility και σχεδιάστηκε για

την αποφυγή των παρεμβολών. Ωστόσο, κανένα από τα δύο αυτά δεν γνώρισε ευρεία αποδοχή [1] [10].

3.4.3 Τεχνικές διαμόρφωσης

Για να διατηρηθεί η συμβατότητα με τα ήδη εγκατεστημένα DSSS συστήματα, το HR/DSSS μπορεί να λειτουργήσει και στα 1 ή 2Mbps χρησιμοποιώντας τις ίδιες τεχνικές και μακριές κεφαλές.

Για μετάδοση στα 5.5Mbps κάθε σύμβολο κωδικοποιεί 4bits δεδομένων. Όπως φαίνεται και στην εικόνα 3.8, το MAC πλαίσιο διαιρείται σε μπλοκ των 4 bits και κάθε ένα από αυτά τα μπλοκ χωρίζεται σε δύο τμήματα των 2 bits. Το πρώτο τμήμα των 2 bits ορίζει μία γωνία αλλαγής της φάσης ανάμεσα στο τρέχον σύμβολο και το προηγούμενο σύμβολο, βάσει της DQPSK (πίνακας 3.4). Τα άρτια και τα περιττά σύμβολα χρησιμοποιούν διαφορετική αλλαγή φάσης. Η αρίθμηση των συμβόλων ξεκινάει με 0 για το πρώτο μπλοκ [1].



Εικόνα 3.8 Μετάδοση στα 5.5Mbps [1]

Bit pattern	Phase angle (even symbols)	Phase angle (odd symbols)
00	0	P
01	$\pi/2$	$3\pi/2$
11	π	0
10	$3\pi/2$	$\pi/2$

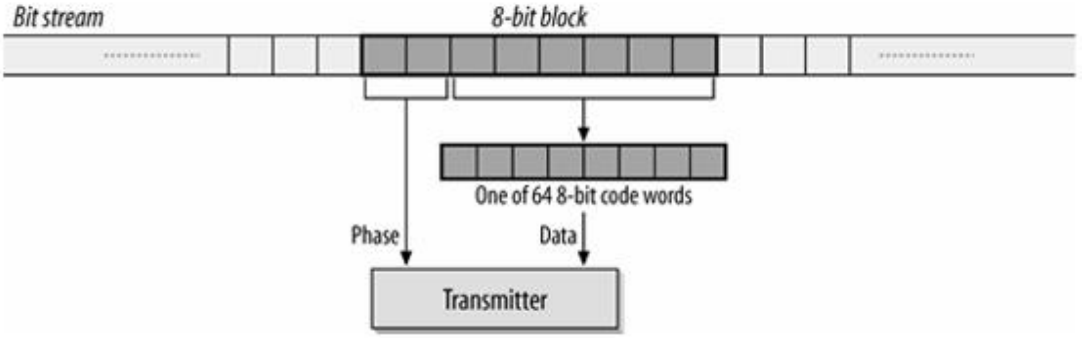
Πίνακας 3.4 DQPSK phase shifts [1]

Το δεύτερο τμήμα των 2 bits χρησιμοποιείται για να επιλεγεί μία από τις κωδικολέξεις των 8 bits (πίνακας 3.5) [1]. Αφού τα δεδομένα κωδικοποιηθούν, διαμορφώνονται με DQPSK [15].

Bit sequence	Code word
00	i,1,i,-1,i,1,-i,1
01	-i,-1,-i,1,1,1,-i,1
10	-i,1,-i,-1,-i,1,i,1
11	i,-1,i,1,-i,1,i,1

Πίνακας 3.5 CCK κωδικολέξεις [1]

Για να προκύψουν τα 11 Mbps, 8 bits πρέπει να κωδικοποιηθούν σε κάθε σύμβολο. Το MAC πλαίσιο διαιρείται σε μπλοκ των 8 bits και κάθε ένα από αυτά τα μπλοκ χωρίζεται σε τέσσερα τμήματα των 2 bits. Όπως και στα 5.5Mbps, το πρώτο τμήμα των 2 bits ορίζει μία γωνία αλλαγής της φάσης ανάμεσα στο τρέχον σύμβολο και το προηγούμενο σύμβολο, βάσει της DQPSK. Κάθε ένα από τα υπόλοιπα τρία τμήματα χρησιμοποιείται για να παραχθεί μία από τις 64 κωδικολέξεις των 8 bits [1]. Η διαδικασία φαίνεται στην εικόνα 3.9.



Εικόνα 3.9 Μετάδοση στα 11Mbps [1]

3.4.4 Δυναμική εναλλαγή ταχύτητας

Το 802.11b παρέχει τη δυνατότητα δυναμικής εναλλαγής της ταχύτητας. Αν οι συνθήκες μετάδοσης είναι καλές τότε οι συσκευές μπορούν να

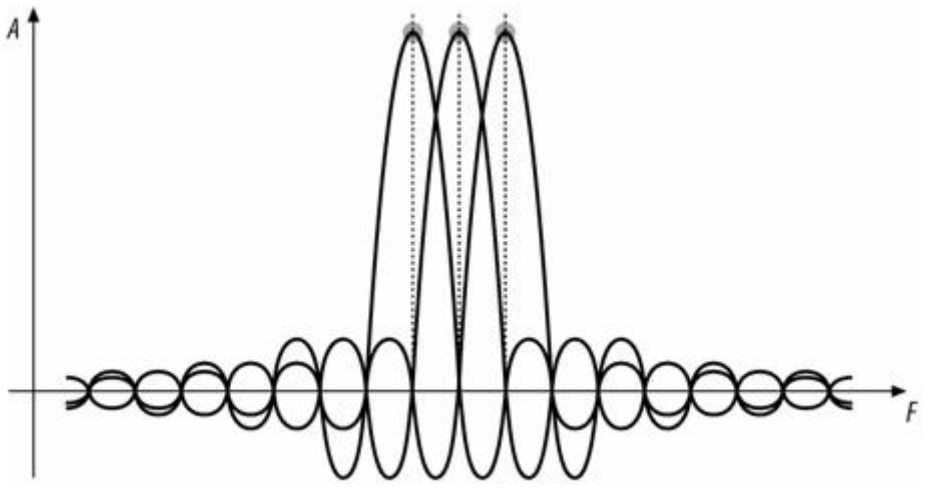
λειτουργούν στα 11Mbps. Όταν οι συνθήκες αλλάζουν, για παράδειγμα λόγω παρεμβολών, οι συσκευές προσαρμόζονται στις χαμηλότερες ταχύτητες των 5.5, 2 και 1 Mbps. Η εναλλαγή ταχύτητας είναι ένας μηχανισμός του φυσικού επιπέδου και είναι διαφανής στους χρήστες και τα ανώτερα επίπεδα [20].

3.5 802.11a Orthogonal Frequency Division Multiplexing (OFDM)

Άλλο ένα φυσικό επίπεδο, που χρησιμοποιεί τη λιγότερο φορτωμένη ζώνη συχνοτήτων των 5GHz, προτυποποιήθηκε το 1999. Το πρότυπο αυτό είναι το 802.11a και σαν βάση έχει την Orthogonal Frequency Division Multiplexing (OFDM) τεχνική. Στόχος ήταν η επίτευξη υψηλών ταχυτήτων έως και 54Mbps.

3.5.1 Orthogonal Frequency Division Multiplexing

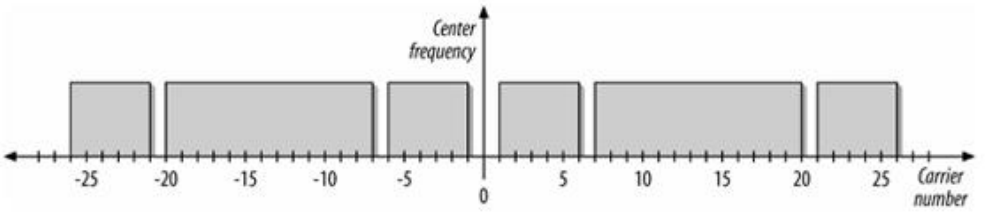
Βασική αρχή λειτουργίας της OFDM διαμόρφωσης είναι ότι χρησιμοποιεί πολλαπλούς υπό-φορείς (sub carriers) για να κωδικοποιήσει μία ενιαία μετάδοση. Κάθε κανάλι χωρίζεται σε 52 υπό-κανάλια ή υπό-φορείς. Τα υπό-κανάλια επικαλύπτονται αλλά δεν παρεμβάλλονται το ένα στο άλλο. Για να συμβεί αυτό, οι συχνότητες των υπό-φορέων επιλέγονται με τέτοιο τρόπο ώστε να είναι ορθογώνιες μεταξύ τους. Όπως φαίνεται στην εικόνα 3.9, η κορυφή κάθε υπό-φορέα κωδικοποιεί δεδομένα και σε αυτό το σημείο οι υπόλοιποι υπό-φορείς έχουν μηδενικό πλάτος [1].



Εικόνα 3.9 Ορθογωνικότητα συχνοτήτων [1]

Κατόπιν, στα κωδικοποιημένα σήματα όλων των υπό-καναλιών εφαρμόζεται Inverse Fast Fourier Transform (IFFT) μετασχηματισμός για να δημιουργηθεί μία σύνθετη κυματομορφή από την ισχύ του κάθε υπό-καναλιού. Οι OFDM δέκτες εφαρμόζουν Fast Fourier Transform (IFFT) μετασχηματισμό στην κυματομορφή που έλαβαν για να εξαγάγουν το πλάτος του κάθε υπό-φορέα [1].

Τέσσερις από τους υπό-φορείς χρησιμοποιούνται ως “πιλότοι” (pilot carriers) για την παρακολούθηση μετατοπίσεων και ICI παρεμβολών και επιτρέπουν στον δέκτη να αντισταθμίσει τυχόν παραμορφώσεις στο σήμα. Οι υπόλοιποι 48 χρησιμοποιούνται για τη μετάδοση δεδομένων. Τα κανάλια αριθμούνται από το -26 έως το 26 και οι υπό-φορείς απέχουν 0.3125MHz ο ένας από τον άλλον. Ο υπό-φορέας 0 δεν χρησιμοποιείται ενώ οι -21, -7, 7 και 21 έχουν ανατεθεί στους υπό-φορείς πιλότους (Εικόνα 3.10) [1].



Εικόνα 3.10 Δομή ενός OFDM καναλιού [1]

3.5.1.1 Ζώνες φρουροί (guard bands)

Όπως αναφέρθηκε παραπάνω, τα υπό-κανάλια δεν επικαλύπτονται. Ωστόσο, μικρές μετατοπίσεις στις συχνότητες των υπό-φορέων μπορεί να συμβούν προκαλώντας παρεμβολές ανάμεσα στους υπό-φορείς. Το φαινόμενο αυτό είναι γνωστό ως Inter-carrier Interference (ICI). Για την αντιμετώπιση των ICI αλλά και των ISI παρεμβολών, οι OFDM πομποδέκτες κρατούν το αρχικό τμήμα του συμβόλου ως φρουρό κι εφαρμόζουν τον μετασχηματισμό Fourier στο υπόλοιπο τμήμα του συμβόλου. Καθυστερήσεις μικρότερες από τη διάρκεια ενός φρουρού δεν προκαλούν ICI. Από την άλλη μεριά, φρουροί μεγάλης διάρκειας μειώνουν τη συνολική απόδοση ενός

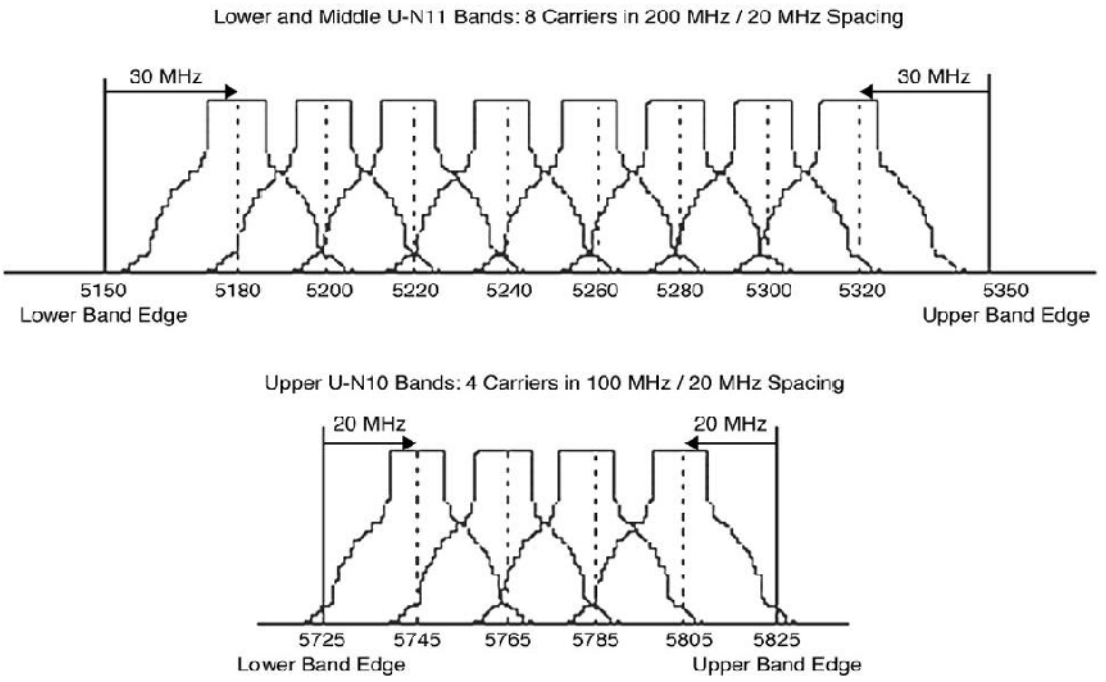
συστήματος καθώς ο χρόνος για τη μετάδοση των δεδομένων είναι λιγότερος. Ένας γενικός κανόνας είναι να χρησιμοποιούνται φρουροί διάρκειας δύο έως τέσσερις φορές μεγαλύτεροι από τον μέσο όρο της καθυστέρησης διάδοσης [1].

3.5.1.2 Convolution coding

Για να ενισχυθεί η αντίσταση της OFDM τεχνικής στις παρεμβολές, το IEEE 802.11a/g υποστηρίζει έναν μηχανισμό για τη διόρθωση σφαλμάτων, που είναι γνωστός ως *convolution coding.* Ο μηχανισμός αυτός λειτουργεί προσθέτοντας επιπλέον bits στα προς μετάδοση δεδομένα. Οι δέκτες χρησιμοποιούν την επιπλέον πληροφορία για να παράγουν τα δεδομένα. Ο *convolution coding* μηχανισμός χρησιμοποιεί μία αναλογία ανάμεσα στα μεταδιδόμενα bits προς τα κωδικοποιημένα bits. Η αναλογία αυτή μπορεί να είναι 1/2, 2/3, ή 3/4. Όσο μικρότερη είναι η αναλογία, η ανοχή του σήματος στις παρεμβολές μειώνεται αλλά ο ρυθμός μετάδοσης αυξάνεται [15] [19].

3.5.2 Κανάλια λειτουργίας του 802.11a

Το 802.11a ορίζει τρεις ζώνες στα 5GHz: τη χαμηλή ζώνη (lower band) , τη μεσαία ζώνη (middle band) και την άνω ζώνη (upper band). Κάθε μία από αυτές τις ζώνες έχει εύρος 100 MHz, 5.15–5.25GHz για τη χαμηλή ζώνη, 5.25–5.35GHz για τη μεσαία και 5.725–5.825GHz για την άνω ζώνη. Η χαμηλή και η μεσαία ζώνη έχουν 8 κανάλια με ένα συνολικό εύρος 200MHz και η άνω ζώνη έχει 4 κανάλια στο εύρος των 100MHz. Στη χαμηλή και τη μεσαία ζώνη το κέντρο των εξωτερικών καναλιών πρέπει να απέχει 30MHz από το άκρο της ζώνης ενώ στην άνω ζώνη η απόσταση αυτή πρέπει να είναι 20MHz [10][19][20]. Η εικόνα 3.11 αναπαριστά τις τρεις ζώνες και τα κανάλια τους. Επειδή το 802.11a χρησιμοποιεί 12 μη επικαλυπτόμενα κανάλια η απόδοση ενός WLAN δικτύου σε μια συγκεκριμένη περιοχή μπορεί να είναι αρκετά μεγάλη. Δώδεκα APs μπορούν να λειτουργούν σε δώδεκα διαφορετικά κανάλια χωρίς να παρεμβάλλονται το ένα στο άλλο [41].



Εικόνα 3.11 Ζώνες λειτουργίας του 802.11a για τις ΗΠΑ [10]

3.5.3 Τεχνικές διαμόρφωσης και ρυθμοί μετάδοσης

Οι ρυθμοί μετάδοσης που υποστηρίζει το 802.11a είναι 6, 9, 12, 18, 24, 36, 48 και 54Mbps χρησιμοποιώντας διάφορες τεχνικές διαμόρφωσης. Σε όλες τις περιπτώσεις ο ρυθμός εκπομπής που χρησιμοποιεί το φυσικό επίπεδο είναι 250,000 σύμβολα το δευτερόλεπτο μέσα από 48 υπό-κανάλια [1]. Οι ρυθμοί μετάδοσης χωρίζονται σε τέσσερα επίπεδα: 6 και 9 Mbps, 12 και 18 Mbps, 24 και 36 Mbps, 48 και 54Mbps. Τα 6, 12 και 24 Mbps είναι υποχρεωτικά. Οι χαμηλότεροι ρυθμοί, 6 και 9 Mbps, χρησιμοποιούν BPSK για να κωδικοποιήσουν ένα bit ανά υπό-κανάλι ή 48 bits ανά σύμβολο. Επειδή όμως το ½ ή το ¼ των bits είναι επιπλέον bits που προστίθενται από τον convolution coding μηχανισμό, τα bits δεδομένων ανά σύμβολο είναι 24 ή 36 αντίστοιχα. Το επόμενο επίπεδο, χρησιμοποιεί QPSK για να κωδικοποιήσει δύο bits ανά υπό-κανάλι ή 96 bits ανά σύμβολο. Αφαιρώντας και πάλι τα bits για τη διόρθωση σφαλμάτων, μένουν 48 ή 72 bits δεδομένων. Στο τρίτο επίπεδο χρησιμοποιείται 16-QAM (Quadrature Amplitude Modulation) κωδικοποιώντας 4 bits ανά υπό-κανάλι ή 192 bits ανά σύμβολο. Και πάλι τα bits δεδομένων είναι 96 ή 144. Τέλος, για τους υψηλότερους ρυθμούς χρησιμοποιείται η 64-QAM η οποία κωδικοποιεί 6 bits ανά υπό-κανάλι ή 288

bits ανά σύμβολο με τελικό αριθμό bits δεδομένων 192 ή 216 ανάλογα με το ποσοστό των bits που χρησιμοποιούνται για τη διόρθωση σφαλμάτων [1]. Όλα αυτά συνοψίζονται στον πίνακα 3.6.

Data rate (Mbps)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Πίνακας 3.6 Παράμετροι διαμόρφωσης και ρυθμοί μετάδοσης [10]

3.6 802.11g Extended-Rate PHY (ERP-OFDM)

Η ανάγκη των χρηστών για μεγαλύτερες ταχύτητες από αυτές του 802.11b, αλλά με ταυτόχρονη διατήρηση της συμβατότητας με αυτό, οδήγησαν στη δημοσίευση του 802.11g. Το 802.11g έχει τη δυνατότητα των ταχυτήτων του 802.11a λειτουργώντας στα 2.4GHz.

3.6.1 Τύποι του 802.11g

Το 802.11g δεν αποτελεί μια καινούρια τεχνολογία. Εφαρμόζοντας κάποιες τροποποιήσεις στις ήδη υπάρχουσες τεχνολογίες διατηρεί τη συμβατότητα με το αρχικό 802.11 και το 802.11b κι έτσι οι 802.11g σταθμοί μπορούν να συνυπάρχουν με παλαιότερες υλοποιήσεις. Υπάρχουν διάφοροι τύποι του 802.11g [1] [19]:

ERP-DSSS και ERP-CCK: με πολύ μικρές αλλαγές στις αρχικές τεχνολογίες, αυτές οι δύο μορφές είναι συμβατές με την αρχική DS προδιαγραφή και με το 802.11b.

ERP-OFDM: πρόκειται για τη βασική μορφή του 802.11g. Χρησιμοποιεί OFDM στα 2.4GHz, με κάποιες μικρές αλλαγές για τη διατήρηση της συμβατότητας. Υποστηρίζει τους ίδιους ρυθμούς μετάδοσης με το 802.11a με τις ταχύτητες 6, 12 και 24 υποχρεωτικούς.

ERP-PBCC: αυτή είναι μια προαιρετική επέκταση του PBCC που παρέχεται από το 802.11b και προσφέρει ρυθμούς μετάδοσης 22Mbps και 33Mbps. Παρόλα αυτά δεν χρησιμοποιείται ιδιαίτερα.

DSSS-OFDM: πρόκειται για άλλη μία προαιρετική και όχι ιδιαίτερα χρησιμοποιούμενη μορφή του 802.11g. Είναι ένας υβριδικός σχηματισμός που χρησιμοποιεί DSSS κεφαλές αλλά OFDM κωδικοποίηση για το τμήμα των δεδομένων.

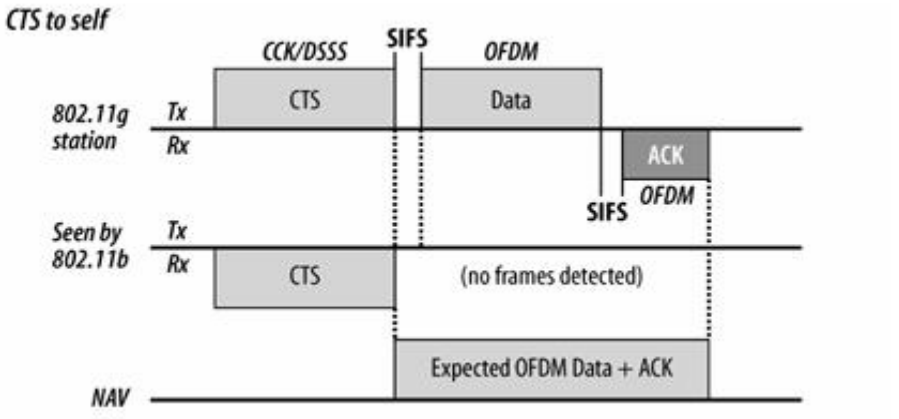
Κάθε 802.11g συσκευή πρέπει υποχρεωτικά να υποστηρίζει DSSS διαμόρφωση για συμβατότητα με το αρχικό 802.11 πρότυπο και CCK διαμόρφωση για συμβατότητα με το 802.11b. Απαραίτητη επίσης είναι η υλοποίηση του ERP-OFDM από τις 802.11g συσκευές. Τέλος, απαιτείται υποστήριξη της OFDM για τα 6, 12 και 24Mbps [1].

3.6.2 Μηχανισμός προστασίας

Το 802.11g είναι προς τα πίσω συμβατό με το 802.11 και το 802.11b. Αυτό σημαίνει ότι μπορεί να λαμβάνει και να αποκωδικοποιεί 802.11b σήματα. Το αντίστροφο όμως δε συμβαίνει κι αυτό είναι ένα από τα προβλήματα που έπρεπε να αντιμετωπίσουν οι σχεδιαστές του 802.11g. Έτσι, σε ένα BSS οι 802.11g σταθμοί πρέπει να μεταδίδουν με ρυθμούς μετάδοσης που υποστηρίζουν όλοι οι σταθμοί της περιοχής. Για παράδειγμα αν ένα 802.11g AP πρέπει να εξυπηρετεί και 802.11b και 802.11g σταθμούς, θα πρέπει να στέλνει τα Beacon πλαίσια με ρυθμούς που δεν ξεπερνούν τα 11Mbps [1].

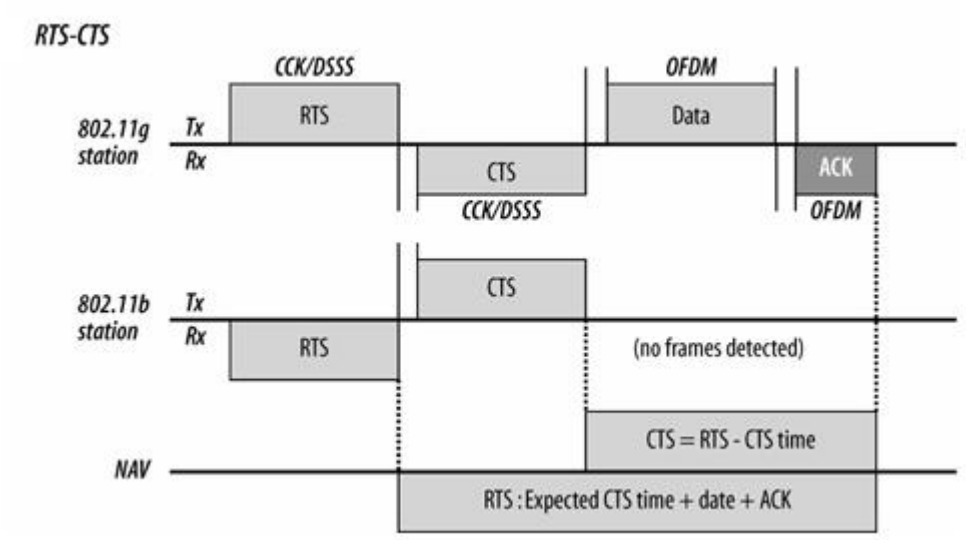
Έπειτα, έπρεπε να αποφευχθούν οι παρεμβολές μεταξύ 802.11b και 802.11g δικτύων. Για να εξασφαλιστεί ότι οι 802.11b σταθμοί αντιλαμβάνονται μία 802.11g μετάδοση και δεν παρεμβάλλονται σε αυτήν, το 802.11g ορίζει έναν μηχανισμό προστασίας για την ενημέρωση του NAV των 802.11b συσκευών. Υπάρχουν δύο τύποι του μηχανισμού προστασίας. Ο πρώτος περιλαμβάνει την αποστολή ενός CTS-to-self πλαισίου και ο δεύτερος περιλαμβάνει μία πλήρη RTS/CTS ανταλλαγή.

Στην πρώτη περίπτωση, που είναι και η πιο συνηθισμένη, όταν ένας 802.11g σταθμός έχει ένα πλαίσιο γι' αποστολή , στέλνει πρώτα ένα CTS-to-self πλαίσιο με διεύθυνση παραλήπτη τη δική του διεύθυνση MAC. Με αυτό το πλαίσιο ενημερώνει τον NAV και όλοι οι άλλοι σταθμοί γνωρίζουν ότι το μέσο θα είναι απασχολημένο για τόσο χρόνο όσο χρειάζεται για την αποστολή του CTS, του OFDM διαμορφωμένου πλαισίου και της OFDM διαμορφωμένης επιβεβαίωσής του (Εικόνα 3.12).



Εικόνα 3.12 Μηχανισμός προστασίας με CTS-to-self [1]

Στη δεύτερη περίπτωση, μία πλήρης RTS/CTS ανταλλαγή συμβαίνει προτού μεταδοθεί το πλαίσιο δεδομένων (Εικόνα 3.13). Αυτή η τεχνική αντιμετωπίζει πολύ καλά το πρόβλημα των κρυφών κόμβων αλλά καταναλώνει πολύ μεγαλύτερο μέρος της χωρητικότητας με αποτέλεσμα να μειώνεται αρκετά η απόδοση.



Εικόνα 3.13 Μηχανισμός προστασίας με RTS/CTS [1]

Τα πλαίσια προστασίας μεταδίδονται είτε με PSK στα 1 ή 2Mbps ή με CCK στα 5.5 ή 11Mbps. Έτσι εξασφαλίζεται ότι οι 802.11b σταθμοί τα λαμβάνουν και ενημερώνουν τον NAV. Ο μηχανισμός της προστασίας ελέγχεται από το στοιχείο ERP information που βρίσκεται στα πλαίσια φάρους (beacon). Το 802.11g προσθέτει ένα bit, το Use protection bit, στο στοιχείο αυτό. Όταν το bit αυτό έχει οριστεί, οι σταθμοί πρέπει να χρησιμοποιήσουν τον μηχανισμό της προστασίας [1].

3.6.3 802.11g vs 802.11a

Το μεγάλο πλεονέκτημα του 802.11g είναι το ότι είναι συμβατό με το 802.11b, γεγονός που καθιστά εύκολη την αναβάθμιση των 802.11b δικτύων. Επίσης, έχει μεγαλύτερο εύρος από το 802.11a καθώς λειτουργεί στις χαμηλότερες συχνότητες της 2.4GHz ζώνης. Όμως, ακριβώς λόγω της λειτουργίας του σε αυτή τη φορτωμένη ζώνη συχνοτήτων, αντιμετωπίζει το πρόβλημα των παρεμβολών, όπως και το 802.11b. Επίσης, η συνολική απόδοση του 802.11a είναι μεγαλύτερη από αυτή του 802.11g. Γιατί μπορεί κάθε κανάλι του 802.11g να έχει παρόμοια απόδοση με ένα κανάλι του 802.11a, αλλά τα διαθέσιμα μη επικαλυπτόμενα κανάλια για το 802.11g είναι μόνο τρία. Αν κάθε κανάλι λειτουργεί με τη μεγαλύτερη ταχύτητα και με 50% αποδοτικότητα, η συνολική απόδοση θα είναι 81Mbps, πολύ χαμηλότερη από

αυτή που μπορεί να προσφέρει το 802.11a [1]. Επιπλέον, η απόδοση των 802.11g συσκευών μειώνεται όταν συνυπάρχουν με 802.11b συσκευές.

Κεφάλαιο 4 Ασφάλεια

4.1 Εισαγωγή

Στα WLANs τα δεδομένα μεταδίδονται μέσω του αέρα κι έτσι είναι διαθέσιμα σε οποιονδήποτε βρίσκεται στο εύρος ενός ασύρματου δικτύου. Επομένως, οι ασύρματες μεταδόσεις είναι πολύ ευαίσθητες σε θέματα ασφάλειας. Η επίθεση σε ένα ασύρματο δίκτυο μπορεί να είναι παθητική (passive) ή ενεργητική (active). Στην πρώτη περίπτωση, ο επιτιθέμενος απλά υποκλέπτει τις μεταδόσεις ενώ στη δεύτερη παρεμβαίνει σε αυτές και μπορεί να δημιουργεί προβλήματα στις επικοινωνίες ή να τροποποιεί τα δεδομένα. Ένας εισβολέας μπορεί να υποκλέψει και να τροποποιήσει δεδομένα, να πλαστογραφήσει διευθύνσεις και να προσποιηθεί ότι είναι νόμιμος χρήστης του δικτύου ή ακόμα και να ανακατευθύνει μεταδόσεις, να προκαλέσει τον τερματισμό συσχετίσεων και πιστοποιήσεων ίσως και να προκαλέσει προβλήματα στη λειτουργία του δικτύου. Μερικές από τις επιθέσεις περιγράφονται παρακάτω.

4.2 Ευπάθειες Ασύρματων Δικτύων

Sniffing, Interception and Eavesdropping - Πρόκειται για την πιο απλή επίθεση σε ένα ασύρματο δίκτυο όπου ο επιτιθέμενος απλά “κρυφακούει” την κίνηση του δικτύου. Αυτή η μέθοδος χρησιμοποιείται για τον εντοπισμό υποψήφιων για επίθεση δικτύων, τη συλλογή χρήσιμων πληροφοριών, όπως κωδικοί πρόσβασης και κλειδιά κρυπτογράφησης, ή την απόκτηση μη κρυπτογραφημένων δεδομένων.

Denial of service (DoS) – ένας επιτιθέμενος πλημμυρίζει μία συσκευή δικτύου με υπερβολική κίνηση, εμποδίζοντας ή επιβραδύνοντας την πρόσβαση των νόμιμων χρηστών στο δίκτυο. Για παράδειγμα, κάποιος μπορεί να κρατά απασχολημένο έναν εξυπηρετητή διαδικτύου (web server), στέλνοντάς του πολλές αιτήσεις για ιστοσελίδες, ή ένα AP στέλνοντάς του απανωτές αιτήσεις συσχέτισης ή πιστοποίησης.

Jamming – πρόκειται για μία μορφή DoS επίθεσης, με την οποία ο επιτιθέμενος πλημμυρίζει τη χρησιμοποιούμενη ζώνη συχνοτήτων (RF band)

ενός δικτύου με παρεμβολές, οδηγώντας προοδευτικά το δίκτυο σε αδράνεια. Στα 2.4GHz αυτό μπορεί να γίνει με τη χρήση Bluetooth συσκευών, ασύρματων τηλεφώνων ή ακόμα και από έναν φούρνο μικροκυμάτων.

Insertion attacks – ένας επιτιθέμενος μπορεί να συνδέσει μία μη πιστοποιημένη συσκευή-πελάτη σε ένα AP, είτε γιατί δεν έγινε έλεγχος ταυτότητας είτε γιατί ο επιτιθέμενος προσποιήθηκε έναν εξουσιοδοτημένο χρήστη.

Replay attack – ο επιτιθέμενος αφού έχει υποκλέψει κίνηση του δικτύου και έχει αποκτήσει πολύτιμα δεδομένα, όπως κωδικούς πρόσβασης, χρησιμοποιεί αυτά τα δεδομένα και αποκτά πρόσβαση στο δίκτυο, παρόλο που πρόκειται για έναν μη πιστοποιημένο χρήστη.

ARP Spoofing (or ARP cache poisoning) – ένας επιτιθέμενος αποκτώντας πρόσβαση στο δίκτυο, μπορεί να αλλοιώσει τον ARP πίνακα στον οποίο είναι αποθηκευμένα ζεύγη MAC-IP διευθύνσεων. Έτσι, χρησιμοποιώντας μία από τις έγκυρες διευθύνσεις MAC, μπορεί να ξεγελάσει το δίκτυο και να δρομολογούνται ευαίσθητα δεδομένα και προς τη δική του συσκευή.

Session hijacking (or man-in-the-middle attack) – είναι μία μορφή της ARP spoofing επίθεσης, με την οποία ο επιτιθέμενος, παριστάνοντας έναν νόμιμο σταθμό, διακόπτει τη συσχέτιση του σταθμού αυτού με το AP και κατόπιν, προσποιείται ότι είναι το AP για να κάνει το σταθμό να συσχετιστεί με αυτόν.

Rogue access point (or evil twin intercept) – ο επιτιθέμενος εγκαθιστά ένα μη εξουσιοδοτημένο AP (rogue AP) με ένα έγκυρο SSID. Αν αυτό το AP έχει ισχυρότερο σήμα από άλλα (πιστοποιημένα) APs, τότε οι σταθμοί-πελάτες θα προτιμήσουν να συσχετιστούν με το rogue AP κι έτσι ευαίσθητα δεδομένα θα τεθούν σε κίνδυνο.

Cryptoanalytic attacks – μία επίθεση κατά την οποία ο επιτιθέμενος χρησιμοποιεί μία θεωρητική αδυναμία για να σπάσει το σύστημα

κρυπτογράφησης. Ένα παράδειγμα είναι η αδυναμία του RC4 αλγόριθμου που κάνει το WEP ιδιαίτερα ευάλωτο στις επιθέσεις.

4.3 Wired Equivalent Privacy (WEP)

Καθώς τα δεδομένα μεταδίδονται μέσω του αέρα, πρέπει να διατηρηθεί η μυστικότητά τους και να εξασφαλιστεί ότι δεν έχουν τροποποιηθεί. Για την αντιμετώπιση των υποκλοπών των δεδομένων χρησιμοποιούνται πρωτόκολλα κρυπτογράφησης. Το 802.11 αρχικά χρησιμοποίησε γι' αυτόν τον σκοπό το WEP. Ωστόσο, πολύ σύντομα αποδείχθηκε η αναποτελεσματικότητά του. Σε πολλές περιπτώσεις όμως, το WEP μπορεί να είναι το μόνο πρωτόκολλο ασφάλειας διαθέσιμο σε μία συσκευή. Η υλοποίηση του είναι εύκολη και δεν απαιτεί την υπολογιστική ισχύ που απαιτούν τα νεότερα πρωτόκολλα κρυπτογράφησης.

4.3.1 Παράμετροι ασφάλειας

Ένα πρωτόκολλο ασφάλειας δεδομένων πρέπει να παρέχει *εμπιστευτικότητα* των δεδομένων (*confidentiality*), προστατεύοντας τα δεδομένα από υποκλοπές, *ακεραιότητα* των δεδομένων (*integrity*), αποτρέποντας την τροποποίηση των δεδομένων και *πιστοποίηση* των χρηστών (*authentication*), εμποδίζοντας μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στο δεδομένα.

Το WEP υποστηρίζει την εμπιστευτικότητα κρυπτογραφώντας το σώμα των πλαισίων ενώ για την ακεραιότητα χρησιμοποιεί μία ακολουθία ελέγχου ακεραιότητας (integrity check sequence).

Οι μέθοδοι που μπορούν να χρησιμοποιηθούν με το WEP για την πιστοποίηση είναι δύο: η Open System authentication και η Shared Key authentication. Στην πρώτη περίπτωση οποιοσδήποτε σταθμός μπορεί να πιστοποιηθεί χωρίς να πρέπει να παρουσιάσει κάποιο αποδεικτικό. Μετά την πιστοποίηση όμως θα χρησιμοποιηθεί το WEP για την κρυπτογράφηση των δεδομένων, οπότε ο σταθμός θα πρέπει να γνωρίζει το κλειδί για να μπορέσει να χρησιμοποιήσει το δίκτυο. Η Shared Key authentication περιλαμβάνει

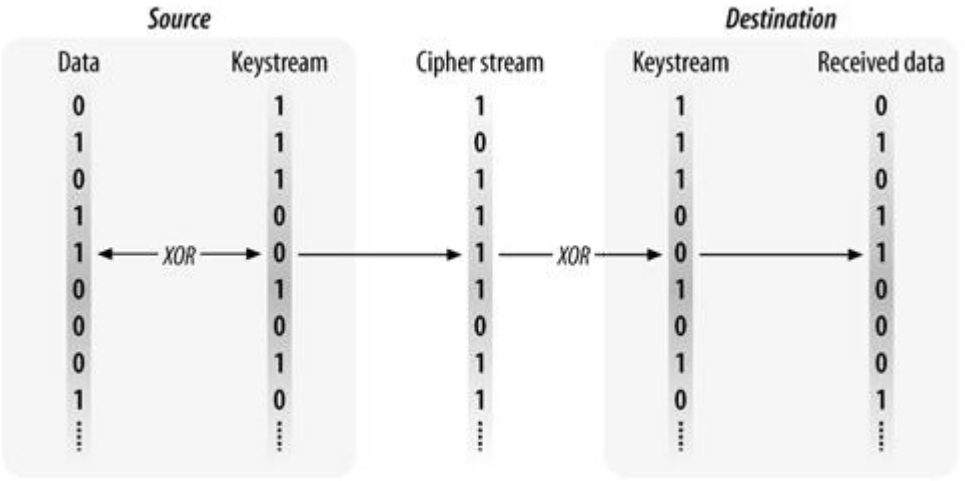
τέσσερα βήματα και ο χρήστης πρέπει να γνωρίζει το WEP κλειδί για να πιστοποιηθεί. Η διαδικασία είναι η εξής:

1. Ο σταθμός στέλνει μία αίτηση πιστοποίησης (authentication request) στο AP.
2. Το AP απαντά με ένα καθαρό κείμενο (clear-text) πρόκληση.
3. Ο σταθμός πρέπει να κρυπτογραφήσει το κείμενο πρόκλησης με το κλειδί που έχει και να το στείλει πίσω στο AP.
4. Το AP αποκρυπτογραφεί το κείμενο που έλαβε και το συγκρίνει με το clear-text. Αν η σύγκριση είναι επιτυχής, το AP στέλνει θετική απάντηση στο σταθμό.

Αν και η δεύτερη μέθοδος φαίνεται πιο ασφαλής, στην πραγματικότητα δεν είναι. Πρώτον, ο χρήστης δεν μπορεί να ξέρει αν το AP γνωρίζει το κλειδί, άρα έχει να κάνει με ένα νόμιμο AP, αλλά και ένας εισβολέας που ακούει, έχει το κείμενο πρόκλησης και το αντίστοιχο κρυπτογραφημένο κείμενο κι έτσι εύκολα μπορεί να ανακαλύψει το κλειδί. Γι' αυτό τα περισσότερα Wi-Fi συστήματα χρησιμοποιούν την Open System authentication [17].

4.3.2 Αλγόριθμος κρυπτογράφησης

Για να προστατεύσει τα δεδομένα, το WEP απαιτεί τη χρήση του RC4 κρυπτογραφήματος (RC4 cipher). Ο RC4 μοιράζεται διάφορες ιδιότητες με όλα τα ρεύματα κρυπτογραφημάτων (stream ciphers). Γενικά, ένα ρεύμα cipher χρησιμοποιεί ένα ρεύμα από bits, γνωστό ως keystream. Το keystream συνδυάζεται έπειτα με το μήνυμα για να παραγάγει το κρυπτογραφημένο κείμενο (ciphertext). Για να ανακτήσει το αρχικό μήνυμα, ο δέκτης επεξεργάζεται το ciphertext με ένα πανομοιότυπο keystream. Η αποκρυπτογράφηση δηλαδή είναι η αντίστροφη διαδικασία και χρησιμοποιεί το ίδιο κλειδί με την κρυπτογράφηση. Γι' αυτό και ο αλγόριθμος λέγεται συμμετρικός (symmetric algorithm) [17]. Ο RC4 χρησιμοποιεί XOR για να συνδυάσει το keystream και το ciphertext. Η εικόνα 4.1 υλοποιεί τη διαδικασία.



Εικόνα 4.1 Γενική λειτουργία του cipher stream [1]

Τα περισσότερα stream ciphers λειτουργούν παίρνοντας ένα σχετικά μικρό μυστικό κλειδί και το επεκτείνουν σε ένα ψευδοτυχαίο keystream, το οποίο έχει το ίδιο μήκος με το μήνυμα. Αυτό γίνεται με τη χρήση μιας γεννήτριας ψευδοτυχαίων αριθμών (pseudorandom number generator, PRNG), η οποία είναι ένα σύνολο κανόνων που χρησιμοποιούνται για να επεκτείνουν το κλειδί σε keystream. Για την ανάκτηση των δεδομένων, ο δέκτης πρέπει να έχει το ίδιο μυστικό κλειδί με τον αποστολέα και να χρησιμοποιήσει τον ίδιο αλγόριθμο για να επεκτείνει το κλειδί σε μια ψευδοτυχαία ακολουθία.

Καθώς ο RC4 δεν απαιτεί τη χρήση κλειδιών με συγκεκριμένο μήκος, το WEP μπορεί να χρησιμοποιηθεί με κλειδιά οποιουδήποτε μήκους. Υπάρχουν κλειδιά με μήκος 64 bits και 128 bits. Μπορεί να υπάρξουν και κλειδιά με μεγαλύτερο μήκος, ωστόσο έχει αποδειχθεί ότι κάτι τέτοιο δε βελτιώνει την προστασία. Το κλειδί που χρησιμοποιούν οι περισσότερες υλοποιήσεις και το 802.11 είναι το κλειδί με τα 64 bits [1].

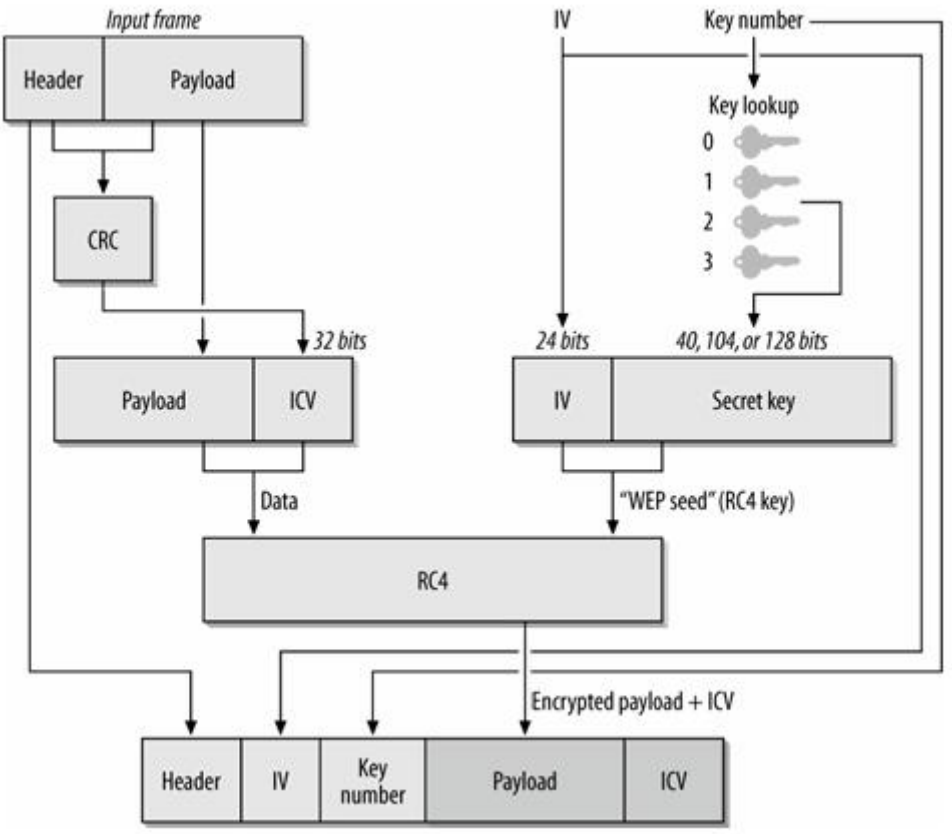
Από αυτά τα bits, τα 24 χρησιμοποιούνται ως ένα διάνυσμα αρχικοποίησης (initialization vector, IV) και τα υπόλοιπα αποτελούν το κρυφό κλειδί, που μοιράζεται ανάμεσα στους σταθμούς που επικοινωνούν. Ο IV συνδυάζεται με το κρυφό κλειδί για να παράγονται διαφορετικά key streams για κάθε πλαίσιο. Το 802.11 δεν θέτει κάποιον περιορισμό στον αλγόριθμο που χρησιμοποιείται για να την επιλογή των IVs. Μερικά προϊόντα ορίζουν

διαδοχικούς IVs, ενώ κάποια άλλα χρησιμοποιούν έναν ψευδοτυχαίο αλγόριθμο. Η επιλογή του IV μπορεί να έχει μερικές επιπτώσεις στην ασφάλεια επειδή μία φτωχή IV επιλογή μπορεί να θέσει σε κίνδυνο τα κλειδιά. Επίσης ο IV στέλνεται ως μέρος της κεφαλίδας και δεν κρυπτογραφείται. Αυτό είναι απαραίτητο για να μπορέσει ο παραλήπτης να παράγει το ίδιο κλειδί που χρησιμοποίησε ο αποστολέας, προσφέρει όμως αρκετή πληροφορία στους επιτιθέμενους για την απόκτηση του μυστικού κλειδιού.

4.3.3 Διαδικασία κρυπτογράφησης με το WEP

Η εμπιστευτικότητα και η ακεραιότητα χειρίζονται ταυτόχρονα. Πριν από την κρυπτογράφηση, εφαρμόζεται στο πλαίσιο ένας cyclic redundancy check (CRC) αλγόριθμος για τον έλεγχο της ακεραιότητας, που παράγει μία τιμή ελέγχου ακεραιότητας (integrity check value, ICV). Η τιμή αυτή προστατεύει το περιεχόμενο από την πλαστογράφηση διαβεβαιώνοντας ότι το πλαίσιο δεν έχει αλλάξει κατά τη μεταφορά. Η ICV τιμή κρυπτογραφείται μαζί με το ωφέλιμο φορτίο του πλαισίου κι έτσι οι επιτιθέμενοι δεν μπορούν να την αλλάξουν και κατ' επέκταση δεν μπορούν να αλλοιώσουν τα δεδομένα. Ο έλεγχος ακολουθίας του πλαισίου (frame check sequence, FCS) δεν έχει υπολογιστεί ακόμα, άρα δεν περιλαμβάνεται στην τιμή ICV.

Παράλληλα παράγεται το κλειδί κρυπτογράφησης. Ο IV συνδυάζεται με ένα μυστικό κλειδί για να προκύψει ένα διαφορετικό key stream για κάθε πλαίσιο. Το WEP επιτρέπει την αποθήκευση τεσσάρων κλειδιών ταυτόχρονα. Έπειτα το RC4 κλειδί χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα και την ICV τιμή. Μετά την επεξεργασία, η έξοδος είναι ένα κρυπτογραφημένο πλαίσιο έτοιμο για μετάδοση με αρκετή πληροφορία που βοηθά τον παραλήπτη στην αποκρυπτογράφηση. Ανάμεσα στην κεφαλίδα MAC και τα κρυπτογραφημένα δεδομένα προστίθεται η κεφαλίδα WEP η οποία περιλαμβάνει το IV και τον αριθμό του κλειδιού που χρησιμοποιήθηκε. Ο FCS έλεγχος μπορεί τώρα να εφαρμοστεί σε ολόκληρο το κρυπτογραφημένο πλαίσιο [1]. Στην εικόνα 4.2 φαίνεται η όλη διαδικασία κρυπτογράφησης ενός πλαισίου με χρήση του WEP.



Εικόνα 4.2 Κρυπτογράφηση με χρήση του WEP [1]

4.3.4 Static vs dynamic WEP

Υπάρχουν δύο τύποι WEP, το manual ή static WEP και το dynamic WEP. Στις αρχικές υλοποιήσεις γινόταν χρήση του static WEP όπου η διανομή των κλειδιών γινόταν χειρωνακτικά. Οι διαχειριστές ήταν αρμόδιοι για τη διανομή ενός ενιαίου προεπιλεγμένου κλειδιού σε όλους τους σταθμούς στο δίκτυο. Οι ενημερώσεις των κλειδιών γινόντουσαν επίσης χειρωνακτικά, ωστόσο, στις περισσότερες περιπτώσεις, το ίδιο κλειδί χρησιμοποιούνταν για αρκετό καιρό. Η χρήση ενός στατικού κλειδιού δεν είναι ιδιαίτερα καλή λύση. Είναι όμως καλύτερη από το τίποτα και χρησιμοποιείται από κάποιες συσκευές που δεν μπορούν να υποστηρίξουν κάτι άλλο.

Το δυναμικό WEP είναι πιο αποτελεσματικό από το στατικό WEP. Αντί για ένα ενιαίο κλειδί που διανέμεται σε όλους τους σταθμούς, κάθε σταθμός χρησιμοποιεί δύο κλειδιά. Το πρώτο είναι ένα κλειδί χαρτογράφησης (mapping key), κοινό μεταξύ του σταθμού και του AP, που χρησιμοποιείται για να προστατεύσει τα unicast πλαίσια. Κάθε σταθμός έχει το δικό του κλειδί

χαρτογράφησης. Το δεύτερο κλειδί είναι ένα default κλειδί, κοινό σε όλους τους σταθμούς στο ίδιο BSS, το οποίο προστατεύει τα broadcast και multicast πλαίσια. Το μεγάλο πλεονέκτημα του δυναμικού WEP έναντι του στατικού είναι ότι τα κλειδιά ανανεώνονται συχνά, άρα μειώνεται η περίοδος χρήσης τους. Αυτό εμποδίζει τους επιτιθέμενους από το να συλλέξουν αρκετά δεδομένα κρυπτογραφημένα με το ίδιο κλειδί και κατά συνέπεια τους εμποδίζει από το να αποκρυπτογραφήσουν το κλειδί. Ο τρόπος που το δυναμικό WEP χειρίζεται τα πλαίσια είναι ίδιος με του στατικού WEP. Αυτό που αλλάζει είναι ότι χρησιμοποιείται ένας βελτιωμένος μηχανισμός για την περιοδική παραγωγή και διανομή νέων κλειδιών, μέσα από τη διαδικασία πιστοποίησης με τη χρήση του πρωτοκόλλου EAP, το οποίο αναλύεται παρακάτω. Με τη ρύθμιση σύντομων διαστημάτων ανανέωσης των κλειδιών, βελτιώνεται η αντιμετώπιση των επιθέσεων στα κλειδιά.

4.3.5 Αδυναμίες του WEP

Το WEP αρχικά μειονεκτεί από τον τρόπο διαχείρισης των κλειδιών. Η χρήση του ίδιου κλειδιού από πολλούς χρήστες επιτρέπει στον καθένα από αυτούς να παρακολουθεί την κίνηση του άλλου. Επίσης, το 802.11 δεν ορίζει κάποια συγκεκριμένη μέθοδο παραγωγής και διανομής των κλειδιών με αποτέλεσμα το ίδιο κλειδί να χρησιμοποιείται για μεγάλο χρονικό διάστημα.

Επίσης, η μέθοδος πιστοποίησης με διαμοιραζόμενο κλειδί (Shared Key authentication) αποδείχθηκε όχι απλά αναποτελεσματική αλλά και επικίνδυνη. Με τη μέθοδο αυτή κάποιος μπορούσε να ανακαλύψει το κλειδί WEP από τη διαδικασία της πιστοποίησης και, καθώς το ίδιο κλειδί χρησιμοποιείται και για την πιστοποίηση και για την κρυπτογράφηση, η ακεραιότητα των δεδομένων είχε πλέον χαθεί. Έτσι, οι χρήστες γρήγορα αντικατέστησαν αυτή τη μέθοδο με την Open System authentication.

Ένα άλλο τρωτό σημείο του WEP είναι το μικρό μήκος του IV. Με 24bits αυξάνονται οι πιθανότητες για συγκρούσεις IV (IV collision). Οι IV collisions συμβαίνουν όταν χρησιμοποιούνται οι ίδιοι IVs. Με 24bits οι τιμές του IV θα αρχίσουν να επαναλαμβάνονται μετά από περίπου 17 εκατομμύρια κρυπτογραφημένα πλαίσια. Αν ένας επιτιθέμενος ανακαλύψει το cipher

stream για ένα συγκεκριμένο IV, μπορεί μετά να αποκρυπτογραφήσει όλα τα πλαίσια που χρησιμοποιούν το ίδιο IV.

Επίσης, διαπιστώθηκε ότι κάποια κλειδιά είχαν μερικά bits τα οποία ουσιαστικά δεν επηρέαζαν την έξοδο. Τα κλειδιά αυτά ονομάστηκαν αδύναμα κλειδιά. Καθώς τα τρία πρώτα bytes του κλειδιού είναι το IV, το οποίο μεταφέρεται ως καθαρό κείμενο, ένας επιτιθέμενος μπορεί εύκολα να διαπιστώσει ποια πλαίσια έχουν κρυπτογραφηθεί με αδύναμο κλειδί. Και αφού συλλέξει αρκετά τέτοια πλαίσια μπορεί να καταφέρει να βρει το κλειδί που θα του επιτρέψει την πρόσβαση στο δίκτυο.

Και αφού ο μηχανισμός κρυπτογράφησης παραβιαστεί, κάθε πακέτο μπορεί να αποκρυπτογραφηθεί. Ο εισβολέας μπορεί τότε να υποκλέψει μία μετάδοση, να τροποποιήσει τα δεδομένα και να αλλάξει και την τιμή του ελέγχου ακεραιότητας (ICV) έτσι ώστε να μη φαίνεται ότι το πλαίσιο τροποποιήθηκε [45].

Το 2001 το WEP είχε επίσημα παραβιαστεί και ήταν επιτακτική η ανάγκη δημιουργίας ισχυρότερων πρωτοκόλλων που θα κάλυπταν τις αδυναμίες του. Το WEP χρησιμοποιείται πλέον μόνο όταν δεν μπορεί να χρησιμοποιηθεί κάτι άλλο [4][6][11][13][21].

4.4 802.11i

Όταν το WEP παραβιάστηκε, η IEEE ανέθεσε στην ομάδα εργασίας i την ανάπτυξη ενός ισχυρού πρότυπου ασφάλειας. Το 802.11i ορίζει δύο νέα πρωτόκολλα ασφάλειας, το Temporal Key Integrity Protocol (TKIP) και το Counter Mode με CBC-MAC Protocol (CCMP). Το TKIP σχεδιάστηκε έτσι ώστε να είναι συμβατό με το ήδη υπάρχον υλικό κι έτσι ολοκληρώθηκε πρώτο ενώ το CCMP σχεδιάστηκε από την αρχή για να προσφέρει το υψηλότερο δυνατό επίπεδο ασφάλειας. Το 802.11i ορίζει επίσης λειτουργίες για την παραγωγή και διανομή των κλειδιών για να δημιουργήσει αυτό που αποκαλείται Robust Security Networks (RSNs). Για τη διανομή των κλειδιών αλλά και για την πιστοποίηση των χρηστών χρησιμοποιεί το 802.1X.

4.4.1 Temporal Key Integrity Protocol (TKIP)

Όταν το WEP παραβιάστηκε, προέκυψε άμεση ανάγκη για ένα νέο πρωτόκολλο ασφάλειας. Η δημιουργία από την αρχή ενός νέου, ισχυρού πρωτοκόλλου θα απαιτούσε χρόνο και πιθανότατα αντικατάσταση όλου του χρησιμοποιούμενου εξοπλισμού. Έτσι προέκυψε το TKIP ως μία αναβάθμιση του WEP. Το TKIP διατηρεί τη βασική αρχιτεκτονική και τις λειτουργίες του WEP αλλά προσθέτει και αρκετά νέα χαρακτηριστικά.

Χρησιμοποιεί έναν νέο μηχανισμό ακεραιότητας, αυξάνει το μήκος του IV, αλλάζει το κλειδί για κάθε πλαίσιο, αλλάζει τον τρόπο με τον οποίο επιλέγονται οι τιμές του IV και βασίζεται στο 802.1X για την παραγωγή και διανομή των κλειδιών [1].

Αντί για ένα μοναδικό κλειδί, το TKIP κάνει χρήση *κύριων κλειδιών (master keys)* και τα κλειδιά που χρησιμοποιούνται τελικά για να κρυπτογραφήσουν τα πλαίσια παράγονται από τα κύρια κλειδιά.

Το μικρό μήκος του IV αλλά και το γεγονός ότι μεταφερόταν ως plaintext, ήταν δύο τρωτά σημεία του WEP. Με 24bits, το IV διάστημα διαρκεί για 16 εκατομμύρια πλαίσια. Σε ένα πολυάσχολο δίκτυο, 16 εκατομμύρια πλαίσια δεν είναι πάρα πολλά, οπότε τα ίδια IVs σύντομα θα ξαναχρησιμοποιηθούν. Επίσης, καθώς το IV αποτελεί τα 24 πρώτα bits του κλειδιού διευκολύνει την απόκτηση των κλειδιών από τρίτους [1].

Για να μετριάσει τις επιθέσεις ενάντια στα IVs, το TKIP διπλασιάζει το μήκος του IV από 24 σε 48bits. Αυτό αυξάνει το μέγεθος του διαστήματος του IV από 16 εκατομμύρια σε 281 τρισεκατομμύρια, τα οποία αποτρέπουν αποτελεσματικά την εξάντληση του IV διαστήματος κατά τη διάρκεια της περιορισμένης διάρκειας ζωής ενός κλειδιού [17].

Το IV εξυπηρετεί πλέον κι έναν άλλο σκοπό. Για την προστασία από επιθέσεις αναπαραγωγής (replay attacks), όπου ένας εισβολέας αντιγράφει αυτούσια πλαίσια και τα ξαναστέλνει στον ίδιο παραλήπτη, το TKIP

χρησιμοποιεί έναν μετρητή ακολουθίας (sequence counter, SC). Για τον μετρητή αυτό χρησιμοποιείται το IV. Κάθε φορά που εγκαθίσταται ένα master key, ο μετρητής αρχικοποιείται στην τιμή 1. Κάθε πλαίσιο που μεταδίδεται αυξάνει τον μετρητή κατά ένα. Το TKIP διατηρεί την τιμή του πιο πρόσφατου μετρητή που λαμβάνει από κάθε σταθμό. Όταν ένας σταθμός λάβει ένα πλαίσιο, συγκρίνει τον μετρητή του με τον πιο πρόσφατο μετρητή που είχε λάβει και αποδέχεται το πλαίσιο μόνο αν ο μετρητής είναι μεγαλύτερος από τις προηγούμενες τιμές. Σε οποιαδήποτε άλλη περίπτωση το πλαίσιο απορρίπτεται [1][17].

Επίσης, ο τρόπος που συνδυάζονται τα κλειδιά είναι διαφορετικός στο TKIP. Χρησιμοποιείται ένας μηχανισμός, γνωστός ως *key mixing* και κάθε πλαίσιο κρυπτογραφείται με ένα μοναδικό RC4 κλειδί. Η διεύθυνση MAC του αποστολέα ενσωματώνεται στον υπολογισμό του κλειδιού κι έτσι δύο σταθμοί μπορούν να χρησιμοποιήσουν το ίδιο IV κι όμως να παράγουν διαφορετικά RC4 κλειδιά.

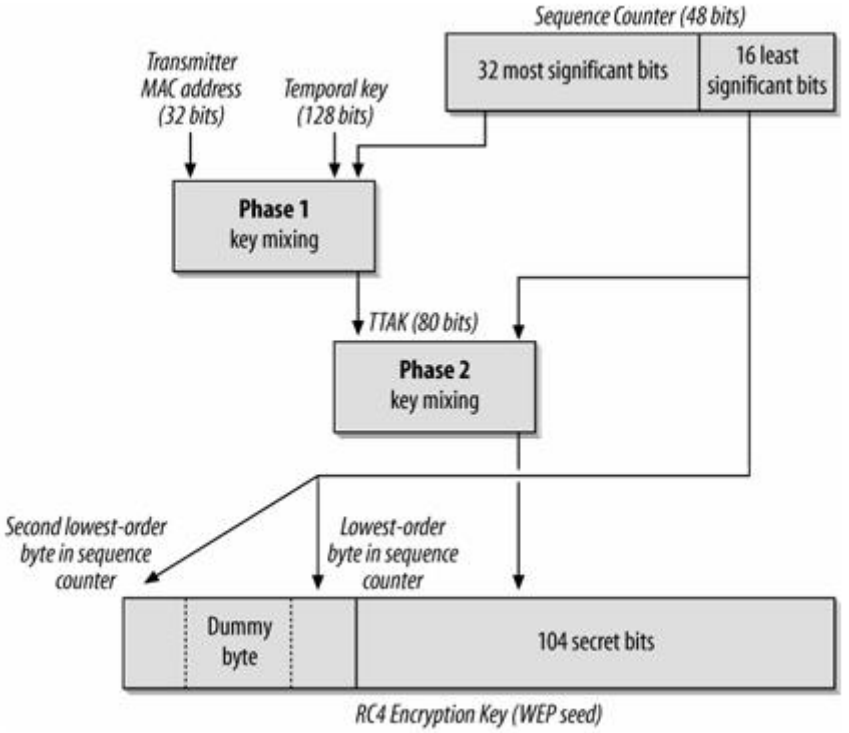
Επιπλέον, το TKIP χρησιμοποιεί έναν πιο ανθεκτικό αλγόριθμο ελέγχου ακεραιότητας, που ονομάζεται *Michael* integrity check (MIC). Ο MIC απαιτεί ένα κλειδί, διαφορετικό από αυτό που χρησιμοποιείται για την κρυπτογράφηση και, εκτός από τα δεδομένα, συμπεριλαμβάνει στη διαδικασία του και τις διευθύνσεις πηγής και προορισμού. Ο MIC μπορεί να είναι καλύτερος από τον CRC αλλά δεν προσφέρει ασφάλεια σε μία επίμονη, επαναλαμβανόμενη επίθεση. Για τον λόγο αυτό, το TKIP συμπεριλαμβάνει ενέργειες πρόληψης (*countermeasures*) για την ανίχνευση και την αντιμετώπιση μιας ενεργούς επίθεσης. Εάν ο MIC αποτύχει δεύτερη φορά σε διάστημα 60 δευτερολέπτων, οι countermeasures επιβάλουν τη διακοπή των επικοινωνιών για 60 δευτερόλεπτα. Οι σταθμοί διαγράφουν τα αντίγραφα των κύριων κλειδιών και ζητούν νέα κλειδιά από τους authenticators. Το 802.11i θέτει τον χρόνο των Michael countermeasures σε 60 δευτερόλεπτα αλλά κάποιοι κατασκευαστές επιτρέπουν τη ρύθμιση του [1].

Ο υπολογισμός του MIC γίνεται σε επίπεδο πακέτων και όχι πλαισίων ενώ η κρυπτογράφηση εφαρμόζεται σε κάθε πλαίσιο χωριστά [17].

4.4.1.1 Key mixing

Το TKIP παράγει ένα μοναδικό κλειδί για κάθε πλαίσιο. Για την παραγωγή κάθε ξεχωριστού κλειδιού χρησιμοποιούνται ο InitializationVector/ SequenceCounter (IV/SC), η διεύθυνση του αποστολέα (transmitter) και το master key. Η διαδικασία, όπως φαίνεται και στην εικόνα 4.3 χωρίζεται σε δύο φάσεις και έχει ως εξής:

Στην πρώτη φάση συνδυάζονται η διεύθυνση αποστολέα, τα 32 τελευταία bits του SC και το 128-bit κλειδί, τα οποία δίνουν ως έξοδο μία τιμή των 80 bits. Η τιμή αυτή είναι σταθερή εφ' όσον τα 32 τελευταία bits του μετρητή ακολουθίας είναι σταθερά, έτσι πρέπει μόνο να υπολογιστεί μια φορά κάθε 65.536 πλαίσια.



Εικόνα 4.3 Key Mixing [1]

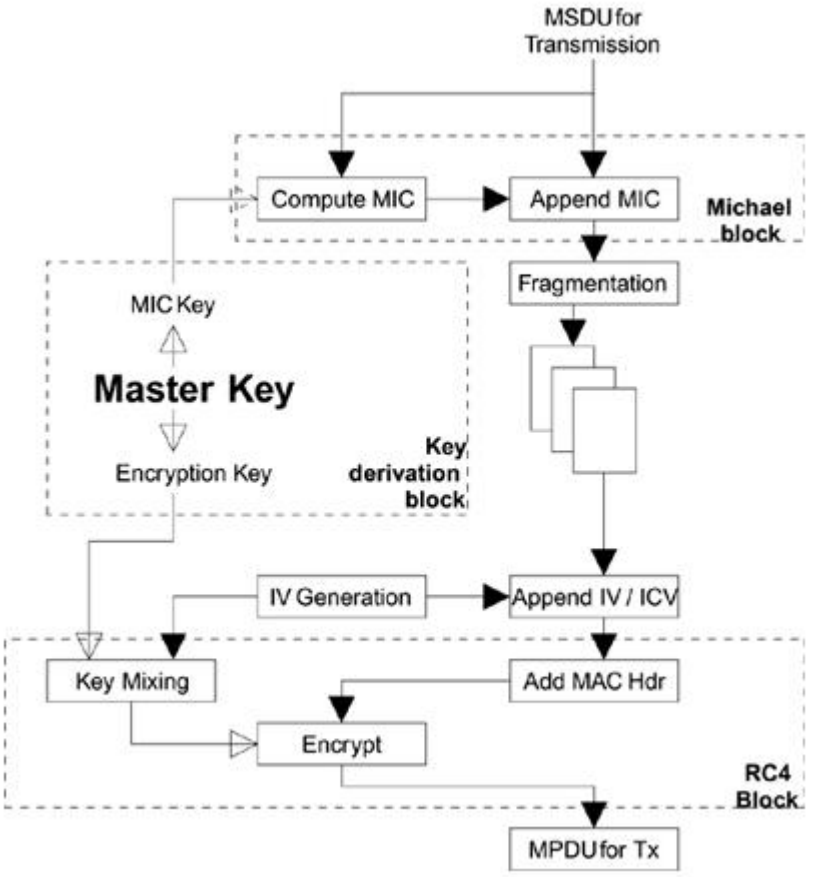
Η φάση δύο υπολογίζεται για κάθε πλαίσιο. Σαν εισαγωγή, παίρνει το αποτέλεσμα της πρώτης φάσης και τα 16 πρώτα bits του μετρητή ακολουθίας, που είναι και ο μόνος που αλλάζει από πλαίσιο σε πλαίσιο. Η έξοδος της δεύτερης φάσης είναι ένα 128-bit RC4 κλειδί. Τα τρία πρώτα bytes αυτού του

κλειδιού μεταδίδονται ως IV του WEP και περιλαμβάνουν τα 16 πρώτα bits του TKIP IV και ένα “Dummy byte”. Το byte αυτό χρησιμοποιείται για την αποφυγή δημιουργίας αδύναμων κλειδιών (weak keys) [17].

4.4.1.2 TKIP Data Processing

Το 802.11 πλαίσιο περιμένει στη σειρά για τη μετάδοση. Όπως το WEP, έτσι και το TKIP προστατεύει μόνο το ωφέλιμο φορτίο του MAC πλαισίου και παρέχει την κρυπτογράφηση και την ακεραιότητα των δεδομένων ως μέρη μίας λειτουργίας. Η διαδικασία έχει ως εξής:

Παράγονται τα κλειδιά (MIC key και encryption key). Ο έλεγχος ακεραιότητας μηνυμάτων (MIC) υπολογίζεται. Ορίζεται ο αριθμός ακολουθίας. Εκτελείται η key mixing διαδικασία και τέλος κάθε πλαίσιο κρυπτογραφείται με ένα μοναδικό κλειδί WEP. Η εικόνα 4.4 περιγράφει τη διαδικασία.



Εικόνα 4.4 TKIP διαδικασία [17]

4.4.2 Counter Mode με CBC-MAC (CCMP)

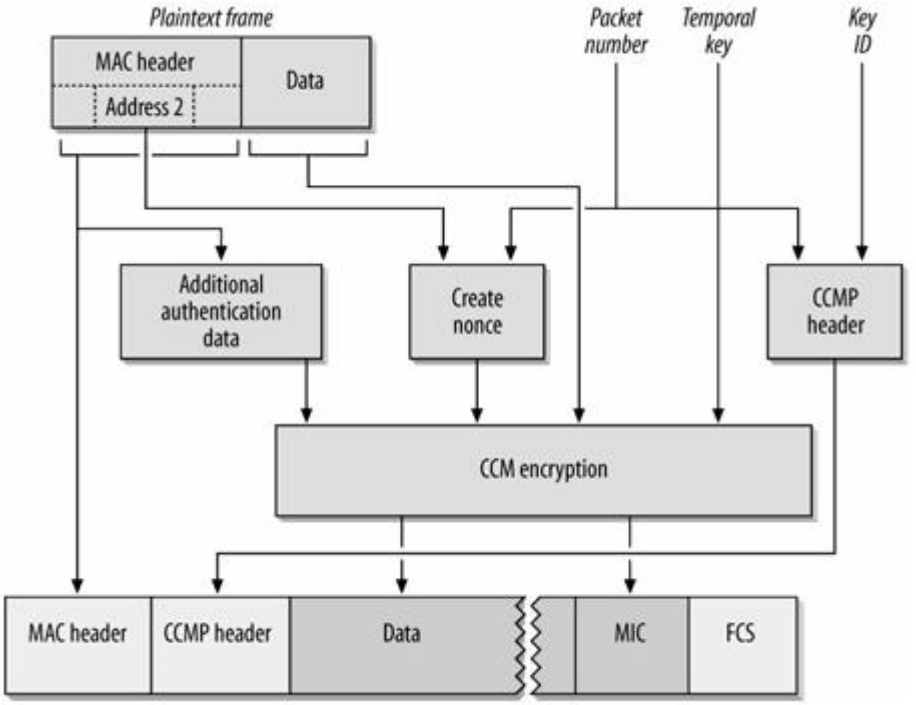
Ο αλγόριθμος κρυπτογράφησης που χρησιμοποιεί το CCMP είναι ο Advanced Encryption Standard (AES). Ο AES είναι ένας block cipher αλγόριθμος. Συνδυάζει ένα κλειδί και ένα block δεδομένων των 128 bits, το οποίο κρυπτογραφεί. Το μέγεθος των block δεδομένων και των κλειδιών μπορεί να επιλεγεί ανάμεσα στις τιμές 128, 192 ή 256 bits. Ωστόσο το 802.11i ορίζει τη χρήση 128 bits και για το κλειδί και για τα blocks [17]. Το CCMP χρησιμοποιεί το ίδιο κλειδί και για την κρυπτογράφηση και για τον έλεγχο ακεραιότητας [1].

CCMP data transmission

Η διαδικασία κρυπτογράφησης στο CCMP φαίνεται στην εικόνα 4.5 και περιλαμβάνει τα ακόλουθα βήματα:

1. Το 802.11 πλαίσιο είναι έτοιμο για μετάδοση. Το CCMP, όπως και τα άλλα πρωτόκολλα, προστατεύει μόνο το ωφέλιμο φορτίο του πλαισίου.
2. Ορίζεται ένας αριθμός πακέτου (Packet Number, PN) των 48 bits. Ο αριθμός αυτός εξυπηρετεί τον ίδιο σκοπό με τον μετρητή ακολουθίας που χρησιμοποιεί το TKIP. Αυξάνεται κατά ένα για κάθε μετάδοση και χρησιμοποιείται για την αντιμετώπιση των επαναλαμβανόμενων επιθέσεων.
3. Συντίθεται ένα πεδίο, το Additional Authentication Data (AAD), το οποίο αποτελείται από τα πεδία της κεφαλίδας του πλαισίου που πρέπει να πιστοποιηθούν. Ο παραλήπτης θα χρησιμοποιήσει το AAD για να βεβαιωθεί ότι τα πεδία αυτά δεν τροποποιήθηκαν κατά τη μετάδοση. Τα πεδία αυτά είναι τα protocol version, frame type, sequence control field, distribution system bits, fragmentation και order bits καθώς επίσης και τα πεδία των διευθύνσεων.
4. Έπειτα δημιουργείται το CCMP nonce. Τα nonces είναι λίγα bits δεδομένων που εξασφαλίζουν ότι η κρυπτογράφηση εφαρμόζεται κάθε φορά σε μοναδικά δεδομένα. Δημιουργούνται από τον αριθμό πακέτου και τη διεύθυνση αποστολέα κι έτσι ο ίδιος αριθμός πακέτου μπορεί να χρησιμοποιηθεί από πολλούς σταθμούς.

5. Δημιουργείται επίσης η CCMP header, η οποία αποτελείται από τον αριθμό πακέτου και το προσδιοριστικό του κλειδιού, καθώς το CCMP μπορεί να χρησιμοποιεί τέσσερα διαφορετικά κλειδιά, όπως το WEP.
6. Το 128-bit temporal key, τα nonce bits, το AAD πεδίο και το σώμα του πλαισίου είναι η είσοδος της CCM διαδικασίας κρυπτογράφησης. Το ίδιο κλειδί που χρησιμοποιείται για την κρυπτογράφηση, χρησιμοποιείται και για τον έλεγχο ακεραιότητας των δεδομένων (MIC) το αποτέλεσμα του οποίου κρυπτογραφείται μαζί με τα δεδομένα.
7. Οι MAC και CCMP κεφαλίδες προστίθενται στο κρυπτογραφημένο πλαίσιο το οποίο είναι έτοιμο για μετάδοση.



Εικόνα 4.5 Διαδικασία της CCMP κρυπτογράφησης [1]

4.4.3 Robust Security Networks (RSNs)

Το 802.11i εκτός από το TKIP και το CCMP, ορίζει και ένα σύνολο διαδικασιών παραγωγής και διαμοιρασμού κλειδιών, για να δημιουργήσει, αυτό που το πρότυπο αποκαλεί, Robust Security Networks (RSNs) [1][4][26].

4.4.3.1 Ιεραρχία κλειδιών στο 802.11i

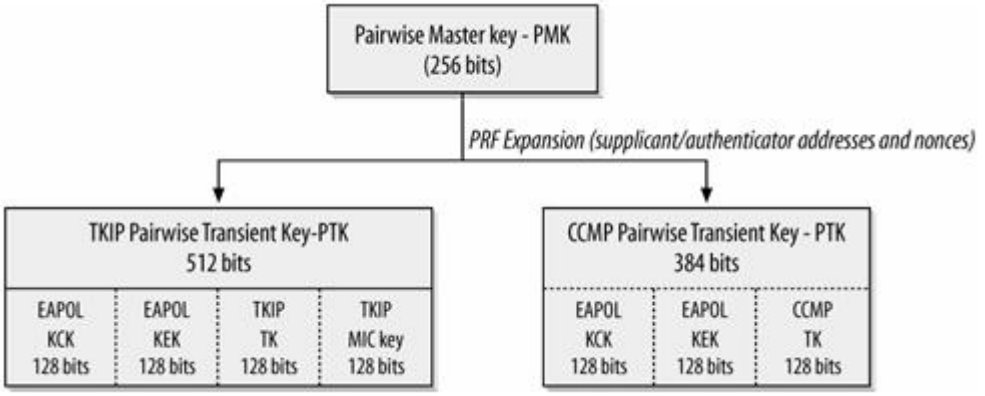
Υπάρχουν δύο τύποι κλειδιών που χρησιμοποιούνται από τα πρωτόκολλα κρυπτογράφησης του επιπέδου συνδέσμου. Τα *pairwise* κλειδιά προστατεύουν την κίνηση μεταξύ του σταθμού και του AP (unicast μεταδόσεις). Τα *group* κλειδιά προστατεύουν τις broadcast και multicast μεταδόσεις από το AP προς τους συσχετισμένους πελάτες. Τα pairwise κλειδιά παράγονται μέσω της διαδικασίας πιστοποίησης, η οποία αναπτύσσεται σε επόμενη. Τα group keys παράγονται τυχαία και διανέμονται σε κάθε σταθμό από το AP.

4.4.3.2 Ιεραρχία pairwise κλειδιών

Και το TKIP και το CCMP παίρνουν ένα μοναδικό master key και το επεκτείνουν στα διάφορα κλειδιά, που απαιτούνται για την προστασία των πλαισίων. Με το μηχανισμό παραγωγής κλειδιών, οι σταθμοί μπορούν να ανανεώνουν τα κλειδιά κρυπτογράφησης χωρίς να πρέπει να επαναλάβουν ολόκληρη τη διαδικασία πιστοποίησης. Το master key είναι η ρίζα που πρέπει να προστατευθεί πολύ προσεκτικά καθώς όλα τα υπόλοιπα κλειδιά παράγονται από αυτό. Ένα μέρος της ιεραρχίας κλειδιών είναι η παραγωγή κλειδιών τα οποία θα χρησιμοποιηθούν για να προστατέψουν τη μετάδοση των temporal κλειδιών.

Η διαδικασία ξεκινά από το master key, το οποίο ονομάζεται *pairwise master key (PMK)*. Το κλειδί αυτό υπολογίζεται από έναν εξυπηρετητή RADIUS και στέλνεται κρυπτογραφημένο στο AP. Κατόπιν, για την απόκτηση των temporal κλειδιών, το PMK επεκτείνεται μέσω μιας καθορισμένης ψευδοτυχαίας συνάρτησης. Τόσο το TKIP όσο και το CCMP χρησιμοποιούν την ψευδοτυχαία συνάρτηση για να επεκτείνουν το PMK σε ένα άλλο κλειδί που ονομάζεται *pairwise transient key (PTK)* από το οποίο τελικά θα προκύψουν τα temporal keys αλλά και τα κλειδιά θα προστατέψουν τα temporal keys κατά τη διανομή. Τα κλειδιά αυτά είναι τα EAPOL Key Confirmation Key (KCK) και EAPOL Key Encryption Key (KEK). Το πρώτο χρησιμοποιείται για τον έλεγχο ακεραιότητας των μηνυμάτων που έχουν να κάνουν με την παραγωγή των temporal κλειδιών και το δεύτερο για την

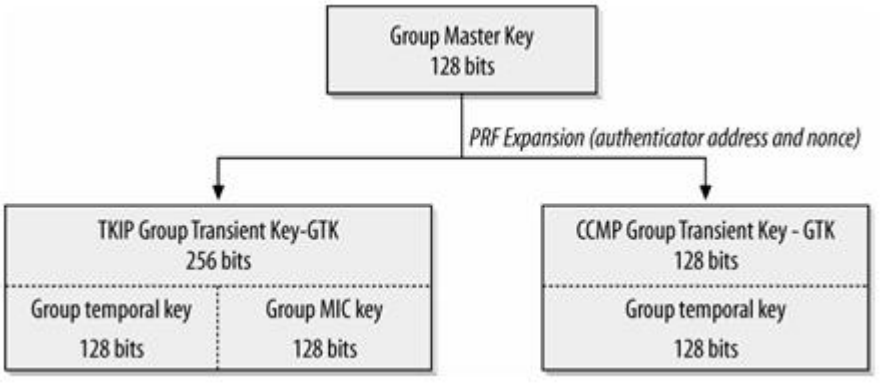
κρυπτογράφηση των μηνυμάτων αυτών. Η ιεραρχία των pairwise κλειδιών φαίνεται στην εικόνα 4.6.



Εικόνα 4.6 Ιεραρχία των pairwise κλειδιών [1].

4.4.3.3 Ιεραρχία των group keys

Το AP διατηρεί ένα *group master key (GMK)*. Το κλειδί αυτό επεκτείνεται επίσης με τη χρήση μιας ψευδοτυχαίας συνάρτησης στα temporal keys. Εδώ δεν χρειάζονται κλειδιά για την κρυπτογράφηση και επιβεβαίωση των temporal keys, καθώς για τη διανομή τους χρησιμοποιούνται τα pairwise EAPOL κλειδιά. Τα APs μπορούν να ανανεώνουν τα group keys όταν οι σταθμοί αφήνουν το δίκτυο. Στο TKIP, η αναπαραγωγή των group keys μπορεί επίσης να προκληθεί από τις countermeasures. Τέλος, την ανανέωση ενός group key μπορούν να ζητήσουν και οι σταθμοί. Η ιεραρχία των group κλειδιών φαίνεται στην εικόνα 4.7.



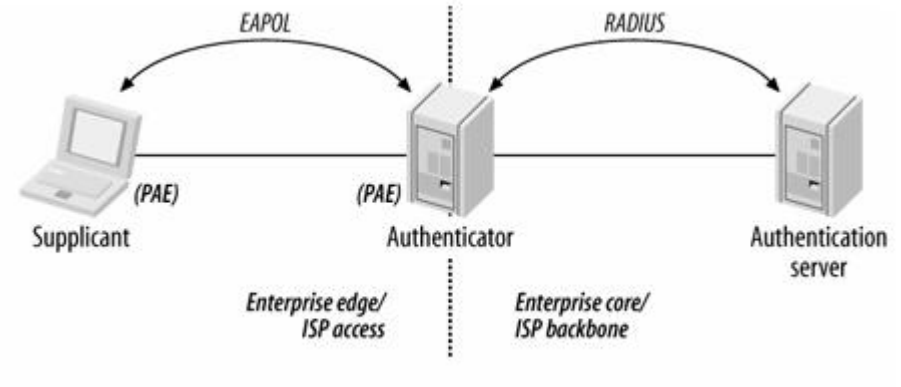
Εικόνα 4.7 Ιεραρχία των group κλειδιών [1].

4.5 Πιστοποίηση χρηστών με το 802.1X

Στις προηγούμενες ενότητες περιγράφηκαν διαδικασίες που αφορούν στη διαφύλαξη της ακεραιότητας των ασύρματων μεταδόσεων. Προτού όμως λάβει χώρα οποιαδήποτε μετάδοση, κάθε σταθμός θα πρέπει να πιστοποιηθεί για να μπορέσει να έχει πρόσβαση στο δίκτυο. Το 802.11i, για την πιστοποίηση των χρηστών χρησιμοποιεί το 802.1X. Το 802.1X υποστηρίζει μεθόδους για την αμοιβαία πιστοποίηση μεταξύ χρηστών και AP. Έτσι οι χρήστες μπορούν να επιβεβαιώνουν ότι στέλνουν πολύτιμες πληροφορίες σε έγκυρα APs και όχι σε κάποιο rogue AP. Επίσης, το 802.1X υποστηρίζει την παραγωγή δυναμικών κλειδιών WEP για μεγαλύτερη ασφάλεια. Το πρωτόκολλο που χρησιμοποιεί για την πιστοποίηση είναι το Extensible Authentication Protocol (EAP). Το 802.1X δεν αποτελεί ένα πρότυπο αποκλειστικά για ασύρματα δίκτυα. Μπορεί να χρησιμοποιηθεί και σε ενσύρματα και σε ασύρματα δίκτυα και αποτελείται από τρία συστατικά:

- Τον *Supplicant* που είναι η συσκευή του τελικού χρήστη και που θέλει να αποκτήσει πρόσβαση στο δίκτυο.
- Τον *Authenticator* που ελέγχει την πρόσβαση στο δίκτυο αλλά δεν διατηρεί τις πληροφορίες των χρηστών και
- Τον *Authentication server (AS)* που επικυρώνει τα στοιχεία του χρήστη κι ενημερώνει τον authenticator ότι ο supplicant έχει πιστοποιηθεί. Ο AS διατηρεί μία βάση δεδομένων των χρηστών για να πιστοποιεί τα στοιχεία τους. Ο AS συνήθως είναι ένας εξυπηρετητής RADIUS [19].

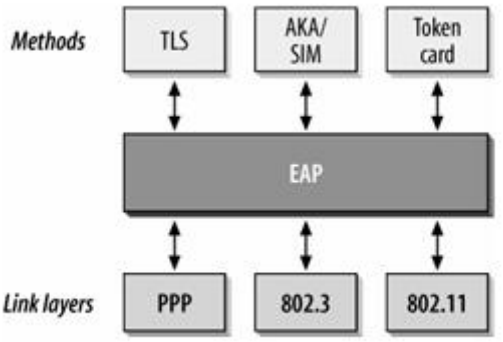
Η διαδικασία της πιστοποίησης πραγματοποιείται μεταξύ του supplicant και του authentication server, με τον authenticator να ενεργεί μόνο ως γέφυρα. Το πρωτόκολλο που χρησιμοποιείται για την επικοινωνία μεταξύ του supplicant και του authenticator είναι το EAP over LANs (EAPOL), όπως ορίζεται από 802.1X. Στην εικόνα 4.8 φαίνεται η αρχιτεκτονική του 802.1X.



Εικόνα 4.8 Αρχιτεκτονική του 802.1X [1]

4.5.1 Extensible Authentication Protocol (EAP)

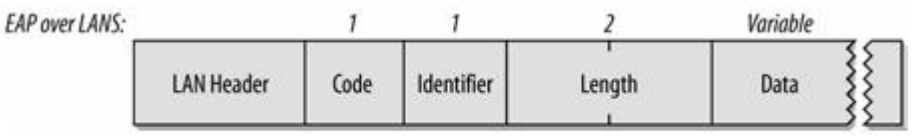
Το 802.1X είναι βασισμένο στο Extensible Authentication Protocol (EAP). Το EAP είναι μια απλή ενθυλάκωση που μπορεί να τρέξει σε οποιοδήποτε επίπεδο συνδέσμου χρησιμοποιώντας διάφορες μεθόδους πιστοποίησης (εικόνα 4.9).



Εικόνα 4.9 Αρχιτεκτονική του EAP [1]

4.5.1.1 Μορφή του EAP πακέτου

Η εικόνα 4.10 δείχνει τη μορφή ενός EAP πακέτου.



Εικόνα 4.10 Μορφή του EAP πακέτου [1]

Code

Το πεδίο Code έχει μήκος 1 byte και προσδιορίζει τον τύπο του πακέτου EAP. Χρησιμοποιείται για την ερμηνεία του πεδίου Data του πακέτου.

Identifier

Το πεδίο Identifier έχει επίσης μήκος 1 byte. Περιέχει έναν μη προσημασμένο ακέραιο αριθμό που χρησιμοποιείται για να αντιστοιχίζει τα αιτήματα με τις απαντήσεις τους. Οι αναμεταδόσεις χρησιμοποιούν τους ίδιους αριθμούς προσδιοριστικών, αλλά για κάθε νέα μετάδοση απαιτείται ένας νέος τέτοιος αριθμός.

Length

Το πεδίο Length έχει μήκος 2 bytes. Είναι ο αριθμός των bytes που βρίσκονται σε ολόκληρο το πακέτο, το οποίο περιλαμβάνει τα πεδία Code, Identifier, Length και Data.

Data

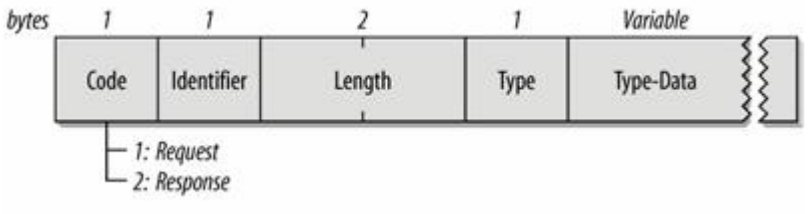
Το τελευταίο πεδίο είναι το μεταβλητού μήκους πεδίο Data. Ανάλογα με τον τύπο του πακέτου, το πεδίο αυτό μπορεί να έχει και μηδενικό μήκος. Η ερμηνεία του πεδίου Data βασίζεται στην τιμή του πεδίου Code.

Το πεδίο code

Οι ανταλλαγές EAP αποτελούνται από αιτήματα (requests) και απαντήσεις (responses). Ο authenticator στέλνει αιτήματα στο supplicant, και βάσει των απαντήσεων, η πρόσβαση μπορεί να επιτραπεί ή να απαγορευτεί.

Το πεδίο Code παίρνει τιμή 1 για τα αιτήματα και τιμή 2 για τις απαντήσεις. Τα πεδία Identifier και Length χρησιμοποιούνται όπως περιγράφηκε παραπάνω και το πεδίο Data μεταφέρει τα δεδομένα που χρησιμοποιούνται στα αιτήματα και τις απαντήσεις. Κάθε πεδίο Data μεταφέρει έναν τύπο

δεδομένων, που χωρίζεται σε έναν αναγνωριστικό κωδικό τύπου και τα σχετικά δεδομένα, όπως φαίνεται στην εικόνα 4.11.



Εικόνα 4.11 EAP πακέτα αιτημάτων και απαντήσεων [1]

Το πεδίο Type έχει μήκος 1 byte και υποδεικνύει τον τύπο του αιτήματος ή της απάντησης. Μόνο ένας τύπος χρησιμοποιείται σε κάθε πακέτο. Το πεδίο Type-Data είναι ένα μεταβλητό πεδίο που ερμηνεύεται σύμφωνα με τους κανόνες για κάθε τύπο.

Type code 1: Identity

Ο authenticator γενικά χρησιμοποιεί αυτόν τον τύπο ως αρχικό αίτημα και συχνά γράφεται ως *EAP-Request/Identity* ή απλά *Request/Identity.* Το πεδίο Type-Data των *Request/Identity* πακέτων συνήθως είναι κενό. Ωστόσο, κάποιες EAP υλοποιήσεις μπορεί να συμπεριλάβουν κάποια πληροφορία στο πεδίο Type-Data για να προτρέψουν το χρήστη να εισάγει την ταυτότητά του, αν και αυτό δεν είναι κάτι που απαιτείται. Μόλις καθοριστεί το όνομα χρήστη, ο πελάτης EAP θα αποκριθεί με ένα πακέτο Response/Identity. Στα Response/Identity πακέτα, το πεδίο Type-Data περιέχει το όνομα χρήστη.

Type code 2: Notification

Ο authenticator μπορεί να χρησιμοποιήσει αυτόν τον τύπο για να στείλει ένα μήνυμα στο χρήστη. Τα μηνύματα αυτά χρησιμοποιούνται για να ειδοποιούν το χρήστη για διάφορες καταστάσεις όπως για παράδειγμα μία ειδοποίηση για έναν κωδικό πρόσβασης που πρόκειται να λήξει. Το 802.1X συνήθως δε χρησιμοποιεί notification μηνύματα και μόνο μερικοί κατασκευαστές τα υλοποιούν. Στα notification αιτήματα πρέπει να στέλνονται

απαντήσεις. Ωστόσο, τα πακέτα Response/Notification χρησιμεύουν ως απλές επιβεβαιώσεις και το πεδίο Type-Data έχει μηδενικό μήκος.

Type code 3: NAK

Οι μηδενικές επιβεβαιώσεις (Null acknowledgements, NAKs) χρησιμοποιούνται για να προτείνουν μια νέα μέθοδο πιστοποίησης. Ο authenticator εκδίδει μια πρόκληση, κωδικοποιημένη με έναν κωδικό τύπου. Οι τύποι πιστοποίησης είναι αριθμημένοι από το 4 και πάνω. Εάν το σύστημα του χρήστη δεν υποστηρίζει τον συγκεκριμένο τύπο πιστοποίησης που ορίζει η πρόκληση, μπορεί να εκδώσει ένα NAK. Το πεδίο Type-Data ενός μηνύματος NAK περιλαμβάνει ένα byte που αντιστοιχεί στον προτεινόμενο τύπο πιστοποίησης. Οι περισσότερες εφαρμογές 802.1X δεν διαπραγματεύονται, και απλά θα εμφανίσουν ένα μήνυμα λάθους εάν ο πελάτης προσπαθήσει να χρησιμοποιήσει έναν τύπο πιστοποίησης που δεν υποστηρίζεται.

4.5.1.2 Δείγμα μιας EAP διαδικασίας

Η διαδικασία EAP είναι μια σειρά βημάτων που ξεκινά με ένα αίτημα για την ταυτότητα του χρήστη και ολοκληρώνεται με ένα μήνυμα επιτυχίας ή αποτυχίας. Μόλις ο authenticator καθορίσει ότι η ανταλλαγή έχει ολοκληρωθεί, μπορεί να εκδώσει ένα EAP-Success (Code 3) ή ένα EAP-Failure (Code 4) πλαίσιο για να τερματίσει τη διαδικασία. Μπορεί να σταλούν πολλές αιτήσεις σε έναν χρήστη προτού διαπιστωθεί μια αποτυχία πιστοποίησης. Η γενική μορφή μίας EAP διαδικασίας φαίνεται στη εικόνα 4.12 και έχει ως εξής:

1. Ο authenticator εκδίδει ένα Request/Identity πακέτο για να προσδιορίσει το χρήστη. Τα πακέτα αυτά εξυπηρετούν δύο σκοπούς. Εκτός από την έναρξη της ανταλλαγής, ειδοποιούν το χρήστη ότι το δίκτυο είναι πιθανό να απορρίψει οποιαδήποτε κίνηση δεδομένων πριν την ολοκλήρωση της πιστοποίησης.
2. Το σύστημα του τελικού χρήστη προτρέπει για την εισαγωγή, συλλέγει το αναγνωριστικό χρήστη και το στέλνει σε ένα μήνυμα Response/Identity.

3. Αφού ο χρήστης αναγνωριστεί, ο authenticator εκδίδει μία πρόκληση πιστοποίησης (στη συγκεκριμένη περίπτωση ο authenticator εκδίδει μια πρόκληση MD-5 με ένα Request/MD-5 Challenge πακέτο).
4. Το σύστημα του χρήστη όμως είναι ρυθμισμένο να χρησιμοποιεί τη μέθοδο Generic Token Card για πιστοποίηση. Έτσι απαντά με ένα Response/NAK, προτείνοντας τη χρήση αυτής της μεθόδου.
5. Ο authenticator εκδίδει μία Request/Generic Token Card πρόκληση, ζητώντας την αριθμητική ακολουθία της κάρτας.
6. Ο χρήστης πληκτρολογεί μια απάντηση η οποία στέλνεται με ένα Response/Generic Token Card πακέτο.
7. Εάν η απάντηση του χρήστη δεν είναι σωστή, η πιστοποίηση δεν είναι δυνατή. Παρόλα αυτά το EAP επιτρέπει πολλαπλά αιτήματα πιστοποίησης, έτσι ένα δεύτερο Request/Generic Token Card εκδίδεται.
8. Και πάλι, ο χρήστης πληκτρολογεί μια απάντηση, η οποία στέλνεται με μία Response/Generic Token Card.
9. Στη δεύτερη προσπάθεια, η απάντηση είναι σωστή, έτσι ο authenticator εκδίδει ένα μήνυμα επιτυχίας (Success message).

Εικόνα 4.12 Διαδικασία EAP [1]

4.5.1.3 Μέθοδοι πιστοποίησης του EAP

Το EAP δεν ορίζει έναν στάνταρ μηχανισμό πιστοποίησης, αλλά χρησιμοποιεί διάφορες μεθόδους. Όταν οι απαιτήσεις αλλάζουν, νέες μέθοδοι EAP μπορούν να αναπτυχθούν για να αντιμετωπίσουν την εκάστοτε πρόκληση. Μερικές από τις μεθόδους που χρησιμοποιεί το EAP είναι οι: EAP-MD-5, EAP-TLS (Transport Layer Security), EAP-PEAP (Protected Extensible Authentication Protocol), EAP-TTLS (Tunnelled TLS), EAP-FAST και Cisco LEAP (Lightweight Extensible Authentication Protocol) [1][4][27].

EAP-MD5 – στη μέθοδο αυτή ο σταθμός και ο AS μοιράζονται ένα κοινό μυστικό, συνήθως έναν κωδικό που σχετίζεται με ένα όνομα χρήστη. Αφού λάβει το όνομα χρήστη, ο AS στέλνει μία πρόκληση στο σταθμό. Ο σταθμός εφαρμόζει στο κείμενο πρόκληση τον αλγόριθμο MD-5 χρησιμοποιώντας το κοινό μυστικό και στέλνει την τιμή hash που προκύπτει στον AS. Ο AS εξακριβώνει την τιμή που έλαβε και ανάλογα εγκρίνει ή απορρίπτει την πιστοποίηση. Μετά την πιστοποίηση τα μηνύματα στέλνονται σε καθαρό κείμενο (cleartext). Εξαιτίας αυτού αλλά και λόγω του ότι δεν παρέχει αμοιβαία πιστοποίηση, η EAP-MD5 δεν αποτελεί καλή επιλογή και δεν συνίσταται ιδιαίτερα [4].

EAP-TLS- αυτή η μέθοδος χρησιμοποιεί ψηφιακά πιστοποιητικά (certificates) αντί για κωδικούς πρόσβασης και προϋποθέτει ότι ο supplicant και ο authentication server έχει ο καθένας το δικό του ξεχωριστό πιστοποιητικό. Επίσης, υποστηρίζει την παραγωγή δυναμικών κλειδιών WEP για την κρυπτογράφηση συνεχόμενων μεταδόσεων μεταξύ του supplicant και του authenticator. Η EAP-TLS παρέχει αμοιβαία πιστοποίηση μεταξύ του supplicant και του authentication server, πιστοποιώντας και τον χρήστη στο δίκτυο και το δίκτυο στο χρήστη. Έτσι οι χρήστες προστατεύονται από τα γνωστά rogue APs. Ωστόσο, η μέθοδος αυτή γνώρισε περιορισμένη χρήση λόγω της διαχειριστικής πολυπλοκότητας των πιστοποιητικών .

EAP-TTLS και EAP-PEAP – είναι εναλλακτικές μορφές του EAP-TLS στις οποίες μόνο ο authentication server χρειάζεται να έχει πιστοποιητικό. Ο

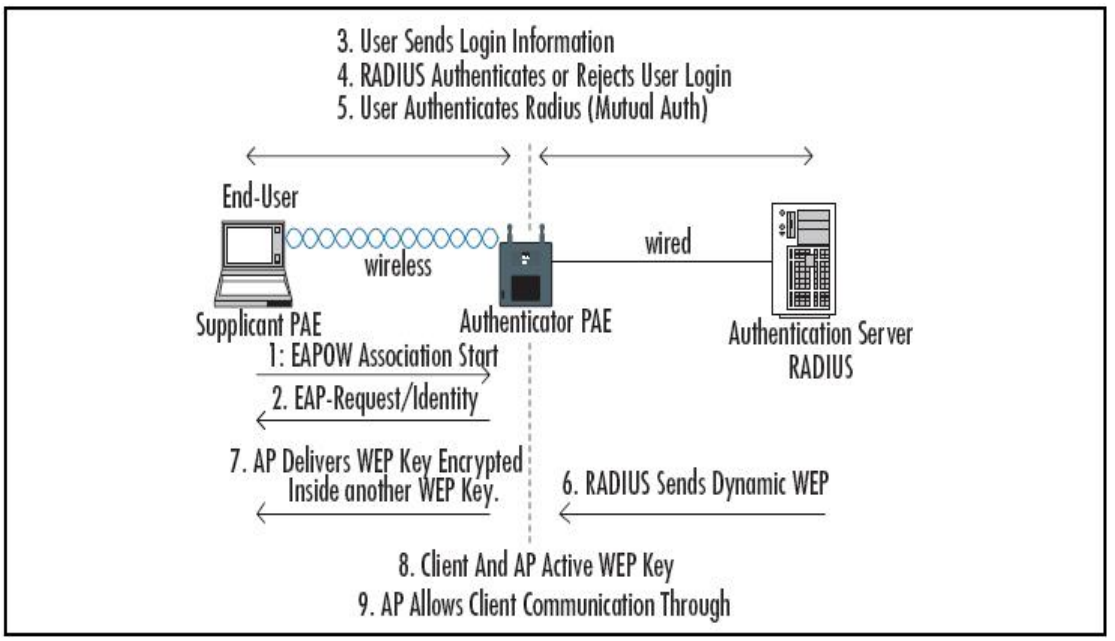
supplicant πιστοποιεί την ταυτότητα του authentication server επιβεβαιώνοντας το ψηφιακό πιστοποιητικό του. Κατόπιν δημιουργείται μία μονόδρομη σήραγγα TLS (TLS tunnel) επιτρέποντας στα δεδομένα πιστοποίησης του χρήστη (password, PIN κτλ) να ενθυλακωθούν ως TLS μηνύματα και να μεταφερθούν με ασφάλεια στον authentication server. Η παραγωγή δυναμικών κλειδιών υποστηρίζεται και από αυτές τις μεθόδους.

EAP-FAST – αυτή η μέθοδος αναπτύχθηκε από τη Cisco, χρησιμοποιεί κωδικούς πρόσβασης και παρέχει αμοιβαία πιστοποίηση χρησιμοποιώντας TLS για να εγκαθιδρύσει μία σήραγγα μέσα από την οποία θα περάσουν τα δεδομένα πιστοποίησης του πελάτη και του authentication server. Τα διαπιστευτήρια (credentials) που χρησιμοποιούνται για την εγκαθίδρυση της TLS σήραγγας ονομάζονται Protected Access Credentials (PAC).

Cisco-LEAP – το Cisco wireless EAP, γνωστό και ως LEAP, αναπτύχθηκε από τη Cisco για να ενισχύσει το EAP. Το LEAP παρέχει αρκετές αναβαθμίσεις και διαφορές από τις υπόλοιπες μεθόδους του EAP. Παρέχει αμοιβαία πιστοποίηση αλλά όχι με τη χρήση πιστοποιητικών όπως το EAP TLS, παρά χρησιμοποιώντας ονόματα χρηστών και κωδικούς πρόσβασης. Αυτό μπορεί να είναι λιγότερο ασφαλές από τα ψηφιακά πιστοποιητικά αλλά αποτελεί μία διαφορετική, γρηγορότερη και με λιγότερες διαχειριστικές απαιτήσεις επιλογή από το TLS. Επίσης, το LEAP υποστηρίζει υλοποίηση δυναμικού WEP, με τα κλειδιά να ανανεώνονται ανά χρήστη και ανά συνεδρία [13].

LEAP Authentication Process

Προτού ξεκινήσει η διαδικασία, ο εξυπηρετητής RADIUS και ο πελάτης πρέπει να έχουν ένα κοινό μυστικό. Στον εξυπηρετητή RADIUS έχει ρυθμιστεί μία βάση δεδομένων με ονόματα-κωδικούς πρόσβασης όλων των χρηστών ενώ κάθε πελάτης έχει το δικό του όνομα χρήστη και κωδικό πρόσβασης. Η διαδικασία πιστοποίησης ενός ασύρματου σταθμού, όταν χρησιμοποιείται το LEAP, είναι η ακόλουθη:



Εικόνα 4.13 Διαδικασία πιστοποίησης με χρήση LEAP [27]

1. Ο σταθμός στέλνει ένα EAPOW-Start για να ξεκινήσει τη διαδικασία της πιστοποίησης.
2. Το AP απαντά με ένα EAP-Request/Identity για να εξακριβώσει την ταυτότητα του χρήστη.
3. Ο σταθμός απαντά στέλνοντας όνομα χρήστη και κωδικό πρόσβασης.
4. Το AP στέλνει τα στοιχεία του πελάτη στον εξυπηρετητή RADIUS όπου τα στοιχεία αυτά εξακριβώνονται. Κατόπιν ο εξυπηρετητής RADIUS στέλνει μία πρόκληση στο σταθμό μέσω του AP. Όταν ο σταθμός λάβει την πρόκληση, εκτελεί τον αλγόριθμο Cisco LEAP συνδυάζοντας την πρόκληση και τον κωδικό του χρήστη. Το αποτέλεσμα είναι μια τιμή hash η οποία στέλνεται στον εξυπηρετητή RADIUS. Στον εξυπηρετητή RADIUS, εκτελείται η ίδια διαδικασία και η τιμή που παράγεται συγκρίνεται με την τιμή που έστειλε ο σταθμός. Αν οι δύο τιμές ταιριάζουν, ο σταθμός πιστοποιείται και ο εξυπηρετητής RADIUS στέλνει ένα μήνυμα επιτυχίας στο σταθμό, πάντα μέσω του AP [13].
5. Ο χρήστης πιστοποιεί τον εξυπηρετητή RADIUS για να διασφαλιστεί η αμοιβαία πιστοποίηση και η ακεραιότητα του ασύρματου δικτύου. Για να γίνει αυτό, ο σταθμός στέλνει μία πρόκληση στον εξυπηρετητή RADIUS. Αν ο εξυπηρετητής απαντήσει σωστά, πιστοποιείται και ο σταθμός στέλνει ένα μήνυμα επιτυχίας στον εξυπηρετητή [13].

6. Όταν η πιστοποίηση ολοκληρωθεί, ο εξυπηρετητής RADIUS στέλνει ένα κλειδί WEP στο AP.
7. Το AP στέλνει το κλειδί WEP στο σταθμό μέσω του EAPOW.
8. Ο σταθμός και το AP εγκαθιστούν το κλειδί αυτό και θα το χρησιμοποιήσουν στο εξής για να επικοινωνούν.
9. Μέχρι να πιστοποιηθεί ο χρήστης, όλες οι επικοινωνίες, εκτός από τα πακέτα EAP, ήταν μπλοκαρισμένες. Σε αυτή τη φάση το AP ανοίγει τις επικοινωνίες και επιτρέπει στο σταθμό να έχει πρόσβαση στο δίκτυο [27].

Παρόλο που η LEAP ήταν η μέθοδος που γνώρισε πρώτη ευρεία αποδοχή, η χρήση του απαρχαιωμένου MS-CHAP για την ανταλλαγή των μηνυμάτων περιόρισε τη χρήση της. Η Cisco πλέον προτείνει τη χρήση του PEAP ή του EAP-FAST [1].

4.5.2 Το 802.1X στα WLANs

Αφού η διαδικασία της συσχέτισης ανάμεσα στον ασύρματο σταθμό και το AP ολοκληρωθεί, η λειτουργία του EAPOL μπορεί να ξεκινήσει. Αφού συσχετιστεί, ένας σταθμός μπορεί να πιστοποιηθεί με την ανταλλαγή 802.1X πλαισίων. Η 802.1X διαδικασία περιλαμβάνει και τη διανομή του κλειδιού.

Δείγμα μιας 802.1X διαδικασίας στο 802.11

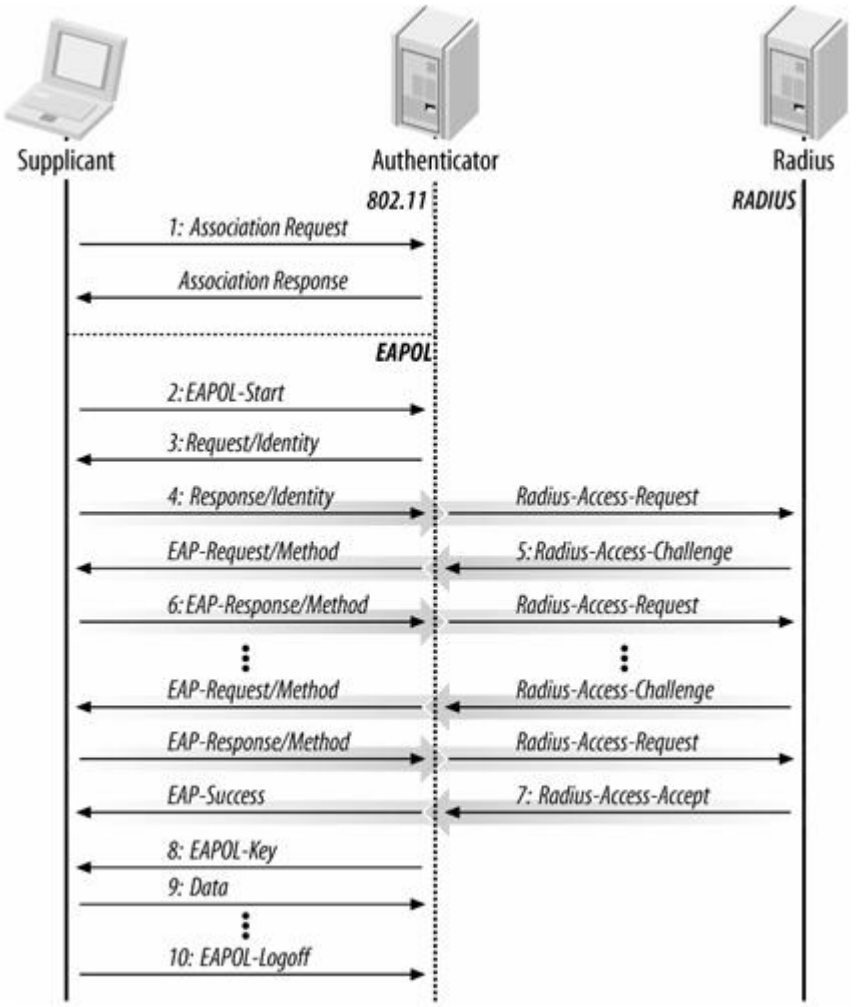
Η EAPOL διαδικασία είναι σχεδόν ίδια με την EAP διαδικασία. Η βασική διαφορά είναι ο supplicant μπορεί να στείλει ένα EAPOL-Start πλαίσιο για να προκαλέσει την εκκίνηση μιας EAP διαδικασίας και μπορεί επίσης να χρησιμοποιήσει ένα EAPOL-Logoff πλαίσιο για να τερματίσει την πιστοποίηση όταν θελήσει να φύγει από το δίκτυο. Η διαδικασία περιγράφεται παρακάτω και απεικονίζεται στην εικόνα 4.13.

1. Ο σταθμός (supplicant) συσχετίζεται με το 802.11 δίκτυο.
2. Ο σταθμός ξεκινά την 802.1X διαδικασία με ένα μήνυμα EAPOL-Start. Αυτό το βήμα είναι προαιρετικό και μπορεί να μην υπάρχει καθώς δε στέλνουν όλοι οι σταθμοί EAPOL-Start μηνύματα.

3. Η «κανονική» διαδικασία EAP αρχίζει. Το AP (authenticator) εκδίδει ένα EAP-Request/Identity πλαίσιο. Τα Request/Identity πλαίσια υποδεικνύουν στο σταθμό ότι απαιτείται 802.1X πιστοποίηση.
4. Ο σταθμός απαντά με ένα EAP-Response/Identity πλαίσιο, το οποίο στέλνεται στον εξυπηρετητή RADIUS ως ένα Radius-Access-Request πακέτο.
5. Ο εξυπηρετητή RADIUS καθορίζει τον τύπο πιστοποίησης που απαιτείται, και στέλνει ένα EAP-Request για τον τύπο της μεθόδου. Το EAP-Request είναι ενθυλακωμένο σε ένα Radius-Access-Challenge πακέτο. Όταν φθάνει στο AP, το EAP-Request στέλνεται στον σταθμό. Τα EAP-Requests συχνά εμφανίζονται ως EAP-Request/Method, όπου το πεδίο Method αναφέρεται στη μέθοδο EAP που χρησιμοποιείται.
6. Ο σταθμός συλλέγει την απάντηση από το χρήστη και στέλνει μια EAP-Response. Η απάντηση μεταφράζεται από τον authenticator σε ένα Radius-Access-Request.

Τα βήματα πέντε και έξι μπορεί να επαναληφθούν πολλές φορές μέχρι να επιλεγεί η κατάλληλη μέθοδος και να ολοκληρωθεί η πιστοποίηση.

7. Ο εξυπηρετητή RADIUS εκχωρεί την πρόσβαση με ένα Radius-Access-Accept πακέτο κι έτσι ο authenticator εκδίδει ένα EAP-Success πλαίσιο και πιστοποιεί τη σύνδεση.
8. Αμέσως μετά την παραλαβή του Access-Accept πακέτου, το AP διανέμει κλειδιά στο σταθμό χρησιμοποιώντας EAPOL-Key μηνύματα.
9. Μόλις εγκατασταθούν τα κλειδιά στο σταθμό, μπορεί να αρχίσει να στέλνει πλαίσια δεδομένων.
10. Όταν ο σταθμός δε χρειάζεται πλέον την πρόσβαση στο δίκτυο, στέλνει ένα EAPOL-Logoff μήνυμα για να ακυρώσει την πιστοποίηση.



Εικόνα 4.13 802.1X διαδικασία στο 802.11 [1]

Τα EAPOL-Key πλαίσια επιτρέπουν την ανταλλαγή κλειδιών. Τα πλαίσια αυτά στέλνονται μόνο αν η πιστοποίηση του χρήστη επιτύχει. Έτσι εμποδίζεται η απόκτηση των κλειδιών από μη εξουσιοδοτημένους χρήστες. Τα EAPOL-Key πλαίσια μπορεί να χρησιμοποιηθούν περιοδικά για τη δυναμική ανανέωση των κλειδιών, αντιμετωπίζοντας έτσι μία από τις μεγάλες αδυναμίες του WEP, που ήταν η χρήση του ίδιου κλειδιού για μεγάλο χρονικό διάστημα.

4.6 Συμπεράσματα

Η ασφάλεια των ασύρματων δικτύων είναι ένα αδύναμο σημείο τους. Τα δεδομένα κινδυνεύουν καθώς διασχίζουν τον αέρα και γι' αυτό πρέπει να υπάρχουν τρόποι προστασίας των επικοινωνιών. Για να προστατευθούν οι επικοινωνίες, θα πρέπει να εξασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα

και η διαθεσιμότητα των δεδομένων. Πρέπει επίσης να εξασφαλίζεται ότι θα έχουν πρόσβαση στο δίκτυο και στα δεδομένα μόνο εξουσιοδοτημένοι χρήστες. Για την κάλυψη αυτών των αναγκών αναπτύχθηκαν διάφορα πρωτόκολλα. Το πρωτόκολλο που χρησιμοποιήθηκε αρχικά στο 802.11 για την προστασία των δεδομένων ήταν το WEP. Το WEP εφαρμόζει έναν αλγόριθμο κρυπτογράφησης για να προστατέψει τα δεδομένα από τις υποκλοπές, εκτελεί έναν έλεγχο ακεραιότητας για να εξασφαλίσει την ακεραιότητα των δεδομένων και υποστηρίζει δύο μεθόδους πιστοποίησης για τον έλεγχο των χρηστών. Όμως, τόσο η μέθοδος κρυπτογράφησης όσο και οι μέθοδοι πιστοποίησης του WEP ήταν αρκετά αδύναμες και πολύ σύντομα αποδείχθηκε η αναποτελεσματικότητά του. Αυτό οδήγησε στην ανάπτυξη νέων πρωτοκόλλων ασφαλείας.

Το 2004 δημοσιεύθηκε το 802.11i, με σκοπό να καλύψει τις αδυναμίες του WEP. Τα βασικά συστατικά του είναι δύο νέα πρωτόκολλα κρυπτογράφησης, το TKIP και το CCMP. Το TKIP σχεδιάστηκε έτσι ώστε να είναι συμβατό με τον ήδη υπάρχων εξοπλισμό ενώ το CCMP σχεδιάστηκε από την αρχή έτσι ώστε να παρέχει το μεγαλύτερο δυνατό επίπεδο ασφάλειας. Το 802.11i εκτός από το TKIP και το CCMP, ορίζει και ένα σύνολο διαδικασιών παραγωγής και διαμοιρασμού κλειδιών, για να αντιμετωπίσει τα προβλήματα που δημιουργούσαν τα στατικά κλειδιά του WEP.

Για την πιστοποίηση των χρηστών το 802.11 υιοθέτησε το 802.1X, το οποίο πιστοποιεί τους χρήστες που θέλουν να συνδεθούν σε ένα δίκτυο εξασφαλίζοντας ταυτόχρονα ότι οι χρήστες συνδέονται σε ένα νόμιμο, ασφαλές δίκτυο.

Ωστόσο, η ασφάλεια είναι ένα θέμα που δεν τελειώνει ποτέ καθώς κάποιοι θα προσπαθούν πάντα να παραβιάζουν κάθε νέο πρωτόκολλο.

Κεφάλαιο 5 Υγεία

5.1 Εισαγωγή

Τα WLANs αυξάνονται συνεχώς σε σπίτια, γραφεία και πολλά δημόσια σημεία, όπως αεροδρόμια, σχολεία κτλ. Παράλληλα με την αύξηση των ασύρματων δικτύων προκύπτουν και ανησυχίες για τις επιπτώσεις που μπορεί να έχει στην υγεία η έκθεση στα ηλεκτρομαγνητικά πεδία που παράγονται από τα δίκτυα αυτά.

5.2 Ηλεκτρομαγνητική ακτινοβολία

Η κίνηση ηλεκτρονίων δημιουργεί ηλεκτρομαγνητικά κύματα. Τα ηλεκτρομαγνητικά κύματα αποτελούνται από ηλεκτρικά και μαγνητικά πεδία (ΗΜΠ) κάθετα μεταξύ τους. Τα ηλεκτρομαγνητικά πεδία, υπάρχουν παντού στο περιβάλλον μας και προέρχονται από φυσικές ή τεχνητές πηγές. Το γήινο ηλεκτρομαγνητικό πεδίο, το ηλιακό φως, οι κεραυνοί, ο χτύπος της καρδιάς, το ανθρώπινο νευρικό σύστημα αποτελούν φυσικές πηγές ηλεκτρομαγνητικών πεδίων. Στις τεχνητές πηγές περιλαμβάνονται οι οικιακές ηλεκτρικές συσκευές (ηλεκτρική σκούπα, φούρνος μικροκυμάτων, ψυγείο, τηλεόραση κ.λ.π.), οι γραμμές μεταφοράς ηλεκτρικού ρεύματος, οι τηλεοπτικοί και ραδιοφωνικοί σταθμοί, οι σταθμοί βάσης κινητής τηλεφωνίας, τα ραντάρ κ.λ.π.

Κατά τη διάδοσή τους τα ηλεκτρομαγνητικά πεδία μεταφέρουν ενέργεια η οποία ονομάζεται ηλεκτρομαγνητική ακτινοβολία. Η ακτινοβολία αυτή μπορεί να είναι ιονίζουσα ή μη ιονίζουσα. Η ιονίζουσα ακτινοβολία έχει υψηλή συχνότητα, μικρό μήκος κύματος και μεταφέρει πολύ υψηλή ενέργεια. Περιλαμβάνει την κοσμική ακτινοβολία, τις ακτίνες Χ και γ. Χαρακτηρίζεται με τον όρο «ιονίζουσα», διότι προκαλεί ιονισμό της ύλης και μπορεί να προκαλέσει άμεση βλάβη στη βιολογική ύλη και συγκεκριμένα στο DNA των κυττάρων.

Η μη ιονίζουσα ακτινοβολία έχει μικρότερη συχνότητα, μεγαλύτερο μήκος κύματος και μεταφέρει μικρή ποσότητα ενέργειας. Έτσι δεν προκαλεί ιονισμό της ύλης. Η ακτινοβολία που μεταφέρουν τα ηλεκτρομαγνητικά πεδία, στα οποία υποβαλλόμαστε καθημερινά (ραδιοκύματα, μικροκύματα, ηλεκτρισμός),

είναι μη ιονίζουσα και φτάνει μέχρι τα 300GHz στο ηλεκτρομαγνητικό φάσμα [47]. Τα ασύρματα δίκτυα λειτουργούν στα 2.4GHz και 5GHz, αποτελούν δηλαδή μέρος της μη ιονίζουσας ακτινοβολίας, οπότε θεωρητικά είναι ασφαλή για τον ανθρώπινο οργανισμό. Όμως, η ανησυχία και η επιφυλακτικότητα των ανθρώπων έχει οδηγήσει πολλούς διεθνείς και κρατικούς οργανισμούς στην έρευνα του συγκεκριμένου θέματος.

Οι επιπτώσεις που προκαλούνται από την έκθεση στην ηλεκτρομαγνητική ακτινοβολία εξαρτώνται κυρίως από δύο παράγοντες: τη συχνότητα εκπομπής και την ισχύ εκπομπής [47].

5.3 Επιστημονικές μελέτες και διεθνείς οργανισμοί

Καθώς αυξάνονται οι ανησυχίες των πολιτών για τις επιπτώσεις που μπορεί να επιφέρει η έκθεση στις ραδιοκυματικές συχνότητες που χρησιμοποιούν οι συσκευές των ασύρματων δικτύων, πολλοί διεθνείς οργανισμοί έχουν διεξάγει έρευνες για να διαπιστωθεί εάν όντως αυτή η νέα τεχνολογία αποτελεί απειλή για την υγεία.

5.3.1 International Commission on Non-Ionizing Radiation Protection (ICNIRP)

Η ICNIRP είναι η Διεθνής Υπηρεσία Προστασίας της Μη-Ιονίζουσας Ακτινοβολίας. Είναι ένα σώμα από ανεξάρτητους επιστημονικούς εμπειρογνώμονες που απαρτίζουν την κύρια Υπηρεσία με 14 μέλη, την Επιστημονική Νομοπαρασκευαστική Επιτροπή η οποία καλύπτει τους τομείς της Επιδημιολογίας, της Βιολογία, της Δοσιμετρίας, της Οπτικής Ακτινοβόλησης και από έναν αριθμό από συμβουλευτικά μέλη. Αυτή η σύνθεση έχει ως σκοπό να τονίσει σημαντικά θέματα πιθανών δυσμενών επιπτώσεων στην ανθρώπινη υγεία που θα επιφέρει η έκθεση σε μη-ιονίζουσα ακτινοβολία.

Η επίσημη θέση της υπηρεσίας είναι πως αν και έχουν γίνει εκατοντάδες έρευνες την τελευταία δεκαετία σχετικά με τις επιπτώσεις που επιφέρουν τα ηλεκτρομαγνητικά κύματα στην ανθρώπινη υγεία δεν υπάρχει καμία

επιστημονική απόδειξη που να το αποδεικνύει πως τα ηλεκτρομαγνητικά κύματα προκαλούν αρνητικές επιπτώσεις στον άνθρωπο [47].

5.3.2 Health Protection Agency (HPA)

Ο HPA είναι ένας ανεξάρτητος οργανισμός που ιδρύθηκε από την κυβέρνηση της Αγγλίας το 2003. Σκοπός του είναι η προστασία των πολιτών από απειλές που προέρχονται από μολυσματικές ασθένειες και περιβαλλοντικούς κινδύνους. Αυτό το πετυχαίνει παρέχοντας συμβουλές σε πολίτες, εργαζόμενους στον τομέα της υγείας και στην κυβέρνηση.

Ο HPA υποστηρίζει ότι μέχρι σήμερα δεν υπάρχουν αποδείξεις ότι τα WLANs έχουν επιπτώσεις στην υγεία των ανθρώπων. Τα σήματα είναι πολύ χαμηλής ισχύος, χαρακτηριστικά 0.1 Watt (100 milliwatts) και στον υπολογιστή και στο AP και μέχρι τώρα, τα αποτελέσματα παρουσιάζουν ότι οι εκθέσεις στα ραδιοκύματα είναι σύμφωνα με τις διεθνώς αποδεκτές προδιαγραφές. Με βάση την τρέχουσα γνώση και εμπειρία, οι εκθέσεις στις ραδιοσυχνότητες από το WI-FI είναι χαμηλότερες εκείνων από τα κινητά τηλέφωνα. Συγκεκριμένα, ο HPA υποστηρίζει ότι ένα άτομο που βρίσκεται στο εύρος ενός Wi-Fi hotspot για ένα χρόνο, δέχεται την ίδια ποσότητα ραδιοκυμάτων με ένα άτομο που χρησιμοποιεί κινητό τηλέφωνο για 20 λεπτά.

Εντούτοις, όπως με οποιαδήποτε νέα τεχνολογία, είναι λογική μία προληπτική προσέγγιση, για να τεθεί η κατάσταση υπό εξέταση έτσι ώστε οι πολίτες να έχουν όσο το δυνατόν μεγαλύτερη διαβεβαίωση για την ασφάλεια των ασύρματων συσκευών.

Έτσι ο HPA οργάνωσε μία έρευνα για τη μέτρηση της ηλεκτρομαγνητικής έκθεσης από συσκευές Wi-Fi. Για την έρευνα αυτή επιλέχθηκαν 15 laptops στα 2.4GHz, από αυτά που χρησιμοποιούνται στα σχολεία. Μετά από μετρήσεις, αποδείχθηκε ότι η συνολική εκπεμπόμενη ισχύς (equivalent isotropic radiated power, EIRP) ήταν μικρότερη από τα 100mW, που ορίζει το ETSI, με τη μεγαλύτερη EIRP να καταγράφεται στα 57 mW. Έτσι, ο HPA δεν βρίσκει κανέναν λόγο για τον οποίο το WI-FI δεν πρέπει να συνεχίσει να χρησιμοποιείται. Επίσης, ο HPA σχεδιάζει εργαστηριακές μετρήσεις που

περιλαμβάνουν την αξιολόγηση της ισχύος του ηλεκτρομαγνητικού πεδίου που δημιουργείται γύρω από τα APs που λειτουργούν στα 2.4GHz. Μετρήσεις επίσης θα γίνουν και για laptop και APs που λειτουργούν στα 5GHz [48][49].

5.3.3 National Radiological Protection Board (NRPB)

Ο NRPB είναι μέλος του Health Protection Agency (HPA), ο οποίος είναι ένας οργανισμός που έχει ως στόχο την προστασία της υγείας των κατοίκων της Αγγλίας και Ουαλίας.

Σύμφωνα με σχετική έρευνα που δημοσιοποίησε τον Ιανουάριο του 2005, δεν υπάρχει κανένα στοιχείο που να αποδεικνύει πως τα ηλεκτρομαγνητικά κύματα δημιουργούν ή επιταχύνουν την εμφάνιση ασθενειών στον ανθρώπινο οργανισμό. Στην έρευνά τους αναφέρουν πολλά παραδείγματα κατοίκων που είχαν εκτεθεί σε υψηλά επίπεδα ηλεκτρομαγνητικής ακτινοβολίας και δεν παρουσίασαν το παραμικρό σύμπτωμα, το οποίο να είχε σχέση με την έκθεση αυτή.

5.3.4 Federal Communications Commission (FCC)

Ο FCC είναι μια μη κυβερνητική οργάνωση που δημιουργήθηκε το 1934 με σκοπό την ρύθμιση των τηλεπικοινωνιών. Σύμφωνα με την FCC, το εάν η χρήση των μικροκυμάτων στις τηλεπικοινωνίες μπορεί να προκαλέσει προβλήματα υγείας στον άνθρωπο είναι ακόμα υπό αμφισβήτηση. Δεν υπάρχουν ακόμα σοβαρές ενδείξεις που να αποδεικνύουν ότι η χρήση των μικροκυμάτων (και συγκεκριμένα των 2,4GHz) στις τηλεπικοινωνίες μπορούν να βλάψουν τον άνθρωπο. Παρά ταύτα, ο οργανισμός παραδέχεται το γεγονός ότι υψηλή έκθεση σε μικροκυματική ακτινοβολία μπορεί να έχει ως αποτέλεσμα την αύξηση της θερμοκρασίας του δερμάτινου ιστού και κατ' επέκταση την αύξηση της θερμοκρασίας του σώματος [47].

5.3.5 World Health Organization (WHO)

Ο Παγκόσμιος Οργανισμός Υγείας είναι τμήμα του Οργανισμού Ηνωμένων Εθνών εξειδικευμένο πάνω σε θέματα υγείας. Σύμφωνα με τον WHO και βάσει των μέχρι τώρα στοιχείων, τα ηλεκτρομαγνητικά πεδία που δημιουργούνται από τα ασύρματα δίκτυα δεν είναι επιβλαβή για την υγεία. Η

μόνη, αναγνωρισμένη από επιστημονικές έρευνες, επίδραση στην υγεία που μπορεί να προκύψει από την έκθεση σε ηλεκτρομαγνητικά πεδία σχετίζεται με την αύξηση της θερμοκρασίας του σώματος (> 1 °C) από την έκθεση σε πολύ ισχυρά πεδία, τα οποία συναντώνται μόνο σε μερικές βιομηχανικές εγκαταστάσεις. Τα επίπεδα της ηλεκτρομαγνητικής έκθεσης (RF exposure) από τα ασύρματα δίκτυα είναι τόσο χαμηλά ώστε η αύξηση της θερμοκρασίας είναι ασήμαντη και δεν μπορεί να δημιουργήσει προβλήματα στην υγεία [50].

5.3.6 National Cancer Institute

Γιατροί από το National Cancer Institute των Ηνωμένων Πολιτειών, εξέτασαν τα δεδομένα υγείας για 40 χρόνια από 40.581 βετεράνους στρατιώτες και ναύτες που πολέμησαν στον πόλεμο της Κορέας από το 1950 έως το 1954. Η ιδιαιτερότητα που χαρακτηρίζει τους βετεράνους αυτούς είναι ότι υποβλήθηκαν κατά τον πόλεμο της Κορέας σε πολύ ψηλές δόσεις ακτινοβολίας μικροκυμάτων από τα ραντάρ(τα ραντάρ χρησιμοποιούν μεγαλύτερες συχνότητες των 2,4GHz). Οι συχνότητες μικροκυμάτων των ραντάρ χρησιμοποιήθηκαν για σκοπούς ανίχνευσης, για τα οπλικά συστήματα και ακόμη για άμεσες βολές. Οι βετεράνοι αυτοί και ιδιαίτερα οι ναυτικοί, υποβλήθηκαν σε πολύ ψηλότερες δόσεις ακτινοβολίας μικροκυμάτων απ' ότι υποβαλλόμαστε εμείς συνήθως σήμερα.

Τα αποτελέσματά της έρευνας έδειξαν ότι η έκθεση σε ψηλά επίπεδα ακτινοβολίας μικροκυμάτων που προερχόταν από τα ραντάρ, δεν προκάλεσε στους βετεράνους αυτούς περισσότερους καρκίνους από ότι στον υπόλοιπο πληθυσμό. Μάλιστα βρέθηκε οι άνδρες αυτοί, είχαν 35% λιγότερες πιθανότητες να πεθάνουν κατά τη διάρκεια των 40 ετών της έρευνας σε σύγκριση με τους υπόλοιπους άνδρες. Το γεγονός αυτό πιστεύουν οι ερευνητές, οφείλεται στο ότι ένα από τα βασικά κριτήρια της επιλογής των ναυτών, είναι η πολύ καλή τους υγεία και υποχρεώνονται να διατηρούνται σε μια πολύ καλή φυσική κατάσταση κατά τη διάρκεια της υπηρεσίας τους. Φαίνεται λοιπόν ότι η έκθεση σε ψηλά επίπεδα ακτινοβολίας μικροκυμάτων από ραντάρ δεν είχε επιπτώσεις με περισσότερους καρκίνους ή αυξημένους θανάτους στη μεγάλη αυτή ομάδα βετεράνων [47].

5.3.7 Η αντίθετη άποψη

Και ενώ οι παραπάνω οργανισμοί υποστηρίζουν ότι τα ασύρματα δίκτυα είναι ακίνδυνα, πολλοί επιστήμονες προειδοποιούν ότι η μη ιονίζουσα ηλεκτρομαγνητική ακτινοβολία (ΜΙΗΜΑ) του συστήματος WLAN (και των κεραιών κινητής τηλεφωνίας) έχει σημαντικές βιολογικές επιπτώσεις που θέτουν σε άμεσο κίνδυνο την ανθρώπινη υγεία [51].

5.3.7.1 Έκθεση ΒιοΠρωτοβουλίας (BioInitiative Report)

Οι μελέτες που αποκαλύπτουν τις μη θερμικές επιπτώσεις του WLAN και γενικότερα όλων των ΜΙΗΜΑ έχουν συνοψισθεί σε μια μακροσκελή (τρίτομη) έκθεση 600 περίπου σελίδων που κυκλοφόρησε διεθνώς τον Αύγουστο του 2007 και ονομάζεται Έκθεση ΒιοΠρωτοβουλίας (BioInitiative Report). Η έκθεση αυτή συντάχθηκε από μια εικοσαμελή διεθνή ομάδα επιστημόνων, ερευνητών και ειδικών σε πολιτικές δημόσιας υγείας, από κοινού με την *Ευρωπαϊκή Υπηρεσία Περιβάλλοντος* της ΕΕ (European Environment Agency) που συνεισέφερε με την Αρχή της Προφύλαξης, στην οποία ενσωμάτωσε την προστασία της υγείας του ανθρώπου από τις ΜΙΗΜΑ [51].

5.3.7.2 International Commission for Electromagnetic Safety (ICEMS)

Με βάση τις υπάρχουσες μελέτες, η επιστημονική οργάνωση *Διεθνής Επιτροπή για την Ηλεκτρομαγνητική Ασφάλεια* (International Commission for Electromagnetic Safety, ICEMS) εξέδωσε την Απόφαση του Benevento το 2006 (Benevento Resolution) και την Απόφαση της Βενετίας το 2008 (Venice Resolution) με τις οποίες επιβεβαιώνεται αφενός μεν η ύπαρξη μη θερμικών βιολογικών επιδράσεων από τις ΜΙΗΜΑ και της ηλεκτρομαγνητικής υπερευαισθησίας ατόμων σε αυτές, και αφετέρου η αναγκαιότητα ισχύος της Αρχής της Προφύλαξης καθώς και του επανακαθορισμού των υφιστάμενων ορίων έκθεσης στις ΜΙΗΜΑ για τη διαφύλαξη της υγείας των πολιτών.

Τόσο η Έκθεση ΒιοΠρωτοβουλίας όσο και η Απόφαση του Benevento αναφορικά με το WLAN στηρίχθηκαν σε ορισμένες από τις έρευνες (σε διάφορα πειραματικά βιολογικά συστήματα) οι οποίες διαπιστώνουν ποικίλες μη θερμικές βιολογικές επιπτώσεις της ηλεκτρομαγνητικής ακτινοβολίας της συχνότητας μικροκυμάτων 2.45 GHz του WLAN [51].

5.3.7.3 Αποφάσεις διεθνών πολιτικών και εκπαιδευτικών θεσμών για το WLAN

Η Γερμανική Κυβέρνηση εξέδωσε απόφαση-προειδοποίηση για τη μη χρήση του WLAN

Η Γερμανική κυβέρνηση θεωρεί ότι δεν έχει ακόμα προσδιοριστεί η ηλικιακά εξαρτώμενη ασφαλής ποσότητα απορρόφησης και η κατανομή της ενέργειας των MIHMA και το Γερμανικό Υπουργείο Περιβάλλοντος πρότεινε στους πολίτες ότι θα πρέπει να αποφεύγουν την έκθεσή τους στην ακτινοβολία του WLAN. Αυτή η απόφαση-οδηγία οδήγησε τη Βαυαρική Βουλή στην έκδοση οδηγίας προς τα σχολεία της Βαυαρίας να αποφεύγουν το WLAN. Ανάλογες αποφάσεις έχουν επίσης ληφθεί από τη *Διεύθυνση Εκπαίδευσης Φρανκφούρτης* (Γερμανίας) και από τη *Διεύθυνση Δημόσιας Υγείας του Salzburg* (Αυστρίας), με τον πρώτο δημόσιο οργανισμό να απαγορεύει και τον δεύτερο να συμβουλεύει τη μη χρήση του WLAN στα σχολεία.

Ο πρόεδρος του Πανεπιστήμιου Lakehead Καναδά απαγόρεψε τη χρήση του WLAN

Ο πρόεδρος του Πανεπιστημίου Lakehead (Οντάριο, Καναδάς) Fred Gilbert, αφού έλαβε υπ' όψιν τα ενδεχόμενα προβλήματα υγείας από την ακτινοβολία του WLAN, αποφάσισε την απαγόρευση της χρήσης του σε χώρους του πανεπιστημίου που καλύπτονται από ενσύρματο δίκτυο οπτικών ινών. Η απόφασή του βασίστηκε στην Έκθεση ΒιοΠρωτοβουλίας και στην Απόφαση Benevento της *Διεθνούς Επιτροπής για την Ηλεκτρομαγνητική Ασφάλεια* (ICEMS).

Ο Δήμαρχος του Παρισιού απαγόρεψε τη χρήση του WLAN στις δημοτικές βιβλιοθήκες

Το 2007 οι εργαζόμενοι στις δημοτικές βιβλιοθήκες του Παρισιού διαμαρτυρήθηκαν για συμπτώματα υπερευαισθησίας από την έκθεση στην ακτινοβολία του συστήματος WLAN. Αυτό είχε ως αφορμή η *Επιτροπή Υγιεινής και Ασφάλειας του Παρισιού* να συστήσει τη διακοπή της λειτουργίας

του WLAN σ' αυτές τις βιβλιοθήκες, που στη συνέχεια υλοποιήθηκε σε σχετική απόφαση του Δημάρχου του Παρισιού.

Η Ευρωπαϊκή Υπηρεσία Περιβάλλοντος προειδοποιεί για το WLAN

Η *Ευρωπαϊκή Υπηρεσία Περιβάλλοντος* (European Environment Agency, EEA), πολιτικό θεσμικό όργανο της ΕΕ, καλεί σε άμεση λήψη αποφάσεων για τη μείωση της έκθεσης στην ακτινοβολία από το WLAN (Wi-Fi) καθώς και από τα κινητά τηλέφωνα και τις κεραίες κινητής τηλεφωνίας. Επισημαίνει ότι κάθε καθυστέρηση μπορεί να οδηγήσει σε μια κρίση για τη δημόσια υγεία παρόμοια με αυτές που ανέκυψαν από τον αμίαντο, το κάπνισμα και τον μόλυβδο στα καύσιμα.

Η προειδοποίηση ακολούθησε την έκδοση της διεθνούς επιστημονικής Έκθεσης ΒιοΠρωτοβουλίας επί των κινδύνων στην υγεία από την έκθεση στην ακτινοβολία των MIHMA και του WLAN, η οποία συμπέρανε ότι τα υφιστάμενα όρια ασφαλείας είναι «χιλιάδες φορές πιο ήπια».

Η καθηγήτρια Jacqueline McGlade, Εκτελεστική Διευθύντρια της EEA, σε πρόσφατη συνέντευξή της δήλωσε ότι: «Πρόσφατες έρευνες και εκθέσεις επί των μακροχρόνιων επιπτώσεων της ακτινοβολίας από τις ασύρματες τηλεπικοινωνίες δείχνουν ότι θα ήταν συνετό από μέρους των [ευρωπαϊκών] υγειονομικών αρχών να προτείνουν δράσεις για τον περιορισμό της έκθεσης ιδιαίτερα ευάλωτων ομάδων όπως τα παιδιά»

Επιτροπή του Ευρωπαϊκού Κοινοβουλίου υιοθετεί Έκθεση της Βελγίδας Υπουργού Εξωτερικών για την επικινδυνότητα του WLAN και την αναγκαιότητα ισχύος της Αρχής της Προφύλαξης

Η *Επιτροπή του Ευρωπαϊκού Κοινοβουλίου για το Περιβάλλον, τη Δημόσια Υγεία και την Ασφάλεια Τροφίμων* (European Parliament Committee on the Environment, Public Health and Food Safety) ψήφισε ομόφωνα Έκθεση της Frédérique Ries, Βελγίδας Υπουργού Εξωτερικών επί Ευρωπαϊκών και Διεθνών Υποθέσεων (Secretary of State for European and Foreign Affairs) σχετική με το WLAN. Ειδικότερα, η έκθεση αυτή, που αναφερόταν στην σύνοψη του *Προγράμματος Δράσης για το Περιβάλλον και την Υγεία 2004-2010* της ΕΕ (European Environment and Health Action Plan 2004-2010),

μεταξύ άλλων προειδοποιεί για την επικινδυνότητα του WLAN και επισημαίνει ότι η Αρχή της Προφύλαξης θα πρέπει να παραμείνει ο ακρογωνιαίος λίθος της ΕΕ για την περιβαλλοντική υγεία. Μάλιστα, το Σημείο 12 της Έκθεσης επισημαίνει ότι «τα όρια έκθεσης στα ηλεκτρομαγνητκά πεδία που έχουν τεθεί για τον πληθυσμό είναι ξεπερασμένα και δεν έχουν προσαρμοστεί από το 1999, κι επομένως δεν λαμβάνουν υπόψιν τις εξελίξεις στις τεχνολογίες πληροφορικής και τηλεπικοινωνιών...» [51].

5.4 Πρότυπο ασφάλειας ETSI

Ο οργανισμός ETSI (European Telecommunications Standards Institute) είναι ένας ανεξάρτητος, μη κερδοσκοπικός οργανισμός του οποίου ο σκοπός είναι να παράγει τηλεπικοινωνιακά πρότυπα. Ο ETSI έχει δημιουργήσει το πρότυπο ETSI EN 300 328 για τις ασύρματες επικοινωνίες. Το πρότυπο αυτό αναφέρει όλες τις προδιαγραφές τις οποίες πρέπει να τηρεί ένα σύστημα για να είναι αποδεκτό από τον οργανισμό ώστε να είναι ασφαλές ως προς το περιβάλλον και τον άνθρωπο, καθώς και να μην δημιουργεί προβλήματα προς άλλα ασύρματα συστήματα. Για τη μέγιστη ισχύ εκπομπής στα 2.4GHz, ο ETSI ορίζει πως αυτή δεν πρέπει να ξεπερνά τα 100 mW. Στην Αγγλία, σε εθνικό επίπεδο, ο OfCom (Office of Communications), ένας ανεξάρτητος οργανισμός για τη ρύθμιση των τηλεπικοινωνιών, ορίζει πως μέγιστη ισχύς εκπομπής στα 2.4GHz δεν πρέπει να ξεπερνά τα 100 mW ενώ οι συσκευές που λειτουργούν στα 5GHz πρέπει να χρησιμοποιούνται μόνο σε εσωτερικούς χώρους με μέγιστη εκπεμπόμενη ισχύ τα 200 mW [49][47].

5.5 Αποστάσεις ασφαλείας

Από πειράματα που έχουν γίνει και σύμφωνα με μεγέθη που ορίζει η FCC, έχουν υπολογιστεί οι παρακάτω αποστάσεις ασφαλείας:

Ισχύς (W)	Επικίνδυνη Απόσταση (m)	Απόσταση Ασφαλείας (m)
1	0.2	0.3
4	0.2	0.6
10	0.3	0.95
40	0.6	2.0
400	1.9	6.0
1000	3.0	9.5

Πίνακας 5.1 Εκπεμπόμενη ισχύς και αποστάσεις ασφαλείας [47].

Έτσι, σε πραγματικές συνθήκες, ανάλογα με την περίπτωση υπολογίζεται ότι:

- Ένα τερματικό WiFi, όπου η EIRP περιορίζεται εκ του νόμου στα 100 mW, δηλαδή 0,1 Watt έχει απόσταση ασφαλείας τα 10 cm.
- Ένα κινητό GSM εκπέμπει 1 με 2 Watt (όταν είναι μακριά από το σταθμό βάσης του), άρα η απόσταση ασφαλείας είναι 30 cm.
- Μία κεραία κινητής τηλεφωνίας στη χειρότερη περίπτωση έχει 40 Watt ισχύ, με κέρδος κεραίας 10 db, άρα EIRP=400 Watt, άρα η ελάχιστη απόσταση είναι 6 μέτρα.
- Ένας πομπός ραδιοφώνου ή τηλεόρασης με ισχύ 30000 Watt έχει ελάχιστη απόσταση 30 μέτρα.

Εύκολα μπορεί κάποιος να διαπιστώσει πως η ισχύς εκπομπής καθώς και η απόσταση ασφαλείας των ασυρμάτων δικτύων είναι κατά πολύ μικρότερα αυτών των κινητών τηλεφώνων. Από τα παραδείγματα φαίνεται πως μια κεραία ασυρμάτων δικτύων εκπέμπει στα 0,1 Watt, ενώ μια κεραία κινητής τηλεφωνίας στα 40 Watt, με αποστάσεις ασφαλείας 10 cm στα ασύρματα και 6 μέτρα στα κινητά. Ακόμη, πρέπει να σημειωθεί ότι για μία απόσταση 1 μέτρου η ένταση πεδίου θα είναι 10000 φορές μικρότερη από το όριο

ασφαλείας και για μία απόσταση 10 μέτρων θα είναι 1000000 φορές μικρότερη. Άρα σε μία απόσταση ενός μέτρου από την κεραία ασυρμάτων δικτύων η ένταση πεδίου είναι ελάχιστη [47].

5.6 Νομικό πλαίσιο στην Ελλάδα

Στην Ελλάδα, από το 1992 (Ν.2075), αρμόδια για την τηλεπικοινωνιακή αγορά και την αγορά είναι η ΕΕΤΤ (Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων). Η ανεξάρτητη αυτή αρχή είναι υπεύθυνη για την ρύθμιση και επίβλεψη των νόμων που αφορούν τις τηλεπικοινωνίες στην Ελλάδα. Σύμφωνα με την απόφαση της 20ής Ιούνη του 2002 από την βουλή, αποφασίστηκε η χρήση της συχνότητας που χρησιμοποιείται στα ασύρματα δίκτυα των 2,4GHz να είναι ελεύθερη και νόμιμη προς μη εμπορική εκμετάλλευση.

Σύμφωνα, λοιπόν, με τον παραπάνω νόμο η ΕΕΤΤ έχει επιβάλει τις παρακάτω προδιαγραφές (σχετικές με την ασφάλεια της δημόσιας υγείας):

1. Η εκπεμπόμενη ισχύ ενός κεραιοσυστήματος να μην υπερβαίνει τα 20 dBm (100mW).
2. Όλες οι συσκευές που χρησιμοποιούνται πρέπει να συμφωνούν με το πρότυπο ETSI EN 300 328.
3. Όλες οι συσκευές πρέπει να φέρουν την σχετική έγκριση ασφαλείας CE της Ευρωπαϊκής Ένωσης για την δημόσια υγεία [47].

ΠΑΡΑΡΤΗΜΑ Ι

Συντομογραφίες

2GFSK	Two-level Gaussian Frequency Shift Keying
4GFSK	Four-level Gaussian Frequency Shift Keying
AAD	Additional Authentication Data
ACK	Acknowledgement
AES	Advanced Encryption Standard
AID	Association Identifier
AP	Access Point
ARP	Address Resolution Protocol
AS	Authentication Server
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CA	Collision Avoidance
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CCMP	Counter Mode με CBC-MAC Protocol
CD	Collision Detection
CFP	Contention-free Period
CP	Contention Period
CRC	Cyclic Redundancy Check
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access/ Collision Avoidance
CTS	Clear to Send
DA	Destination Address
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function

DFS	Dynamic Frequency Selection
DIFS	DCF Interframe Space
DLL	Data Link Layer
DoS	Denial of service
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EEA	European Environment Agency
EIFS	Extended Interframe Space
EIRP	Equivalent Isotropic Radiated Power
ERP- OFDM	Extended Rate OFDM
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FH	Frequency Hopping
FHSS	Frequency Hopping Spread Spectrum
GMK	Group Master Key
HPA	Health Protection Agency
HR-DSSS	High-Rate DSSS
IAPP	Inter-Access Point Protocol
IBSS	Independent BSS
ICEMS	International Commission for Electromagnetic Safety
ICI	Inter-carrier Interference
ICNIRP	International Commission on Non-Ionizing Radiation Protection
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronic Engineers
IFFT	Inverse Fast Fourier Transform
IP	Internet Protocol

IR	Infrared light
ISI	Inter-symbol Interference
ISM	Industrial Scientific and Medical
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
MAC	Media Access Control
MIC	Michael Integrity Check
MIMO	Multiple-Input-Multiple-Output
MTU	Maximum Transmission Unit
NAK	Null Acknowledgement
NAV	Network Allocation Vector
NIC	Network Interface Card
NRPB	National Radiological Protection Board
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnection
PBCC	Packet Binary Convolutional Coding
PC	Point Coordinator
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PHY	Physical layer
PIFS	PCF Interframe Space
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Depende
PMK	Pairwise Master Key
PN	Pseudorandom Noise
PN	Packet Number
PRNG	Pseudorandom Number Generator
PSK	Phase Shift Keying
PS-mode	Power Save Mode
PTK	Pairwise Ttransient Key

QAM	Quadrature Amplitude Modulation
QoS	Quality-of-Service
QPSK	Quadrature Phase Shift Keying
RA	Receiver Address
RC4	Rivest Cipher 4
RSNs	Robust Security Networks
RTS	Request to Send
SA	Source Address
SC	Sequence Counter
SIFS	Short Interframe Space
SS	Spread Spectrum
SSID	Service Set Identifier
TA	Transmitter Address
TBTT	Target Beacon Transmission Time
TIM	Traffic Indication Map
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmit Power Control
TTLS	Tunnelled TLS
VoIP	Voice over IP
WDS	Wireless Distribution System
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WHO	World Health Organization
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WMM	Wi-Fi Multimedia
WNIC	Wireless NIC
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

ΕΕΤΤ	Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΗΜΠ	Ηλεκτρικά και Μαγνητικά Πεδία
ΜΙΗΜΑ	Μη Ιονίζουσα Ηλεκτρομαγνητική Ακτινοβολία

Βιβλιογραφία

[1] Gast, Matthew. 802.11 Wireless Networks: The Definitive Guide. 2η έκδ. USA: O'Reilly Media, 2005.

[2] Ohrtman, Frank και Konrad Roeder. Wi-Fi Handbook: Building 802.11b Wireless Networks. USA: McGraw-Hill Companies, 2003.

[3]Clark, Martin. Wireless Access Networks Fixed Wireless Access and WLL Networks - Desing and Operation. USA: John Wiley & Sons Ltd, 2000.

[4] Shin-Lin Wu και Yu-Chee Tseng. Wireless Ad Hoc Networking. New York: Auerbach Publications, 2007.

[5] Alexander, Bruce. 802.11 Wireless Network Site Surveying and Installation. USA: Cisco Press, 2005.

[6] Ouellet, Eric κ.α. Building a Cisco Wireless LAN. USA: Syngress Publishing, Inc., 2002.

[7] Geier, Jim. Wireless Networks first-step. USA: Cisco Press, 2004.

[8] Olexa, Ron. Implementing 802.11 802.16 and 802.20 Wireless Networks. USA: Elsevier Inc., 2005.

[9] Peikari, Cyrus και Seth Foqie. Maximum Wireless Security. USA: Sams Publishing, 2003.

[10] Minoli, Daniel. Hotspot Networks: Wi-Fi for Public Access Locations. USA: McGraw-Hill Companies, 2003.

[11] Jahanzeb, Khan και Anis Khwaja. Building Secure Wireless Networks with 802.11. Indianapolis, Indiana: Wiley Publishing, Inc., 2003.

[12] Harold, Davis. Absolute Beginner's Guide to Wi-Fi Wireless Networking. USA: Que, 2004.

[13] Held, Gilbert. Securing Wireless LANs. England: John Wiley & Sons Ltd, 2003.

[14] Basavaraj, Patil κ.ά. IP in Wireless Networks. USA: Prentice Hall Professional Technical Reference, 2003.

[15] Carpenter, Tom και Joel Barrett. CWNA® Certified Wireless Network Administrator Official Study Guide. 4η έκδ. USA: McGraw-Hill Companies, 2008.

[16] Ross, John. The Book of Wireless: A Painless Guide to Wi-Fi and Broadband Wireless. 2η έκδ. San Francisco: William Pollock, 2008.

[17] Edney, Jon και William A. Arbaugh. Real 802.11 Security: Wi-Fi Protected Access and 802.11i. USA: Addison Wesley, 2003.

[18] Mooi Choo Chuah και Qinqing Zhang. Design and Performance of 3G Wireless Networks and Wireless LANS. USA: Springer Science-I-Business Media, Inc., 2006.

[19] Coleman, David και David Westcott. CWNA Certified Wireless Network Administrator Study Guide. Indianapolis, Indiana: Wiley Publishing, Inc., 2006.

[20] Garg, Vijay. Wireless Communications and Networking. USA: Elsevier Inc., 2007.

[21] Certified Wireless Network Administrator, Official Study Guide. USA: Planet 3Wireless, Inc., 2002.

[22] Goldsmith, Andrea. Wireless Communications. USA: Cambridge University Press, 2005.

[23] McCullough, Jack. Caution! Wireless Networking: Preventing a Data Disaster. Indianapolis, Indiana: Wiley Publishing, Inc., 2004.

[24] Heltzel, Paul. Complete Home Wireless Networking: Windows® XP Edition. USA: Pearson Education, Inc., 2003.

[25] Tanenbaum, Andrew S. *Δίκτυα Υπολογιστών.* 4η έκδ. Μετάφρ. Γ. Ξυλωμένος. Αθήνα: Κλειδάριθμος, 2003.

[26] Rackley, Steve. Wireless Networking Technology. Oxford: Elsevier, 2007.

[27] Wall, David κ.α. Managing and Securing a Cisco Structured Wireless-Aware Network. USA: Syngress Publishing, Inc., 2004.

[28] Macaulay, Tyson. «Hardening IEEE 802.11 Wireless Networks» magnoliaroad.net 18 Φεβ. 2002 <http://magnoliaroad.net/downloads/hardening_802.11.pdf>.

[29] About the Wi-Fi Alliance. 2009. Wi-Fi Alliance. 26 Μαϊου 2009 <http://www.wi-fi.org/about_overview.php>.

[30] IEEE Standards Status Report for 802.11 2009. IEEE. 26 Μαϊου 2009 <http://standards.ieee.org/cgi-bin/status>.

[31] Mitchel, Bradley. “Wired vs Wireless Networking.” About.com 15 Μαΐου 2009 <http://compnetworking.about.com/cs/homenetworking/a/homewiredless_2.htm>.

[32] Rodriquez, Erik. “Wired vs. Wireless.” Skullbox.net. 3 Δεκεμβ. 2005. 15 Μαΐου 2009. <http://www.skullbox.net/wiredvswireless.php>.

[33] Cristian L. ““Wired vs. Wireless Networking.” Helpero.com. 12 Ιουν. 2006. 15 Μαΐου 2009. <http://news.helperocom/article/Wired-vs-Wireless-Networking_17.html>.

[34] Goldman, Jeff. “Introducing IEEE 802.11r.” Wi-Fiplanet.com . 7 Οκτωμβ. 2008. 20 Μαΐου 2009. <http://www.wi-fiplanet.com/news/article.php/3776351 >.

[35] IEEE Wireless Communication Standards. IEEE Standards Association. 5 Απριλ. 2009. <http://standards.ieee.org/cgi-bin/status>.

[36] IEEE Standards Association. 2005. IEEE Standards Association. 5 Απριλ. 2009. <http://standards.ieee.org/announcements/bkgnd_sa.html> .

[37] Geier, Jim. “Understanding Wireless LAN Bridges.” Wi-Fiplanet.com. 3 Ιανουαρ. 2003. 20 Μαΐου 2009. <http://www.wi-fiplanet.com/tutorials/article.php/1563991>.

[38] Geier, Jim. “Extending WLAN Range with Repeaters.” Wi-Fiplanet.com. 17 Ιανουαρ. 2003. 20 Μαΐου 2009. <http://www.wi-fiplanet.com/tutorials/article.php/1571601>.

[39] Geier, Jim. “Understanding WLAN Routers.” SmallBusinessComputing.com. 26 Φεβρ. 2003. 21 Μαΐου 2009. <http://www.smallbusinesscomputing.com/webmaster/article.php/1607711>.

[40] Intel WiFi Products. 27 Δεκεμβ. 2006. Intel. 10 Μαΐου 2009. <http://www.intel.com/support/wireless/wlan/sb/CS-025325.htm>.

[41] Geier, Jim. “Making the choice : 802.11a or 802.11g.” Wi-Fiplanet.com. 15 Απριλ. 2002. 5 Νοεμβρ. 2009. < http://www.wi-fiplanet.com/tutorials/article.php/1009431>.

[42] Κωνσταντίνος Γεωργακόπουλος. «Τεχνολογίες Σύγχρονων Ασύρματων Δικτύων Δεδομένων.» de.teikav.edu.gr Δεκέμβριος 2007. Τ.Ε.Ι. Καβάλας 9 Νοέμβρ. 2009. <http://de.teikav.edu.gr/telematics/pdf/3o_Meros_Asyrmata_thlematikh.pdf>.

[43] Sowmya L Mulukutla. “Optimum Data Rates and Packet Sizes for a Wireless Integrated Emergency Medical Services Environment.” hires.uab.edu. 2005. 10 Οκτωβρίου 2009. < www.hires.uab.edu/SowmyasThesis.htm >.

[44] Cisco Systems Inc. “Wireless Quality-of-Service.” www.cisco.com. 20 Νοεμβρίου 2009. <http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a0080144498.html>.

[45] Elio Perez. “802.11i(How we got there and where are we ahead).” sans.org 2004. 4 Δεκεμβρίου 2009 < http://www.sans.org/reading_room/whitepapers/wireless/802_11i_how_we_got_here_and_where_are_we_headed_1467?show=1467.php&cat=wireless >

[46] Wi-Fi Alliance. “Wi-Fi Certified products.” www.wi-fi.org. 7 Δεκεμβρίου 2009. http://www.wi-fi.org/certified_products.php

[47] Δράκος Ανδρέας, Ματεεβίτσι Βίκτωρας. “Επιπτώσεις Ασύρματων Δικτύων και Επικοινωνιών (WiFi) στην δημόσια υγεία.” Έκδοση 2.4. Τμήμα Επιστήμης και Τεχνολογίας Τηλεπικοινωνιών Πανεπιστήμιο Πελοποννήσου, 2005. 10 Φεβρουαρίου 2009.

[48] Health Protection Agency. “Understanding Radiation, Electromagnetic Fields, Wi-Fi.” www.hpa.org.uk. 2009. 18 Φεβρουαρίου 2009. <http://www.hpa.org.uk/HPA/Topics/Radiation/UnderstandingRadiation/1199451940308/>.

[49] Peyman Azabeh, Mann Simon. “Wi-Fi in Schools.” www.hpa.org.uk. 2007. 18 Φεβρουαρίου 2009. <http://www.hpa.org.uk/web/HPAwebFile/HPAweb_C/1254510618866>.

[50] World Health Organization. “Electromagnetic fields and public health.” www.who.int. 2006. 17 Φεβρουαρίου 2009. < http://www.who.int/mediacentre/factsheets/fs304/en/index.html>.

[51] Γεωργίου Χρήστος. “ΑΣΥΡΜΑΤΗ ΔΙΚΤΥΩΣΗ Wi-Fi Βιολογικές επιπτώσεις, νόμοι για την προστασία της δημόσιας υγείας, διεθνής πρακτική.” www.upatras.gr 2008. 26 Φεβρουαρίου 2010. <http://www.biology.upatras.gr/cgeorgiou/>