



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



## ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

<<Τεχνολογίες και πρωτόκολλα ασύρματων Τοπικών  
Δικτύων Υπολογιστών>>



Της φοιτήτριας  
Πηνελόπης Γιωβανίτσα  
Αρ. Μητρώου: 04/2578

Επιβλέπων καθηγητής  
κος Βασίλειος Βίτσας

Θεσσαλονίκη 2012

## **ΠΡΟΛΟΓΟΣ**

Η παρούσα πτυχιακή εργασία εκπονήθηκε στα πλαίσια του προγράμματος σπουδών του τμήματος Πληροφορικής της Σχολής Τεχνολογικών Εφαρμογών του Αλεξάνδρειου Τεχνολογικού Ιδρύματος Θεσσαλονίκης, από τη φοιτήτρια Πηνελόπη Γιωβανίτσα (Α.Μ: 04/2578) και τον επιβλέποντα καθηγητή κ. Βίτσα Βασίλειο. Σκοπός της παρούσας πτυχιακής ήταν η παρουσίαση των ασύρματων τοπικών δικτύων καθώς και των λόγων ανάπτυξης αλλά και των βασικών λειτουργιών τους, μιας και αποτελούν σημαντικό μέρος της επικοινωνίας σήμερα.

## **ΠΕΡΙΛΗΨΗ**

Η διπλωματική αυτή εργασία πραγματεύεται την σχετικά νέα αλλά και πολλά υποσχόμενη τεχνολογία των ασύρματων τοπικών δικτύων που γνωρίζουν μεγάλη απήχηση τόσο από τους απλούς χρήστες όσο και από τις ίδιες τις επιχειρήσεις. Στην αρχή γίνεται μία αναφορά στην ιστορική αναδρομή των ασύρματων τοπικών δικτύων, στους λόγους για τους οποίους αναπτύχθηκαν αλλά και στη χρησιμότητά τους. Ακολουθεί μία σύγκριση μεταξύ της τεχνολογίας των ενσύρματων τοπικών δικτύων και της τεχνολογίας των ασύρματων τοπικών δικτύων. Γίνεται μια αναλυτική παρουσίαση του γενικού τρόπου λειτουργίας της εν λόγω τεχνολογίας καθώς και των επιμέρους επεκτάσεων της που δημιουργήθηκαν με σκοπό να γίνει αποδοτικότερη η λειτουργία των δικτύων αυτών. Παράλληλα, παρουσιάζονται συνηθισμένα προβλήματα που εμφανίζονται στα ασύρματα τοπικά δίκτυα αλλά και οι τρόποι αντιμετώπισής τους. Τέλος γίνεται μια αναφορά στην τεχνολογία που διέπει τα ασύρματα μητροπολιτικά δίκτυα και σύγκριση αυτής με τα ασύρματα τοπικά δίκτυα.

## **Λέξεις κλειδιά**

Ασύρματα τοπικά δίκτυα, τοπολογίες ασύρματων δικτύων, σύγκριση τοπικών δικτύων, μοντέλο διαστρωμάτωσης OSI, φυσικό επίπεδο, τεχνικές μετάδοσης, υπόστρωμα MAC, τεχνικές πρόσβασης, επεκτάσεις 802.11, ασύρματα μητροπολιτικά δίκτυα.

## **ABSTRACT**

This thesis discusses the relatively new and promising technology of wireless local area networks that has been a great impact on both ordinary users and the companies themselves. In the beginning, there is a reference to the history of wireless LANs, the reasons for its development and its usefulness. Afterwards, there is a comparison between wired local area networks and wireless local area networks. Furthermore, a detailed presentation of both the general functions of the technology and the various extensions that were created to make it more efficient in functioning is being made. At the same time, there is presentation of common problems that occur in wireless local area networks and also the ways that were developed to deal with them. Finally, there is a reference to the underlying technology of wireless metropolitan area networks and a comparison of them with wireless local area networks.

## **Key words**

Wireless local area networks (WLANs), network topologies, local area network comparison, OSI model, physical layer, transmission techniques, MAC layer, access methods, 802.11 extensions, wireless metropolitan networks (WiMAX).

## **ΕΥΧΑΡΙΣΤΙΕΣ**

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα της παρούσας εργασίας, καθηγητή κ. Βίτσα Βασίλειο για την υποστήριξη του και την καθοδήγησή του για την εκπόνηση και την ανάπτυξη της εν λόγω πτυχιακής.

Επιπροσθέτως, ευχαριστώ θερμά τον καθηγητή κ. Χατζημίσιο Περικλή για τη βοήθεια και την υποστήριξή που μου προσέφερε.

Τέλος, θα ήθελα να ευχαριστήσω θερμά την οικογένειά μου για την αμέριστη συμπαράσταση και υποστήριξη καθ' όλη τη διάρκεια των σπουδών μου.

## ΠΕΡΙΕΧΟΜΕΝΑ

1.	Ασύρματα τοπικά δίκτυα.....	13
1.1	Γενικά.....	13
1.2	Ιστορική αναδρομή.....	13
1.3	Τοπολογίες ασύρματων τοπικών δικτύων.....	14
1.3.1	IBSS (Independent Basic Service Set) / Ad-hoc.....	14
1.3.2	BSS (Basic Service Set).....	15
1.3.3	ESS (Extended Service Set).....	16
1.3.4	Multi-BSS (virtual AP).....	17
1.4	Σύγκριση Ασύρματων - Ενσύρματων τοπικών δικτύων.....	18
1.5	Επιπτώσεις στην υγεία.....	21
2	Το μοντέλο αναφοράς OSI.....	23
2.1	Φυσικό επίπεδο (Physical Layer).....	25
2.2	Επίπεδο σύνδεσης δεδομένων (Data Link Layer).....	25
2.3	Επίπεδο δικτύου (Network Layer).....	26
2.4	Επίπεδο μεταφοράς (Transport Layer).....	27
2.5	Επίπεδο συνόδου (Session Layer).....	28
2.6	Επίπεδο παρουσίασης (Presentation Layer).....	29
2.7	Επίπεδο εφαρμογών (Application Layer).....	30
3	802.11 Physical Layer.....	32
3.1	DSSS (Direct Sequence Spread Spectrum).....	34
3.2	FHSS (Frequency Hopping Spread Spectrum).....	38
3.3	IR (Infrared).....	42
3.4	DSSS vs. FHSS.....	45
4	802.11 MAC Layer.....	47
4.1	802.11 Frame.....	53
4.2	Σχετικά με τους μετρητές των μεθόδων.....	56

4.3	DCF (Distributed Coordination Function).....	60
4.3.1	DCF Basic Access Mechanism (Βασική CSMA/CA)....	61
4.3.2	CSMA/CA-RTS/CTS.....	62
4.4	PCF (Point Coordination Function).....	64
5	Σούίτα πρωτοκόλλων 802.11.....	69
5.1	802.11b.....	72
5.2	802.11a.....	78
5.3	802.11g.....	84
5.4	802.11e.....	93
5.4.1	EDCA (Enhanced Distributed Channel Access).....	96
5.4.2	HCCA (HCF Control Channel Access).....	99
5.5	802.11n.....	105
6	Πρωτόκολλα 802.16 και 802.11.....	113
6.1	Πρωτόκολλο 802.16.....	113
6.1.1	WiMAX Physical Layer.....	117
6.1.2	WiMAX MAC Layer.....	119
6.2	Σύγκριση WiMAX με WiFi.....	122

## Ευρετήριο Εικόνων

Εικόνα 1.1 : Ad-hoc τοπολογία.....	15
Εικόνα 1.2 : BSS τοπολογία.....	16
Εικόνα 1.3 : ESS τοπολογία.....	17
Εικόνα 1.4 : Multi-BSS τοπολογία.....	18
Εικόνα 2.1: Τα 7 επίπεδα του μοντέλου διαστρωμάτωσης OSI.....	24
Εικόνα 3.1 : Διαστρωμάτωση του προτύπου 802.11.....	33
Εικόνα 3.2 : Πλαίσιο PLCP της DSSS για το φυσικό στρώμα του 802.11.....	37
Εικόνα 3.3 : Πλαίσιο PLCP της FHSS για το φυσικό στρώμα του 802.11.....	41
Εικόνα 3.4 : Πλαίσιο PLCP της υπέρυθρης ακτινοβολίας για το φυσικό στρώμα του 802.11.....	44
Εικόνα 4.1 : Το πρόβλημα του κρυμμένου κόμβου.....	48
Εικόνα 4.2 : Το πρόβλημα του εκτεθειμένου κόμβου.....	50
Εικόνα 4.3 : Η γενική μορφή του πλαισίου του υποστρώματος .....	54
Εικόνα 4.4 : Διαδικασίες CSMA/CA και CSMA/CA-RTS/CTS.....	64
Εικόνα 4.5 : Υλοποίηση της μεθόδου PCF.....	67
Εικόνα 5.1 : Μορφή πλαισίων φυσικού υποστρώματος 802.11b.....	76
Εικόνα 5.2 : PPDU πλαίσιο του 802.11a.....	82
Εικόνα 5.3 : Πλαίσιο φυσικού επιπέδου ERP-DSSS CCK.....	89
Εικόνα 5.4 : Πλαίσιο φυσικού επιπέδου ERP-OFDM.....	90
Εικόνα 5.5 : Πλαίσιο υποστρώματος MAC του 802.11e.....	101
Εικόνα 5.6 : QoS Control Field.....	102
Εικόνα 5.7 : Πλαίσια υποστρώματος MAC για το 802.11n.....	110
Εικόνα 5.8 : Μορφές πλαισίων συνδυασμού για τις MSDU και MPDU.....	112



Εικόνα 6.1 : Βασικά χαρακτηριστικά των επεκτάσεων του 802.16.....	115
Εικόνα 6.2 : Διαδρομές LOS και NLOS.....	116
Εικόνα 6.3 : Συνδυασμός τοπολογιών P2P και PMP.....	116
Εικόνα 6.4 : Καταχώρηση υποκαναλιών από την OFDMA στους χρήστες.....	119
Εικόνα 6.5 : Στοίβα πρωτοκόλλων για το 802.16.....	120
Εικόνα 6.6 : Σύγκριση προτύπων 802.16 και 802.11.....	125

### **Ευρετήριο Πινάκων**

Πίνακας 3.1 : Τα κανάλια συχνοτήτων που χρησιμοποιούνται στην DSSS.....	37
Πίνακας 3.2 : Τα κανάλια συχνοτήτων που χρησιμοποιούνται στην FHSS.....	40
Πίνακας 4.1 : Μέγιστες και ελάχιστες τιμές του παραθύρου ανταγωνισμού.....	53
Πίνακας 4.2 : Χρονική διάρκεια του SIFS.....	57
Πίνακας 4.3 : Χρονική διάρκεια του PIFS.....	58
Πίνακας 4.4 : Χρονική διάρκεια του DIFS.....	58
Πίνακας 5.1 : Διαθέσιμα κανάλια χρήσης του προτύπου 802.11b.....	74
Πίνακας 5.2 : Βασικά χαρακτηριστικά του 802.11b.....	77
Πίνακας 5.3 : Διαθέσιμα κανάλια χρήσης του προτύπου 802.11a στις ΗΠΑ.....	79
Πίνακας 5.4: Ρυθμοί μετάδοσης και σχήματα διαμόρφωσης/κωδικοποίησης του φυσικού επιπέδου του 802.11a.....	81
Πίνακας 5.5 : Ρυθμοί μετάδοσης του πλαισίου 802.11.....	82
Πίνακας 5.6 : Βασικά χαρακτηριστικά του 802.11a.....	84
Πίνακας 5.7 : Ρυθμοί μετάδοσης φυσικών επιπέδων του 802.11g.....	86
Πίνακας 5.8 : Τιμές πεδίου Signal ανά φυσικό επίπεδο.....	91

Πίνακας 5.9 : Βασικά χαρακτηριστικά του 802.11g.....	91
Πίνακας 5.10 : Κατηγορίες πρόσβασης του 802.11e.....	96
Πίνακας 5.11 : Τιμές του μετρητή AIFS ανά κατηγορία.....	97
Πίνακας 5.12 : Τιμές του CW για το QoS στο 802.11b φυσικό επίπεδο.....	98
Πίνακας 5.13: Τιμές του CW για το QoS στο 802.11a/g φυσικό επίπεδο.....	98
Πίνακας 5.14: Βασικά χαρακτηριστικά του 802.11n.....	106

## **ΕΙΣΑΓΩΓΗ**

Τα τελευταία χρόνια έχει παρατηρηθεί αλματώδης ανάπτυξη στον τομέα των ασύρματων τοπικών δικτύων. Η μεγάλη επιτυχία των ενσύρματων τοπικών δικτύων οδήγησε στην ανάπτυξη των ασύρματων δικτύων που προσφέρουν επικοινωνία παρέχοντας ταυτόχρονα τη δυνατότητα μετακίνησης των χρηστών τους εντός της εμβέλειας των εν λόγω δικτύων. Στα ασύρματα τοπικά δίκτυα παρουσιάζονται συνήθως τοπολογίες σύμφωνα με τις οποίες είτε ένας σταθμός επικοινωνεί απευθείας με κάποιον άλλο που βρίσκεται στο ίδιο δίκτυο μεταφέροντάς του τα δεδομένα του, είτε ο σταθμός αυτός επικοινωνεί πρώτα με κάποιον μεσολαβητή που αναλαμβάνει εκείνος να μεταδώσει τα δεδομένα στον εκάστοτε προορισμό.

Όπως σε όλες τις τεχνολογίες, έτσι και στα ασύρματα τοπικά δίκτυα εμφανίζονται προβλήματα που οφείλονται κυρίως στη φύση του μέσου μετάδοσης αλλά και στη θέση στην οποία βρίσκονται τοποθετημένοι οι σταθμοί του δικτύου. Βέβαια, έχουν αναπτυχθεί κατάλληλες μέθοδοι και τεχνικές που βοηθούν στην ελαχιστοποίηση των προβλημάτων αυτών παρέχοντας στους χρήστες ένα αποδοτικότερο και λειτουργικότερο δίκτυο επικοινωνίας.

Ο λόγος που έχουν διαδοθεί ευρέως τα τοπικά ασύρματα δίκτυα είναι γιατί συνδυάζουν το χαμηλό κόστος με την αρκετά αξιόπιστη παροχή υπηρεσιών αλλά και τη δυνατότητα περιορισμένης βέβαια κινητικότητας στους χρήστες τους.

Σκοπός αυτής της εργασίας είναι να γίνει μια ιστορική αναδρομή στην εξέλιξη των δικτύων αυτών και να παρουσιαστούν οι λόγοι ανάπτυξης αλλά και η χρησιμότητα τους. Συγκρίνονται τα ασύρματα με τα ενσύρματα δίκτυα και παρουσιάζονται οι εφαρμογές τους όπως και οι βασικοί στόχοι δημιουργίας τους. Αναλύονται οι βασικές αρχές λειτουργίας αλλά η χρήση των μέσων μετάδοσης του σήματος. Περιγράφεται ο τρόπος λειτουργίας της γενικής μορφής του προτύπου αλλά και των επεκτάσεών του. Παρουσιάζονται τα προβλήματα που εμφανίζονται στα ασύρματα δίκτυα καθώς και οι τρόποι αντιμετώπισης τους.

Στο πρώτο κεφάλαιο της παρούσας πτυχιακής γίνεται μια ιστορική αναδρομή στην εξέλιξη των ασύρματων τοπικών δικτύων και στις τοπολογίες τους. Συγκρίνονται τα εν λόγω δίκτυα με την αντίστοιχη ενσύρματη τεχνολογία και τέλος γίνεται αναφορά στις πιθανές επιπτώσεις που μπορεί να έχει η χρήση των ασύρματων δικτύων στην υγεία των χρηστών τους.

Στο δεύτερο κεφάλαιο παρουσιάζεται το μοντέλο διαστρωμάτωσης OSI και γίνεται εκτενής αναφορά στα επτά επίπεδα που το απαρτίζουν.

Στο τρίτο κεφάλαιο παρουσιάζεται το φυσικό επίπεδο του πρωτοκόλλου 802.11 που περιγράφει τα ασύρματα τοπικά δίκτυα και γίνεται ανάλυση των τριών διαφορετικών κατηγοριών του φυσικού επιπέδου DSSS, FHSS και Infrared. Τέλος, προχωράμε σε μία σύγκριση των δύο βασικότερων φυσικών επιπέδων DSSS και FHSS.

Στο τέταρτο κεφάλαιο παρουσιάζεται αναλυτικά το υπόστρωμα MAC του επιπέδου δεδομένων του 802.11. Παρουσιάζονται τα συνηθισμένα προβλήματα που εμφανίζονται στα ασύρματα τοπικά δίκτυα όπως είναι το πρόβλημα του κρυμμένου αλλά και του εκτεθειμένου κόμβου, καθώς και οι τρόποι αντιμετώπισής τους (RTS/CTS, NAV, EIFS). Αναλύονται οι τεχνικές πρόσβασης στο ασύρματο μέσο DCF, PCF και CSMA/CA και γίνεται αναφορά στους μετρητές που χρησιμοποιούν οι τεχνικές αυτές.

Στο πέμπτο κεφάλαιο αναλύονται οι βασικότερες επεκτάσεις του 802.11 που δημιουργήθηκαν για την επίτευξη ενός αποδοτικότερου ασύρματου δικτύου αλλά και για την παροχή συγκεκριμένων υπηρεσιών. Οι επεκτάσεις που αναλύονται είναι τα 802.11b, 802.11a, 802.11g, 802.11e και 802.11n.

Στο έκτο και τελευταίο κεφάλαιο παρουσιάζεται η τεχνολογία WiMAX των ασύρματων μητροπολιτικών δικτύων και γίνεται σύγκριση αυτής με τα ασύρματα τοπικά δίκτυα.

# 1. Ασύρματα τοπικά δίκτυα

## 1.1 Γενικά

Ένα ασύρματο τοπικό δίκτυο **WLAN (Wireless Local Area Network-WLAN)** [1] είναι μια σχετικά καινούργια μορφή τοπικού δικτύου που προσφέρει την σύνδεση και την επικοινωνία μεταξύ των χρηστών του χωρίς να απαιτεί την ύπαρξη καλωδίωσης.

Στα WLANs συμπεριλαμβάνονται και τα συστήματα κατανομής ή αλλιώς **DS (Distribution Systems)** στα οποία χρησιμοποιείται καλωδίωση μεταξύ των σταθμών που παρέχουν την πρόσβαση στο δίκτυο κυρίως για λόγους επεκτασιμότητας του εν λόγω δικτύου.

Στα ασύρματα δίκτυα, η πληροφορία μεταφέρεται μέσω ηλεκτρομαγνητικών κυμάτων με συχνότητα και ρυθμό μετάδοσης που προδιαγράφονται στο πρωτόκολλο επικοινωνίας που χρησιμοποιείται στο εκάστοτε δίκτυο. Η κινητικότητα που προσφέρουν είναι ουσιαστικά το κύριο πλεονέκτημά των δικτύων αυτών αλλά και ο λόγος που χρησιμοποιούνται ευρέως σήμερα.

## 1.2 Ιστορική αναδρομή

Το 1971, μια ομάδα ερευνητών υπό την καθοδήγηση του Norman Abramson του πανεπιστημίου της Hawaii, δημιούργησε το πρώτο δίκτυο μεταγωγής πακέτου με τη χρήση ραδιοκυμάτων, ονόματι "Alohanet" [2]. Το Alohanet ήταν το πρώτο ασύρματο δίκτυο στο οποίο συνδέονταν επτά ηλεκτρονικοί υπολογιστές που επικοινωνούσαν μεταξύ τους, ενώ γεωγραφικά ήταν τοποθετημένοι σε τέσσερα νησιά του συμπλέγματος της Hawaii.

Λίγο αργότερα, το 1972, το Alohanet συνδέθηκε με το ασύρματο δίκτυο του Arpanet (δίκτυο μεταγωγής πακέτων αρχικά σχεδιασμένο για στρατιωτικούς σκοπούς), γεγονός που αποτέλεσε μεγάλη καινοτομία κυρίως λόγω της απόστασης που μεσολαβούσε στην ασύρματη επικοινωνία των ηλεκτρονικών υπολογιστών.

Το 1990 δημιουργήθηκε μια ομάδα εργασίας με σκοπό την ανάπτυξη του πρωτοκόλλου ασύρματης επικοινωνίας 802.11, προκειμένου να μπορεί χρησιμοποιηθεί το εν λόγω πρωτόκολλο από τους ηλεκτρονικούς υπολογιστές στην ασύρματη πλέον επικοινωνία τους.

Τέλος, το 1997, το IEEE 802.11 καθιερώθηκε ως το πρότυπο αποστολής και λήψης δεδομένων στα ασύρματα τοπικά δίκτυα.

Σήμερα, η τεχνολογία που αφορά στα ασύρματα δίκτυα συνεχώς βελτιώνεται και μπορούμε με σιγουριά πλέον να πούμε πως θα συνεχίσει να χρησιμοποιείται και στις επόμενες δεκαετίες.

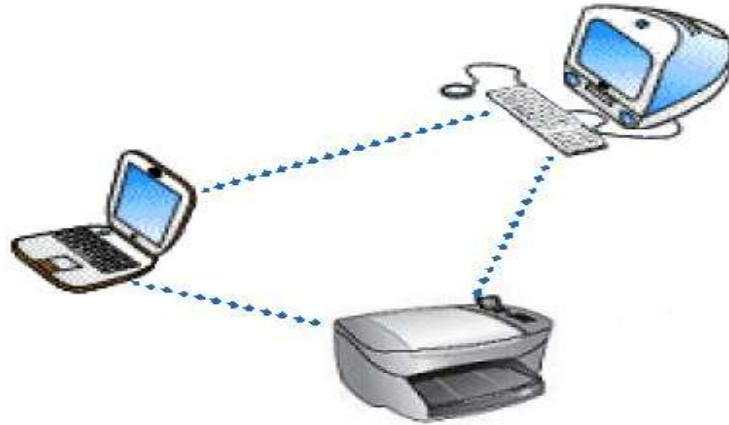
### 1.3 Τοπολογίες ασύρματων δικτύων

Οι τοπολογίες των ασύρματων τοπικών δικτύων ποικίλουν. Οι βασικές δομές αυτών των τοπολογιών αυτών είναι το **BSS (Basic Service Set)** όπου χρησιμοποιούνται σταθμοί πρόσβασης **AP (Access Points)** προκειμένου να επικοινωνήσουν οι συσκευές και να ανταλλάξουν πληροφορίες μεταξύ τους, αλλά και το **IBSS (Independent Basic Service Set)** ή αλλιώς Ad-hoc, στο οποίο οι σταθμοί μπορούν να ανταλλάξουν πληροφορίες δίχως την ύπαρξη κάποιας συσκευής που θα μεσολαβεί στην επικοινωνία τους. Πιο συγκεκριμένα:

#### 1.3.1 IBSS (Independent Basic Service Set) / Ad-hoc

Τα ασύρματα δίκτυα μπορούν να λειτουργήσουν χωρίς να είναι απαραίτητη η παρουσία κάποιου AP. Σε αυτή τη λογική βασίζονται και οι τοπολογίες Ad-hoc [3] μιας και προσφέρουν τη δυνατότητα στους σταθμούς να επικοινωνούν μεταξύ τους δίχως την ύπαρξη κάποιου μεσολαβητή.

Γενικά, τα Ad-hoc δίκτυα απαρτίζονται από μικρό αριθμό σταθμών και χρησιμοποιούνται σε συγκεκριμένες περιπτώσεις όπως είναι η ανταλλαγή των δεδομένων σε αίθουσες συνεδριάσεων ή σε μέσα μαζικής μεταφοράς όπου δεν υπάρχει κάποιος σταθμός πρόσβασης.

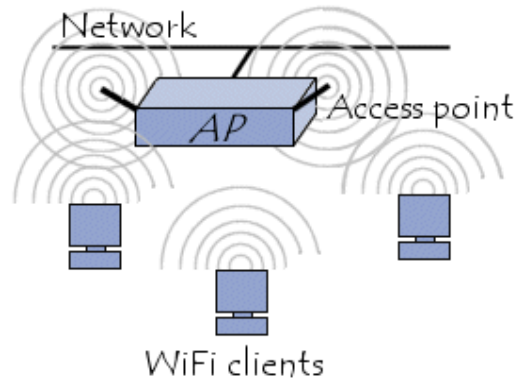


Εικόνα 1.1: Ad-hoc τοπολογία

### 1.3.2 BSS (Basic Service Set)

Βασικό χαρακτηριστικό των BSS [4] δικτύων είναι η ύπαρξη πολλών ασύρματων σταθμών και ενός ή περισσότερων σταθμών πρόσβασης AP. Κάθε BSS δίκτυο χρησιμοποιεί και ένα μοναδικό αναγνωριστικό **SSID (Service Set Identifier)** που εγγράφεται σε όλα τα πακέτα του. Όλοι οι σταθμοί είναι υποχρεωμένοι να βρίσκονται σε τέτοια απόσταση από το AP ώστε να μπορούν να μεταδώσουν τα δεδομένα τους σε αυτό αλλά δεν υπάρχει περιορισμός για την απόσταση των σταθμών μεταξύ τους. Στη περίπτωση που ένας σταθμός θέλει να επικοινωνήσει με κάποιον άλλο που βρίσκεται στην ίδια περιοχή **BSA (Basic Service Area)**, θα πρέπει να ακολουθηθούν δύο βασικά βήματα. Ο αρχικός σταθμός θα αποστείλει τα δεδομένα που προορίζονται για τον δεύτερο όχι απευθείας σε εκείνον αλλά στο AP και εκείνο ακολούθως θα μεταβιβάσει τα δεδομένα στον συγκεκριμένο αποδέκτη.

Ένας σταθμός μπορεί να ξεκινήσει τη διαδικασία επικοινωνίας μόνο με ένα AP, παρ'όλα αυτά δεν υπάρχει κάποιος περιορισμός για το αριθμό των σταθμών που μπορούν να συνδεθούν σε ένα AP.



Εικόνα 1.2: BSS τοπολογία

Το εύρος της περιοχής BSA που καλύπτεται από ένα AP είναι η απόσταση εντός της οποίας μπορούν να ληφθούν τα δεδομένα που μεταδίδει το AP και συνήθως υπολογίζεται στα 50 μέτρα. Για να επεκταθεί το εύρος της περιοχής προτείνεται η χρήση περισσότερων AP.

Πέραν του μειονεκτήματος των BSS δικτύων ότι χρειάζονται περισσότερα από ένα βήματα για τη μετάδοση των δεδομένων άρα και αυξημένο εύρος μετάδοσης (bandwidth), η χρήση του AP έχει και ένα βασικό πλεονέκτημα. Το AP είναι σε θέση να βοηθήσει στην εξοικονόμηση ενέργειας των σταθμών που εξυπηρετεί. Εάν κάποιος από τους σταθμούς βρίσκεται σε power-saving κατάσταση, το AP μπορεί να αποθηκεύσει προσωρινά τα δεδομένα που προορίζονταν γι' αυτόν και να τα μεταδώσει όταν ο σταθμός αυτός επανέλθει στην βασική του κατάσταση.

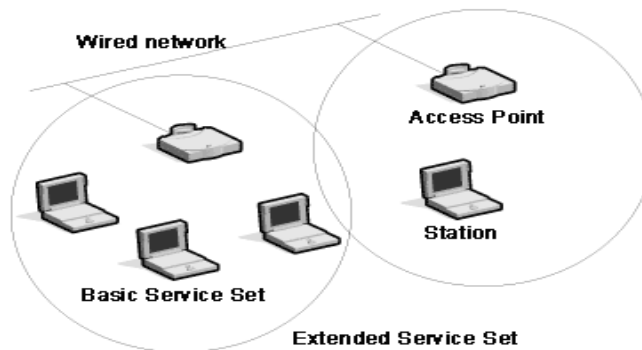
### 1.3.3 ESS (Extended Service Set)

Για την ανάπτυξη μεγάλων ασύρματων δικτύων, ενώνονται δύο ή και περισσότερα BSS δίκτυα δημιουργώντας ένα **ESS (Extended Service Set)** [5]. Όλα τα AP σε ένα ESS έχουν το ίδιο αναγνωριστικό SSID αλλά διαχωρίζονται το ένα από το άλλο με τη χρήση του **BSSID (Basic Service Set Identifier)** αναγνωριστικού που υπολογίζεται βάσει της MAC διεύθυνσης της συγκεκριμένης συσκευής.

Οι σταθμοί σε ένα ESS δίκτυο μπορούν να επικοινωνούν μεταξύ τους ακόμα και αν ανήκουν σε διαφορετικό BSS ή αν μετακινούνται από το ένα BSS στο άλλο. Αρχικά στέλνουν τα δεδομένα τους στο δικό τους AP, αυτό με τη σειρά του τα



μεταβιβάζει στο AP της περιοχής που ανήκει ο παραλήπτης και το δεύτερο αναλαμβάνει τη μετάδοση των μηνυμάτων αυτών στον τελικό παραλήπτη.

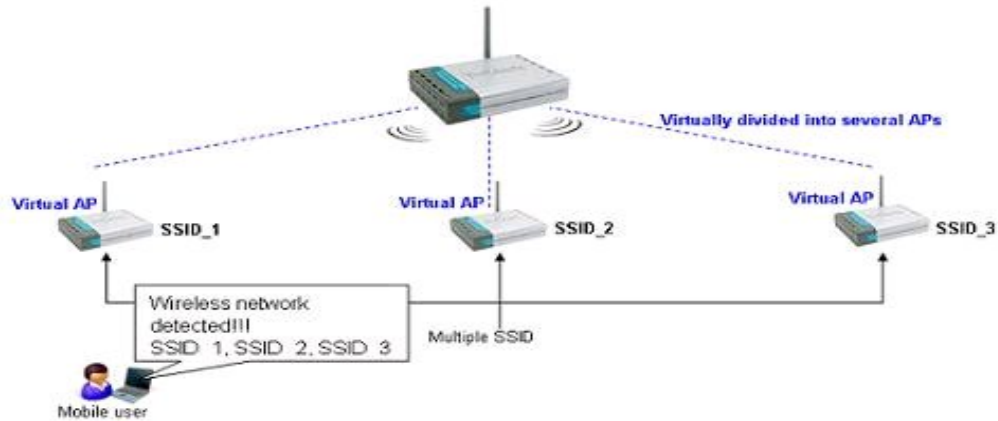


Εικόνα 1.3: ESS τοπολογία

### 1.3.4 Multi-BSS (virtual AP)

Στην αρχή της δημιουργίας των ασύρματων δικτύων, όλοι οι σταθμοί που συνδέονταν σε ένα AP είχαν τα ίδια δικαιώματα χρήσης. Για να καλυφθούν όμως οι περιπτώσεις των σταθμών που δε θεωρούνται έμπιστοι από το AP όπως είναι οι προσωρινοί χρήστες του δικτύου (guests), η λύση είναι να δημιουργηθούν δύο BSS δίκτυα στην ίδια φυσική υποδομή.

Βάσει του 802.11 περισσότερα από ένα δίκτυα μπορούν να χρησιμοποιήσουν το ίδιο φάσμα συχνοτήτων. Επιπλέον, ένα AP μπορεί να δημιουργήσει δύο BSS δίκτυα όπου κάθε SSID σχετίζεται με ένα εικονικό τοπικό δίκτυο **VLAN (virtual LAN)** δημιουργώντας ένα **multi-BSS (multiple Basic Service Set)** δίκτυο [6]. Οι σταθμοί αναγνωρίζουν τα δύο δίκτυα και συνδέονται με αυτό που εξυπηρετεί τις ανάγκες τους βάσει των δικαιωμάτων που μπορούν να έχουν στο δίκτυο αυτό.



Εικόνα 1.4: Multi-BSS τοπολογία

## 1.4 Σύγκριση Ασύρματων – Ενσύρματων τοπικών δικτύων

Τα WLANs έχουν πλεονεκτήματα αλλά και αρκετούς περιορισμούς σε σύγκριση με τα ενσύρματα τοπικά δίκτυα. Ένα WLAN θα καταστήσει εύκολη την προσπάθεια του διαχειριστή του όσον αφορά στην εισαγωγή ή την μετακίνηση των σταθμών εργασίας στο δίκτυο, αλλά και στην εγκατάσταση των απαιτούμενων AP ώστε να παρέχεται η σύνδεση στους χρήστες ακόμη και σε περιοχές που είναι δύσκολη η εγκατάσταση δομημένης καλωδίωσης.

Μερικά από τα πλεονεκτήματα των ασύρματων δικτύων έναντι των ενσύρματων είναι τα εξής:

### **Κόστος:**

Ενώ το αρχικό κόστος για τον εξοπλισμό που θα υλοποιήσει ένα ασύρματο τοπικό δίκτυο (ακριβότερες κάρτες δικτύου και αγορά σταθμών πρόσβασης) είναι μεγαλύτερο από αυτό ενός ενσύρματου δικτύου, τα συνολικά έξοδα εγκατάστασης είναι αισθητά μικρότερα. Μακροπρόθεσμα, τα οφέλη είναι ακόμα μεγαλύτερα στις περιπτώσεις δυναμικών χώρων στις οποίες παρατηρούνται συχνές μετακινήσεις από τους σταθμούς που απαρτίζουν το δίκτυο.

### **Ευκολία στη χρήση:**

Σήμερα, όλοι οι φορητοί υπολογιστές και πολλά κινητά τηλέφωνα είναι εξοπλισμένα με τεχνολογία **WiFi (Wireless Fidelity)** που χρησιμοποιείται για απευθείας σύνδεση σε ένα ασύρματο δίκτυο. Οι χρήστες μπορούν να συνδέονται με ασφάλεια στους πόρους του δικτύου από οποιοδήποτε σημείο που βρίσκεται εντός της εμβέλειας κάλυψης του δικτύου. Η περιοχή κάλυψης είναι κατά κανόνα οι εγκαταστάσεις μιας επιχείρησης, ένα γραφείο, ή ένα σπίτι, ωστόσο μπορεί να επεκτείνεται και σε περισσότερα κτήρια.

### **Διαχείριση:**

Εφόσον δεν απαιτείται η τοποθέτηση καλωδίων σε ένα χώρο, η εγκατάσταση μπορεί να ολοκληρωθεί σε μικρότερο χρονικό διάστημα τοποθετώντας απλώς ένα ή και περισσότερα AP που θα συνθέτουν το δίκτυο. Επιπροσθέτως, διευκολύνεται και η συνδεσιμότητα αλλά και η αξιοπιστία του δικτύου σε δυσπρόσιτους χώρους, όπως οι αποθήκες ή οι εγκαταστάσεις εργοστασιακής παραγωγής όπου παρατηρείται μεγάλο ποσοστό θορύβου που μπορεί να επηρεάσει αρνητικά (αποτυχία λήψης δεδομένων ή λήψη λανθασμένων δεδομένων), τις περιπτώσεις που χρησιμοποιείται η ενσύρματη επικοινωνία.

### **Εξοικονόμηση ενέργειας:**

Πολλά AP παρέχουν τη δυνατότητα προσωρινής αποθήκευσης των δεδομένων που προορίζονται για ένα σταθμό του δικτύου σε περίπτωση που ο τελευταίος βρίσκεται σε κατάσταση εξοικονόμησης ενέργειας. Τα δεδομένα αυτά θα μεταφερθούν από το AP στον σταθμό όταν αυτός επανέλθει στην βασική κατάσταση λειτουργίας του.

### **Κινητικότητα:**

Τα ασύρματα δίκτυα προσφέρουν στους χρήστες τη δυνατότητα πρόσβασης από οπουδήποτε κι αν βρίσκονται με την προϋπόθεση βέβαια να είναι εντός της εμβέλειας του δικτύου. Η δυνατότητα αυτή μπορεί να αυξήσει την αποδοτικότητα και την παραγωγικότητα των χρηστών κυρίως στα εργασιακά περιβάλλοντα μιας και η πρόσβαση στα δεδομένα που χρειάζονται είναι δυνατή ανά πάσα στιγμή ακόμα κι αν δεν βρίσκονται στα γραφεία τους.

### **Επεκτασιμότητα:**

Τα ασύρματα τοπικά δίκτυα εμφανίζονται ως περισσότερο ευέλικτα από τα ενσύρματα όσον αφορά στην επεκτασιμότητά τους. Καθίσταται αρκετά πιο εύκολη σαν διαδικασία η τοποθέτηση περισσότερων AP για την διεύρυνση του δικτύου από την εγκατάσταση δομημένης καλωδίωσης που απαιτούν τα ενσύρματα τοπικά δίκτυα.

Στον αντίποδα όλων των παραπάνω πλεονεκτημάτων υπάρχουν και κάποιοι περιορισμοί που συναντώνται στα ασύρματα τοπικά δίκτυα. Μερικά από τα αυτά τα μειονεκτήματα είναι τα εξής:

### **Παρεμβολές:**

Τα ραδιοκύματα δεν προστατεύονται από εξωτερικούς παράγοντες όπως τα καλώδια που περικλείονται από κάποιο περίβλημα. Βάσει αυτού, παρατηρείται το φαινόμενο κατά το οποίο ενώ τα ραδιοκύματα λειτουργούν ανεξάρτητα το ένα από το άλλο στην ίδια περιοχή, όταν χρησιμοποιηθούν ίδιες ή παρόμοιες συχνότητες εμφανίζεται το πρόβλημα των παρεμβολών που μπορεί να προκληθούν και από γειτονικές ηλεκτρονικές συσκευές όπως είναι οι φούρνοι μικροκυμάτων.

### **Ασφάλεια:**

Είναι αρκετά δύσκολο να εγγυηθεί κάποιος την ασφάλεια του ασύρματου δικτύου καθώς αυτό το είδος δικτύου είναι αρκετά ευάλωτο σε κακόβουλες επιθέσεις ή υποκλοπές των δεδομένων που μεταδίδονται, από κάποιον που βρίσκεται εντός της εμβέλειας του δικτύου και χρησιμοποιεί έναν δέκτη. Απαιτείται λοιπόν κάποια μέθοδος κρυπτογράφησης των εκπεμπόμενων δεδομένων, γεγονός που μειώνει την απόδοση του συστήματος μιας και η επεξεργασία των δεδομένων αυτών καθίσταται χρονοβόρα.

### **Πολυπλοκότητα σχεδίασης:**

Το ασύρματο δίκτυο θα πρέπει να προβλέπει τις περιπτώσεις που οι χρήστες του μετακινούνται μέσα στη περιοχή του, γεγονός που κάνει αρκετά περίπλοκη τη σχεδίαση του.

### **Καιρικές συνθήκες:**

Οι καιρικές συνθήκες που επικρατούν επηρεάζουν σε ένα πολύ μεγάλο ποσοστό την μετάδοση των δεδομένων και κατ' επέκταση την αποδοτικότητα του δικτύου. Ορισμένες φορές, ο εξοπλισμός των ασύρματων δικτύων τόσο στους σταθμούς πρόσβασης όσο και στους απλούς σταθμούς δεν είναι ικανός να λάβει ή να μεταδώσει δεδομένα σε περιπτώσεις έντονης ομίχλης ή σύννεφων σκόνης.

### **1.5 Επιπτώσεις στην υγεία**

Τα ασύρματα δίκτυα που χρησιμοποιούνται για πρόσβαση στο διαδίκτυο και στις υπηρεσίες που αυτό προσφέρει όπως είναι η ανταλλαγή ηλεκτρονικών μηνυμάτων, η μεταφορά αρχείων ή η περιήγηση σε ιστοσελίδες, αυξάνονται στον αριθμό σε καθημερινή βάση και τα συναντάμε τόσο σε σπίτια, όσο και σε γραφεία αλλά και σε πολλούς κοινόχρηστους χώρους (αεροδρόμια, σχολεία κτλ). Δεδομένου ότι ο αριθμός των τοπικών ασύρματων δικτύων αυξάνεται, κάτι ανάλογο παρατηρείται και στην έκθεση των χρηστών στην ακτινοβολία που εκπέμπεται από τις συσκευές που απαρτίζουν τα ασύρματα δίκτυα.

Έντονες είναι οι ανησυχίες για τις πιθανές επιπτώσεις στην υγεία που μπορεί να προκληθούν από την έκθεση σε πεδία ραδιοσυχνοτήτων που παράγονται από ασύρματες τεχνολογίες και κυρίως από τους σταθμούς βάσης (AP-Access Points) που απαρτίζουν τα ασύρματα τοπικά δίκτυα. Το θέμα που κυρίως εξετάζεται είναι κατά πόσο τα ραδιοκύματα αυτά μπορούν να έχουν συμμετοχή στην μεταβολή του γενετικού κώδικα του κάθε ανθρώπου προκαλώντας ανωμαλίες ή εμφάνιση κάποιου είδους καρκίνου.

Μέχρι σήμερα, η μόνη επίπτωση στην υγεία από τα πεδία ραδιοσυχνοτήτων που αποδεικνύεται σε επιστημονικές έρευνες, είναι η αύξηση της θερμοκρασίας του ανθρωπίνου σώματος λιγότερο από ένα βαθμό ( $< 1^\circ \text{C}$ ), από την έκθεση σε πολύ υψηλής έντασης πεδία ραδιοσυχνοτήτων όπως είναι ορισμένες βιομηχανικές εγκαταστάσεις (π.χ. θερμαντήρες). Στην πραγματικότητα, τα επίπεδα έκθεσης στις

ραδιοσυχνότητες είναι τόσο χαμηλά που οι αυξήσεις της θερμοκρασίας είναι αμελητέες και κατά πάσα πιθανότητα δεν επηρεάζουν την υγεία του ανθρώπου.

Σε γενικές γραμμές, οι έρευνες που πραγματοποιήθηκαν σε ανθρώπους και ζώα στις οποίες εξετάζονται τα τμήματα του εγκεφάλου, η γνωστική λειτουργία και η συμπεριφορά μετά την έκθεση τους σε πεδία ραδιοσυχνότητας, δεν έχουν προσδιορίσει αρνητικές επιπτώσεις.

Τα ραδιοκύματα που χρησιμοποιήθηκαν σε αυτές τις μελέτες ήταν περίπου 1000 φορές υψηλότερα από αυτά που εκπέμπονται από τους σταθμούς βάσης στα κοινά ασύρματα τοπικά δίκτυα. Επιπροσθέτως, στις έρευνες που έγιναν δεν υπήρξαν τεκμηριωμένες ενδείξεις για μεταβολές στον ύπνο των ανθρώπων ούτε καρδιαγγειακές παθήσεις που θα μπορούσαν να σχετίζονται με τα εν λόγω ραδιοκύματα.

Σε αντίθεση με όλα τα προηγούμενα, παρουσιάζεται η επίσης τεκμηριωμένη άποψη ορισμένων βιολόγων πως οι μη θερμικές επιδράσεις της ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπουν οι κεραιές των σταθμών βάσης των ασύρματων δικτύων, είναι αθροιστικές και συσσωρεύσιμες. Οι δε επιπτώσεις τους είναι τόσο βραχυχρόνιες όσο και μακροχρόνιες. Υποστηρίζεται πως οι επιπτώσεις αυτές καλύπτουν ένα μεγάλο φάσμα βιολογικών θεμάτων όπως είναι η καταστροφή του DNA, οι καρκινογενέσεις με μέσο χρόνο εμφάνισης τα 10 χρόνια έκθεσης σε ραδιοκύματα, η σκλήρυνση κατά πλάκας αλλά και η νόσος Αλτσχάιμερ, η μείωση της προσοχής αλλά και της μαθησιακής ικανότητας, η εξασθένηση της βραχυπρόθεσμης κυρίως μνήμης, η εξασθένηση του ανοσοποιητικού συστήματος και κατ' επέκταση της άμυνας του οργανισμού, οι ίλιγγοι, οι πονοκέφαλοι, οι αναπαραγωγικές δυσλειτουργίες κ.α.

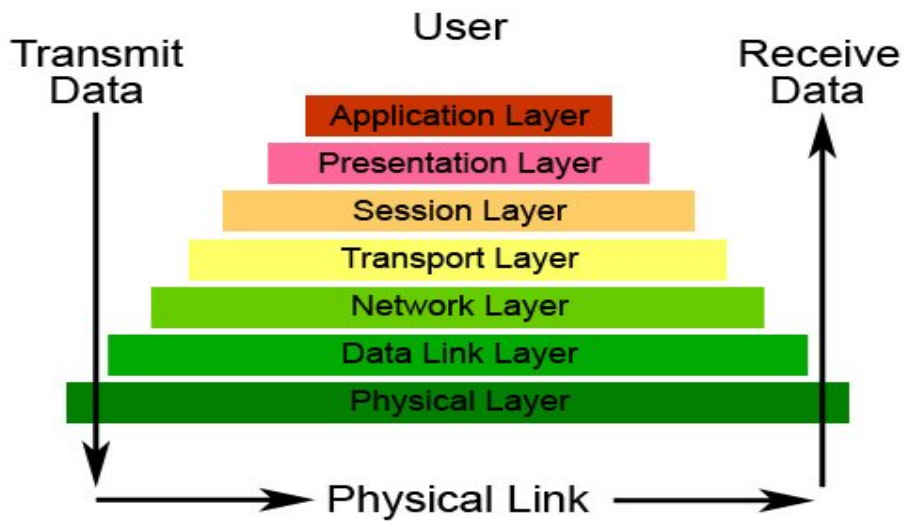
## 2. Το μοντέλο αναφοράς OSI

Για να ελαττωθεί η πολυπλοκότητα σχεδίασης, τα δίκτυα οργανώνονται σε επίπεδα ή στρώματα που το καθένα χτίζεται πάνω στο προηγούμενό του και έχουν ως βασικό στόχο την επίτευξη της επικοινωνίας μεταξύ των σταθμών ακόμα κι αν οι συσκευές που χρησιμοποιούνται ανήκουν σε διαφορετικούς κατασκευαστές [7]. Ο σκοπός κάθε επιπέδου είναι να προσφέρει συγκεκριμένες υπηρεσίες στα υψηλότερα επίπεδα, απομονώνοντας αυτά τα επίπεδα από τις λεπτομέρειες σχετικά με το πώς πραγματικά υλοποιούνται οι παρεχόμενες υπηρεσίες έτσι ώστε τυχόν αλλαγές που μπορεί να υπάρξουν σε ένα επίπεδο να μην έχουν επιπτώσεις στα υπόλοιπα. Ο έλεγχος του συστήματος μεταφέρεται από το ένα επίπεδο στο αμέσως επόμενο του ξεκινώντας πάντα από το έβδομο επίπεδο ή αλλιώς το επίπεδο της εφαρμογής. Κάθε ένα από αυτά τα επίπεδα υπόκειται στους εξής κανονισμούς [8]:

- Ένα επίπεδο θα πρέπει να δημιουργείται εκεί που είναι απαραίτητη η ύπαρξη αφαίρεσης (abstraction) προκειμένου να ομαδοποιηθούν οι επί μέρους κανόνες που θα συμπληρώνουν το εν λόγω επίπεδο.
- Κάθε επίπεδο θα πρέπει να χρησιμοποιείται για ένα ακριβή σκοπό ακολουθώντας μία συγκεκριμένη διαδικασία.
- Η λειτουργία του κάθε επιπέδου θα πρέπει να επιλεγεί με τέτοιο τρόπο ώστε να καθιστά συμβατές τις συσκευές που ανήκουν σε διαφορετικούς κατασκευαστές.
- Ο αριθμός των επιπέδων σε ένα μοντέλο αναφοράς θα πρέπει να είναι τόσο μεγάλος ώστε να διαχωρίζονται οι λειτουργίες του κάθε επιπέδου και τόσο μικρός ώστε να μην καθίσταται δύσχρηστο και πολύπλοκο το μοντέλο αυτό.

Το μοντέλο που προτάθηκε από τον Διεθνή Οργανισμό Τυποποίησης **ISO (International Standards Organization)** για την τυποποίηση της

διαστρωμάτωσης πρωτοκόλλων ονομάζεται μοντέλο αναφοράς **OSI (Open System Interconnection)**. Η χρησιμότητά του μοντέλου αυτού απαντάται στο γεγονός πως μπορούν να συνδυαστούν και να χρησιμοποιηθούν προϊόντα αλλά και επίπεδα διαστρωμάτωσης από διαφορετικούς κατασκευαστές (κάρτες δικτύου, access points κτλ) με ελάχιστες ή καθόλου παραμετροποιήσεις από τους διαχειριστές των συστημάτων. Το μοντέλο του OSI αποτελείται από 7 επίπεδα [9] τα οποία παρουσιάζονται στο παρακάτω σχήμα και περιγράφονται στη συνέχεια.



Εικόνα 2.1: Τα 7 επίπεδα του μοντέλου διαστρωμάτωσης OSI.

Στο μοντέλο αναφοράς OSI τα τρία χαμηλότερα επίπεδα βασίζονται καθαρά στην επικοινωνία των σταθμών του δικτύου αφού αναφέρονται στους τρόπους μετάδοσης της πληροφορίας και υλοποιούνται από τις συσκευές επικοινωνίας. Τα υψηλότερα επίπεδα αναφέρονται κυρίως στις λειτουργίες που σχετίζονται με τις εφαρμογές που ανταλλάσσουν πληροφορίες.



## **2.1 Φυσικό επίπεδο (Physical Layer)**

Το πρώτο επίπεδο του μοντέλου OSI, το φυσικό επίπεδο, περιγράφει το φυσικό μέσο που παρέχει τη σύνδεση μεταξύ των μερών που απαρτίζουν το δίκτυο όπως είναι τα ομοαξονικά καλώδια, τα συνεστραμμένα ζεύγη καλωδίων, οι οπτικές ίνες, οι ραδιοσυχνότητες κτλ.

Το φυσικό επίπεδο ασχολείται κυρίως με την μετάδοση των bits στο κανάλι επικοινωνίας. Οι κανόνες που διέπουν το συγκεκριμένο επίπεδο έχουν να κάνουν με τον αριθμό των volt που χρησιμοποιούνται στην αναπαράσταση των bits ώστε να διαχωρίζεται το 0 bit από το 1 bit , με τη διάρκεια σε microseconds που θα πρέπει να διαρκεί ένα bit, με το χρονικό σημείο στο οποίο η μετάδοση μπορεί να γίνει ταυτόχρονα και από τις δύο κατευθύνσεις, με την αρχικοποίηση της επικοινωνίας στις δύο πλευρές της αλλά και με τον τερματισμό της όταν και οι δύο πλευρές έχουν ολοκληρώσει την μετάδοση των δεδομένων τους, με τον συγχρονισμό των συσκευών και τέλος με την επισήμανση τυχόν σφαλμάτων που προέκυψαν κατά τη μετάδοση.

## **2.2 Επίπεδο σύνδεσης δεδομένων (Data Link Layer)**

Το επίπεδο αυτό καθορίζει την πρόσβαση στο μέσο μετάδοσης, τον τρόπο με τον οποίο μία συσκευή ανιχνεύει τυχόν λάθη μεταφοράς, παρέχει λειτουργίες ελέγχου, χειρίζεται και οριοθετεί πλαίσια δεδομένων (data frames) και επιβεβαιώνει τη λήψη τους.

Στόχος του είναι να παρουσιάσει και να μεταφέρει στο επίπεδο δικτύου τα δεδομένα της μετάδοσης δίχως την ύπαρξη τυχόν σφαλμάτων. Η αποφυγή των σφαλμάτων επιτυγχάνεται με την εξής διαδικασία: Ο αποστολέας “σπάει” τα δεδομένα του σε μικρότερα κομμάτια, γνωστά και ως πλαίσια δεδομένων μεγέθους μερικών εκατοντάδων byte. Τα πακέτα δεδομένων αποστέλλονται από τον πομπό σειριακά ώστε να μπορέσει ο δέκτης να τα ομαδοποιήσει στην αρχική τους μορφή και έπειτα να στείλει με τη σειρά του μηνύματα επιβεβαίωσης ορθής λήψης των πλαισίων αυτών πίσω στον πομπό.

Δεδομένου ότι το φυσικό στρώμα απλώς δέχεται και μεταδίδει μια σειρά από bits, η αναγνώριση των ορίων των πλαισίων δεδομένων είναι λειτουργία του επιπέδου σύνδεσης δεδομένων. Η αναγνώριση των ορίων των πλαισίων μπορεί να επιτευχθεί με την προσθήκη δύο ειδικών μοτίβων (flags) της μορφής «01111110» στην αρχή και δύο στο τέλος του κάθε πλαισίου. Για να αποφευχθούν τυχόν παρανοήσεις όσων αφορά τα bits που απαρτίζουν ένα flag και τα bits που είναι τμήμα των δεδομένων του πλαισίου, χρησιμοποιείται μεμονωμένα το bit «0» που προστίθεται από τον πομπό και αφαιρείται από τον δέκτη. Πιο συγκεκριμένα, στην περίπτωση που τα δεδομένα περιέχουν την ακολουθία «011111» θα πρέπει ο πομπός να προσθέσει ένα bit με τιμή «0» μετά το πέμπτο «1» ώστε να μη θεωρηθεί από τον δέκτη πως η ακολουθία αυτή αποτελεί ένα flag. Αντίστοιχα, όταν ο δέκτης παραλάβει την ακολουθία αυτή θα πρέπει να αφαιρέσει το «0» μετατρέποντας την πληροφορία στην αρχική της μορφή «011111» και να συνεχίσει να διαβάσει τα υπόλοιπα bits της ακολουθίας. Εάν η ακολουθία περιέχει τα bits «0111111» θα προστεθεί από τον πομπό ένα μηδενικό μετά το πέμπτο «1» και θα μετατραπεί σε «01111101» ενώ ο δέκτης θα αφαιρέσει το επιπρόσθετο «0» για να πάρει την αρχική μορφή «0111111». Τέλος εάν η ακολουθία περιέχει το «0111110» θα μετατραπεί σε «01111100» από τον πομπό και ακολούθως σε «0111110» από τον δέκτη .

## 2.3 Επίπεδο δικτύου (Network Layer)

Το επίπεδο δικτύου ασχολείται κυρίως με τον έλεγχο της λειτουργίας του δικτύου. Οι βασικές λειτουργίες του επιπέδου αυτού είναι η αποκατάσταση και ο τερματισμός της σύνδεσης μεταξύ δύο ακραίων σημείων ενός μεγάλου δικτύου αλλά και ο προσδιορισμός τους με χρήση διευθύνσεων, η μεταφορά των δεδομένων σε μορφή πακέτων καθώς και η απαρίθμησή τους.

Ένα σημαντικό ζήτημα σχεδιασμού του επιπέδου αυτού είναι ο καθορισμός του τρόπου βάσει του οποίου δρομολογούνται τα πακέτα δεδομένων από την πηγή στον προορισμό. Οι διαδρομές των πακέτων δεδομένων βασίζονται είτε σε στατικές εγγραφές στους πίνακες δρομολόγησης των δρομολογητών του δικτύου

είτε σε δυναμικές εγγραφές που τροποποιούνται ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο κάθε φορά.

Όταν ένα πακέτο διασχίζει κάποια δίκτυα προκειμένου να φτάσει στον τελικό προορισμό του μπορεί να προκύψουν αρκετά θέματα προς αντιμετώπιση. Ο τρόπος χειρισμού των ληφθέντων πακέτων που χρησιμοποιείται από κάποιο ενδιάμεσο δίκτυο μπορεί να είναι διαφορετικός από το αρχικό δίκτυο που αποστέλλει το πακέτο αυτό. Για παράδειγμα, το ενδιάμεσο δίκτυο δεν μπορεί να απορρίψει ένα πακέτο επειδή είναι πολύ μεγάλο, οι συσκευές που χρησιμοποιούνται μπορεί να διαφέρουν μεταξύ τους και ούτω καθεξής. Το επίπεδο δικτύου είναι υπεύθυνο για να ξεπεράσουν όλα αυτά τα προβλήματα και να επιτραπεί η διασύνδεση και η ομαλή συνεργασία των ετερογενών δικτύων.

## **2.4 Επίπεδο μεταφοράς (Transport Layer)**

Το επίπεδο μεταφοράς ασχολείται με την αποδοχή δεδομένων από το επίπεδο συνόδου, την τμηματοποίηση των πακέτων σε μικρότερα, την μεταφορά τους στο επίπεδο δικτύου, την πολυπλεξία των δεδομένων διαφόρων σταθμών του δικτύου στο ίδιο κανάλι επικοινωνίας. Το επίπεδο αυτό διασφαλίζει την επιτυχημένη από άκρη σε άκρη μετάδοση των δεδομένων. Όλες αυτές οι λειτουργίες θα πρέπει να γίνουν με τέτοιο τρόπο ώστε να απομονώνεται το επίπεδο συνόδου από τυχόν αλλαγές στις συσκευές που απαρτίζουν το δίκτυο.

Ουσιαστικά, το επίπεδο αυτό είναι ένας συνδετικός κρίκος μεταξύ των τριών χαμηλότερων επιπέδων που σχετίζονται κυρίως με τις συσκευές που απαρτίζουν ένα σύστημα και τριών ανώτερων επιπέδων που σχετίζονται στενότερα με τους σταθμούς και τις εφαρμογές που αυτοί εξυπηρετούν.

Υπό κανονικές συνθήκες, το επίπεδο μεταφοράς δημιουργεί μία ξεχωριστή σύνδεση για κάθε μεταφορά που απαιτείται από το επίπεδο συνόδου. Εάν η σύνδεση απαιτεί υψηλούς ρυθμούς απόδοσης από το δίκτυο (throughput), το επίπεδο μεταφοράς δημιουργεί πολλαπλές συνδέσεις διαμοιράζοντας τα δεδομένα στις επιμέρους αυτές συνδέσεις προκειμένου να αυξηθεί η απόδοση του δικτύου.

Το επίπεδο μεταφοράς καθορίζει και το είδος των υπηρεσιών που παρέχονται στο στρώμα συνόδου και ακολούθως στους χρήστες του δικτύου. Ο πιο δημοφιλής τύπος σύνδεσης μεταφοράς είναι η δημιουργία ενός καναλιού που συνδέει ένα σημείο με ένα άλλο μεταφέροντας τα μηνύματα με τη σειρά με την οποία είχαν αποσταλεί. Με τη βοήθεια του επιπέδου μεταφοράς, ένα πρόγραμμα που εκτελείται στον αποστολέα επικοινωνεί με ένα παρόμοιο πρόγραμμα στον προορισμό χρησιμοποιώντας τις κεφαλίδες των μηνυμάτων αλλά και τα μηνύματα ελέγχου.

Σε ορισμένες περιπτώσεις, οι σταθμοί του δικτύου μπορούν να υποστηρίξουν την ύπαρξη πολλαπλών εισερχόμενων και εξερχόμενων συνδέσεων. Πρέπει λοιπόν να υπάρχει ένας τρόπος βάσει του οποίου θα καθορίζεται ποια μήνυμα ανήκουν σε ποιες συνδέσεις. Η πληροφορία αυτή αποθηκεύεται στην κεφαλίδα του πακέτου του επιπέδου μεταφοράς.

Εκτός από την δημιουργία πολλαπλών συνδέσεων σε ένα κανάλι, το στρώμα μεταφοράς πρέπει να λάβει υπόψη την ίδρυση και τη κατάργηση των συνδέσεων σε όλο το δίκτυο. Αυτό απαιτεί κάποιο είδος μηχανισμού αναγνώρισης του ονόματος, έτσι ώστε μια διαδικασία σε έναν σταθμό να μπορεί να περιγράψει την αντίστοιχη διαδικασία στον σταθμό με τον οποίο επιθυμεί να επικοινωνήσει. Τέλος, το επίπεδο μεταφοράς παρέχει μηχανισμούς για τη ρύθμιση της ροής των δεδομένων, έτσι ώστε ένας γρήγορος σταθμός να μη μπορεί να υποσκιάσει έναν αργό.

## **2.5 Επίπεδο συνόδου (Session Layer)**

Το επίπεδο συνόδου είναι υπεύθυνο κυρίως για τη δημιουργία και την αποκατάσταση των συνεδριών μεταξύ των σταθμών του δικτύου. Μια τέτοια συνεδρία επιτρέπει την μεταφορά των δεδομένων, όπως συναντάται και στο επίπεδο μεταφοράς, αλλά παρέχει επίσης και κάποιες βελτιωμένες υπηρεσίες που θα μπορούσαν να φανούν χρήσιμες σε επίπεδο εφαρμογών. Για παράδειγμα, μια συνεδρία μπορεί να χρησιμοποιηθεί για να επιτρέψει σε έναν χρήστη τη σύνδεση του σε ένα απομακρυσμένο σύστημα ή τη μεταφορά ενός αρχείου.

Μία ακόμα από τις υπηρεσίες που παρέχονται στο επίπεδο συνόδου είναι η έναρξη και η συντήρηση του διαλόγου μεταξύ δύο συσκευών. Οι συνεδρίες που δημιουργούνται από αυτό το επίπεδο μπορούν να επιτρέψουν την κυκλοφορία των μηνυμάτων από και προς στις δύο κατευθύνσεις είτε ταυτόχρονα είτε μεμονωμένα, ή και σε μία μόνο κατεύθυνση.

Μια άλλη υπηρεσία που προσφέρεται από το επίπεδο συνόδου είναι η παροχή και η χρήση κουπονιών (tokens). Σε μερικά πρωτόκολλα, είναι απαραίτητο και οι δύο πλευρές που συμμετέχουν στην επικοινωνία να μην επιχειρήσουν να εκτελέσουν την ίδια λειτουργία την ίδια χρονική στιγμή. Για την διαχείριση αυτών των δραστηριοτήτων, το επίπεδο συνόδου παρέχει κουπόνια που ανταλλάσσονται μεταξύ των σταθμών. Μόνο η πλευρά που κατέχει ένα κουπόνι μπορεί να εκτελέσει μια κρίσιμη λειτουργία κάθε φορά.

Τέλος, μία ακόμη υπηρεσία του επιπέδου αυτού είναι ο συγχρονισμός. Ενδέχεται να προκύψουν σημαντικά προβλήματα όταν για παράδειγμα γίνεται προσπάθεια μεταφοράς αρχείων μεταξύ δύο σταθμών ενός δικτύου για ένα μεγάλο χρονικό διάστημα και το δίκτυο για κάποιο λόγο καταρρέει. Χωρίς την υπηρεσία του συγχρονισμού, όταν ματαιώνεται κάποια μεταφορά, η διαδικασία θα πρέπει να ξεκινήσει πάλι από την αρχή με σοβαρό ενδεχόμενο να καταρρεύσει εκ νέου το σύστημα, εάν αυτή η μεταφορά ήταν η αιτία που προκάλεσε την κατάρρευσή του, και να χρειαστεί να επαναληφθεί η διαδικασία περισσότερες από μία φορές. Για να εξαλειφθεί αυτό το ενδεχόμενο, το επίπεδο συνόδου παρέχει έναν μηχανισμό εισαγωγής σημείων ελέγχου (checkpoints) στην ροή των δεδομένων, έτσι ώστε μετά από μία κατάρρευση του συστήματος, να συνεχιστεί η εν λόγω μεταφορά μόνο από το σημείο του τελευταίου σημείου ελέγχου.

## **2.6 Επίπεδο παρουσίασης (Presentation Layer)**

Το επίπεδο παρουσίασης σε αντίθεση με τα υπόλοιπα χαμηλότερα επίπεδα, τα οποία είναι υπεύθυνα κυρίως για την αξιόπιστη μετακίνηση των πακέτων δεδομένων, ασχολείται με την αναπαράσταση αλλά και την τροποποίηση των διαβιβαζόμενων πληροφοριών.

Ένα βασικό πλεονέκτημα μιας υπηρεσίας παρουσίασης είναι η τροποποίηση των δεδομένων με τέτοιο τρόπο ώστε να γίνονται αντιληπτά και κατανοητά από τις εφαρμογές χωρίς να απαιτείται η χρήση κοινού κώδικα στις συνδέσεις των δύο σταθμών που επικοινωνούν.

Επιπλέον, οι διάφορες εφαρμογές ανταλλάσσουν πληροφορίες όπως είναι οι αριθμοί, οι ημερομηνίες, τα χρηματικά ποσά κτλ που εμφανίζονται ως συμβολοσειρές χαρακτήρων, ακέραιοι αριθμοί, αριθμοί κινητής υποδιαστολής και δομές δεδομένων. Τα συστήματα υπολογιστών έχουν διαφορετικούς τρόπους για την αναπαράσταση των συμβολοσειρών χαρακτήρων, των ακεραίων κοκ. Για να καταστεί λοιπόν δυνατή η επικοινωνία και η ανταλλαγή μηνυμάτων σε υπολογιστές με διαφορετικούς τρόπους αναπαράστασης, οι δομές δεδομένων που ανταλλάσσονται θα πρέπει να οριστούν με έναν αφηρημένο τρόπο και να μεταδοθούν με βάση ένα πρότυπο κωδικοποίησης που θα χρησιμοποιηθεί στην εν λόγω επικοινωνία. Η διαχείριση αυτών των αφηρημένων δομών δεδομένων καθώς και η μετατροπή από την μέθοδο αναπαράστασης που χρησιμοποιείται από μία συγκεκριμένη συσκευή στο πρότυπο αναπαράστασης που χρησιμοποιείται στο κανάλι επικοινωνίας, πραγματοποιούνται από το επίπεδο παρουσίασης.

Τέλος, το επίπεδο αυτό ασχολείται και με την τροποποίηση των πληροφοριών. Για παράδειγμα, μπορεί να χρησιμοποιηθεί τόσο η συμπίεση των δεδομένων για να μειωθεί ο αριθμός των bits που πρέπει να μεταδοθούν όσο και η κρυπτογράφηση των δεδομένων που είναι απαραίτητη για την προστασία και την ασφάλεια των δεδομένων.

## **2.7 Επίπεδο εφαρμογών (Application Layer)**

Το επίπεδο εφαρμογών είναι το τελευταίο από τα επίπεδα του μοντέλου αναφοράς και σχετίζεται με τον τρόπο κατά τον οποίο μία εφαρμογή ενός σταθμού επικοινωνεί με την αντίστοιχη εφαρμογή ενός άλλου σταθμού μέσω του δικτύου. Οι λειτουργίες του επιπέδου αυτού καθορίζονται σε μεγάλο βαθμό από τον εκάστοτε χρήστη και γι' αυτόν τον λόγο οι τυποποιήσεις του είναι λιγότερο καθορισμένες.

Μία συνηθισμένη λειτουργία του επιπέδου εφαρμογών είναι η μεταφορά των αρχείων. Τα διαφορετικά συστήματα αρχείων έχουν διαφορετικούς τρόπους ονομασίας αρχείων, διαφορετικούς τρόπους με τους οποίους αντιπροσωπεύονται οι γραμμές κειμένου κ.ο.κ. Η μεταφορά λοιπόν ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί τον χειρισμό αυτών των περιορισμών. Το έργο αυτό ανήκει στο επίπεδο εφαρμογών, όπως και πολλές άλλες εφαρμογές όπως είναι το ηλεκτρονικό ταχυδρομείο, η απομακρυσμένη σύνδεση, η αναζήτηση καταλόγου κ.α.

### 3. 802.11 Physical Layer

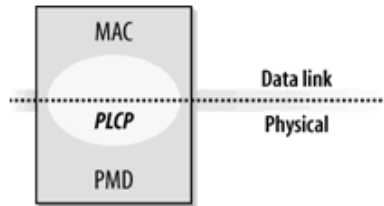
Το 802.11 που ανακοινώθηκε επίσημα το 1997, είναι μία οικογένεια προτύπων της **IEEE (Institute of Electrical and Electronics Engineer)** που σχετίζεται με τα ασύρματα τοπικά δίκτυα ως επέκταση του προτύπου 802.3 που είναι και το συνηθέστερο πρωτόκολλο ενσύρματης δικτύωσης υπολογιστών. Στην οικογένεια προτύπων του 802.11 ανήκουν τα πιο γνωστά μεμονωμένα πρότυπα 802.11a,b,g,e,m,n με κάποιες τροποποιήσεις ανάλογες πάντα με τον σκοπό που εξυπηρετεί κάθε ένα από αυτά τα πρότυπα.

Προσπαθώντας να κάνουμε μια ιστορική αναδρομή στην εξέλιξη των ασύρματων τοπικών δικτύων [10] θα λέγαμε πως η πρώτη προσπάθεια προσέγγισης της τεχνολογίας που θα χρησιμοποιούσε διευρυμένα φάσματα συχνοτήτων έγινε το 1940. Σαράντα χρόνια αργότερα, το 1980, γίνεται η πρώτη χρήση της τεχνολογίας που αφορά στις στενές ζώνες συχνοτήτων. Το 1989 στις ΗΠΑ αποδίδονται συχνότητες μετάδοσης για εμπορική χρήση από την ομοσπονδιακή επιτροπή επικοινωνιών **FCC (Federal Communications Commission)**. Ένα χρόνο αργότερα κατασκευάζονται τα πρώτα προϊόντα που λειτουργούν σε συχνότητες των 900 MHz, γεγονός που συμπίπτει με τις πρώτες προσπάθειες από την IEEE για την προτυποποίηση των ασύρματων τοπικών δικτύων. Το 1994 κατασκευάζονται τα πρώτα προϊόντα που λειτουργούν στη συχνότητα των 2.4 GHz και τρία χρόνια αργότερα, το 1997, εγκρίνεται το πρότυπο IEEE 802.11. Το 1999 ξεκινάει η κυκλοφορία των προϊόντων που συμβατά με το 802.11b και τέλος το 2000 η ονομασία WiFi (Wireless Fidelity) χρησιμοποιείται για να περιγράψει το πρότυπο 802.11b.

Το 802.11 αναφέρεται στα δύο χαμηλότερα στρώματα του μοντέλου διαστρωμάτωσης OSI, δηλαδή στο φυσικό επίπεδο (Physical Layer) το οποίο θα αναλυθεί στο παρόν κεφάλαιο και στο υπόστρωμα **MAC (Medium Access Control)** του επιπέδου σύνδεσης δεδομένων (Data Link Layer) το οποίο και θα αναλυθεί στο κεφάλαιο που ακολουθεί.



Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο υποστρώματος MAC που μπορεί να υποστηρίξει περισσότερα του ενός φυσικά στρώματα, καθένα από τα οποία χωρίζεται σε δύο επιμέρους υποστρώματα όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 3.1 : Διαστρωμάτωση του προτύπου 802.11

Το υπόστρωμα **PLCP (Physical Layer Convergence Procedure)** [11] δέχεται τα πακέτα πληροφοριών του υποστρώματος MAC, γνωστά και ως **MPDUs (Mac Protocol Data Units)**, προσθέτει τις απαραίτητες πληροφορίες που χρειάζεται το φυσικό επίπεδο για τη μετάδοση των πληροφοριών αυτών και συνθέτει τα δικά του πλαίσια γνωστά και ως **PPDUs (PLCP Protocol Data Units)**. Ουσιαστικά το υπόστρωμα PLCP παίζει τον ρόλο του μεσολαβητή μεταξύ του υποστρώματος MAC και του **PMD (Physical Medium Dependent)** υποστρώματος αφού προετοιμάζει τα πακέτα που πρόκειται να μεταδοθούν με πληροφορίες σχετικές με τον πομπό και τον δέκτη. Το υπόστρωμα PMD περιέχει τις λειτουργίες εκείνες που απαιτούνται για την μετάδοση της πληροφορίας μέσω του εκάστοτε φυσικού στρώματος με το οποίο είναι άμεσα συνδεδεμένο, όπως είναι η διαμόρφωση και η αποδιαμόρφωση του μεταδιδόμενου σήματος.

Το αρχικό πρότυπο του 802.11 καθορίζει τρία είδη φυσικών επιπέδων που είναι τα εξής:

- **DSSS (Direct Sequence Spread Spectrum)**: λειτουργεί στη συχνότητα των 2.4 GHz ενώ οι ρυθμοί μετάδοσης που υποστηρίζονται είναι 1 και 2 Mbps.
- **FHSS (Frequency Hopping Spread Spectrum)**: και αυτός ο τύπος φυσικού επιπέδου λειτουργεί στη συχνότητα των 2.4 GHz ενώ οι ρυθμοί μετάδοσης που υποστηρίζονται είναι 1 και 2 Mbps.

- **IR (Infrared):** υποστηρίζει ρυθμούς μετάδοσης 1 και 2 Mbps αλλά λόγω της αδυναμίας του να γίνει επιτυχημένο εμπορικά, η χρήση του ως φυσικό επίπεδο στις ασύρματες τεχνολογίες δεν είναι ιδιαίτερα διαδεδομένη.

### 3.1 DSSS (Direct Sequence Spread Spectrum)

Χαρακτηριστικό αυτής της τεχνικής μετάδοσης είναι πως κάθε bit πληροφορίας αντιπροσωπεύεται από ένα πλήθος από bits και έχει ως αποτέλεσμα την φασματική εξάπλωση του σήματος. Αυτή η διαδικασία επιτυγχάνεται με τον δυαδικό πολλαπλασιασμό (XOR) των bits της αρχικής πληροφορίας με μια ακολουθία ψευδοτυχαίων bits υψηλότερου ρυθμού η οποία είναι γνωστή ως κώδικας εξάπλωσης ή αλλιώς spreading code. Η ροή που προκύπτει έχει ρυθμό μετάδοσης ίσο με αυτόν του spreading code που χρησιμοποιήθηκε για τη δημιουργία της. Επιπλέον, το σήμα της πληροφορίας διευρύνεται σε ένα μεγαλύτερο φάσμα συχνοτήτων, χωρίς όμως να χάσει την συνολική του ενέργεια.

Η DSSS χρησιμοποιεί μία μέθοδο μετατροπής και αντικατάστασης της πληροφορίας που είναι γνωστή εκ των προτέρων τόσο από τον πομπό όσο και από τον δέκτη. Ο πομπός αναλαμβάνει να μετατρέψει τα bits της αρχικής πληροφορίας βάσει της ακολουθίας Barker και εν συνεχεία, ο δέκτης θα χρησιμοποιήσει την ίδια ακολουθία προκειμένου να ανακατασκευάσει το σήμα της πληροφορίας.

Στην προδιαγραφή του φυσικού στρώματος του DSSS ορίστηκε σαν spreading code μία λέξη της ακολουθίας Barker των 11 bits και συγκεκριμένα η λέξη «10110111000». Αυτό σημαίνει πως για τα bit με τιμή «1» η ακολουθία που μεταδίδεται είναι η λέξη Barker με όλα τα bit ανεστραμμένα που είναι η «01001000111», ενώ για τα bit με τιμή «0» μεταδίδεται αυτούσια η λέξη Barker.

Μερικά από τα χαρακτηριστικά της τεχνικής αυτής είναι τα εξής [12]:

- Λειτουργεί σε συχνότητες των 2.4 GHz δίνοντας παράλληλα τη δυνατότητα μετακίνησης σε πολλαπλά κανάλια μεταξύ των 2.4 και 2.4835 GHz.

- Υποστηρίζει ρυθμούς μετάδοσης των 1 και 2 Mbps.
- Χρήση ακολουθίας Barker με 11 chips.

Όπως και κάθε άλλη μέθοδος, έτσι και η DSSS παρουσιάζει σημεία στα οποία υποδεικνύεται καλύτερη από τις άλλες μεθόδους μετάδοσης δεδομένων αλλά και σημεία βάσει των οποίων θα έπρεπε να μην επιλεγθεί ως τεχνική μετάδοσης δεδομένων .

Η χρήση της εν λόγω τεχνικής μπορεί αυξάνει το μέγεθος της πλεονάζουσας πληροφορίας , φαίνεται όμως πολύ αποτελεσματική στην αποφυγή των διαφόρων παρεμβολών που μπορεί να υπάρξουν στο σύστημα αλλά και στην ασφάλεια του διότι για τις συσκευές που λειτουργούν μόνο σε στενές φασματικές ζώνες το διευρυμένο αυτό σήμα μοιάζει πολύ με θόρυβο.

Στην πραγματικότητα, οι πιθανότητες να υπάρξουν παρεμβολές με άλλα σήματα στην ίδια συχνότητα είναι αρκετά μικρές, επομένως μπορούμε να συμπεράνουμε πως η βασική χρήση της εν λόγω τεχνικής είναι η δυνατότητα συνύπαρξης και λειτουργίας περισσότερων από ένα ασύρματων δικτύων στην ίδια γεωγραφική περιοχή.

Στην περίπτωση όμως που υπάρξει κάποια παρεμβολή σε ένα ή και περισσότερα από τα κανάλια συχνότητας κατά τη διάρκεια μετάδοσης της ακολουθίας των chips, μόνο μερικά από τα chips της ακολουθίας αυτής θα επηρεαστούν κι αυτό διότι το μεταδιδόμενο σήμα απλώνεται σε κανάλια πλάτους 22 MHz. Ο δέκτης είναι θέση να ανακατασκευάσει την εν λόγω ακολουθία εξετάζοντας τα chips που έχει ήδη λάβει. Εάν αυτά τα bits υποδεικνύουν πως μεταδόθηκε αυτούσια η λέξη Barker, ο δέκτης θα αντικαταστήσει την ακολουθία αυτή με το bit «0». Αντίθετα, εάν το μέρος των bits που έλαβε ο δέκτης υποδεικνύει πως η λέξη Barker χρησιμοποιήθηκε ανεστραμμένη, τότε στην θέση της ακολουθίας αυτής θα τοποθετηθεί το bit «1». Στην περίπτωση που δεν χρησιμοποιούνταν η DSSS και αποστέλλονταν τα δεδομένα ατόφια, ο πομπός θα έπρεπε να προχωρήσει σε αναμετάδοση της πληροφορίας εάν παρουσιάζονταν κάποια παρεμβολή στο σύστημα που θα επηρέαζε την πληροφορία αυτή.

Στον αντίποδα των παραπάνω, υπάρχουν σημεία στα οποία η χρήση της μεθόδου αυτής εμφανίζει μειονεκτήματα. Η υλοποίησή της μεθόδου αυτής είναι σχετικά πολύπλοκη, γεγονός που μπορεί να συμβάλλει στην δυσκολία διαχείρισης του συστήματος.

Στα προτερήματα αυτής της τεχνικής παρουσιάστηκε η συνεργασία περισσότερων του ενός συστημάτων στον ίδιο γεωγραφικό χώρο. Το μειονέκτημα της συνεργασίας αυτής είναι ο αριθμός των διαφορετικών δικτύων που μπορούν να λειτουργούν στην ίδια περιοχή χωρίς να παρουσιάζονται προβλήματα στις μεταδόσεις των δεδομένων τους. Για την ακρίβεια, το πλήθος των διαφορετικών ακολουθιών που μπορούν να χρησιμοποιηθούν μεταξύ πομπών και δεκτών ώστε να εξυπηρετούνται τα συστήματα αυτά είναι αρκετά μικρό. Η DSSS βασίζεται στην κατανομή εύρους ζώνης για κάθε σύστημα που εξυπηρετείται. Κάθε σύστημα θα χρειαστεί ένα συνεχόμενο φάσμα συχνότητας πλάτους 22 MHz και κάθε τέτοιο φάσμα θα πρέπει να απέχει από τα γειτονικά του κατά 30 MHz. Βάσει αυτής της παραδοχής μόλις τρία συστήματα μπορούν να λειτουργήσουν ταυτόχρονα στην ίδια περιοχή χωρίς απώλειες δεδομένων.

Η ασφάλεια στην μετάδοση των δεδομένων είναι θέμα ζωτικής σημασίας και δεν θα μπορούσε να απέχει από την προσπάθεια αξιολόγησης της τεχνικής αυτής. Η τεχνική αυτή χρησιμοποιεί μία αρκετά διαδεδομένη ακολουθία, την Barker, και μπορεί να λειτουργήσει σε ένα από τα 14 κανάλια που περιγράφονται στην προτυποποίηση του 802.11. Είναι αρκετά εύκολο λοιπόν για κάποιον να καταφέρει να υποκλέψει τα μηνύματα που αποστέλλονται βάσει αυτής της τεχνικής. Ο μόνος τρόπος για να προστατευθούν τα δεδομένα είναι η κρυπτογράφησή τους, μία μέθοδος που απαιτεί κόστος και παράλληλα μειώνει την απόδοση του δικτύου μιας και απαιτείται περισσότερη ενέργεια για να κρυπτογραφηθούν τα δεδομένα.

Τέλος, η χρήση του εύρους ζώνης θεωρείται ανεπαρκής μιας και το μεγαλύτερο κομμάτι του αποτελείται από πλεονάζοντα chips της ακολουθίας που χρησιμοποιείται.

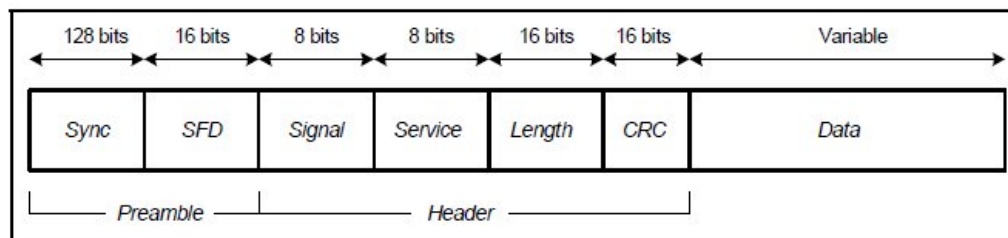
Τα κανάλια συχνότητων που χρησιμοποιούνται ανά τον κόσμο στην τεχνική DSSS φαίνονται στον παρακάτω πίνακα:

Channel ID	FCC channel Frequencies	ETSI channel frequencies	Japan Frequency
1	2412 MHz	N/A	N/A
2	2417 MHz	N/A	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	N/A	2484 MHz

Πίνακας 3.1: Τα κανάλια συχνοτήτων που χρησιμοποιούνται στην DSSS

### DSSS PLCP Frame Format

Το πλαίσιο του PLCP υποστρώματος του φυσικού επιπέδου για την τεχνική DSSS φαίνεται στο παρακάτω σχήμα :



Εικόνα 3.2: Εικόνα : Πλαίσιο PLCP της DSSS για το φυσικό στρώμα του 802.11

Τα πρώτα 144 bits συνθέτουν το **PLCP Preamble** που χρησιμεύει τόσο στον συγχρονισμό μεταξύ πομπού και δέκτη όσο και στην αρχικοποίηση του πλαισίου και αποτελείται από τα επί μέρους:

- *Sync* (128 bits): χρησιμοποιείται για τον συγχρονισμό πομπού και δέκτη.
- *SFD* (16 bits): χρησιμεύει στον εντοπισμό της αρχής του πλαισίου.

Τα επόμενα 48 bits αποτελούν το **PLCP Header** με τα εξής πεδία:

- *Signal* (8 bits): κωδικοποίηση του ρυθμού μετάδοσης των δεδομένων.
- *Service* (8 bits): δεσμευμένο πεδίο για μελλοντική χρήση.
- *Length* (16 bits): περιέχει τον αριθμό των microseconds που απαιτούνται για την αποστολή του πλαισίου.
- *CRC* (16 bits): κώδικας για προστασία των υπολοίπων πεδίων.

Ακολουθεί το πεδίο των δεδομένων χωρίς να υπόκειται σε περιορισμούς σχετικούς με το μέγεθος του πλαισίου.

### 3.2 FHSS (Frequency Hopping Spread Spectrum)

Η τεχνική μεταπήδησης φάσματος **FHSS (Frequency Hopping Spread Spectrum)** [13] χρησιμοποιείται στην εκπομπή σημάτων διαχωρίζοντας το φάσμα των συχνοτήτων σε μικρότερα υποκανάλια. Τα κανάλια αυτά στη συχνότητα των 2.4 GHz που χρησιμοποιείται, είναι 79 στον αριθμό, μη επικαλυπτόμενα και λειτουργούν στο 1 MHz.

Στην πραγματικότητα για να αποφευχθεί η πιθανότητα σύγκρουσης των πλαισίων και απώλειας των δεδομένων μεταξύ των διαφορετικών συστημάτων που λειτουργούν στην ίδια περιοχή, συστήνεται ο αριθμός των διαφορετικών αυτών δικτύων να μην ξεπερνά τα δεκαπέντε σε περιπτώσεις που δεν χρησιμοποιείται συγχρονισμός για τις ακολουθίες μεταπήδησης και κάθε σύστημα λειτουργεί ανεξάρτητα από το άλλο. Στις περιπτώσεις που χρησιμοποιείται ο συγχρονισμός για τις ακολουθίες μεταπήδησης μπορούν να λειτουργήσουν περισσότερα δίκτυα μαζί αλλά αυτή η πρακτική θα είχε ως αποτέλεσμα τη μείωση της απόδοσης των εν λόγω συστημάτων.

Ο πομπός του μηνύματος μεταπηδά από κανάλι σε κανάλι βάσει μιας προκαθορισμένης μεθόδου και στέλνει διαδοχικά μικρά πακέτα πληροφοριών σε ένα συγκεκριμένο χρονικό διάστημα. Ο μέγιστος χρόνος που μπορεί ένας πομπός να παραμείνει σε ένα από τα υποκανάλια στέλνοντας τις πληροφορίες του είναι καθορισμένος συνήθως στα 100 ms και ονομάζεται dwell time (χρόνος παραμονής). Προκειμένου να λειτουργήσει σωστά η εν λόγω τεχνική, οι δύο πλευρές (της αποστολής και της λήψης των πληροφοριών) θα πρέπει να συγχρονιστούν, γεγονός που απαιτεί την χρήση της ίδιας μορφής αναπήδησης και από τους δύο. Σε αντίθετη περίπτωση, τα δεδομένα που είναι προς αποστολή δεν θα φτάσουν ποτέ στον προορισμό τους.

Συνοψίζοντας, τα κύρια χαρακτηριστικά της τεχνικής αυτής είναι [14]:

- Χρησιμοποιείται στην μπάντα συχνοτήτων των 2.4 GHz και δημιουργεί 79 υποκανάλια με συχνότητα που κυμαίνεται από τα 2.402 GHz στα 2.48 GHz.
- Κάθε υποκανάλι που δημιουργείται έχει πλάτος 1 MHz και προσφέρει ρυθμούς μετάδοσης στο 1 ή 2 Mbps.

Μερικά από τα οφέλη της χρήσης της εν λόγω τεχνικής είναι τα εξής:

- Αντιμετώπιση προβλημάτων θορύβου και παρεμβολών που προέρχονται από άλλες πηγές ραδιοκυμάτων, διότι η συχνότητα μετάδοσης αλλάζει συνεχώς τιμή. Έτσι, τυχόν παρεμβολές γίνονται αντιληπτές μόνο για ένα μικρό διάστημα του χρόνου, στο οποίο τυχαίνει να είναι κοντά η συχνότητα μετάδοσης με την συχνότητα στην οποία παρουσιάζονται οι παρεμβολές.
- Με τη χρήση της εν λόγω τεχνικής υπάρχει η δυνατότητα χρήσης του ίδιου φάσματος συχνότητας από δύο συσκευές ταυτόχρονα χωρίς να ανταγωνίζονται για την κατοχή του μέσου. Θα υπάρξουν βέβαια συγκρούσεις που θα διαρκέσουν για πολύ μικρό χρονικό διάστημα αλλά η εμφάνισή τους δεν θα είναι τόσο συχνή ώστε να προκαλέσουν αποτυχία μετάδοσης δεδομένων.

Και η FHSS, όπως και κάθε άλλη τεχνική έχει τα μειονεκτήματά της [15]. Το βασικότερο όλων είναι η μέση απόδοση του δικτύου που φαίνεται να είναι σχετικά χαμηλή μιας και ο ρυθμός μετάδοσης δεδομένων φαίνεται να είναι περιορισμένος.

Τα κανάλια συχνοτήτων που χρησιμοποιούνται από την τεχνική αυτή παρουσιάζονται στον παρακάτω πίνακα:

Ήπειρος	Φάσμα συχνότητας	Διαθέσιμα κανάλια
Ευρώπη	2.4 - 2.4835 GHz	>75
Αμερική	2.4 - 2.4835 GHz	>20
Ασία	2.471 – 2.497 GHz	>10

Πίνακας 3.2: Τα κανάλια συχνοτήτων που χρησιμοποιούνται στην FHSS

Τα πέντε βασικά βήματα που χρησιμοποιεί η τεχνική μεταπήδησης στο φάσμα των συχνοτήτων για την αρχικοποίηση της επικοινωνίας μεταξύ πομπού και δέκτη είναι τα εξής [16]:

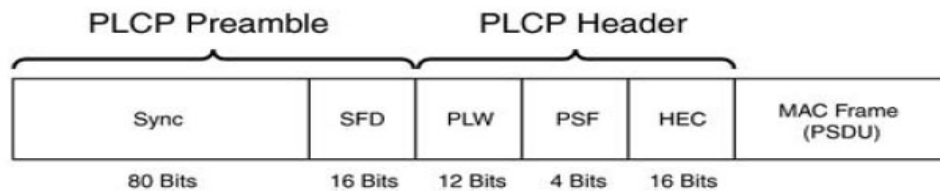
- Βήμα 1 - Αποστέλλεται αίτηση από τον πομπό για επικοινωνία μέσω ενός καναλιού ελέγχου ή μέσω κάποιας προκαθορισμένης συχνότητας.
- Βήμα 2 – Ο δέκτης που λαμβάνει το σήμα απαντά στέλνοντας ένα τυχαίο αριθμό πίσω στον πομπό.
- Βήμα 3 – Ο τυχαίος αριθμός χρησιμοποιείται ως βασική μεταβλητή στο προκαθορισμένο αλγόριθμο για τις συσκευές που θα χρησιμοποιήσουν την τεχνική FHSS, οι οποίες στη συνέχεια θα υπολογίσουν την σειρά των συχνοτήτων που θα χρησιμοποιηθούν σε όλη τη διάρκεια της συνόδου της επικοινωνίας. Πολλές φορές, αυτή η διαδικασία της εναλλαγής της συχνότητας είναι προκαθορισμένη, έτσι ώστε ένας σταθμός να μπορέσει να εξυπηρετήσει έναν συγκεκριμένο αριθμό συνδέσεων επικοινωνίας.
- Βήμα 4 – Ο πομπός στη συνέχεια στέλνει ένα σήμα συγχρονισμού στην πρώτη συχνότητα που έχει υπολογισθεί από την ακολουθία.



- Βήμα 5 - Η σύνοδος της επικοινωνίας μεταξύ του πομπού και του δέκτη ξεκινά και κάθε ένας από αυτούς μετατοπίζει το σήμα του σε συχνότητες συγχρονισμένες με τον άλλο.

### FHSS PLCP Frame Format

Το πλαίσιο FHSS του υποστρώματος του φυσικού επιπέδου παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 3.3: Πλαίσιο PLCP της FHSS για το φυσικό στρώμα του 802.11

Τα πρώτα 144 bits συνθέτουν το **PLCP Preamble** που χρησιμεύει τόσο στον συγχρονισμό μεταξύ πομπού και δέκτη όσο και στην αρχικοποίηση του πλαισίου και αποτελείται από τα επί μέρους:

- *Sync (80 bits)*: Χρησιμοποιείται για τον συγχρονισμό μεταξύ πομπού και δέκτη, καθώς επίσης και για την ανίχνευση του σήματος.
- *SDF (16 bits)*: χρησιμοποιείται κυρίως για την ανίχνευση της αρχής του πλαισίου που μεταδίδεται.

Τα επόμενα 32 bits αποτελούν το **PLCP Header** με τα εξής πεδία:

- *PLW (12 bits)*: φέρει τον αριθμό του μεγέθους των πακέτων που αποστέλλονται.
- *PSF (4 bits)*: δεσμευμένο πεδίο για μελλοντική χρήση.
- *HEC (16 bits)*: χρησιμοποιείται για τον έλεγχο της αξιόπιστης και έγκυρης μετάδοσης των δεδομένων.

### 3.3 IR (Infrared)

Η υπέρυθη ακτινοβολία έχει παρόμοιες ιδιότητες με την ορατή ακτινοβολία. Οι τυπικές επιφάνειες που μπορούμε να βρούμε στους εσωτερικούς χώρους, στους χώρους δηλαδή που εξαπλώνονται τα ασύρματα τοπικά δίκτυα, είναι ανακλαστήρες της ακτινοβολίας αυτής. Μπορούμε λοιπόν να συμπεράνουμε πως η χρήση της υπέρυθρης ακτινοβολίας σε πολλές περιπτώσεις βασίζεται στην ύπαρξη των αντανακλάσεων αυτών προκειμένου να μεταδοθεί η πληροφορία στον δέκτη. Τα εμπόδια όμως αυτά μπορεί να προκαλέσουν εξασθένηση της ενέργειας στην προσπάθεια για τη μετάδοση των δεδομένων, πρόβλημα γνωστό και ως σκίαση (shadowing).

Πέρα από τα φυσικά εμπόδια που υπάρχουν στον χώρο που λειτουργεί το ασύρματο δίκτυο, πρέπει να λαμβάνονται υπόψη και άλλοι παράγοντες όπως είναι οι πηγές φωτισμού. Οι λαμπτήρες φθορισμού ακτινοβολούν στα ίδια μήκη κύματος με την υπέρυθη ακτινοβολία, γεγονός που μπορεί να έχει επιπτώσεις στην απόδοση του συστήματος μιας και λαμβάνεται ως θόρυβος από τις συσκευές που απαρτίζουν το σύστημα.

Τα δύο βασικά ζητήματα που πρέπει να αντιμετωπίσει η υπέρυθη ακτινοβολία, ο θόρυβος δηλαδή και η σκίαση, οδηγούν στην ανάγκη χρήσης οπτικής ισχύος υψηλών επιπέδων. Ωστόσο, η ισχύς του οπτικού πεδίου και η κατανάλωση της ενέργειας από τους σταθμούς είναι προκαθορισμένες από τους διεθνείς κανονισμούς λόγω των επιπτώσεων στην όραση των χρηστών που μπορεί να έχει η εν λόγω δέσμη φωτός. Ως εκ τούτου, τα δεδομένα που πρόκειται να μεταδοθούν θα πρέπει πρώτα να τύχουν επεξεργασίας ώστε να γίνεται επιτρεπτή η ανίχνευσή τους μειώνοντας τα περιθώρια για εμφάνιση θορύβου.

Η υπέρυθη ακτινοβολία βασίζεται στην εκπομπή παλμών διάρκειας 250 ns, καλύπτει αποστάσεις μέχρι και τα 20 μέτρα σε ελεύθερο φυσικό πεδίο και υποστηρίζει δύο ρυθμούς μετάδοσης δεδομένων αυτούς του ενός και των δύο Mbps. Οι προδιαγραφές των δύο αυτών ρυθμών μετάδοσης έχουν σκοπό να επιτρέψουν την ομαλή μελλοντική μετάβαση σε υψηλότερες ταχύτητες μετάδοσης.

Η τεχνική που χρησιμοποιείται στην υπέρυθη ακτινοβολία ονομάζεται **PPM (Pulse Position Modulation)** και είναι αυτή που υποβάλλει το μεταδιδόμενο σήμα

σε επεξεργασία προκειμένου να μειωθεί ο θόρυβος που μπορεί να υπάρξει στο σύστημα.

Για κάθε έναν από τους δύο ρυθμούς μετάδοσης, χρησιμοποιείται με διαφορετικό τρόπο η τεχνική PPM, προκειμένου να εξασφαλιστεί πως ο βασικός παλμός αποστέλλεται τελικά με τον ίδιο τρόπο και στους δύο ρυθμούς μετάδοσης ελαχιστοποιώντας έτσι την πρόσθετη πολυπλοκότητα που εισήγαγε ο ρυθμός μετάδοσης των 2 Mbps.

Η βασική λειτουργία της PPM είναι ουσιαστικά η αλλαγή της θέσης ενός παλμού ώστε να αντιπροσωπεύει διαφορετικά δυαδικά σύμβολα χωρίς να υπάρξει πρόβλημα στο περιεχόμενο του μεταδιδόμενου σήματος εάν ο παλμός μεταφερθεί [17]. Για τον ρυθμό του 1 Mbps χρησιμοποιείται η διαμόρφωση 16-PPM. Κάθε 4 bits πληροφορίας μεταδίδονται με μία από τις 16 πιθανές θέσεις παλμών που χρησιμοποιεί η εν λόγω τεχνική. Κάθε παλμός διαρκεί 250 ns και κάθε ακολουθία από bits που χρησιμοποιείται έχει μόνο ένα από αυτά ίσο με «1» και όλα τα υπόλοιπα έχουν την τιμή «0». Το bit με την τιμή «1» προσδιορίζει τη θέση του παλμού που αντιπροσωπεύει την τετράδα των bits. Για το ρυθμό των 2 Mbps χρησιμοποιείται η 4-PPM κατά την οποία κάθε ζευγάρι από bits μεταδίδεται με μία ακολουθία των τεσσάρων bits αντιπροσωπεύοντας ένα παλμό.

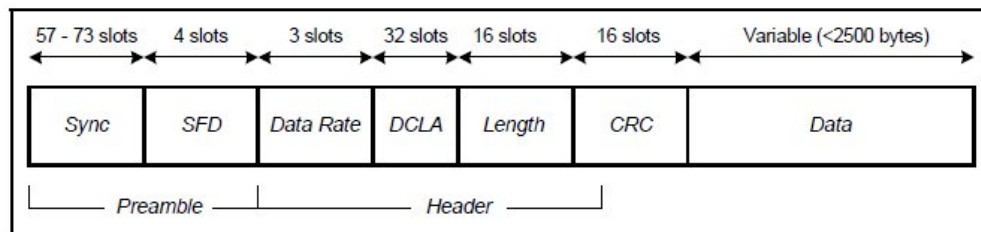
Ορισμένα από τα χαρακτηριστικά της υπέρυθρης ακτινοβολίας στα ασύρματα τοπικά δίκτυα είναι τα εξής [18]:

- Υψηλότερη ασφάλεια: Το υπέρυθρο φως δεν περνάει μέσα από φυσικά εμπόδια, έτσι είναι σχεδόν αδύνατο για ένα μη εξουσιοδοτημένο άτομο που βρίσκεται εκτός φυσικής περιοχής του δικτύου να υποκλέψει τις μεταδιδόμενες πληροφορίες του συστήματος.
- Παρεμβολές συχνοτήτων: επειδή οι υπέρυθρες ακτινοβολίες στα ασύρματα τοπικά δίκτυα λειτουργούν σε χαμηλό φάσμα συχνοτήτων, δεν υπάρχει καμία πιθανότητα παρεμβολής με άλλα συστήματα συχνοτήτων. Στην πράξη, ένα υπέρυθρο ασύρματο τοπικό δίκτυο μπορεί να ικανοποιήσει συγκεκριμένες περιπτώσεις που απαιτείται υψηλό επίπεδο ασφάλειας.

- Περιορισμένο εύρος: η υπέρυθρη ακτινοβολία δεν διαδίδεται μέσα από τοίχους, γεγονός που απαιτεί ένα σημείο πρόσβασης σε κάθε δωμάτιο, όταν απαιτείται κάλυψη σε εγκαταστάσεις με περισσότερα του ενός δωμάτια. Αυτό το γεγονός θα μπορούσε να αυξήσει κατά πολύ το κόστος του συστήματος.

### Infrared frame

Το πλαίσιο της υπέρυθρης ακτινοβολίας στο φυσικό υπόστρωμα για το 802.11 φαίνεται στην παρακάτω εικόνα:



Εικόνα 3.4: Πλαίσιο PLCP της υπέρυθρης ακτινοβολίας για το φυσικό στρώμα του 802.11

Τα πρώτα 61-77 slots συνθέτουν το **PLCP Preamble** που χρησιμεύει τόσο στον συγχρονισμό μεταξύ πομπού και δέκτη όσο και στην αρχικοποίηση του πλαισίου και αποτελείται από τα επί μέρους:

- *Sync (57-73 slots)*: Χρησιμοποιείται κυρίως για τον συγχρονισμό του πομπού με τον δέκτη.
- *SFD (4 slots)*: Χρησιμοποιείται για την υπόδειξη της αρχής του πλαισίου.

Τα επόμενα 67 slots αποτελούν το **PLCP Header** με τα εξής πεδία:

- *DR (3 slots)*: Στο πεδίο αυτό κωδικοποιείται ο ρυθμός μετάδοσης της πληροφορίας.
- *DCLA (32 slots)*: Περιέχει μία ακολουθία από slots επιτρέποντας στον δέκτη να λάβει αποφάσεις σχετικά με την τιμή του κάθε bit.

- *Length (16 slots)*: Περιέχει τον αριθμό του μεγέθους της μεταδιδόμενης πληροφορίας.
- *CRC (16 slots)*: κώδικας προστασίας υπολοίπων πεδίων.

Ακολουθεί το πεδίο της πληροφορίας χωρίς να υπόκεινται σε περιορισμούς σχετικά με το μέγεθός του.

### 3.4 DSSS vs. FHSS

Σε μία προσπάθεια να γίνει η σύγκριση μεταξύ των δύο αυτών τεχνικών θα πρέπει να λάβουμε υπόψη μας πως δεν υπάρχει κακή και καλή τεχνολογία, απλώς υπάρχουν εφαρμογές στις οποίες εφαρμόζεται καλύτερα η μία ή η άλλη τεχνική [19].

Σε γενικές γραμμές, η τεχνική DSSS έχει το πλεονέκτημα να παρέχει υψηλότερη αποδοτικότητα από την FHSS, αλλά είναι μια πολύ ευαίσθητη τεχνολογία που επηρεάζεται από πολλούς περιβαλλοντικούς παράγοντες όπως είναι οι αντανakλάσεις ή οι παρεμβολές. Ο καλύτερος τρόπος για την ελαχιστοποίηση αυτών των επιρροών είναι να χρησιμοποιηθεί η εν λόγω τεχνολογία είτε συνδέοντας ένα σημείο με πολλά σε μικρές αποστάσεις, είτε σε εφαρμογές που επικοινωνούν από μεγάλες αποστάσεις αλλά η τοπολογία τους είναι τέτοια που επιτρέπει τη σύνδεση από ένα συγκεκριμένο σημείο σε ένα άλλο σημείο (point to point).

Στα ασύρματα δίκτυα υπάρχουν προβλήματα που προκαλούνται σε ένα δέκτη από τους γειτονικούς του πομπούς. Για παράδειγμα τα σήματα ενός γειτονικού ραδιοπομπού μπορούν να ληφθούν από τον δέκτη του συστήματος που μας αφορά σε υψηλότερα επίπεδα ενέργειας. Αυτό μπορεί να έχει ως αποτέλεσμα την αδυναμία του δέκτη να αντιληφθεί και να λάβει τα μηνύματα που προορίζονται για αυτόν από τον αντίστοιχο πομπό. Στην DSSS το πρόβλημα αυτό είναι ιδιαίτερα σημαντικό όμως εάν ο πομπός και ο δέκτης λειτουργούν βάσει της FHSS, το χειρότερο σενάριο θα ήταν να μπλοκαριστούν ορισμένες αναπηδήσεις στη μετάδοση του μηνύματος και να μειωθεί η απόδοση του συστήματος.

Στις τυπικές εφαρμογές της τεχνικής DSSS συμπεριλαμβάνονται τα εσωτερικά ασύρματα τοπικά δίκτυα σε γραφεία , οι συνδέσεις από κτίριο σε κτίριο κλπ.

Από την άλλη πλευρά, η FHSS είναι μια πολύ ισχυρή τεχνολογία, με μικρή επιρροή από θορύβους, αντανάκλασεις, ραδιοφωνικούς σταθμούς ή άλλους παράγοντες του περιβάλλοντος. Επιπλέον, ο αριθμός των ταυτόχρονων ενεργών συστημάτων στην ίδια γεωγραφική περιοχή είναι σημαντικά μεγαλύτερος από τον αντίστοιχο αριθμό στα DSSS συστήματα.

Τα παραπάνω χαρακτηριστικά κάνουν την FHSS την τεχνολογία που θα επιλεγεί για τις εγκαταστάσεις που έχουν σχεδιαστεί για να καλύψουν μεγάλες αποστάσεις όπου απαιτείται ένας μεγάλος αριθμός συστημάτων και όπου η χρήση των κατευθυντικών κεραιών είναι αδύνατη λόγω φυσικών εμποδίων.

Στις τυπικές εφαρμογές για την τεχνική FHSS περιλαμβάνεται και η ασύρματη ευρυζωνική πρόσβαση **BWA (Broadband Wireless Access)**, όπου η χρήση της DSSS είναι σχεδόν αδύνατη, λόγω των περιορισμών που αφορούν στην μικρή γεωγραφική απόσταση μεταξύ των συσκευών.

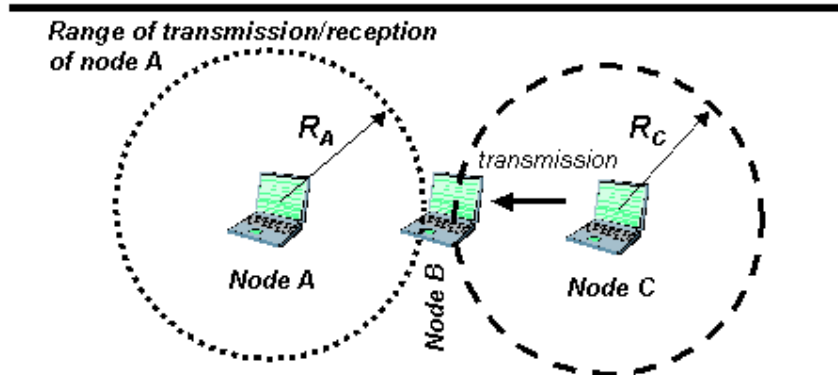
## 4. 802.11 MAC Layer

Η λειτουργία του υποστρώματος MAC στοχεύει κυρίως στον τρόπο πρόσβασης των σταθμών του δικτύου στο ασύρματο μέσο προκειμένου να σταλούν τα πλαίσια δεδομένων, στην ανίχνευση των λαθών που μπορεί να προκύψουν κατά την μετάδοση και στην προσχώρηση των σταθμών στο δίκτυο, παρέχοντας ταυτόχρονα λειτουργίες όπως είναι η ασφάλεια της μετάδοσης και η αυθεντικοποίηση των χρηστών. Για την επίτευξη των εν λόγω στόχων, χρησιμοποιούνται βασικές μέθοδοι και μετρητές που θα αναπτυχθούν παρακάτω.

Εξαιτίας της ασύρματης φύσης του δικτύου, εμφανίζονται προβλήματα όπως η πιθανότητα να βγει ένας κόμβος εκτός περιοχής κάλυψης του δικτύου και η ύπαρξη των κρυμμένων κόμβων [20].

Πιο συγκεκριμένα, το πρόβλημα του κρυμμένου κόμβου (*hidden node problem*) περιγράφει την κατάσταση κατά την οποία ένας σταθμός του δικτύου δεν βρίσκεται εντός της εμβέλειας μετάδοσης ενός άλλου σταθμού του ίδιου δικτύου και ενώ ο δεύτερος μεταδίδει τις πληροφορίες του σε κάποιον άλλο σταθμό, ο πρώτος δεν είναι σε θέση να τις ανιχνεύσει λόγω της απόστασης που μεσολαβεί μεταξύ των δύο αυτών σταθμών. Ο πρώτος σταθμός ξεκινά την μετάδοση των δικών του δεδομένων και λόγω της αδυναμίας του δεύτερου να ακούσει την εν λόγω μετάδοση, υπάρχει περίπτωση να ξεκινήσει να μεταδίδει κι αυτός ταυτόχρονα τα δεδομένα του, γεγονός που οδηγεί στην εμφάνιση συγκρούσεων των πλαισίων δεδομένων. Οι συγκρούσεις αυτές έχουν ως αποτέλεσμα τη μείωση της αποδοτικότητας του δικτύου μιας και υπάρχουν πλαίσια δεδομένων που πρέπει εκ νέου να μεταδοθούν. Στην παρακάτω εικόνα φαίνεται το πρόβλημα του κρυμμένου κόμβου χρησιμοποιώντας τρεις σταθμούς του ίδιου δικτύου που προσπαθούν να μεταδώσουν τα δεδομένα τους και αναπόφευκτα εμφανίζονται συγκρούσεις στα δεδομένα λόγω της αδυναμίας μερικών από αυτούς να ανιχνεύσουν την οποιαδήποτε κίνηση στο εν λόγω δίκτυο κυρίως λόγω της απομακρυσμένης θέσης στην οποία βρίσκονται.

## Hidden Node Problem



Εικόνα 4.1: Το πρόβλημα του κρυμμένου κόμβου.

Ο σταθμός C βρίσκεται σε επικοινωνία με τον σταθμό B στέλνοντάς του τα δεδομένα του. Ο σταθμός A θέλει κι αυτός με τη σειρά του να στείλει τις πληροφορίες του στον σταθμό B αλλά παρόλο που γνωρίζει πότε ο σταθμός B στέλνει τα δεδομένα του κι αυτό γιατί βρίσκεται εντός της εμβέλειάς του, δε μπορεί να γνωρίζει πότε λαμβάνει δεδομένα από κάποιον άλλο σταθμό που βρίσκεται αρκετά μακριά του και δεν μπορεί να ανιχνεύσει την οποιαδήποτε μετάδοση δεδομένων. Έτσι, ο σταθμός A μη γνωρίζοντας πως βρίσκεται σε εξέλιξη η αποστολή των δεδομένων από τον σταθμό C στον σταθμό B, ξεκινάει να αποστείλει και αυτός τα δεδομένα του στον σταθμό B, προκαλώντας συγκρούσεις των δεδομένων με αποτέλεσμα να μειώνεται η απόδοση του δικτύου μιας και οι πληροφορίες αυτές θα πρέπει να μεταδοθούν εκ νέου και από τους δύο σταθμούς.

Ένας μηχανισμός που χρησιμοποιείται για να ξεπεραστεί το πρόβλημα του κρυμμένου κόμβου είναι η χρήση του διανύσματος κατανομής του δικτύου **NAV (Network Allocation Vector)** που θα αναλυθεί παρακάτω. Γενικά, κάθε πλαίσιο του υποστρώματος MAC περιλαμβάνει ένα πεδίο, αυτό της διάρκειας, που χρησιμοποιείται ώστε να ενημερώσει τους μετρητές NAV όλων σταθμών του δικτύου και όχι μόνο του σταθμού για τον οποίο προορίζεται το πλαίσιο που είναι σε κατάσταση μετάδοσης. Το πεδίο της διάρκειας καταγράφει τη χρονική περίοδο που απαιτείται για να αποσταλεί το πλαίσιο στον παραλήπτη του. Κατ' αυτόν τον τρόπο όλοι οι σταθμοί του δικτύου ενημερώνονται είτε από τον ίδιο

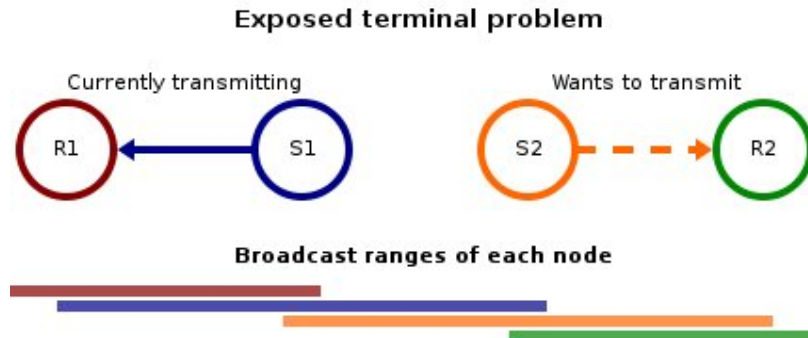


τον αποστολέα είτε από τους γειτονικούς τους σταθμούς, πως για ένα συγκεκριμένο χρονικό διάστημα δεν είναι σε θέση να προσπαθήσουν να μεταδώσουν τα δεδομένα τους όσο μακριά κι αν βρίσκεται ο ένας από τον άλλο μιας και γνωρίζουν πως μία μετάδοση βρίσκεται σε εξέλιξη ακόμα κι αν δεν μπορούν να την ανιχνεύσουν.

Για την προστασία της μετάδοσης των δεδομένων ενός σταθμού από πιθανές συγκρούσεις που μπορεί να προκληθούν από τους κρυμμένους κόμβους, χρησιμοποιείται και η ανταλλαγή μηνυμάτων **RTS (Request To Send)** και **CTS (Clear To Send)** μεταξύ του πομπού και του δέκτη, τα οποία λαμβάνονται εξίσου και από τους υπόλοιπους σταθμούς του δικτύου. Μέσω της αποστολής ενός μηνύματος RTS ο πομπός ζητάει την άδεια από τον δέκτη να αποστείλει τα δεδομένα του, και ο δέκτης με τη σειρά του απαντάει στέλνοντάς του ένα μήνυμα CTS ενημερώνοντάς τον για να ξεκινήσει την αποστολή. Σε αυτή την περίπτωση, η πιθανότητα να υπάρξουν συγκρούσεις μεταξύ των πλαισίων δεδομένων εμφανίζεται μόνο κατά την αποστολή ενός μηνύματος RTS. Εάν υπάρξει σύγκρουση, αυτή θα ανιχνευθεί σχετικά γρήγορα κι αυτό γιατί ο αποστολέας δε θα λάβει ποτέ την έγκριση του δέκτη για τη μετάδοση των δεδομένων του (CTS). Επίσης, η αποστολή εκ νέου ενός μηνύματος RTS είναι πολύ πιο γρήγορη και έχει λιγότερες επιπτώσεις στην απόδοση του δικτύου από την δεύτερη αποστολή ενός πλαισίου δεδομένων.

Τέλος, για την αποφυγή του προβλήματος του κρυμμένου κόμβου χρησιμοποιούνται και κάποιοι μετρητές όπως ο **EIFS (Extended Inter-Frame Space)** που θα αναλυθεί παρακάτω με τους υπόλοιπους μετρητές που χρησιμοποιούνται από το MAC υπόστρωμα. Ο μετρητής αυτός χρησιμοποιείται από τον δέκτη του πλαισίου στην περίπτωση που αυτός δεν μπορεί να κατανοήσει το περιεχόμενο του, το οποίο και έχει καταστραφεί λόγω κάποιων συγκρούσεων που συνέβησαν κατά την μετάδοσή του. Με τη χρήση του μετρητή, ο δέκτης περιμένει ένα συγκεκριμένο χρονικό διάστημα ώστε να μην υπάρξουν συγκρούσεις με άλλες μεταδόσεις που υφίστανται εκείνη τη στιγμή, για να ενημερώσει τον αποστολέα ότι πρέπει να ξαναστείλει το εν λόγω πλαίσιο.

Για την περιγραφή του προβλήματος του εκτεθειμένου κόμβου θα χρησιμοποιήσουμε ένα ασύρματο δίκτυο με τέσσερις σταθμούς όπως φαίνεται στην παρακάτω εικόνα.



Εικόνα 4.2: Το πρόβλημα του εκτεθειμένου κόμβου.

Ας υποθέσουμε πως έχουμε ένα δίκτυο με τέσσερις σταθμούς, τους R1,S1,S2 και R2. Οι δύο δέκτες R1 και R2 βρίσκονται εκτός της εμβέλειας του ενός από τον άλλο. Από την άλλη, οι δύο πομποί S1 και S2 βρισκόμενοι εντός εμβέλειας μπορούν να ανιχνεύσουν τυχόν μεταδόσεις του ενός ή του άλλου. Στην περίπτωση που ο σταθμός S1 επικοινωνεί με τον σταθμό R1 αποστέλλοντάς του τα δεδομένα του, ο σταθμός S2 δεν είναι σε θέση να αποστείλει τα δικά του δεδομένα στον σταθμό R2 διότι ανιχνεύει μία κίνηση στο δίκτυο από τον γειτονικό του σταθμό S1 και θέλει να αποφύγει τις πιθανές συγκρούσεις με αυτόν. Παρόλα αυτά, ο σταθμός S2 θα μπορούσε να αποστείλει τα δεδομένα του στον R2 χωρίς να υπάρξει πιθανότητα σύγκρουσης πλαισίων με τον S1 αφού ο τελευταίος βρίσκεται εκτός εμβέλειας του R2. Σε αυτή την περίπτωση λέμε πως ο σταθμός S2 είναι ο εκτεθειμένος κόμβος (**exposed node problem**).

Ο μηχανισμός RTS/CTS χρησιμοποιείται και στην περίπτωση του εκτεθειμένου κόμβου προκειμένου να αποφευχθούν πιθανές συγκρούσεις, με τον ίδιο τρόπο που χρησιμοποιείται και στο πρόβλημα του κρυμμένου κόμβου. Ουσιαστικά, ζητείται η άδεια από τον αποστολέα για τη μετάδοση των δεδομένων του η οποία και του παραχωρείται από τον δέκτη, διαδικασία που γίνεται γνωστή σε όλους τους σταθμούς του δικτύου αποτρέποντάς τους από την ταυτόχρονη αποστολή των δεδομένων τους.

Για να αντιμετωπιστούν τυχόν προβλήματα στην μετάδοση των δεδομένων, το υπόστρωμα MAC του 802.11 χρησιμοποιεί κατάλληλους μηχανισμούς. Ο βασικός μηχανισμός πρόσβασης στο ασύρματο μέσο είναι ο **DCF (Distributed Coordination Function)**, ενώ προαιρετικά μπορούν να χρησιμοποιηθούν και άλλοι μηχανισμοί πρόσβασης όπως ο **PCF (Point Coordination Function)**.

Στην τεχνική DCF, όταν ένας σταθμός θέλει να μεταδώσει τα δεδομένα του θα πρέπει να περιμένει για ένα συγκεκριμένο χρονικό διάστημα μέχρι να ανιχνεύσει πως το ασύρματο μέσο είναι διαθέσιμο για μετάδοση, κι αυτό διότι για την κατοχή και τη χρήση του μέσου ανταγωνίζονται όλοι οι σταθμοί που απαρτίζουν το δίκτυο.

Η τεχνική PCF χρησιμοποιείται σε συνδυασμό με την DCF σε περιπτώσεις όπου δεν υπάρχει ανταγωνισμός μεταξύ των σταθμών του δικτύου για τη χρήση του μέσου, τεχνική που επιτυγχάνεται με τη χρήση κατάλληλων μετρητών χρόνου.

Όπως και το πρωτόκολλο των ενσύρματων δικτύων (Ethernet), έτσι και το 802.11 χρησιμοποιεί τη μέθοδο πολλαπλής πρόσβασης στο μέσο ανιχνεύοντας το φέρον σήμα **CSMA (Carrier Sense Multiple Access)** για να προσπελάσει το ασύρματο μέσο με μία βασική διαφορά. Αντί της τεχνικής ανίχνευσης συγκρούσεων **CSMA/CD (Carrier Sense Multiple Access/ Collision Detection)**, χρησιμοποιείται η τεχνική αποφυγής συγκρούσεων **CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)**.

Συνήθως, για να αποφευχθούν τα προβλήματα που παρουσιάζονται στα ασύρματα δίκτυα, η τεχνική αποφυγής συγκρούσεων CA συνδυάζεται με μηνύματα θετικής επιβεβαίωσης (**positive acknowledgments**). Ο σταθμός που θέλει να μεταδώσει θα πρέπει πρώτα να ανιχνεύσει το μέσο. Στην περίπτωση που το ανιχνεύσει διαθέσιμο, ο σταθμός θα πρέπει να περιμένει για ένα συγκεκριμένο χρονικό διάστημα, ίσο με έναν μετρητή που χρησιμοποιείται (DIFS), ο οποίος και θα αναλυθεί παρακάτω. Μόλις παρέλθει το χρονικό αυτό διάστημα, ο σταθμός είναι σε θέση να αποστείλει τα δεδομένα του κάνοντας χρήση του ασύρματου μέσου. Εάν το μέσο ανιχνευθεί κατειλημμένο, ο σταθμός συνεχίζει να το ανιχνεύει μέχρι να το βρει διαθέσιμο. Όταν το βρει διαθέσιμο θα πρέπει να περιμένει ένα χρονικό διάστημα και να εκτελέσει έναν αλγόριθμο οπισθοχώρησης (**exponential**

**backoff algorithm**) [21]. Μόλις παρέλθει το διάστημα οπισθοχώρησης και ο μετρητής του φτάσει στο «0», ο σταθμός είναι σε θέση να καταλάβει το μέσο και να προχωρήσει στη μετάδοση των δεδομένων του.

Ο αλγόριθμος οπισθοχώρησης χρησιμοποιείται για να αντιμετωπίσει προβλήματα ανταγωνισμού μεταξύ των σταθμών ενός δικτύου που θέλουν να μεταδώσουν ταυτόχρονα τα δεδομένα τους. Όταν ένας σταθμός εκτελεί τον αλγόριθμο οπισθοχώρησης θα πρέπει να περιμένει για ένα επιπλέον χρονικό διάστημα τυχαία επιλεγμένο που αποτελείται από διαστήματα χρόνου ή αλλιώς χρονοθυρίδες (**time slots**). Ο αριθμός των time slots που επιλέγονται κατά τη διαδικασία οπισθοχώρησης θα πρέπει να είναι μεγαλύτερος του μηδενός και μικρότερος από το μέγιστο μήκος που μπορεί να πάρει το παράθυρο ανταγωνισμού ή αλλιώς **contention window**. Κατά τη διάρκεια της αναμονής, ο σταθμός συνεχίζει να ανιχνεύει το μέσο μέχρι να το βρει διαθέσιμο. Όταν παρέλθει το χρονικό διάστημα που χρησιμοποιείται από τον μετρητή και εάν το μέσο είναι ακόμα διαθέσιμο, τότε ο σταθμός μπορεί να μεταδώσει τα δεδομένα του. Εάν όμως κατά τη διάρκεια της χρήσης του παραθύρου αναμονής, συμβεί άλλη μετάδοση από κάποιον άλλο σταθμό του δικτύου, ο μετρητής της διαδικασίας οπισθοχώρησης σταματά και ενεργοποιείται ξανά όταν το μέσο ανιχνευθεί ως διαθέσιμο. Όταν ο μετρητής αυτός φτάσει στην τιμή «0», είναι η σειρά του εν λόγω σταθμού να μεταδώσει τα δεδομένα του.

Το μέγεθος του παραθύρου είναι πολύ σημαντικός παράγοντας και μπορεί να αλλάξει με βάση τις συνθήκες του δικτύου. Εάν το παράθυρο είναι μικρό, υπάρχει αυξημένη πιθανότητα δύο ή και περισσότεροι σταθμοί να έχουν τον ίδιο αριθμό από time slots για οπισθοχώρηση και να προσπαθήσουν να μεταδώσουν ταυτόχρονα. Αν το παράθυρο είναι πολύ μεγάλο, οι σταθμοί μπορεί να είναι αδρανείς και να περιμένουν για ένα μεγάλο χρονικό διάστημα πριν ξεκινήσουν τη διαδικασία της μετάδοσης μειώνοντας έτσι το ποσοστό αξιοποίησης του συστήματος. Στον παρακάτω πίνακα φαίνονται οι μέγιστες αλλά και οι ελάχιστες τιμές του παραθύρου ανταγωνισμού για τα δύο φυσικά επίπεδα DSSS και FHSS που αναλύθηκαν στο προηγούμενο κεφάλαιο.

Φυσικό επίπεδο	CWmin (slots)	CWmax (slots)
DSSS	31	1023
FHSS	15	1023

Πίνακας 4.1: Μέγιστες και ελάχιστες τιμές του παραθύρου ανταγωνισμού

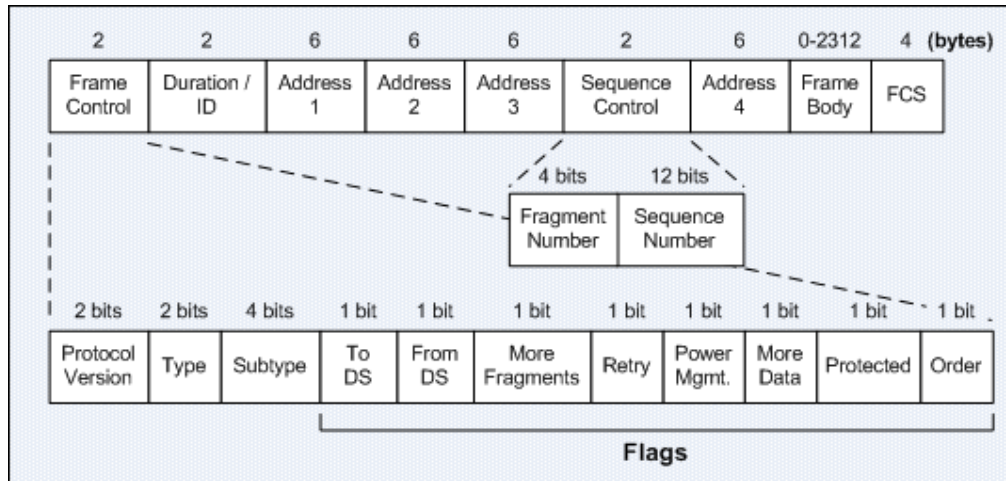
## 4.1 802.11 Frame

Στο υπόστρωμα MAC του 802.11 πρωτοκόλλου χρησιμοποιούνται τρία διαφορετικά πλαίσια, ανάλογα πάντα με τον σκοπό που εξυπηρετούν. Οι τρεις αυτές κατηγορίες είναι οι εξής:

- **Control frames:** τα πλαίσια ελέγχου χρησιμοποιούνται για να εξυπηρετήσουν την μετάδοση των δεδομένων από έναν σταθμό σε κάποιον άλλο. Τα control frames είναι τα μηνύματα που ζητούν άδεια αποστολής δεδομένων RTS, τα μηνύματα που αποδέχονται την αποστολή CTS και τα μηνύματα επιβεβαίωσης ορθής λήψης των δεδομένων ACK.
- **Management frames:** τα πλαίσια διαχείρισης ενεργοποιούν τους σταθμούς προκειμένου να αρχικοποιήσουν και να διατηρήσουν την επικοινωνία με τους άλλους σταθμούς του δικτύου. Μία από τις μορφές του είναι τα μηνύματα πιστοποίησης που στέλνει ένας σταθμός σε ένα AP προκειμένου να του επιτραπεί η ασφαλής επικοινωνία με αυτό στέλνοντας συνήθως στο AP τον κωδικό πρόσβασης στο δίκτυο. Αντίστοιχα υπάρχουν και μηνύματα τερματισμού πιστοποίησης που τερματίζουν την ασφαλή επικοινωνία μεταξύ δύο σταθμών. Στις μορφές αυτού του πλαισίου συμπεριλαμβάνονται τα μηνύματα εγκαθίδρυσης επικοινωνίας ενός σταθμού με το AP αλλά και ο τερματισμός της αντίστοιχα.
- **Data frames:** είναι τα πλαίσια που περιέχουν τα δεδομένα που ανταλλάσσουν οι σταθμοί μεταξύ τους.

Οι τρεις αυτοί τύποι πλαισίων βασίζονται στη γενική μορφή του πλαισίου του 802.11 πρωτοκόλλου και οι διαφοροποιήσεις τους παρατηρούνται σε ορισμένα από τα πεδία του προκειμένου να επιτευχθεί ο σκοπός για τον οποίο

χρησιμοποιούνται. Η γενική μορφή του πλαισίου φαίνεται στην παρακάτω εικόνα και τα επιμέρους πεδία του αναλύονται παρακάτω [22].



Εικόνα 4.3 : Η γενική μορφή του πλαισίου του υποστρώματος MAC.

- **Frame Control (16 bits):** Το πεδίο ελέγχου αποτελείται από 11 επιμέρους πεδία [23] :

*Protocol version (2 bits):* Το πεδίο αυτό προσδιορίζει την έκδοση του πρωτοκόλλου 802.11.

*Type (2 bits):* Προσδιορίζει τον τύπο του πλαισίου που μπορεί να είναι ελέγχου, διαχείρισης και δεδομένων.

*Subtype (4 bits):* Το πεδίο αυτό είναι συμπληρωματικό του πεδίου type και προσδιορίζει την ακριβή μορφή του τύπου του πλαισίου όπως είναι τα RTS, CTS και τα ACK για τα πλαίσια ελέγχου, τα data, CF-Poll, CF-Ack κτλ για τα πλαίσια δεδομένων και τα association, disassociation, authentication και deauthentication για τα πλαίσια διαχείρισης.

*To DS (1 bit):* Προσδιορίζει εάν το πλαίσιο θα μεταδοθεί σε ένα δίκτυο υποδομής όταν η τιμή του είναι «1» ή σε ένα ad-hoc δίκτυο όταν η τιμή του είναι «0».

*From DS (1 bit)*: Προσδιορίζει εάν το πλαίσιο μεταδίδεται από ένα δίκτυο υποδομής (DS=1) ή όχι (DS=0).

*More fragments (1 bit)*: Το πεδίο αυτό προσδιορίζει εάν το πλαίσιο διαχείρισης μεταδίδεται αυτούσιο ή εάν ο παραλήπτης θα πρέπει να περιμένει την αποστολή των επιμέρους τμημάτων του.

*Retry (1 bit)*: Το πεδίο αυτό ενημερώνει τον παραλήπτη εάν το συγκεκριμένο πλαίσιο έχει μεταδοθεί ξανά για να μπορέσει να το απορρίψει.

*Power Management (1 bit)*: Προσδιορίζει την κατάσταση λειτουργίας του σταθμού. Εάν η τιμή είναι «1» σημαίνει πως ο σταθμός βρίσκεται σε κατάσταση αναμονής, ενώ αν είναι «0» τότε ο σταθμός είναι ενεργός. Τα AP βρίσκονται πάντα σε ενεργή κατάσταση.

*More Data (1 bit)*: Όταν το πεδίο αυτό έχει την τιμή «1» σημαίνει πως ο παραλήπτης πρόκειται να λάβει περισσότερα πλαίσια που προορίζονται για αυτόν και είναι προσωρινά αποθηκευμένα στο AP.

*Protected (1 bit)*: Το πεδίο αυτό συναντάται και ως WEP (από την ισοδύναμη μορφή ασφαλείας της ενσύρματης επικοινωνίας) για να ενημερώσει αν χρησιμοποιείται η κρυπτογράφηση ή όχι των δεδομένων.

*Order (1 bit)*: Το πεδίο αυτό έχει την τιμή «1» όταν πρέπει να κρατείται η σειρά που αποστέλλονται και λαμβάνονται τα πλαίσια.

- ***Duration/ID (16 bits)***: Το πεδίο αυτό χρησιμοποιείται με διάφορους τρόπους ανάλογα με τον σκοπό που πρόκειται να εξυπηρετήσει. Εάν το τελευταίο του bit έχει την τιμή «0» τότε χρησιμοποιείται για να καθορίσει τον μετρητή NAV που προσδιορίζει την χρονική διάρκεια που απαιτείται για να μεταδοθεί το τρέχον πλαίσιο. Εάν τα δύο τελευταία του bits έχουν τις τιμές «0» και «1» αντίστοιχα σημαίνει πως η πρόσβαση στο δίκτυο γίνεται από τους σταθμούς χωρίς να ανταγωνιστούν μεταξύ τους. Εάν τα δύο τελευταία του bits έχουν την τιμή «0» σημαίνει πως ο σταθμός βρισκόταν σε κατάσταση αναμονής και τώρα που είναι ενεργός ζητάει από το AP να τον

ενημερώσει εάν υπάρχουν προσωρινά αποθηκευμένα πλαίσια στο AP που προορίζονται για αυτόν.

- **Address 1, 2, 3 και 4 (από 48 bits):** Τα πεδία των διευθύνσεων χρησιμοποιούνται με διαφορετικό τρόπο ανάλογα πάντα με τον τύπο του πλαισίου. Γενικώς η πρώτη διεύθυνση προσδιορίζει τον παραλήπτη, η δεύτερη τον αποστολέα και η τρίτη χρησιμοποιείται από τον παραλήπτη για τεχνικές φιλτραρίσματος ενώ η τέταρτη είναι προαιρετική. Εάν το πρώτο bit της διεύθυνσης έχει την τιμή «0» τότε προορίζεται για έναν σταθμό του δικτύου (unicast), εάν έχει την τιμή «1» προορίζεται για μία ομάδα σταθμών στο δίκτυο (multicast) και τέλος εάν όλα του τα bits έχουν την τιμή «1» το πλαίσιο προορίζεται για όλους τους σταθμούς του δικτύου (broadcast).
- **Sequence (16 bits):** Το πεδίο αυτό αποτελείται από τα επιμέρους πεδία *Fragment Number (4 bits)* που χρησιμοποιείται για να ενημερώσει εάν το πλαίσιο μεταδίδεται αυτούσιο ή χωρίζεται σε τμήματα και το *sequence number (12 bits)* που χρησιμοποιείται για να ενημερώσει για τον αριθμό του πλαισίου όταν κρατείται η σειρά της μετάδοσής τους.
- **Frame body (0 – 18,496 bits):** Είναι το πεδίο που περιέχει την καθαρή πληροφορία που πρόκειται να μεταδοθεί από τον αποστολέα στον παραλήπτη.
- **FCS (32 bits):** Αναφέρεται στον κυκλικό έλεγχο πλεονασμού (CRC) και χρησιμοποιείται για να αποδειχθεί η ακεραιότητα των δεδομένων όλων των υπολοίπων πεδίων.

## 4.2 Σχετικά με τους μετρητές των μεθόδων

Στο 802.11 χρησιμοποιούνται διάφοροι μετρητές χρονικών διαστημάτων προκειμένου να επιτευχθεί η αποστολή και η λήψη των πλαισίων δεδομένων [24]. Οι τιμές των διαστημάτων αυτών καθορίζονται από το φυσικό στρώμα, παραμένουν αμετάβλητες και είναι ανεξάρτητες από τον ρυθμό μετάδοσης που χρησιμοποιείται.



Ο χρόνος που μεσολαβεί μεταξύ των μεταδιδόμενων από ένα σταθμό, πλαισίων ονομάζεται **IFS (InterFrame Spacing)** και χωρίζεται στις εξής κατηγορίες:

- **SIFS (Short InterFrame Space):** Το SIFS χρησιμοποιείται κυρίως στην αποστολή των ACK (Acknowledgement) που είναι τα πλαίσια επιβεβαίωσης λήψης δεδομένων από τον δέκτη στον πομπό και στην αποστολή των CTS (Clear To Send) πλαισίων που επιτρέπουν στον δέκτη να ξεκινήσει την διαδικασία μετάδοσης των δεδομένων του. Έχει τη μικρότερη διάρκεια από όλους τους υπόλοιπους μετρητές δίνοντας έτσι στον σταθμό την υψηλότερη προτεραιότητα για μετάδοση δεδομένων, αναγκάζοντας όλους τους υπόλοιπους σταθμούς που χρησιμοποιούν μεγαλύτερους μετρητές να περιμένουν την ολοκλήρωση της αποστολής του πρώτου για να μεταδώσουν τα δικά τους πλαίσια.

Ο SIFS χρόνος που απαιτείται σε κάθε μία προδιαγραφή του 802.11 φαίνεται στον παρακάτω πίνακα:

Standards	SIFS (μs)
802.11b	10
802.11a	16
802.11g	10

Πίνακας 4.2: Χρονική διάρκεια του SIFS

- **PIFS (PCF InterFrame Space):** Το PIFS χρησιμοποιείται από τους σταθμούς που συμμετέχουν στην PCF τεχνική, προκειμένου να λάβουν προτεραιότητα για την κατοχή του ώστε να μεταδώσουν τα πλαίσιά τους. Συνήθως, αυτός ο μετρητής χρησιμοποιείται από τα AP ώστε να έχουν προτεραιότητα στην κατοχή και τη χρήση του μέσου πριν προλάβει κάποιος από τους σταθμούς του δικτύου να το καταλάβει. Η τιμή του PIFS υπολογίζεται βάσει του τύπου:

$$PIFS = 1 \text{ Slot Time} + SIFS$$

Ο PIFS χρόνος που απαιτείται σε κάθε μία προδιαγραφή του 802.11 φαίνεται στον παρακάτω πίνακα:

Standards	Slot time (μs)	PIFS (μs)
802.11b	20	30
802.11a	9	25
802.11g	9 ή 20	19 ή 30

Πίνακας 4.3: Χρονική διάρκεια του PIFS

- DIFS (DCF InterFrame Space):** Το χρονικό αυτό διάστημα χρησιμοποιείται στην βασική μέθοδο πρόσβασης στο μέσο, DCF. Όπως ειπώθηκε προηγουμένως, ο σταθμός που θέλει να μεταδώσει θα πρέπει να ανιχνεύσει το μέσο πριν ξεκινήσει τη μετάδοση των πλαισίων του. Αν το μέσο παραμένει αδρανές για διάστημα ίσο με τον DIFS τότε και μόνο τότε ο σταθμός θα μπορέσει να ξεκινήσει τη διαδικασία της μετάδοσης. Αν όχι, τότε ο σταθμός θα πρέπει να περιμένει εκτελώντας τον exponential backoff αλγόριθμο μέχρι το μέσο να ανιχνευτεί ως αδρανές. Η τιμή του DIFS υπολογίζεται με βάση τον τύπο:

$$DIFS = SIFS + (2 * Slot\ time)$$

Ο DIFS χρόνος που απαιτείται σε κάθε μία προδιαγραφή του 802.11 φαίνεται στον παρακάτω πίνακα:

Standards	Slot time (μs)	PIFS (μs)
802.11b	20	50
802.11a	9	34
802.11g	9 ή 20	28 ή 50

Πίνακας 4.4: Χρονική διάρκεια του DIFS

- EIFS (Extended InterFrame Space):** Είναι ο μεγαλύτερος σε τιμή μετρητής και χρησιμοποιείται σε συγκεκριμένες μόνο περιπτώσεις. Στην περίπτωση που το πλαίσιο που μεταδόθηκε περιέχει σφάλματα που αναγνωρίστηκαν από την τεχνική **FCS (Frame Check Sequence)** και ο δέκτης δεν μπορεί να το καταλάβει είτε στην περίπτωση που το μήνυμα επιβεβαίωσης ACK από τον δέκτη στον πομπό για την ενημέρωση ορθής λήψης του πλαισίου, δεν

έχει παραληφθεί λόγω συγκρούσεων στο δίκτυο, χρησιμοποιείται ο μετρητής EIFS. Έχει τη χαμηλότερη προτεραιότητα από όλους τους υπόλοιπους μετρητές, άρα και τη μεγαλύτερη διάρκεια διότι ο δέκτης μιας και δεν γνωρίζει το λόγο που έλαβε ένα πλαίσιο που δεν μπορεί να αναγνωρίσει, θα πρέπει να περιμένει ένα αρκετά μεγάλο χρονικό διάστημα για να αναφέρει το γεγονός ώστε να αποφύγει τη σύγκρουση με κάποιο άλλο πλαίσιο που μεταδίδεται εκείνη τη στιγμή στο δίκτυο.

Ο EIFS χρόνος υπολογίζεται βάσει του τύπου:

$$\mathbf{EIFS = Transmission\ time\ of\ ACK\ frame\ at\ lowest\ basic\ rate + SIFS + DIFS}$$

Τέλος, μία άλλη εναλλακτική λύση που χρησιμοποιείται για να ενημερώσει όλους τους σταθμούς του συστήματος για πόσο χρονικό διάστημα θα είναι κατειλημμένο το μέσο, είναι το διάνυσμα κατανομής δικτύου NAV (Network Allocation Vector). Κάθε πλαίσιο που αποστέλλεται μέσα στο δίκτυο περιέχει ένα πεδίο (duration field) που αναφέρεται στο χρονικό διάστημα που θα χρειαστεί προκειμένου να μεταφερθεί το συγκεκριμένο πλαίσιο στον παραλήπτη του. Οι σταθμοί που ανιχνεύουν το μέσο για τη διαθεσιμότητά του, θα λάβουν αυτό το πλαίσιο και θα κοιτάξουν μέσα στο πεδίο της διάρκειας το χρονικό διάστημα κατά το οποίο το μέσο θα είναι κατειλημμένο. Θέτουν λοιπόν στον μετρητή NAV στην τιμή που έχουν διαβάσει από το πεδίο της διάρκειας και μόνο όταν αυτός φτάσει στο μηδέν και περιμένει για ένα επιπλέον χρονικό διάστημα ίσο με το DIFS θα μπορέσει να λάβει μέρος στη διαδικασία ανταγωνισμού με τους άλλους σταθμούς για την κατοχή του μέσου.

Με τη χρήση του NAV, όλοι οι σταθμοί γνωρίζουν ότι δεν υπάρχει ανάγκη να ελέγξουν τη διαθεσιμότητά του μέσου τουλάχιστον για το χρονικό διάστημα που υποδεικνύεται από τον NAV. Ένα από τα μεγαλύτερα πλεονεκτήματα της χρήσης του NAV είναι πως μειώνει σημαντικά την κατανάλωση ενέργειας από τους σταθμούς του δικτύου αφού δεν υπάρχει ανάγκη να προχωρήσουν σε διαδικασίες ανίχνευσης αδρανούς καναλιού για ένα συγκεκριμένο χρονικό διάστημα.

Το διάνυσμα κατανομής δικτύου είναι μια από τις βασικές μεθόδους που υλοποιούνται κατά την ανίχνευση σήματος στο δίκτυο από τους σταθμούς που το απαρτίζουν. Χρησιμοποιείται και στις δύο μεθόδους πρόσβασης που αναφέρθηκαν, DCF και PCF.

### **Τρόποι πρόσβασης στο ασύρματο μέσο**

Όπως αναφέρθηκε και νωρίτερα, δύο είναι οι βασικοί τρόποι πρόσβασης ενός σταθμού στο ασύρματο μέσο προκειμένου να μεταδοθούν τα πλαίσια των δεδομένων τους. Οι μέθοδοι είναι οι εξής:

### **4.3 DCF (Distributed Coordination Function)**

Στο πρωτόκολλο IEEE 802.11, ο βασικός μηχανισμός πρόσβασης στο μέσο ονομάζεται κατανεμημένη λειτουργία συντονισμού ή αλλιώς DCF [25], που βασίζεται στο πρωτόκολλο CSMA / CA κατά το οποίο υπάρχει πολλαπλή πρόσβαση από τους σταθμούς στο δίκτυο αφού το ανιχνεύσουν για ύπαρξη σήματος, αποφεύγοντας έτσι τις συγκρούσεις των πακέτων τους. Εάν κάποιος σταθμός έχει ένα πακέτο για μετάδοση, ανιχνεύει τη δραστηριότητα του καναλιού. Αν το κανάλι απελευθερωθεί από την προηγούμενη μετάδοση και παραμείνει ελεύθερο για ένα ισοδύναμο χρονικό διάστημα με ένα DIFS, ο σταθμός περιμένει ένα τυχαίο χρονικό διάστημα που υπαγορεύεται από τον αλγόριθμο οπισθοχώρησης και στη συνέχεια μεταδίδει το πακέτο του. Εάν το κανάλι είναι κατειλημμένο, ο σταθμός εξακολουθεί να παρακολουθεί το κανάλι μέχρι να βρεθεί αδρανές και τέλος, εάν το κανάλι ανιχνευθεί ελεύθερο εξαρχής ο σταθμός θα πρέπει να περιμένει ένα διάστημα ίσο με τον μετρητή DIFS και να αποστείλει κατευθείαν τα δεδομένα του.

Για λόγους αποτελεσματικότητας, η DCF υλοποιεί τη μέθοδο οπισθοχώρησης διακριτού χρόνου (discrete-time backoff). Ο χρόνος αμέσως μετά την πάροδο ενός μετρητή DIFS χωρίζεται σε χρονοθυρίδες (slots) και η διάρκειά τους είναι ίση με τον μέγιστο χρόνο που απαιτείται από έναν σταθμό ώστε να ανιχνεύσει τη μετάδοση ενός άλλου πλαισίου δεδομένων στο δίκτυο από κάποιον άλλο σταθμό. Σύμφωνα με τον αλγόριθμο οπισθοχώρησης, κάθε σταθμός έχει το δικαίωμα να μεταδώσει τα δεδομένα του μόνο στην αρχή κάποιου από τα slots.

Η χρήση αυτών των slots εξασφαλίζει πως η σύγκρουση των πλαισίων δεδομένων είναι αναπόφευκτη μόνο στην περίπτωση που δύο σταθμοί επιλέξουν το ίδιο time slot για τη μετάδοση των δεδομένων τους. Σε κάθε μετάδοση πλαισίου δεδομένων, ο χρόνος που θα οπισθοχωρήσει βάσει του αλγορίθμου ο σταθμός επιλέγεται από το διάστημα  $(0, w-1)$ . Η μεταβλητή  $w$  αντιπροσωπεύει το contention window που αναφέρθηκε παραπάνω και εξαρτάται άμεσα από τον αριθμό των αποτυχημένων προσπαθειών μετάδοσης του συγκεκριμένου πακέτου. Στην πρώτη προσπάθεια μετάδοσης του πλαισίου, η μεταβλητή  $w$  παίρνει την τιμή της από την μικρότερη τιμή που θα μπορούσε να έχει το contention window, γνωστή ως **CWmin**. Κάθε φορά που αποτυγχάνει η μετάδοση του συγκεκριμένου πλαισίου, η τιμή της μεταβλητής αυτής διπλασιάζεται μέχρι να γίνει ίση με την μεγαλύτερη δυνατή τιμή που μπορεί να έχει το contention window, **CWmax**.

Ο μετρητής του αλγορίθμου οπισθοχώρησης, μειώνεται συνεχώς όσο το κανάλι ανιχνευθεί ως αδρανές, σταματάει όταν ανιχνεύσει κάποια μετάδοση δεδομένων στο δίκτυο και ενεργοποιείται εκ νέου όταν το κανάλι παραμένει ανενεργό για χρονικό διάστημα μεγαλύτερο του DIFS. Ο σταθμός θα είναι σε θέση να μεταδώσει τα δεδομένα του μόνο εάν έχει παρέλθει το χρονικό διάστημα που διαρκεί ο DIFS και ο μετρητής οπισθοχώρησής του έχει μηδενιστεί.

Η DCF χρησιμοποιεί δύο τεχνικές για την μετάδοση των πλαισίων δεδομένων από ένα σταθμό σε έναν άλλο μέσω του δικτύου.

#### **4.3.1 DCF Basic Access Mechanism (Βασική CSMA/CA)**

Η βασική μέθοδος πρόσβασης της DCF [26] χρησιμοποιεί μηνύματα επιβεβαίωσης για τα πλαίσια δεδομένων που αποστέλλονται μεταξύ πομπού και δέκτη, δεδομένου πως η τεχνική CSMA/CA δεν βασίζεται στην ικανότητα των σταθμών να αντιληφθούν πιθανές συγκρούσεις των πλαισίων τους με άλλα που μεταφέρονται από το δίκτυο την ίδια χρονική στιγμή.

Πιο συγκεκριμένα, ο σταθμός που θέλει να μεταδώσει τα δεδομένα του ανιχνεύει το μέσο για να καταλάβει εάν είναι αδρανές ή όχι. Εάν το μέσο είναι αδρανές για χρονικό διάστημα ίσο με DIFS ξεκινάει την μετάδοση των δεδομένων. Εάν το μέσο είναι κατειλημμένο από κάποιον άλλο σταθμό, αναβάλλει τη μετάδοση και

εξακολουθεί να ανιχνεύει το δίκτυο μέχρι να το βρει αδρανές. Εάν παρέλθει ένα χρονικό διάστημα ίσο με τον DIFS και το χρονικό διάστημα που απαιτείται από τον αλγόριθμο οπισθοχώρησης χωρίς εν τω μεταξύ να ανιχνευθεί άλλη κίνηση στο δίκτυο, ο σταθμός μπορεί να ξεκινήσει την μετάδοση των δεδομένων του.

Όταν η μετάδοση ολοκληρωθεί και ο δέκτης παραλάβει ορθώς το πλαίσιο των δεδομένων που προορίζονταν για αυτόν, περιμένει για ένα χρονικό διάστημα διάρκειας ίσης με τον SIFS και έπειτα αποστέλλει ένα μήνυμα επιβεβαίωσης λήψης ACK πίσω στον πομπό ώστε να τον ενημερώσει για την ορθή λήψη του πλαισίου. Δεδομένου πως ο μετρητής SIFS είναι μικρότερος από τον DIFS, κανένας άλλος σταθμός δεν θα προσπαθήσει να μεταδώσει τα πλαίσιά του μέχρι τουλάχιστον να αποσταλεί το ACK, αποφεύγοντας κατ' αυτόν τον τρόπο τη σύγκρουση. Εάν ο πομπός δεν λάβει το ACK λόγω σύγκρουσης στο δίκτυο ή λόγω σφαλμάτων μετάδοσης, περιμένει για ένα χρονικό διάστημα ίσο με τον μετρητή EIFS καθώς και για το χρονικό διάστημα που καθορίζεται από τον αλγόριθμο οπισθοχώρησης και αρχικοποιεί εκ νέου τη διαδικασία αποστολής του πλαισίου θεωρώντας πως το πλαίσιο δεν έχει φτάσει στον προορισμό του.

#### **4.3.2 CSMA/CA –RTS/CTS**

Και σε αυτή την τεχνική μετάδοσης, ακολουθείται η βασική αρχή της CSMA/CA. Ο σταθμός που θέλει να μεταδώσει τα δεδομένα του ανιχνεύει το μέσο για να καταλάβει εάν είναι αδρανές ή όχι. Εάν το μέσο είναι αδρανές για χρονικό διάστημα ίσο με DIFS αρχικοποιεί την διαδικασία μετάδοσης των δεδομένων. Εάν το μέσο είναι κατειλημμένο από κάποιον άλλο σταθμό, αναβάλλει τη μετάδοση και εξακολουθεί να ανιχνεύει το δίκτυο μέχρι να το βρει αδρανές. Εάν παρέλθει ένα χρονικό διάστημα ίσο με τον DIFS και το χρονικό διάστημα που απαιτείται από τον αλγόριθμο οπισθοχώρησης χωρίς εν τω μεταξύ να ανιχνευθεί άλλη κίνηση στο δίκτυο, ο σταθμός μπορεί να αρχικοποιήσει την μετάδοση των δεδομένων του.

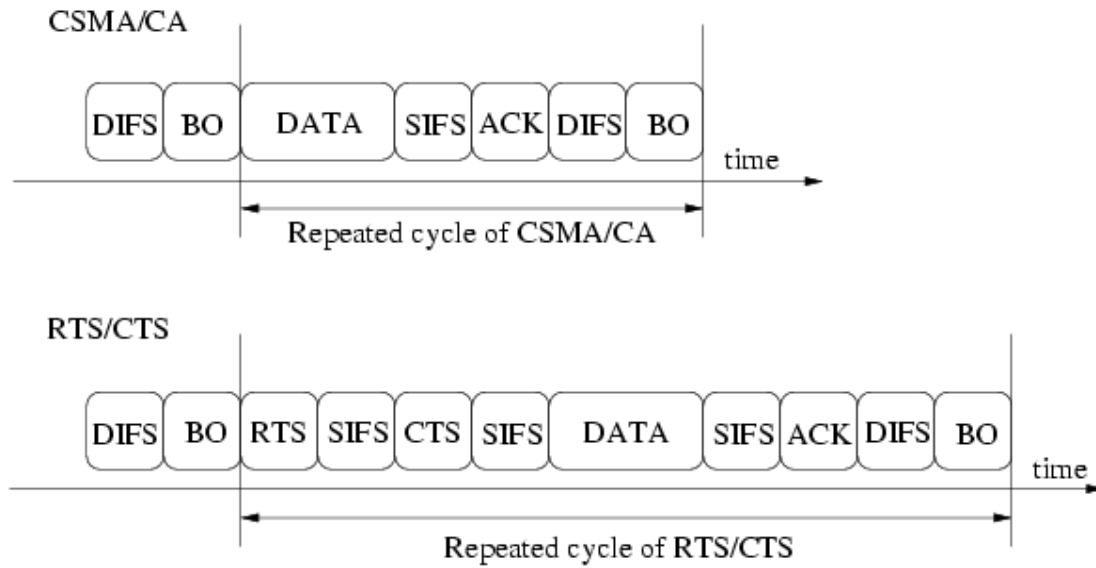
Πριν μεταδώσει το πλαίσιο των δεδομένων του, ο σταθμός καταλαμβάνει το μέσο στέλνοντας ένα μήνυμα τύπου RTS στον προορισμό ζητώντας του την άδεια να αποστείλει τα δεδομένα του. Εάν ο δέκτης δεν λαμβάνει πλαίσια από κάποιον άλλο σταθμό θα απαντήσει στον πομπό με ένα μήνυμα τύπου CTS ώστε να τον

ενημερώσει για να ξεκινήσει τη διαδικασία μετάδοσης. Μόλις παραληφθεί το πλαίσιο από τον δέκτη, αυτός θα πρέπει να στείλει ένα μήνυμα θετικής επιβεβαίωσης στον πομπό για να τον ενημερώσει για την ορθή λήψη των δεδομένων αναμένοντας ένα χρονικό διάστημα ίσο με τον μετρητή SIFS. Και εδώ, δεδομένου πως ο μετρητής SIFS είναι μικρότερος από τον DIFS, κανένας άλλος σταθμός δεν θα προσπαθήσει να μεταδώσει τα πλαίσιά του μέχρι τουλάχιστον να αποσταλεί το ACK, αποφεύγοντας κατ' αυτόν τον τρόπο τη σύγκρουση. Μεταξύ των μηνυμάτων RTS και CTS, CTS και Data, Data και ACK το χρονικό διάστημα που μεσολαβεί είναι ίσο με SIFS.

Εάν ο πομπός δεν λάβει το ACK λόγω σύγκρουσης στο δίκτυο ή λόγω σφαλμάτων μετάδοσης, περιμένει για ένα χρονικό διάστημα ίσο με τον μετρητή EIFS καθώς και για το χρονικό διάστημα που καθορίζεται από τον αλγόριθμο οπισθοχώρησης και αρχικοποιεί εκ νέου τη διαδικασία αποστολής του πλαισίου θεωρώντας πως το πλαίσιο δεν έχει φτάσει στον προορισμό του.

Θέματα συγκρούσεων μπορούν να προκύψουν μόνο κατά τη διάρκεια αποστολής του αρχικού RTS και θα γίνουν αμέσως αντιληπτά διότι δεν θα φτάσει κανένα μήνυμα τύπου CTS από τον δέκτη στον πομπό. Κατ' αυτόν τον τρόπο, η απόδοση του δικτύου βελτιώνεται αισθητά και μάλιστα περισσότερο από την περίπτωση που θα χρησιμοποιούνταν η βασική CSMA/CA τεχνική, αφού μειώνει δραστικά το χρόνο που μπορεί να προκύψουν οι συγκρούσεις παρέχοντας τη δυνατότητα αποστολής μεγαλύτερου μεγέθους πλαισίων.

Στην εικόνα φαίνονται οι μετρητές χρόνου και τα μηνύματα που αποστέλλονται κατά τη διαδικασία CSMA/CA αλλά και κατά τη διαδικασία CSMA/CA –RTS/CTS.



Εικόνα 4.4: Διαδικασίες CSMA/CA και CSMA/CA –RTS/CTS

#### 4.4 PCF (Point Coordination Function)

Η μέθοδος πρόσβασης PCF [27] προσφέρει στους σταθμούς των ασύρματων τοπικών δικτύων μία δίκαιη διαδικασία κατοχής και πρόσβασης στο μέσο ώστε να μεταδώσουν τα δεδομένα τους. Κατά κάποιο τρόπο μοιάζει με άλλες μεθόδους που βασίζονται στον διαμοιρασμό κουπονιών (token based) στους σταθμούς προσφέροντάς τους παράλληλα την πρόσβαση στο μέσο.

Βασικό χαρακτηριστικό της μεθόδου αυτής είναι πως χρησιμοποιείται σε περιπτώσεις που δεν θέλουμε να υπάρχει ανταγωνισμός μεταξύ των σταθμών για την κατοχή και τη χρήση του μέσου όπως συμβαίνει στην τεχνική DCF. Η περίπτωση που συνήθως χρησιμοποιείται η τεχνική αυτή είναι τα δίκτυα υποδομής, δίκτυα που απαρτίζονται από έναν ή και περισσότερους σταθμούς και ένα AP το οποίο παίζει και τον ρόλο του μεσολαβητή στην επικοινωνία μεταξύ των σταθμών αυτών.

Όταν χρησιμοποιείται η PCF, ο χρόνος χρήσης και κατοχής του μέσου χωρίζεται σε δύο περιόδους. Η πρώτη περίοδος είναι αυτή που χρησιμοποιείται από την PCF και στην οποία δεν υπάρχει ανταγωνισμός των σταθμών για την κατοχή του μέσου (**contention-free period**). Η δεύτερη περίοδος χαρακτηρίζεται από τον



ανταγωνισμό που υπάρχει μεταξύ των χρηστών και χρησιμοποιείται από την τεχνική DCF (**contention period**). Η χρονική διάρκεια της περιόδου ανταγωνισμού θα πρέπει να είναι ίση ή και μεγαλύτερη από την διάρκεια που απαιτείται για να μεταδοθεί ένα πλαίσιο μέγιστου μήκους μαζί με το μήνυμα της επιβεβαίωσης ορθής λήψης του.

Στα δίκτυα υποδομής, το AP μεταδίδει ένα πλαίσιο Beacon που περιέχει όλες τις πληροφορίες σχετικά με το ασύρματο δίκτυο και μεταδίδεται σε συχνά χρονικά διαστήματα από το AP ώστε να ανακοινώνει την ύπαρξη και τη λειτουργία του δικτύου. Επίσης, στην περίπτωση χρήσης της PCF χρησιμοποιείται και για την εκλογή του σταθμού που θα πάρει το δικαίωμα για την κατοχή και τη χρήση του μέσου.

Στην αρχή της περιόδου ανταγωνισμού, το AP εκπέμπει ένα πλαίσιο beacon. Ένα από τα πεδία το πλαισίου αυτού αφορά στη μέγιστη διάρκεια που μπορεί να διαρκέσει η περίοδος που δεν ανταγωνίζονται οι σταθμοί. Όλοι οι σταθμοί που θα λάβουν αυτό το πλαίσιο θα πρέπει να θέσουν τον NAV μετρητή τους στη μέγιστη διάρκειά του ώστε να εξασφαλιστεί πως δεν θα χρησιμοποιηθεί η τεχνική DCF τουλάχιστον για αυτό το χρονικό διάστημα. Προκειμένου να αποφευχθούν τυχόν παρεμβολές, όλοι οι σταθμοί που συμμετέχουν στην τεχνική PCF χρησιμοποιούν τους μετρητές SIFS και PIFS, που είναι αρκετά μικρότεροι σε διάρκεια από τον DIFS, εξασφαλίζοντας πως κανένας σταθμός που κάνει χρήση της DCF δεν θα καταλάβει το μέσο.

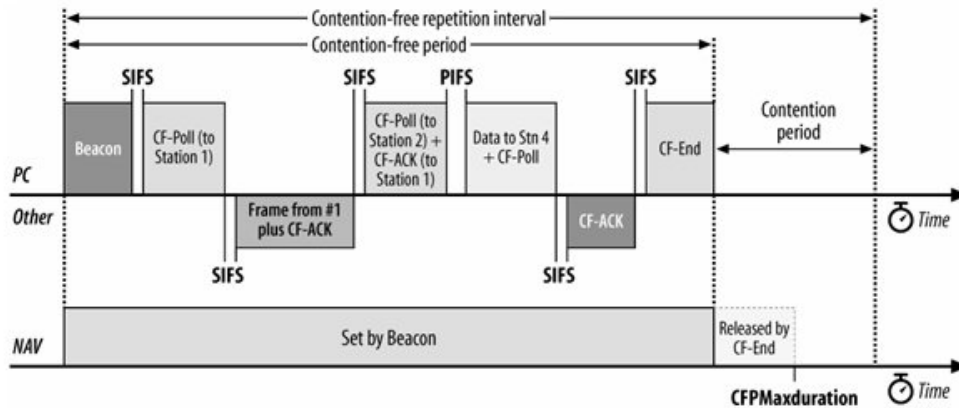
Μόλις το AP αποκτήσει την κατοχή του μέσου, ελέγχει μία λίστα (**polling list**) με όλους τους σταθμούς που είναι διαθέσιμοι για μετάδοση. Η λίστα αυτή συμπληρώνεται στο AP όταν οι σταθμοί προσπαθούν να συσχετιστούν με αυτό στέλλοντάς του ένα αίτημα συσχέτισης (**association request**) [28] στο οποίο αναφέρουν πληροφορίες σχετικές με αυτούς όπως είναι ο προβλεπόμενος ρυθμός μετάδοσης και το SSID με το οποίο επιθυμούν να συσχετιστούν. Το πλαίσιο συσχέτισης περιλαμβάνει και ένα πεδίο στο οποίο αναφέρεται εάν ο σταθμός

αυτός μπορεί να λάβει μέρος στην διαδικασία εκλογής του από το AP ώστε να μεταδώσει τα δεδομένα του κάνοντας χρήση της μεθόδου PCF. Όλοι οι υπόλοιποι σταθμοί του δικτύου που δεν μπορούν να υλοποιήσουν την τεχνική PCF, θα πρέπει να περιμένουν να τερματιστεί η περίοδος χωρίς ανταγωνισμό και να λάβει την πρόσβαση στο μέσο η τεχνική DCF ώστε να ανταγωνιστούν με τους άλλους σταθμούς για την κατοχή του μέσου.

Κατά τη διάρκεια που δεν υφίσταται ανταγωνισμός, οι σταθμοί μπορούν να μεταδώσουν τα πλαίσια τους μόνο όταν τους ζητηθεί από το AP μέσω ενός polling πλαίσιο που θα τους σταλεί, γνωστό και ως **CF-Poll**. Κάθε CF-Poll είναι ουσιαστικά η άδεια που δίνεται από το AP στον σταθμό για να μεταδώσει ένα και μόνο πλαίσιο του. Πολλαπλά πλαίσια μπορούν να μεταδοθούν μόνο στην περίπτωση που το AP θα στείλει ισάριθμα CF-Poll στον σταθμό.

Γενικά, όλες οι μεταδώσεις που λαμβάνουν χώρα στην περίοδο που δεν υφίσταται ανταγωνισμός, διαφέρουν χρονικά μεταξύ τους κατά ένα SIFS. Όταν τελειώσει η μετάδοση του πρώτου σταθμού στη λίστα, το AP στέλνει ένα CF-Poll στον επόμενο σταθμό που είναι εγγεγραμμένος στη λίστα του. Εάν ο σταθμός δεν απατήσει με τη μετάδοση του πλαισίου του για ένα χρονικό διάστημα ίσο με τον PIFS, το AP θα παραδώσει τη σκυτάλη κατοχής του μέσου στον επόμενο σταθμό που εμφανίζεται στη λίστα του, παρατείνοντας κατ' αυτόν τον τρόπο τη διάρκεια της περιόδου χωρίς ανταγωνισμό.

Στην εικόνα φαίνεται ο τρόπος λειτουργίας της PCF καθώς και η χρήση των μετρητών της.



Εικόνα 4.5: Υλοποίηση της μεθόδου PCF.

Το AP μεταδίδει διαφόρων τύπων πλαίσια κατά τη διάρκεια της περιόδου χωρίς ανταγωνισμό, μερικά εκ των οποίων είναι τα εξής:

- **Data:** είναι το μόνο πλαίσιο που είναι κοινό τόσο στην περίοδο ανταγωνισμού όσο και στην περίοδο χωρίς ανταγωνισμό. Χρησιμοποιείται για να ενημερώσει τον σταθμό πως το AP δεν χρειάζεται μηνύματα επιβεβαίωσης από εκείνον.
- **CF-Ack:** αυτό το πλαίσιο χρησιμοποιείται από τους σταθμούς για να επιβεβαιώσουν πως έλαβαν ένα πλαίσιο από τον πομπό χωρίς να χρειάζεται να μεταδοθούν δεδομένα.
- **CF-Poll:** στέλνεται από το AP σε ένα σταθμό ώστε να του παραχωρήσει το δικαίωμα της μετάδοσης ενός μόνο πλαισίου. Χρησιμοποιείται όταν το AP δεν έχει δεδομένα προς μετάδοση σε αυτόν τον σταθμό.
- **Data+CF-Ack:** το πλαίσιο αυτό χρησιμοποιείται από το AP και περιέχει τα δεδομένα που προωθούνται στον παραλήπτη τους αλλά και το μήνυμα της θετικής επιβεβαίωσης του προηγούμενου πλαισίου που θα προωθηθεί στον προηγούμενο σταθμό.

- Data+CF-Poll: το πλαίσιο αυτό αποστέλλεται από το AP σε έναν σταθμό για να παραδώσει τα δεδομένα που προορίζονται για αυτόν και να του ζητηθεί παράλληλα να μεταδώσει το δικό του πλαίσιο.
- CF-End: με το πλαίσιο αυτό το AP τερματίζει την περίοδο χωρίς ανταγωνισμό και παραχωρεί την πρόσβαση στο μέσο στην τεχνική DCF.

## 5. Σουίτα πρωτοκόλλων 802.11

Όπως αναφέρθηκε και νωρίτερα, το 802.11 είναι μια οικογένεια προδιαγραφών που αναπτύχθηκαν από την IEEE για τα ασύρματα τοπικά δίκτυα. Το αρχικό πρότυπο του πρωτοκόλλου 802.11, το οποίο και έγινε αποδεκτό από την IEEE το 1997, προέβλεπε την ασύρματη επικοινωνία μεταξύ των σταθμών ενός δικτύου. Οι ομάδες εργασίας της IEEE ανέπτυξαν όμως και επεκτάσεις για την βασική αυτή έκδοση του πρωτοκόλλου ώστε να γίνει περισσότερο ευέλικτο αλλά και λειτουργικό. Κάθε επέκταση του πρωτοκόλλου έχει λάβει το όνομά της από την ομάδα εργασίας που ήταν υπεύθυνη για την ανάπτυξή του. Τα πιο διαδεδομένα πρότυπα που απαρτίζουν την οικογένεια του 802.11 είναι τα 802.11a, 802.11b, 802.11e, 802.11g και 802.11n και θα αναλυθούν παρακάτω.

Το αρχικό 802.11 ορίζει για όλα τα πρότυπα, εννέα υπηρεσίες [29] που θα πρέπει να υλοποιούνται και να λειτουργούν βάσει των κανόνων που διέπουν τα ασύρματα δίκτυα. Οι υπηρεσίες αυτές χωρίζονται σε δύο κατηγορίες, οι πέντε εξ αυτών αφορούν τις συνδέσεις στο δίκτυο υποδομής και οι υπόλοιπες τέσσερις αφορούν τους σταθμούς που απαρτίζουν το δίκτυο.

Οι πέντε υπηρεσίες που σχετίζονται με το δίκτυο υποδομής παρέχονται από τα AP και αφορούν κυρίως την είσοδο και την έξοδο των ασύρματων σταθμών στο δίκτυο καθώς και την συνεργασία αυτών με τα AP. Οι υπηρεσίες είναι οι εξής:

- **Association** (συσχετισμός): Η υπηρεσία αυτή χρησιμοποιείται για την εγκαθίδρυση επικοινωνίας των ασύρματων σταθμών με το AP. Τυπικά, ως διαδικασία λαμβάνει χώρα αμέσως μόλις ο σταθμός βρεθεί εντός της εμβέλειας του AP. Ο σταθμός που θέλει να ξεκινήσει την διαδικασία αρχικοποίησης θα πρέπει να αποστείλει στο AP τον κωδικό πρόσβασης στο δίκτυο καθώς και επιπλέον πληροφορίες που αφορούν στους ρυθμούς δεδομένων που υποστηρίζει καθώς και πληροφορίες σχετικές με την κατανάλωση ενέργειας. Το AP με τη σειρά του είναι σε θέση είτε να αποδεχτεί τον σταθμό αυτό είτε να τον απορρίψει. Στην περίπτωση που ο

σταθμός γίνει αποδεκτός θα πρέπει αμέσως μετά να στείλει τις πληροφορίες που αφορούν στην αυθεντικοποίησή του.

- **Disassociation** (τερματισμός συσχετισμού): Ο τερματισμός της επικοινωνίας μεταξύ του σταθμού και του AP μπορεί να διακοπεί και από τις δύο πλευρές. Ένας σταθμός μπορεί να κάνει χρήση αυτής της υπηρεσίας όταν τερματίζει τη λειτουργία του ή όταν εγκαταλείπει το ασύρματο δίκτυο, ενώ ένα AP μπορεί να κάνει χρήση της εν λόγω υπηρεσίας και στην περίπτωση που πρόκειται να τεθεί υπό συντήρηση από τον διαχειριστή του δικτύου.
- **Reassociation** (επανάληψη συσχετισμού): Ένας σταθμός μπορεί να θελήσει να εγκαθιδρύσει επικοινωνία με κάποιο AP διαφορετικό από αυτό που συνήθως επικοινωνεί κυρίως σε περιπτώσεις που μετακινείται σε ένα άλλο ασύρματο δίκτυο χωρίς να υπάρξει κάποια απώλεια δεδομένων εάν ο σταθμός μεταδίδει τα δεδομένα του εκείνη τη στιγμή.
- **Distribution** (διανομή): Η υπηρεσία αυτή καθορίζει τη διαδρομή που θα ακολουθήσει ένα πακέτο δεδομένων που έχει σταλεί στο AP. Εάν ο παραλήπτης των δεδομένων αυτών είναι στο ίδιο δίκτυο με το AP τότε αυτό θα το στείλει απευθείας στον παραλήπτη του. Εάν όχι, τότε το πακέτο δεδομένων θα πρέπει πρώτα να μεταφερθεί ενσύρματα σε κάποιο άλλο AP το οποίο και θα το προωθήσει στον παραλήπτη του.
- **Integration** (ενσωμάτωση): Σε περίπτωση που το πακέτο δεδομένων πρέπει να μεταφερθεί σε ένα δίκτυο που απαιτεί διαφορετικό σχήμα διευθυνσιοδότησης ή διαφορετικό σχήμα διαμόρφωσης πλαισίου π.χ. σε ένα ενσύρματο δίκτυο, η υπηρεσία αυτή αναλαμβάνει να μετατρέψει την πληροφορία του ασύρματου δικτύου στην κατάλληλη μορφή που απαιτείται από το άλλο δίκτυο.

Οι υπόλοιπες τέσσερις υπηρεσίες αφορούν μόνο τις λειτουργίες που λαμβάνουν χώρα μέσα σε ένα συγκεκριμένο δίκτυο και συμβαίνουν όταν ολοκληρωθεί η

διαδικασία της εγκαθίδρυσης της επικοινωνίας μεταξύ του AP και του σταθμού. Οι υπηρεσίες αυτές είναι οι εξής:

- **Authentication** (αυθεντικοποίηση): Για να αποφευχθεί η πιθανότητα λήψης ή αποστολής δεδομένων από κάποιον μη εξουσιοδοτημένο χρήστη του συστήματος, κάθε σταθμός του δικτύου θα πρέπει να αυθεντικοποιηθεί προτού επιχειρηθεί η οποιαδήποτε μετάδοση και παραλαβή δεδομένων αμέσως μετά την εγκαθίδρυση της επικοινωνίας του σταθμού αυτού με το AP του συστήματος. Μόλις ο σταθμός εγκαθιδρύσει την επικοινωνία του με το AP, το τελευταίο του στέλνει ένα μήνυμα ζητώντας του πληροφορίες σχετικές με κωδικό πρόσβασης στο δίκτυο. Ο σταθμός του απαντάει με ένα κρυπτογραφημένο πλαίσιο που περιέχει τον κωδικό πρόσβασης του δικτύου. Εάν ο κωδικός αυτός είναι ο σωστός τότε ο σταθμός αποκτά πρόσβαση στο δίκτυο, ενώ αν δεν είναι σωστός θα ζητηθεί ξανά από το AP η αποστολή του κωδικού από τον σταθμό.
- **Deauthentication** (τερματισμός αυθεντικοποίησης): Όταν ένας σταθμός θελήσει να διακόψει την επικοινωνία του με το δίκτυο, θα πρέπει να προχωρήσει στη διαδικασία του τερματισμού της αυθεντικοποίησης αποστέλλοντας ένα μήνυμα στο AP. Πλέον, για να μπορέσει ο σταθμός να έχει πρόσβαση στο δίκτυο θα πρέπει να εκτελέσει εκ νέου τις διαδικασίες συσχέτισμού και αυθεντικοποίησης.
- **Privacy** (ιδιωτικοποίηση): Προκειμένου να διατηρηθεί η εμπιστευτικότητα των δεδομένων που μεταδίδονται στο δίκτυο, χρησιμοποιείται ο αλγόριθμος RC4 για να κρυπτογραφηθούν τα δεδομένα όταν πρόκειται να αποσταλούν και αντίστοιχα να αποκρυπτογραφηθούν από τους παραλήπτες για να επεξεργαστούν την καθαρή πλέον πληροφορία.
- **Data delivery** (μεταφορά δεδομένων): Η μεταφορά των δεδομένων είναι ο λόγος ύπαρξης όλων των δικτύων. Επειδή το 802.11 βασίζεται στο προγενέστερό του πρωτόκολλο Ethernet, δεν είναι εξολοκλήρου αξιόπιστο

στη μεταφορά των δεδομένων. Τα υψηλότερα επίπεδα είναι υπεύθυνα για την διατήρηση της αξιοπιστίας του δικτύου στη μετάδοση των δεδομένων.

## 5.1 802.11b

Το πρότυπο 802.11b [30] ή αλλιώς γνωστό και ως **WiFi (Wireless Fidelity)** ανακοινώθηκε από την IEEE το 1999. Λειτουργεί στην μπάντα συχνοτήτων των 2.4 GHz και προσφέρει ρυθμούς μετάδοσης που μπορούν να φτάσουν τα 11 Mbps υποστηρίζοντας πάντα τους αρχικούς ρυθμούς μετάδοσης των 1,2 και 5.5 Mbps. Τα κανάλια που χρησιμοποιούνται ποικίλουν στον αριθμό ανά ήπειρο αλλά τρία είναι σε όλες τις περιπτώσεις τα επιπρόσθετα που δεν επικαλύπτονται, ενώ το εύρος ζώνης όλων αυτών των καναλιών είναι στα 22 MHz.

Ως τεχνική πρόσβασης στο μέσο χρησιμοποιείται η **HR/DSSS (High Rate / Direct Sequence Spread Spectrum)**, που θεωρείται η επέκταση της αρχικής DSSS και δίνει τη δυνατότητα επίτευξης μεγαλύτερου ρυθμού μετάδοσης από εκείνη στα 11 Mbps. Ο τρόπος λειτουργίας της είναι ο ίδιος με την απλή DSSS. Το σήμα που μεταδίδεται διευρύνεται στο φασματικό εύρος χρησιμοποιώντας μία μέθοδο μετατροπής και αντικατάστασης της πληροφορίας που είναι γνωστή εκ των προτέρων τόσο από τον πομπό όσο και από τον δέκτη. Ο πομπός αναλαμβάνει να μετατρέψει τα bits της αρχικής πληροφορίας βάσει μίας ακολουθίας και εν συνεχεία, ο δέκτης θα χρησιμοποιήσει την ίδια ακολουθία προκειμένου να ανακατασκευάσει το σήμα της πληροφορίας.

Η συνηθέστερη τεχνική διαμόρφωσης που χρησιμοποιείται είναι η **CCK (Complementary Code Keying)** [31] που θεωρείται ως η αντικατάσταση της ακολουθίας Barker για τις ασύρματες επικοινωνίες μιας και κάνει πιο αποτελεσματική την χρήση των ακολουθιών από bits, γεγονός που συμβάλλει κι αυτό με τη σειρά του στην επίτευξη υψηλότερων ρυθμών μετάδοσης από τα 2 Mbps που επιτυγχάνει η χρήση της ακολουθίας Barker. Ο μόνος περιορισμός που εμφανίζεται στην προσπάθεια να επιτευχθεί μεγαλύτερος ρυθμός μετάδοσης με την CCK είναι οι μικρές αποστάσεις στις οποίες πρέπει να λειτουργεί το δίκτυο. Οι υψηλότεροι ρυθμοί μετάδοσης επιτυγχάνονται με την χρήση 8 chips για την ακολουθία που αντικαθιστά τα bits της καθαρής πληροφορίας, έναντι των 11 που



χρησιμοποιούνται στην ακολουθία Barker. Η χρήση των λιγότερων chips στην ακολουθία που θα αντικαταστήσει την αρχική πληροφορία έχει ως αποτέλεσμα την μικρότερη διασπορά του σήματος στην συχνότητα κατά την μετάδοσή του με αποτέλεσμα να επιτυγχάνονται υψηλότερες ταχύτητες μεταφοράς δεδομένων. Βέβαια, το σήμα κατ' αυτόν τον τρόπο γίνεται πιο επιρρεπές σε παρεμβολές που εμφανίζονται κυρίως στις στενές ζώνες συχνοτήτων.

Η τεχνική CCK χρησιμοποιείται στα ασύρματα τοπικά δίκτυα μέσω του προτύπου 802.11 ώστε να επιτυγχάνονται οι ρυθμοί μετάδοσης τόσο των 5.5 Mbps όσο και των 11 Mbps.

Στο 802.11b υπάρχουν τέσσερις διαφορετικές μορφές διαμόρφωσης, όσοι είναι και ρυθμοί μετάδοσης που χρησιμοποιούνται [32]. Η τεχνική **DBPSK (Differential Binary Phase Shift Keying)** χρησιμοποιείται για τον ρυθμό μετάδοσης του ενός Mbps, η **DQPSK (Differential Quadrature Phase Shift Keying)** για ρυθμό μετάδοσης των 2 Mbps.

Κάθε ψηφιακό σχήμα που χρησιμοποιείται στην διαμόρφωση των δεδομένων χρησιμοποιεί ένα πεπερασμένο αριθμό από σήματα για να αντιπροσωπεύσει τα μεταδιδόμενα δεδομένα. Γενικώς, οι τεχνικές διαμόρφωσης με αλλαγή φάσης **PSK (Phase Shift Keying)** χρησιμοποιούν ένα πεπερασμένο αριθμό φάσεων που αντιπροσωπεύεται από μία ακολουθία από κωδικοποιημένα bits τα οποία και θα αποσταλούν στον δέκτη. Ο δέκτης με τη σειρά του θα πρέπει να αναγνωρίσει την διαφοροποίηση της φάσης του σήματος που χρησιμοποιήθηκε συγκρίνοντάς το με την προκαθορισμένη φάση με την οποία στέλνονται τα σήματα και να αποκωδικοποιήσει τα δεδομένα στην αρχική τους μορφή.

Η τεχνική CCK χρησιμοποιείται για τους ρυθμούς μετάδοσης των 5.5 και 11 Mbps. Η τέταρτη τεχνική διαμόρφωσης, γνωστή ως **PBCC (Packet Binary Convolutional Coding)** χρησιμοποιείται για τους ρυθμούς μετάδοσης των 5.5 και 11 Mbps σε περιπτώσεις δικτύων που απαιτείται υψηλός βαθμός απόδοσης του συστήματος χωρίς να λαμβάνεται ιδιαίτερα υπόψη η ακεραιότητα των δεδομένων που μεταδίδονται. Στην πιο απλή της μορφή, η PBCC μειώνει αισθητά το μέγεθος της πλεονάζουσας πληροφορίας που μεταδίδεται με τα καθαρά δεδομένα όπως

είναι τα μηνύματα ορθής λήψης, οι κεφαλίδες που μεταφέρουν πληροφορίες σχετικά με το πρωτόκολλο που χρησιμοποιείται, τα σήματα ελέγχου λαθών κτλ και χρησιμοποιεί μικρότερα πλαίσια δεδομένων, παρέχοντας έτσι τη δυνατότητα να αποστέλλεται μεγαλύτερος αριθμός πλαισίων στην ίδια χρονική διάρκεια με τις υπόλοιπες τεχνικές.

Επιπλέον, το 802.11b υποστηρίζει τον αλγόριθμο ασφαλείας **WEP (Wired Equivalent Privacy)** [33] που προσφέρει εμπιστευτικότητα στην μεταφορά των δεδομένων. Ο αλγόριθμος WEP χρησιμοποιεί ακολουθίες από 40, 104, 152 ή 256 bits, γνωστά και ως κλειδιά για να κρυπτογραφήσει την μεταδιδόμενη πληροφορία ώστε να μην καθίσταται εύκολη η διαδικασία υποκλοπής της. Τα κλειδιά αυτά δεν μεταφέρονται στο δίκτυο αλλά είναι γνωστά εκ των προτέρων στους σταθμούς του δικτύου. Εδώ θα πρέπει να σημειωθεί πως η χρήση της συγκεκριμένης τεχνικής δεν ενδείκνυται πλέον μιας και έχει αντικατασταθεί από τεχνικές με υψηλότερα ποσοστά ασφαλείας στη μετάδοση των δεδομένων όπως είναι η **WPA (WiFi Protected Access)**.

Τα κανάλια των συχνοτήτων που χρησιμοποιούνται από την τεχνική HR/DSSS στο πρότυπο 802.11b παρουσιάζονται στον ακόλουθο πίνακα [34].

Κανάλι	Κεντρική συχνότητα	Πλάτος συχνότητας	Επικαλυπτόμενα κανάλια
1	2.412 GHz	2.401-2.423 GHz	2,3,4,5
2	2.417 GHz	2.406-2.428 GHz	1,3,4,5,6
3	2.422 GHz	2.411-2.433 GHz	2,4,5,6,7
4	2.427 GHz	2.416-2.438 GHz	3,5,6,7,8
5	2.432 GHz	2.421-2.443 GHz	4,6,7,8,9
6	2.437 GHz	2.426-2.448 GHz	5,7,8,9,10
7	2.442 GHz	2.431-2.453 GHz	6,8,9,10,11
8	2.447 GHz	2.436-2.458 GHz	7,9,10,11,12

<b>9</b>	2.452 GHz	2.441-2.463 GHz	8,10,11,12,13
<b>10</b>	2.457 GHz	2.446-2.468 GHz	9,11,12,13
<b>11</b>	2.462 GHz	2.451-2.473 GHz	10,12,13,14
<b>12</b>	2.467 GHz	2.456-2.478 GHz	11,13,14
<b>13</b>	2.472 GHz	2.461-2.483 GHz	12,14
<b>14</b>	2.484 GHz	2.473-2.495 GHz	

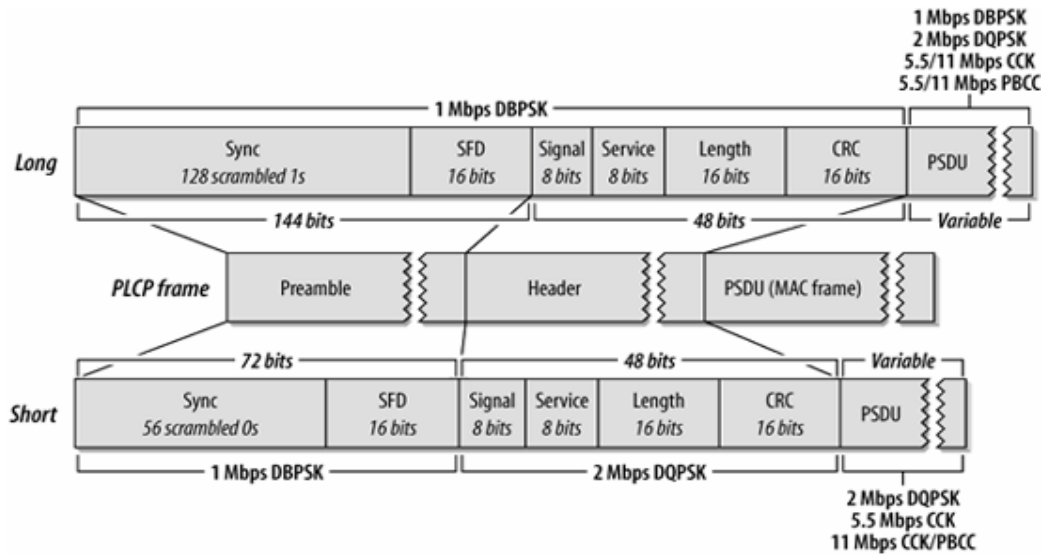
*Πίνακας 5.1: Διαθέσιμα κανάλια χρήσης του προτύπου 802.11b*

Εδώ θα πρέπει να σημειωθεί πως το κανάλι με τον αριθμό 14 χρησιμοποιείται μόνο στην Ιαπωνία και τα κανάλια 12 και 13 χρησιμοποιούνται σε όλον τον κόσμο πέραν των ΗΠΑ.

Το υπόστρωμα PLCP της τεχνικής HR/DSSS χρησιμοποιεί δύο τύπους πλαισίου σε αντίθεση με τα υπόλοιπα πρότυπα, ένα long (κανονικό) και ένα short (σύντομο). Το πλαίσιο long στην πραγματικότητα είναι το ίδιο με το πλαίσιο που χρησιμοποιείται στην DSSS του 802.11 ενώ τα πεδία του preamble και header μεταφέρονται πάντα με ρυθμό μετάδοσης στο 1 Mbps για να διατηρήσουν τη συμβατότητα του εν λόγω πλαισίου με το αρχικό DSSS. Το πλαίσιο short είναι προαιρετικό και μπορεί να χρησιμοποιηθεί μόνο αν όλοι οι σταθμοί στο σύστημα υποστηρίζουν τη λειτουργία του.

Επειδή και τα δύο πλαίσια, long και short, έχουν την ίδια μορφή, παρακάτω θα δοθεί έμφαση στις βασικές διαφορές τους όταν θα αναλυθούν τα πεδία τα οποία τα απαρτίζουν.

Η μορφή των δύο πλαισίων φαίνεται στην εικόνα [35]:



Εικόνα 5.1: Μορφή πλαισίων φυσικού υποστρώματος 802.11b

**Preamble:** Αποτελείται από δύο πεδία, το Sync μήκους 128 και 56 bits αντίστοιχα για το long Sync και το Short Sync και το SFD μήκους 16 bits. Το long SFD πεδίο περιέχει την ακολουθία «1111 0011 1010 0000» ενώ το short SFD πεδίο περιέχει την αντίστροφη ακολουθία «0000 1100 0101 1111». Εδώ θα πρέπει να τονιστεί πως το preamble στο long πλαίσιο μεταδίδεται με ρυθμό μετάδοσης 1 Mbps για λόγους συμβατότητας με την αρχική υλοποίηση της DSSS.

**Header:** Το τμήμα αυτό περιέχει τα πεδία Signal, Service, Length και CRC με μήκος 8,8,16 και 16 bits αντίστοιχα και στις δύο περιπτώσεις των πλαισίων.

- Το πεδίο Signal κωδικοποιεί τον ρυθμό μετάδοσης της πληροφορίας. Στο long πλαίσιο οι ρυθμοί αυτοί είναι των 1,2,5.5 και 11 Mbps ενώ στο short πλαίσιο οι ρυθμοί είναι 2,5.5 και 11 Mbps.
- Το πεδίο Length περιέχει τον χρόνο σε msec που απαιτείται για τη μετάδοση του ενσωματωμένου MAC πλαισίου.
- Το πεδίο Service αποτελείται από 8 bits, εκ των οποίων χρησιμοποιούνται μόνο τρία bits ενώ τα υπόλοιπα είναι δεσμευμένα και έχουν την τιμή «0». Το τελευταίο bit χρησιμοποιείται ως συμπληρωματικό για το πεδίο length, το τρίτο bit χρησιμοποιείται για πληροφορίες σχετικές με τη συχνότητα της μετάδοσης και τέλος το τέταρτο bit χρησιμοποιείται για να προσδιορίσει τη

μορφή της κωδικοποίησης. Εάν η τιμή του είναι «1» τότε χρησιμοποιείται η τεχνική PBCC, ενώ για την τιμή «0» χρησιμοποιείται η τεχνική CCK .

- Τέλος, το πεδίο CRC περιέχει τον κυκλικό κώδικα που χρησιμεύει στην προστασία της κεφαλίδας του πλαισίου.

Τα βασικότερα σημεία του προτύπου αυτού είναι τα εξής:

---

<b>802.11b</b>	
<b>Έκδοση</b>	1999
<b>Συχνότητα</b>	2.4 GHz
<b>Μέγιστος Ρυθμός μετάδοσης</b>	11 Mbps
<b>Φυσικό επίπεδο</b>	CCK
<b>Εμβέλεια</b>	30-90 m

*Πίνακας 5.2: Βασικά χαρακτηριστικά του 802.11b*

Το 802.11b είναι το πιο διαδεδομένο πρότυπο που χρησιμοποιείται για τα ασύρματα τοπικά δίκτυα. Χρησιμοποιείται κυρίως σε μικρά οικιακά δίκτυα και σε επιχειρήσεις παρέχοντας δυνατότητες δικτύωσης χωρίς καλωδίωση ενώ παράλληλα προσφέρει σχετικά υψηλούς ρυθμούς μετάδοσης.

Παρόλα αυτά υπάρχουν ζητήματα σχετικά με την αποφυγή χρήσης του εν λόγω προτύπου [36]. Η ζώνη των 2.4 GHz στην οποία λειτουργεί το 802.11b είναι διαδεδομένη και χρησιμοποιείται σε περιπτώσεις διαφορετικές από αυτές των ασύρματων τοπικών δικτύων. Οι φούρνοι μικροκυμάτων καθώς και τα ασύρματα τηλέφωνα λειτουργούν στην ίδια συχνότητα και υπάρχει πιθανότητα μείωσης της απόδοσης αλλά και της λειτουργικότητας του δικτύου.

Επιπλέον οι διαδεδομένες συσκευές Bluetooth που λειτουργούν στη συχνότητα των 2.4 GHz είναι υπεύθυνες για την ύπαρξη παρεμβολών και κατ' επέκταση τη μείωση της αποδοτικότητας του δικτύου. Είναι αξιοσημείωτο πως η χρήση των συσκευών Bluetooth δεν επηρεάζεται σχεδόν καθόλου από την ύπαρξη των

ασύρματων δικτύων στον ίδιο χώρο χωρίς αυτό να σημαίνει πως τα ασύρματα τοπικά δίκτυα δεν επηρεάζονται από αυτές τις συσκευές. Ευτυχώς, οι συσκευές Bluetooth δεν μεταφέρουν μεγάλο μεγέθους πακέτα και έτσι δεν δημιουργούνται σοβαρά προβλήματα στα ασύρματα δίκτυα. Ο χρόνος αποστολής των πακέτων αυτών λόγω του μεγέθους τους είναι σχετικά μικρός με αποτέλεσμα ακόμα κι αν προκληθεί κάποια σύγκρουση να είναι εύκολο να αντιμετωπισθεί σε μικρό χρονικό διάστημα. Παρόλα αυτά, για να εξαιρεθεί η πιθανότητα να προκληθούν σφάλματα από τη χρήση τέτοιων συσκευών, προτείνεται στον διαχειριστή του συστήματος να προχωρήσει σε ρυθμίσεις στο ασύρματο δίκτυο το οποίο θα λειτουργεί στο ένα άκρο του φάσματος συχνοτήτων των 2.4 GHz και σε ρυθμίσεις στις συσκευές Bluetooth που θα λειτουργούν στο άλλο άκρο.

## 5.2 802.11a

Το πρότυπο 802.11a [30] εγκρίθηκε τον Δεκέμβριο του 1999 ως μέλος της οικογένειας του πρωτοκόλλου 802.11. Είναι ουσιαστικά μία προέκταση του αρχικού 802.11 και παρέχει τη δυνατότητα επίτευξης ρυθμών μετάδοσης έως και 54Mbps λειτουργώντας στην μπάντα συχνοτήτων των 5GHz. Στις ΗΠΑ η ελεύθερη για χρήση μπάντα των 5GHz ονομάζεται **UNII (Unlicensed National Information Infrastructure)**.

Η μπάντα των 5GHz επιλέχθηκε για δύο βασικούς λόγους.

- Χρησιμοποιείται λιγότερο από την μπάντα των 2.4GHz που εμφανίζεται στην αρχική έκδοση του 802.11.
- Προσφέρει μεγαλύτερο εύρος ζώνης (bandwidth).

Βασική διαφορά που ξεχωρίζει τις δύο μπάντες συχνοτήτων είναι η εξυπηρέτηση περισσότερων από ένα καναλιών την ίδια χρονική στιγμή. Η μπάντα των 2.4GHz προσφέρει τη δυνατότητα συνύπαρξης και ταυτόχρονης λειτουργίας σε τρία μόνο μη επικαλυπτόμενα κανάλια. Από την άλλη μεριά, η μπάντα των 5GHz δίνει τη δυνατότητα σε οχτώ κανάλια να λειτουργούν ταυτόχρονα με το μέγιστο δυνατό εύρος ζώνης στο καθένα από αυτά δημιουργώντας έτσι ένα μεγάλο πλεονέκτημα

έναντι της μπάντας των 2.4GHz αφού πλέον μπορούν να εξυπηρετηθούν περισσότεροι χρήστες στην εν λόγω συχνότητα.

Στον αντίποδα των παραπάνω βρίσκεται και το βασικό μειονέκτημα της χρήσης του συγκεκριμένου προτύπου που δεν είναι άλλο από το κόστος των προϊόντων του 802.11a που είναι και αισθητά μεγαλύτερο από αυτό των συσκευών του 802.11b. Στην πραγματικότητα, η απόκλιση των τιμών ήδη έχει αρχίσει να μειώνεται αλλά ακόμη και τώρα το υψηλότερο κόστος αναγκάζει ορισμένες επιχειρήσεις ή και οικιακούς χρήστες να εγκαθιστούν το 802.11b με στόχο να μειώσουν το κόστος.

Στον πίνακα παρουσιάζεται το εύρος της συχνότητας των 5GHz που χρησιμοποιείται στο εν λόγω πρότυπο στις ΗΠΑ [37].

Μπάντα	Αναγνωριστικό καναλιού	Κεντρική Συχνότητα (GHz)
<b>UNII lower band</b>	36	5.18
	40	5.20
	44	5.22
	48	5.24
<b>UNII mid band</b>	52	5.26
	56	5.28
	60	5.30
	64	5.32
<b>UNII upper band</b>	149	5.745
	153	5.765
	157	5.785
	161	5.805

Πίνακας 5.3: Διαθέσιμα κανάλια χρήσης του προτύπου 802.11a στις ΗΠΑ.

Το πρότυπο 802.11a χρησιμοποιεί την τεχνική πολυπλεξίας και διαίρεσης της συχνότητας **OFDM (Orthogonal Frequency Division Multiplexing)** [38] αντί της DSSS ή της FHSS που χρησιμοποιεί το αρχικό 802.11. Η βασική ιδέα πίσω από αυτήν την τεχνική είναι η διαίρεση ενός καναλιού με υψηλό ρυθμό μετάδοσης σε περισσότερα από ένα κανάλια με μικρότερους ρυθμούς μετάδοσης αλλά και η χρήση αυτών των καναλιών για την ταυτόχρονη μετάδοση της πληροφορίας.

Η OFDM τεχνική βασίστηκε στην **FDM (Frequency Division Multiplexing)** η οποία και διαχωρίζει το εύρος ζώνης ενός καναλιού σε μικρότερου εύρους ζώνης κανάλια. Στην FDM, όλοι οι σταθμοί εκπέμπουν την ίδια χρονική στιγμή αλλά δεν παρεμβάλουν μεταξύ τους επειδή χρησιμοποιούν για την μετάδοση διαφορετικές φέρουσες συχνότητες. Επιπλέον είναι περιορισμένου εύρους ζώνης και αρκετά απομακρυσμένοι στο πεδίο της συχνότητας έτσι ώστε τα εκπεμπόμενα σήματά τους να μην επικαλύπτονται. Στο δέκτη, κάθε σήμα λαμβάνεται ανεξάρτητα χρησιμοποιώντας φίλτρα για την απομάκρυνση όλων των άλλων σημάτων εκτός του σταθμού με τον οποίο βρίσκεται σε επικοινωνία. Το φιλτραρισμένο αυτό σήμα μπορεί στη συνέχεια να αποδιαμορφωθεί ώστε να ανακτηθεί η αρχική πληροφορία που μεταδόθηκε.

Το μειονέκτημά της είναι πως ο τρόπος υλοποίησής της αφήνει αρκετά κενά μεταξύ των καναλιών που δημιουργούνται με αποτέλεσμα να εμφανίζεται σπατάλη στο συνολικό εύρος ζώνης του συστήματος. Το πρόβλημα αυτό αντιμετωπίζεται με την τεχνική της ορθογωνιότητας που χρησιμοποιείται στην OFDM δημιουργώντας ακόμα και υπερκαλυπτόμενα κανάλια στις συχνότητες που χρησιμοποιούνται χωρίς να εμφανίζονται ζητήματα παρεμβολών. Σε μια μετάδοση που χρησιμοποιεί OFDM, τα σήματα από τους διάφορους σταθμούς που περιέχουν την πληροφορία συνδυάζονται και προκύπτει μια ομαδοποιημένη ακολουθία δεδομένων. Τα δεδομένα αυτά μεταδίδονται κατόπιν όλα μαζί δημιουργώντας ένα σύνολο από συχνότητες. Οι συχνότητες αυτές είναι συγχρονισμένες ώστε να αποτρέπουν την μεταξύ τους παρεμβολή. Έτσι, παρόλο που το φάσμα των συχνοτήτων παρουσιάζει επικάλυψη, δεν προκαλείται στην ουσία κάποια παρεμβολή. Κατ' αυτόν τον τρόπο επιτυγχάνεται η μείωση των απαιτούμενων διαστημάτων μεταξύ των συχνοτήτων άρα και υψηλότερη



φασματική απόδοση μειώνοντας παράλληλα την πιθανότητα για απώλεια δεδομένων που μπορεί να οφείλεται σε παρεμβολές στην συχνότητα.

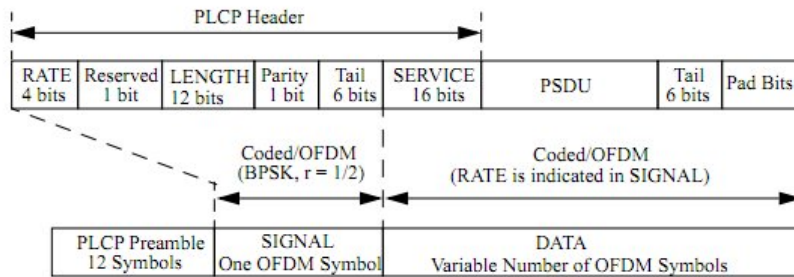
Όπως και κάθε άλλο πρότυπο, έτσι και το 802.11a αφορά τόσο στο PMD υπόστρωμα όσο και στο PLCP υπόστρωμα του φυσικού επιπέδου. Στο PMD υπόστρωμα χρησιμοποιούνται διάφορα σχήματα διαμόρφωσης και κωδικοποίησης και προβλέπεται η υποστήριξη ρυθμών μετάδοσης από 6 έως 54 Mbps. Σε κάθε περίπτωση το φυσικό αυτό υπόστρωμα μεταδίδει 250.000 σύμβολα ανά δευτερόλεπτο στα 48 κανάλια που είναι διαθέσιμα για μετάδοση και αυτό που μεταβάλλεται είναι ο αριθμός των bits που χρησιμοποιούνται για να αναπαραστήσουν ένα σύμβολο που έχει ως αποτέλεσμα τη διαφοροποίηση στους ρυθμούς μετάδοσης.

<b>Ρυθμός μετάδοσης (Mbps)</b>	<b>Σχήμα διαμόρφωσης</b>	<b>Κωδικοποιημένα bits ανά σύμβολο</b>	<b>Bits δεδομένων ανά σύμβολο</b>
<b>6</b>	BPSK	48	24
<b>9</b>	BPSK	48	36
<b>12</b>	QPSK	96	48
<b>18</b>	QPSK	96	72
<b>24</b>	16-QAM	192	96
<b>36</b>	16-QAM	192	144
<b>48</b>	64-QAM	288	192
<b>54</b>	64-QAM	288	216

*Πίνακας 5.4: Ρυθμοί μετάδοσης και σχήματα διαμόρφωσης / κωδικοποίησης του φυσικού επιπέδου του 802.11a*

Όσον αφορά το PLCP υπόστρωμα, δημιουργείται ένα πλαίσιο PPDU (PLCP Protocol Data Unit) που περιλαμβάνει τα PLCP preamble, PLCP Header, PSDU ,

tail bits και pad bits, τα οποία φαίνονται στην παρακάτω εικόνα [35].



Εικόνα 5.2: PPDU πλαίσιο του 802.11a

**PLCP Preamble (12 symbols):** Το πεδίο αυτό αποτελείται από 12 σύμβολα και χρησιμοποιείται από τον δέκτη στη λήψη του OFDM σήματος καθώς και στον συγχρονισμό του πομπού με τον δέκτη.

**PLCP Header (40 bits):** Περιλαμβάνει τα πεδία rate, reserved, length, parity, tail και service μήκους 4,1,12,1,6 και 16 bits αντίστοιχα.

- **Rate (4 bits):** Το πεδίο αυτό, ανάλογα με την τιμή που παίρνει, προσδιορίζει τον ρυθμό μετάδοσης των πλαισίων αν και τις περισσότερες φορές επιλέγεται ο χαμηλότερος ρυθμός μετάδοσης των 6 Mbps. Στον πίνακα παρουσιάζονται οι τιμές που μπορεί να πάρει το πεδίο αυτό καθώς και οι ρυθμοί μετάδοσης στους οποίους αντιστοιχούνται.

Τιμή πεδίου	Ρυθμός μετάδοσης
1101	6 Mbps
1111	9 Mbps
0101	12 Mbps
0111	18 Mbps
1001	24 Mbps
1011	36 Mbps

0001	48 Mbps
0011	54 Mbps

Πίνακας 5.5: Ρυθμοί μετάδοσης πλαισίου 802.11

- *Reserved (1 bit)*: Το πεδίο αυτό έχει την τιμή «0» και είναι δεσμευμένο για μελλοντική χρήση.
- *Length (12 bits)*: Η τιμή του πεδίου αυτού αντιπροσωπεύει το μέγεθος του MAC πλαισίου.
- *Parity (1 bit)*: Λαμβάνοντας υπόψη τα πεδία Rate, Reserved και Length, το πεδίο αυτό παίρνει την τιμή «0» ή «1» ώστε να εξασφαλιστεί η άρτια ισοτιμία.
- *Tail (6 bits)*: Το πεδίο αυτό περιέχει έξι συνεχόμενα bits με τιμή «0».
- *Service (16 bits)*: Όλα τα bits του πεδίου αυτού έχουν την τιμή «0». Τα πρώτα επτά χρησιμοποιούνται στον συγχρονισμό του πομπού με τον δέκτη και τα υπόλοιπα εννέα είναι δεσμευμένα για μελλοντική χρήση.

*Data*: Το πεδίο αυτό είναι μεταβλητού μήκους καθώς περιλαμβάνει το πλαίσιο του MAC καθώς και τα επιμέρους πεδία Service, PSDU, Tail και Pad.

***PSDU (Physical Layer Service Data Unit)***: αντιπροσωπεύει τα περιεχόμενα του πραγματικού 802.11 πλαισίου που αποστέλλεται.

- *Tail (6 bits)*: Τα έξι bit του πεδίου αυτού έχουν την τιμή «0» και χρησιμοποιούνται κυρίως από τον κώδικα διόρθωσης λαθών του δέκτη.
- *Pad bit*: Το πεδίο αυτό είναι μεταβλητού μήκους και χρησιμοποιείται στο να κάνει το μήκος του τμήματος Data κατάλληλο για μεταφορά όπως απαιτεί η μέθοδος OFDM.

Στον πίνακα που ακολουθεί αναφέρονται συνοπτικά ορισμένα από τα βασικότερα χαρακτηριστικά του εν λόγω προτύπου.

<b>802.11a</b>	
<b>Έκδοση</b>	1999
<b>Συχνότητα</b>	5 GHz
<b>Μέγιστος Ρυθμός μετάδοσης</b>	54 Mbps
<b>Φυσικό επίπεδο/Διαμόρφωση</b>	OFDM
<b>Εμβέλεια</b>	50-100 m
<b>Εύρος ζώνης</b>	300 MHz

*Πίνακας 5.6: Βασικά χαρακτηριστικά του 802.11a*

Τέλος, σχετικά με τις περιπτώσεις στις οποίες γίνεται χρήση του συγκεκριμένου προτύπου, θα πρέπει να αναφερθεί πως δεν είναι ιδιαίτερα διαδεδομένη η χρήση της εν λόγω τεχνολογίας [30]. Το 802.11a εμφανίζεται κυρίως στα δίκτυα κορμού μικρών επιχειρήσεων και γενικώς σε όλες τις εφαρμογές που απαιτούν μεγάλο εύρος ζώνης, αξιοπιστία, ταχύτητα στη μετάδοση αλλά και αποφυγή πιθανών παρεμβολών.

Το βασικό μειονέκτημά του που το κάνει και λιγότερο χρηστικό, είναι το θέμα ασυμβατότητας που παρουσιάζεται στις περιπτώσεις που πρέπει να υπάρξει συνεργασία με άλλα πρότυπα όπως είναι το 802.11b ή ακόμα και το ίδιο το 802.11 καθώς τα τελευταία λειτουργούν σε διαφορετικές μπάντες συχνοτήτων.

### **5.3 802.11g**

Το πρότυπο 802.11g [39] ανακοινώθηκε από την IEEE τον Ιούνιο του 2003. Σχεδιάστηκε με σκοπό να επιτευχθούν υψηλότεροι ρυθμοί μετάδοσης δεδομένων σε σύγκριση με τα προηγούμενα πρότυπα. Λειτουργεί στην μπάντα συχνοτήτων των 2.4GHz και υποστηρίζει ρυθμούς μετάδοσης έως και 54 Mbps διατηρώντας παράλληλα την απαιτούμενη συμβατότητα με τους χαμηλότερους ρυθμούς του προτύπου 802.11b. Χαρακτηριστικό του προτύπου αυτού είναι η χρήση της OFDM του 802.11a ως τεχνική διαμόρφωσης στις περιπτώσεις που οι ρυθμοί μετάδοσης

που επιτυγχάνονται είναι μεγαλύτεροι των 20 Mbps αυξάνοντας κατ' αυτόν τον τρόπο την αποδοτικότητα του δικτύου.

Το πρότυπο 802.11g συμπληρώνουν τέσσερις νέες λειτουργίες που το κάνουν να ξεχωρίζει από τα προηγούμενα πρότυπα. Οι λειτουργίες αυτές είναι οι εξής:

- Το πρότυπο αυτό παρέχει υποστήριξη για τέσσερα διαφορετικά φυσικά επίπεδα.
- Η υποχρεωτική χρήση του σύντομου πλαισίου (short) που εμφανίζεται στο 802.11b.
- Το ERP δίκτυο.

Ενώ το 802.11b χρησιμοποιεί μόνο την DSSS ως φυσικό επίπεδο, το 802.11g μπορεί να χρησιμοποιήσει τόσο την DSSS, την OFDM ή και των συνδυασμό τους στην μπάντα των 2.4 GHz για την επίτευξη του ρυθμού μετάδοσης των 54 Mbps. Ο συνδυασμός αυτών των δύο επιτυγχάνεται με την χρήση τεσσάρων φυσικών επιπέδων, γνωστών και ως **ERP (Extended Rate Physicals)** που συνυπάρχουν κατά την μετάδοση ενός πλαισίου δεδομένων παρέχοντας στον πομπό και στον δέκτη τη δυνατότητα να επιλέξουν ενός από αυτά τα επίπεδα για να παίξει τον ρόλο του φυσικού επιπέδου. Τα τέσσερα αυτά φυσικά επίπεδα είναι τα:

- ERP-DSSS/CCK: Είναι το φυσικό στρώμα που χρησιμοποιείται στο 802.11b. Η τεχνική μετάδοσης του σήματος είναι η DSSS και η τεχνική διαμόρφωσης η CCK. Οι ρυθμοί μετάδοσης που επιτυγχάνονται είναι οι ρυθμοί που προσφέρονται και από το 802.11b, δηλαδή τα 1,2,5.5 και 11 Mbps.
- ERP-OFDM: Χρησιμοποιείται η τεχνική διαμόρφωσης OFDM που πρωτοεμφανίστηκε στο 802.11a αλλά στη συχνότητα των 2.4 GHz αυτή τη φορά. Οι ρυθμοί μετάδοσης που επιτυγχάνονται είναι οι ίδιοι με τους ρυθμούς του 802.11a με μέγιστο τα 54 Mbps.
- ERP-DSSS/PBCC: Είναι το φυσικό επίπεδο του 802.11b και προσφέρει τους ίδιους ρυθμούς μετάδοσης με το ERP-DSSS/CCK. Η μόνη τους διαφορά είναι πως σαν τεχνική διαμόρφωσης δεν χρησιμοποιείται η CCK

αλλά η PBCC. Η IEEE επέκτεινε το φυσικό αυτό επίπεδο προσφέροντας για χρήση τους ρυθμούς μετάδοσης των 22 και των 33 Mbps.

- DSSS-OFDM: Είναι ένα νέο φυσικό επίπεδο που χρησιμοποιεί ένα συνδυασμό των τεχνικών DSSS και OFDM. Η κεφαλίδα του φυσικού επιπέδου του πακέτου μεταφέρεται χρησιμοποιώντας την DSSS, ενώ η καθαρή πληροφορία του πακέτου μεταδίδεται με την χρήση της OFDM.

Από τα τέσσερα φυσικά επίπεδα που αναφέρθηκαν, τα πρώτα δύο, δηλαδή το ERP-DSSS/CCK και το ERP-OFDM είναι υποχρεωτικά για κάθε συσκευή που υλοποιεί το 802.11g ενώ τα τελευταία δύο (ERP-DSSS/PBCC και DSSS-OFDM) είναι προαιρετικά. Οι ρυθμοί μετάδοσης που επιτυγχάνονται φαίνονται παρακάτω.

Φυσικό επίπεδο	Ρυθμοί μετάδοσης (Mbps)
ERP-DSSS/CCK	1,2, 5.5 και 11
ERP-OFDM	6,9,12,18,24,36,48 και 54
ERP-DSSS/PBCC	1,2, 5.5 ,11, 22 και 33
DSSS-OFDM	6,9,12,18,24,36,48 και 54

Πίνακας 5.7: Ρυθμοί μετάδοσης φυσικών επιπέδων του 802.11g

Στο 802.11b, το PLCP preamble του πακέτου του φυσικού επιπέδου που χρησιμοποιείται κυρίως για τον συγχρονισμό μεταξύ του πομπού και του δέκτη χωρίζεται σε δύο κατηγορίες, αυτό της κανονικής μορφής που περιέχει πλεονάζουσα πληροφορία και αυτό της σύντομης μορφής που βοηθάει στην βελτίωση της απόδοσης του δικτύου. Στο 802.11g η χρήση του σύντομου αυτού πλαισίου είναι υποχρεωτική.

Όσον αφορά το ERP δίκτυο, στο 802.11b οι τιμές για το slot time αλλά και για το ελάχιστο μήκος παραθύρου ισχυρισμού είναι οι 20μs και 31 slots αντίστοιχα. Το 802.11g υιοθετεί τις παραμέτρους αυτές κυρίως για λόγους συμβατότητας. Οι προδιαγραφές όμως του 802.11b για τους ρυθμούς μετάδοσης φτάνουν μέχρι τα 11 Mbps. Όταν το φυσικό επίπεδο του 802.11g είναι το ERP-OFDM με ρυθμούς

μετάδοσης από 6 έως 54 Mbps, οι τιμές αυτές μειώνουν την απόδοση του δικτύου. Σε αυτήν την περίπτωση, οι προτεινόμενες τιμές για το slot time και το minimum contention window είναι αυτές που χρησιμοποιούνται στο 802.11a, δηλαδή τα 9μs και τα 15 slots αντίστοιχα.

Το 802.11g παρέχει τη δυνατότητα για δυναμική προσαρμογή των τιμών για το slot time και το ελάχιστο μήκος του contention window, προσθέτοντας ένα ERP flag στο πλαίσιο beacon που στέλνεται στους σταθμούς του δικτύου και παρέχει πληροφορίες σχετικά με το δίκτυο. Το flag αυτό ενεργοποιείται και χρησιμοποιείται μόνο στην περίπτωση που οι σταθμοί χρησιμοποιούν ως ρυθμούς μετάδοσης αυτούς που προσφέρει το ERP-OFDM φυσικό επίπεδο. Στην περίπτωση λοιπόν που όλοι οι σταθμοί μπορούν να υποστηρίξουν αυτό το φυσικό επίπεδο, οι τιμές των slot time και contention window εξαρτώνται από το είδος του δικτύου. Για τα BSS δίκτυα οι τιμές που παίρνουν είναι τα 9μs και 15 slots αντίστοιχα και βασική προϋπόθεση είναι η υποστήριξη των ρυθμών μετάδοσης του ERP-OFDM φυσικού επιπέδου στις ανταλλαγές των δεδομένων. Κάτι αντίστοιχο ισχύει και για τα IBSS δίκτυα, με τη μόνη διαφορά πως το slot time είναι στα 20 μs.

Ένα από τα σημαντικότερα πλεονεκτήματα του 802.11g είναι η δυνατότητα που παρέχει στην επικοινωνία και συνεργασία των 802.11g και 802.11b συσκευών. Ωστόσο, οι συσκευές που υλοποιούν το 802.11g επηρεάζουν διαφορετικά την απόδοση του δικτύου όταν χρησιμοποιούν τους ρυθμούς μετάδοσης του ERP-OFDM φυσικού επιπέδου, εάν υπάρχουν συσκευές που υλοποιούν το 802.11b στο ίδιο δίκτυο. Για παράδειγμα, σε ένα αμιγώς 802.11b δίκτυο το μέγιστο throughput που μπορεί να επιτευχθεί είναι τα 5.8 Mbps ανάλογα πάντα με την απόσταση των σταθμών και τους ρυθμούς μετάδοσης που χρησιμοποιούνται. Σε ένα δίκτυο που υλοποιείται αμιγώς το 802.11g το throughput μπορεί να φτάσει στα 22-24 Mbps εάν χρησιμοποιούνται ρυθμοί μετάδοσης των 54 Mbps.

Σε ένα δίκτυο που υλοποιούνται και τα δύο πρότυπα επειδή η πλεονάζουσα πληροφορία έχει αντίκτυπο στην μείωση του throughput, χρησιμοποιούνται δύο τεχνικές προκειμένου να διατηρηθεί η απόδοση του δικτύου μέσω της προστασίας που παρέχεται στην επικοινωνία των διαφορετικών αυτών συσκευών. Οι συσκευές που υλοποιούν το 802.11b στο δίκτυο, δεν είναι σε θέση να αναγνωρίσουν τα

μηνύματα που μεταδίδονται από τις συσκευές που υλοποιούν το 802.11g και χρησιμοποιούν ως τεχνική μετάδοσης την OFDM, με αποτέλεσμα να προκαλούνται συγκρούσεις όταν οι πρώτοι σταθμοί μεταδίδουν ταυτόχρονα χωρίς να αντιληφθούν την κίνηση στο δίκτυο. Οι 802.11g σταθμοί συνεχίζουν να ανταλλάσσουν τα δεδομένα τους σύμφωνα με τους ρυθμούς μετάδοσης της OFDM αλλά ενημερώνουν τους 802.11b σταθμούς αποστέλλοντας τους ένα μήνυμα στον δικό τους ρυθμό μετάδοσης πως για ένα χρονικό διάστημα θα είναι σε εξέλιξη μία μετάδοση του δικού τους πλαισίου. Οι δύο τεχνικές που χρησιμοποιούνται για την προστασία των δεδομένων και την διατήρηση της απόδοσης του δικτύου είναι η γνωστή **RTS/CTS** και η **CTS-To Self**.

Όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, στην RTS/CTS [40] τεχνική, όλοι οι 802.11b σταθμοί του δικτύου που θέλουν να μεταδώσουν τα δεδομένα τους θα πρέπει να στείλουν ένα πλαίσιο τύπου RTS στον παραλήπτη της πληροφορίας για να ζητήσουν την άδεια ώστε να προχωρήσουν στη μετάδοση και αυτός με τη σειρά του να απαντήσει με ένα πλαίσιο τύπου CTS για να τους παραχωρήσει την πρόσβαση στο μέσο. Η διαδικασία αυτή μειώνει τις πιθανότητες να αποσταλούν πλαίσια από 802.11b σταθμούς ενώ ταυτόχρονα μεταδίδουν οι 802.11g σταθμοί και έχει ως αποτέλεσμα την διατήρηση της απόδοσης του δικτύου μιας και οι συγκρούσεις δεν είναι τόσο συχνές. Στην πραγματικότητα όμως με την πλεονάζουσα πληροφορία που αποστέλλεται από τα RTS και τα CTS πλαίσια αναπόφευκτα μειώνεται.

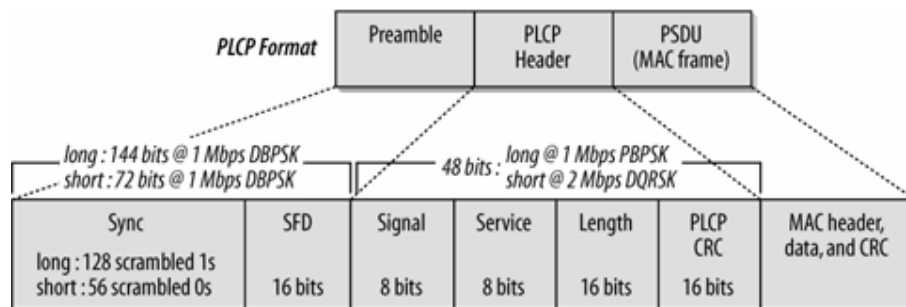
Παρόλα αυτά, λόγω της ιδιαιτερότητάς του ένα τέτοιο μεικτό δίκτυο μπορεί να αποφύγει τις συγκρούσεις των πλαισίων χρησιμοποιώντας και τις τιμές των slot time και contention window για αυξηθεί η απόδοση του δικτύου. Οι σταθμοί που λειτουργούν βάσει του 802.11b στο δίκτυο έχουν για slot time τα 20 μs και μήκος του contention window τα 31 slots, ενώ οι 802.11g σταθμοί έχουν 9 μs και 15 slots αντίστοιχα (τιμές που προδιαγράφονται στο 802.11a). Αυτό σημαίνει πως όταν προκύψει μία σύγκρουση στο μεικτό δίκτυο όλοι οι σταθμοί θα υλοποιήσουν τους αλγορίθμους οπισθοχώρησής βάσει του 802.11b. Εάν το δίκτυο αποτελείται πλήρως από 802.11g σταθμούς οι τιμές που χρησιμοποιούνται είναι του 802.11a.



Η τεχνική CTS-To Self [41] χρησιμοποιείται κυρίως για να μειώσει την πλεονάζουσα πληροφορία που κυκλοφορεί στο δίκτυο χρησιμοποιώντας την προηγούμενη τεχνική αλλά δεν είναι τόσο καλή όσο αυτή στην αντιμετώπιση του προβλήματος του κρυμμένου κόμβου. Στην τεχνική αυτή, ο σταθμός που θέλει να μεταδώσει τα δεδομένα του θα πρέπει να αποστείλει ένα πλαίσιο τύπου CTS στο δίκτυο με τους ρυθμούς μετάδοσης που χρησιμοποιούνται στο 802.11b, το οποίο και θα λάβουν όλοι οι υπόλοιποι σταθμοί που βρίσκονται στην εμβέλειά του. Η ιδιαιτερότητα του πλαισίου αυτού είναι πως ο αποστολέας ορίζει στο πλαίσιο της διεύθυνσης ως παραλήπτη τον ίδιο του τον εαυτό ώστε να ενημερώσουν όλοι οι υπόλοιποι τους NAV μετρητές τους και να μην προσπαθήσουν να αποστείλουν τα δικά τους δεδομένα τουλάχιστον για τη χρονική διάρκεια που απαιτείται ώστε να αποσταλούν τα δεδομένα αλλά και το μήνυμα επιβεβαίωσης της ορθής λήψης ACK σε ρυθμούς μετάδοσης του 802.11a από τους σταθμούς που υλοποιούν το 802.11g.

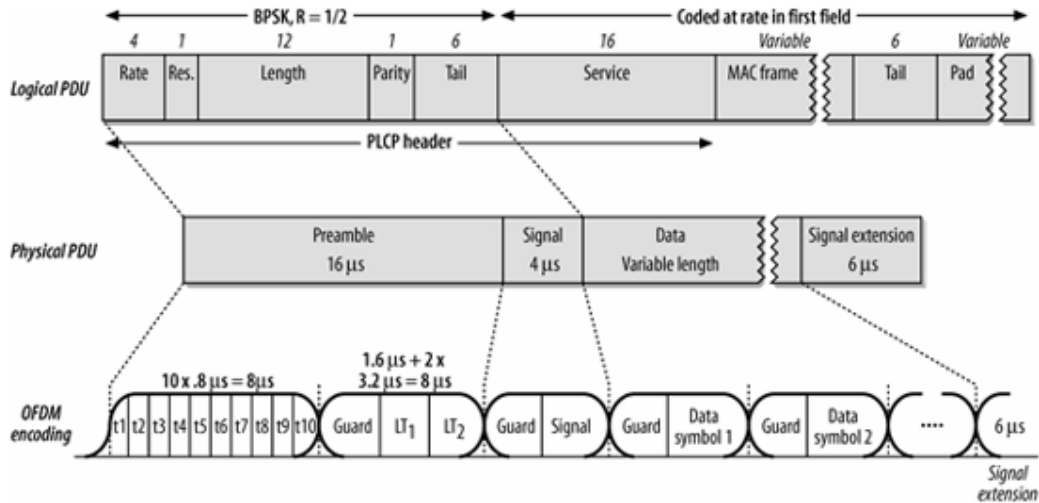
Όπως αναφέρθηκε και νωρίτερα, το 802.11g καθορίζει ως υποχρεωτικά φυσικά επίπεδα τα ERP-DSSS/CCK και ERP-OFDM ενώ τα ERP-DSSS/PBCC και DSSS-OFDM θεωρούνται προαιρετικά. Ανάλογα με τους σταθμούς που απαρτίζουν το δίκτυο χρησιμοποιούνται και διαφορετικά πλαίσια. Παρακάτω παρουσιάζονται τα πλαίσια των δύο υποχρεωτικών φυσικών επιπέδων [42] .

Εάν το δίκτυο αποτελείται τόσο από 802.11b σταθμούς όσο και από 802.11g, το πλαίσιο που χρησιμοποιείται είναι το εξής:



Εικόνα 5.3: Πλαίσιο φυσικού επιπέδου ERP-DSSS CCK

Ενώ στην περίπτωση που το δίκτυο αποτελείται αμιγώς από 802.11g συσκευές θα χρησιμοποιηθεί το:



Εικόνα 5.4: Πλαίσιο φυσικού επιπέδου ERP-OFDM

### Preamble

Το Preamble αποτελείται από τα πεδία Sync και SFD που χρησιμοποιούνται για τον συγχρονισμό και την αρχικοποίηση του πλαισίου αντίστοιχα. Συναντάται είτε στην κανονική του μορφή των 144 bits είτε στην σύντομη του εκδοχή των 72 bits. Και στις δύο περιπτώσεις το preamble μεταδίδεται με ταχύτητα του ενός Mbps.

### Header

Η κεφαλίδα του πλαισίου αποτελείται από τα επιμέρους πεδία Signal, Service, Length και CRC με τα δύο τελευταία πεδία να είναι πανομοιότυπα με τα αντίστοιχα πεδία του 802.11b. Τα πεδία αυτά προσδιορίζουν τον ρυθμό μετάδοσης ανάλογα με το φυσικό επίπεδο που χρησιμοποιείται, την τεχνική της κωδικοποίησης, τον χρόνο σε μs που απαιτείται για την μετάδοση του πλαισίου και τέλος τον κώδικα προστασίας των πληροφοριών του πλαισίου. Πιο συγκεκριμένα, το πεδίο Service περιέχει bits ελέγχου προκειμένου να βοηθήσει τον δέκτη να αποκωδικοποιήσει το πλαίσιο. Τα bits 0, 1, και 4 παίρνουν πάντα την τιμή «0». Σε όλους τους σταθμούς 802.11g, το δεύτερο bit έχει πάντα την τιμή «1». Το τρίτο bit όταν η τεχνική διαμόρφωσης είναι η PBCC παίρνει την τιμή «1» και την τιμή «0» για τις τεχνικές DSSS, CCK, και DSSS-OFDM. Τα τελευταία τρία bits του πεδίου αυτού χρησιμοποιούνται από το πεδίο Length των σταθμών που θα λάβουν το πλαίσιο για να καθορίσουν το μήκος του πλαισίου αυτού.

Όσον αφορά το πεδίο Signal και τις πληροφορίες που μεταφέρει σχετικά με τους ρυθμούς μετάδοσης των διαφορετικών φυσικών επιπέδων, στον παρακάτω πίνακα παρουσιάζονται οι τιμές που προσδιορίζουν τα διαφορετικά αυτά φυσικά επίπεδα.

Ταχύτητα / φυσικό επίπεδο	Κωδικοποίηση
1 Mbps / ERP-DSSS	10
2 Mbps / ERP-DSSS	20
5.5 Mbps (ERP-CCK, ERP-PBCC)	55
11 Mbps (ERP-CCK, ERP-PBCC)	110
22 Mbps (ERP-PBCC)	220
33 Mbps (ERP-PBCC)	33

Πίνακας 5.8: Τιμές πεδίου Signal ανά φυσικό επίπεδο

### Data

Το πεδίο αυτό περιέχει την καθαρή πληροφορία που είναι προς μετάδοση. Τα δεδομένα του πεδίου αυτού μπορούν να έχουν διαμορφωθεί είτε με την PBCC τεχνική είτε με την OFDM.

Τα βασικότερα σημεία του 802.11g παρουσιάζονται στον παρακάτω πίνακα.

802.11g	
Έκδοση	2003
Συχνότητα	2.4 GHz
Μέγιστος Ρυθμός μετάδοσης	54 Mbps
Φυσικό επίπεδο	DSSS / CCK / OFDM
Εμβέλεια	100 m

Πίνακας 5.9: Βασικά χαρακτηριστικά του 802.11g

Η πιο σημαντική βελτίωση που προσφέρει το πρότυπο 802.11g έναντι των προγενέστερων του και κυρίως του 802.11b είναι η επίτευξη υψηλότερης ταχύτητας στη μεταφορά των δεδομένων [30]. Η ικανότητα του να λειτουργεί σε ρυθμούς μετάδοσης έως και 54 Mbps προσφέρει στο 802.11g υψηλότερη υπεροχή σε σχέση με τις άλλες συσκευές που είναι συμβατές με το αρχικό 802.11 και λειτουργούν στην μπάνα συχνοτήτων των 2.4-GHz. Επιπλέον, η υποστήριξη της τεχνικής OFDM είναι ένα άλλο πλεονέκτημα που προσφέρει το 802.11g έναντι του βασικού 802.11 προτύπου. Η OFDM επιτρέπει στις 802.11g συσκευές να λειτουργήσουν με πιο αποτελεσματικό τρόπο από τις υπόλοιπες συσκευές που λειτουργούν στα 2.4GHz.

Οι απλοί χρήστες στα οικιακά δίκτυα πιθανώς να επιλέξουν την χρήση μιας συσκευής που λειτουργεί βάσει του προτύπου 802.11b ακόμα κι αν συμβιβάζονται με την χαμηλότερη απόδοση που αυτό προσφέρει για ένα και μόνο λόγο. Η αγορά των συσκευών αυτών έχει μικρότερο κόστος από τις 802.11g συσκευές αν και η προώθηση του συγκεκριμένου προτύπου το έχει φέρει στην πρώτη θέση προτίμησης των χρηστών κάνοντας πιο συμβατό το κόστος του. Τα μεγαλύτερα τοπικά δίκτυα, κυρίως τα δίκτυα υποδομής ή τα ασύρματα δίκτυα που λειτουργούν σε επιχειρήσεις απαρτίζονται σχεδόν εξ' ολοκλήρου από 802.11g συσκευές μιας και οι διαχειριστές των συγκεκριμένων δικτύων ενδιαφέρονται πρώτα απ' όλα για την επίτευξη της βέλτιστης απόδοσης του δικτύου τους αλλά και την γρηγορότερη εξυπηρέτηση των χρηστών τους.

Και στις δύο περιπτώσεις, η αναβάθμιση των συσκευών από το 802.11b στο 802.11g είναι σχετικά εύκολη διαδικασία μιας και ένα από τα βασικότερα χαρακτηριστικά του τελευταίου και ίσως ο λόγος που έγινε τόσο επιτυχημένο είναι η συμβατότητα που προσφέρει με τις παλαιότερες συσκευές.

Από την άλλη μεριά, ένα από τα βασικότερα μειονεκτήματα της τεχνολογίας αυτής είναι η ύπαρξη παρεμβολών λόγω της πολύ διαδεδομένης συχνότητας που χρησιμοποιείται, αυτή των 2.4 GHz. Όπως αναφέρθηκε και στα μειονεκτήματα του 802.11b που λειτουργεί στην ίδια συχνότητα, οι συσκευές που επιλέγουν για να λειτουργήσουν σε αυτή τη συχνότητα είναι αρκετές με πιο δημοφιλείς τα Bluetooth

που είναι και τα κυρίως υπεύθυνα για την ύπαρξη παρεμβολών στα τοπικά ασύρματα δίκτυα των 2.4GHz.

Συνοψίζοντας, θα μπορούσαμε να πούμε πως το πρότυπο 802.11g υιοθέτησε τα πλεονεκτήματα των δύο προγενέστερων προτύπων, παίρνοντας από το 802.11a τους ρυθμούς μετάδοσης που είναι πολύ μεγαλύτεροι από τους αντίστοιχους της τεχνολογίας του 802.11b, και από το 802.11b τη συχνότητα μετάδοσης που είναι πιο διαδεδομένη και περισσότερο αποδοτική όσον αφορά την κατανάλωση της ενέργειας από τους σταθμούς του δικτύου από την συχνότητα μετάδοσης που χρησιμοποιείται στο 802.11a. Βάσει αυτών των δύο χαρακτηριστικών, το 802.11g είναι σε θέση να συνεργαστεί με τους σταθμούς που λειτουργούν στις ίδιες συχνότητες αλλά με προγενέστερα πρότυπα χρησιμοποιώντας τεχνικές διαμόρφωσης αλλά και μετάδοσης του σήματος που προσαρμόζονται ανάλογα με το είδος των συσκευών που απαρτίζουν το δίκτυο.

#### **5.4 802.11e**

Τα MAC πρωτόκολλα του IEEE 802.11 που έχουμε αναλύσει έως τώρα, δεν παρέχουν υπηρεσίες ώστε να δίνουν προτεραιότητα σε ορισμένους από τους σταθμούς που μεταδίδουν. Όλοι οι σταθμοί έχουν την ίδια προτεραιότητα, με αποτέλεσμα να μη μπορούν να υποστηριχθούν εφαρμογές που απαιτούν ποιότητα υπηρεσίας όπως για παράδειγμα αποστέλλονται δεδομένα φωνής ή εικόνας.

Το 802.11e [35] ανακοινώθηκε το 2000 από την IEEE και έγινε διαθέσιμο για χρήση στα τέλη του 2001. Βασικός στόχος της ομάδας εργασίας του 802.11e ήταν η ενίσχυση του ήδη υπάρχοντος υποστρώματος MAC του αρχικού 802.11 ώστε να υποστηρίζεται η αμφίδρομη ποιότητα υπηρεσιών **QoS (Quality Of Service)** σε εφαρμογές όπως είναι η μετάδοση της φωνής και της εικόνας που παρουσιάζονται ως ευαίσθητες σε σύγκριση με τη μετάδοση των απλού τύπου δεδομένων. Ουσιαστικά, ο μηχανισμός της παροχής ποιότητας υπηρεσιών QoS χρησιμοποιείται για να εξασφαλιστεί ότι οι εφαρμογές φωνής και εικόνας έχουν προτεραιότητα έναντι της μετάδοσης των δεδομένων όπως είναι οι περιπτώσεις του ηλεκτρονικού ταχυδρομείου ή και την περιήγηση στο διαδίκτυο.

Γενικώς, τα ασύρματα τοπικά δίκτυα λειτουργούν σε ικανοποιητικό βαθμό όταν χρησιμοποιούνται εφαρμογές που δεν παρουσιάζουν ευαισθησία στην μετάδοση των δεδομένων τους όπως είναι η πρόσβαση σε αρχεία ή η αποστολή και η λήψη e-mail χωρίς σημαντικές απώλειες στην απόδοση του συστήματος. Καθώς όμως οι επιχειρήσεις αρχίζουν να χρησιμοποιούν τα ασύρματα δίκτυα ως βασικό μέσο για την μετάδοση των δεδομένων τους, η ανάγκη για υποστήριξη της μετάδοσης της φωνής και της εικόνας είναι πλέον υποχρεωτική.

Και στο πρότυπο 802.11e, το πρόβλημα του κρυμμένου κόμβου αποτελεί τροχοπέδη στην προσπάθεια για παροχή ποιότητας στις υπηρεσίες που χρησιμοποιούνται. Βέβαια με την ανταλλαγή μηνυμάτων τύπου RTS/CTS το πρόβλημα του κρυμμένου κόμβου αντιμετωπίζεται αλλά δεν πρέπει να παραβλέψουμε το γεγονός πως η τεχνική αυτή συνήθως τίθεται σε λειτουργία μετά την ανίχνευση κάποιας σύγκρουσης και αφού οπισθοχωρήσει ο σταθμός βάσει ενός αλγορίθμου. Η αυξημένη αυτή ευαισθησία του δικτύου μπορεί να έχει αντίκτυπο σε εφαρμογές που είναι από τη φύση τους ευαίσθητες. Επιπλέον, οι σταθμοί που χρησιμοποιούν την τεχνική του RTS / CTS για κάθε πλαίσιο, συμβάλλουν στην μείωση της απόδοσης του δικτύου μεταφέροντας ουσιαστικά μεγάλο όγκο πλεονάζουσας πληροφορίας.

Το 802.11e, ως πρότυπο βελτίωσης των προγενέστερων 802.11a και 802.11b, λειτουργεί είτε μεταξύ των συχνοτήτων 5.725 GHz και 5.850 GHz που είναι και οι συχνότητες που χρησιμοποιεί το 802.11a, είτε μεταξύ των συχνοτήτων 2.4 GHz και 2.4835 GHz που είναι και οι συχνότητες του 802.11b αντίστοιχα.

Στο φυσικό επίπεδο του 802.11e δεν υπάρχουν σημαντικές διαφορές με τα προγενέστερα πρότυπα, ενώ στο MAC υπόστρωμα διάφορες τεχνικές συνεργάζονται για την επίτευξη της ποιότητας των υπηρεσιών. Η μετάδοση των δεδομένων στο δίκτυο γίνεται βάσει δύο περιόδων, όπως και στην PCF τεχνική, αυτή του ανταγωνισμού των σταθμών για την κατοχή του μέσου (contention period - CP) και αυτήν της ελεύθερης από ανταγωνισμό κατοχής (contention free period - CFP). Η τεχνική μετάδοσης **HCF (Hybrid Coordination Function)** που χρησιμοποιείται στο 802.11e, αποτελείται από δύο βασικές επιμέρους τεχνικές: την **EDCA (Enhanced Distributed Channel Access)** και την **HCCA (HCF**

**Control Channel Access**) [43]. Η EDCA είναι ο βασικός αλλά και υποχρεωτικός μηχανισμός πρόσβασης στο μέσο του 802.11e και χρησιμοποιείται στις περιόδους ανταγωνισμού, ενώ η HCCA είναι προαιρετική και χρησιμοποιείται στις περιόδους ανταγωνισμού αλλά και στις περιπτώσεις που δεν υφίσταται ανταγωνισμός μεταξύ των σταθμών για την κατοχή του μέσου. Γενικώς, η HCF χρησιμοποιεί και τις δύο μεθόδους πρόσβασης στο μέσο DCF και PCF και γι' αυτό το λόγο χαρακτηρίστηκε ως υβριδική.

Ο σταθμός που λειτουργεί ως κεντρικός συντονιστής για την υποστήριξη των λειτουργιών της ποιότητας των υπηρεσιών QoS σε ένα ασύρματο δίκτυο, ονομάζεται υβριδικός συντονιστής **HC (Hybrid Coordinator)**. Συνήθως, ένας τέτοιος συντονιστής είναι ένα 802.11e AP (QAP-QoS Access Point).

Βασικό χαρακτηριστικό του 802.11e αποτελεί η διάρκεια κατά την οποία ένας σταθμός που λειτουργεί βάσει του προτύπου αυτού (QSTA-QoS Station) μπορεί να απασχολεί το μέσο με τη μετάδοση των δεδομένων του. Κάθε σταθμός δεσμεύεται να χρησιμοποιήσει το μέσο για ένα συγκεκριμένο και προκαθορισμένο χρονικό διάστημα. Το χαρακτηριστικό αυτό αναφέρεται στο 802.11e ως πιθανότητα μετάδοσης **TXOP (Transmission Opportunity)**.

Στην HCF ο κύριος τρόπος απόκτησης δικαιώματος εκπομπής στο ασύρματο μέσο είναι το TXOP. Κάθε TXOP χαρακτηρίζεται από μία χρονική στιγμή έναρξης και μια καθορισμένη μέγιστη διάρκεια. Οι σταθμοί έχουν τη δυνατότητα να αποκτήσουν TXOPs χρησιμοποιώντας τον ένα ή και τους δύο μηχανισμούς πρόσβασης του καναλιού. Αν ένα TXOP παρέχεται μέσω της πρόσβασης του μέσου με ανταγωνισμό τότε καλείται EDCA TXOP, ενώ όταν

αποκτηθεί χρησιμοποιώντας την ελεγχόμενη πρόσβαση στο μέσο χαρακτηρίζεται ως HCCA TXOP.

Είναι γνωστό πως η διαδικασία τεμαχισμού (fragmentation) ενός MSDU σε μικρότερα πακέτα υποστρώματος MAC έχει ως σκοπό την αύξηση της απόδοσης του δικτύου αφού μεγιστοποιεί την πιθανότητα επιτυχούς μετάδοσης μεγάλου όγκου δεδομένων σε ένα επιβαρυσμένο από φόρτο δίκτυο.

Στο 802.11e όμως, οι σταθμοί που έχουν την δυνατότητα να χρησιμοποιούν την τεχνική αυτή θα πρέπει να λαμβάνουν υπόψη τους την χρονική διάρκεια που τους έχει παραχωρηθεί από το TXOP ώστε να προλάβουν να ολοκληρώσουν την αποστολή των δεδομένων τους.

Το 802.11e καθορίζει 8 προτεραιότητες χρήστη για την παροχή της ποιότητας των υπηρεσιών (QoS). Αυτές οι 8 προτεραιότητες χρήστη ομαδοποιούνται σε 4 κατηγορίες πρόσβασης (AC-Access Categories) [44] και είναι το voice, το video, το best effort και το background και παρουσιάζονται στον παρακάτω πίνακα.

Προτεραιότητα	Κατηγορία Πρόσβασης (AC)	Ονομασία
1	0	Background
2	0	Background
0	0	Best Effort
3	1	Best Effort
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

Πίνακας 5.10: Κατηγορίες πρόσβασης του 802.11e

#### 5.4.1 EDCA (Enhanced Distributed Channel Access)

Η χρήση των κατηγοριών προτεραιότητας βασίζεται σε τρεις σημαντικές αλλαγές στη λειτουργία της DCF του αρχικού 802.11, οι οποίες και απαρτίζουν την EDCA. Οι τρεις σημαντικές αλλαγές είναι:

- Σύσταση τεσσάρων ουρών πρόσβασης που υλοποιούνται στους σταθμούς.



- Χρήση του μετρητή **AIFS (Arbitrated Inter-Frame Space)** με διαφορετικές τιμές για καθεμία από τις τέσσερις ουρές προτεραιότητας ώστε να αντικατασταθεί ο DIFS που χρησιμοποιείται στο αρχικό 802.11.
- Τυχαίες τιμές για το μέγιστο και το ελάχιστο μήκος του παραθύρου ανταγωνισμού για καθεμία από τις τέσσερις ουρές προτεραιότητας.

Σε αντίθεση με τον μετρητή DIFS που χρησιμοποιείται για όλα τα πλαίσια δεδομένων ανεξαρτήτων είδους και παραμένει σταθερός, για την χρήση του AIFS, κάθε σταθμός που πρόκειται να αποστείλει τα δεδομένα του θα πρέπει να περιμένει το μέσο να δηλωθεί ως διαθέσιμο, να οπισθοχωρήσει για ένα συγκεκριμένο χρονικό διάστημα που καθορίζεται από το παράθυρο ανταγωνισμού και να περιμένει για ένα ακόμη χρονικό διάστημα του οποίου η διάρκεια εξαρτάται από το είδος των δεδομένων που πρόκειται να μεταδοθούν και της ουράς στην οποία ανήκουν.

Παράλληλα χρησιμοποιείται και ο SIFS που μεσολαβεί στα πλαίσια RTS,CTS,Data και ACK όπως και σε όλες τις άλλες τεχνικές μετάδοσης. Πιο συγκεκριμένα, οι τιμές που παίρνει ο AIFS είναι οι εξής:

Κατηγορία	Τρόπος υπολογισμού	AIFS
<b>voice</b>	1 SIFS + 2 * slot time	2
<b>video</b>	1 SIFS + 2 * slot time	2
<b>best effort</b>	1 SIFS + 3 * slot time	3
<b>background</b>	1 SIFS + 7 * slot time	7

Πίνακας 5.11: Τιμές του μετρητή AIFS ανά κατηγορία

Όπως αναφέρθηκε και νωρίτερα, το 802.11e μπορεί να υλοποιηθεί βάσει των προτύπων 802.11b και 802.11a/g. Οι μέγιστες αλλά και οι ελάχιστες τιμές που μπορεί να πάρει το παράθυρο ανταγωνισμού βάσει του προτύπου πάνω στο οποίο υλοποιείται η παροχή ποιότητας των υπηρεσιών, με χρήση της μεθόδου EDCA είναι οι εξής:

Κατηγορία	CWmin	CWmax
voice	7	15
video	15	31
best effort	31	1023
background	31	1023

Πίνακας 5.12: Τιμές του CW για το QoS στο 802.11b φυσικό επίπεδο

Κατηγορία	CWmin	CWmax
voice	3	7
video	7	15
best effort	15	1023
background	15	1023

Πίνακας 5.13: Τιμές του CW για το QoS στο 802.11a/g φυσικό επίπεδο

Όταν χρησιμοποιείται η EDCA [45], πριν τη μετάδοση οποιουδήποτε μηνύματος το AP μέσω πλαισίων τύπου beacon ενημερώνει όλους τους σταθμούς του δικτύου για τις παραμέτρους της EDCA. Σε περίπτωση που το AP δεν ενημερώσει τους σταθμούς, θα χρησιμοποιηθούν οι αρχικές ρυθμίσεις που είναι καταγεγραμμένες σε κάθε σταθμό για την EDCA.

Πριν την είσοδο στο υπόστρωμα MAC, σε κάθε πακέτο δεδομένων που λαμβάνεται από υψηλότερο επίπεδο έχει ανατεθεί μια συγκεκριμένη τιμή όσον αφορά την προτεραιότητα του χρήστη του. Κάθε πακέτο δεδομένων από το υψηλότερο επίπεδο μαζί με την τιμή της προτεραιότητας αντιστοιχίζονται με μία αντίστοιχη κατηγορία πρόσβασης και δημιουργείται ο TXOP που ουσιαστικά είναι και η καθορισμένη διάρκεια κατά την οποία ο σταθμός μπορεί να μεταδώσει τα δεδομένα μόνο της συγκεκριμένης κατηγορίας. Εδώ θα πρέπει να σημειωθεί πως τα δεδομένα ενός σταθμού διαχωρίζονται με βάση την κατηγορία στην οποία ανήκουν. Οι δέσμες δεδομένων που δημιουργούνται αντιμετωπίζονται διαφορετικά

από τον σταθμό μιας και κάθε μία από αυτές λαμβάνει διαφορετικές παραμέτρους από την κατηγορία στην οποία ανήκει, όπως είναι η διαφορετική προτεραιότητα, το διαφορετικό ΤΧΟΡ και το διαφορετικό ΑΙΦΣ.

Κατά την περίοδο στην οποία οι σταθμοί ανταγωνίζονται για την κατοχή του μέσου, κάθε κατηγορία πρόσβασης μέσα στους σταθμούς ανταγωνίζεται για την κατοχή ενός ΤΧΟΡ και ανεξάρτητα η μία από την άλλη ξεκινά έναν αλγόριθμο οπισθοχώρησης αφού ανιχνεύσει ότι το κανάλι είναι αδρανές για ένα διάστημα ΑΙΦΣ. Οι αλγόριθμοι οπισθοχώρησης λαμβάνουν τυχαία τις τιμές τους από το διάστημα που ορίζεται ανά κατηγορία για το παράθυρο ανταγωνισμού.

Ένας σταθμός μπορεί να έχει έως και οκτώ ουρές μετάδοσης δημιουργώντας έτσι εικονικούς σταθμούς μέσα σε αυτόν με την καθεμία από αυτές να έχει διαφορετικές παραμέτρους που καθορίζονται από τις προτεραιότητές τους. Εάν οι μετρητές δύο ή και περισσότερων ουρών μηδενιστούν την ίδια χρονική στιγμή, χρησιμοποιείται ένα χρονοδιάγραμμα στο εσωτερικό του σταθμού ώστε να αποφευχθεί η εικονική σύγκρουση. Το χρονοδιάγραμμα αυτό χορηγεί το ΤΧΟΡ στην κατηγορία πρόσβασης με την υψηλότερη προτεραιότητα από αυτές που φαίνεται να συγκρούστηκαν εντός του σταθμού.

Όπως και στην βασική DCF, όταν το μέσο παραμένει απασχολημένο πριν ο μετρητής φτάσει στο μηδέν, η διαδικασία οπισθοχώρησης θα πρέπει να περιμένει και να παγώσει τον μετρητή μέχρι το μέσο να ανιχνευθεί αδρανές για διάστημα ίσο με τον ΑΙΦΣ, πριν ξεκινήσει και πάλι να μειώνει τον μετρητή της.

#### **5.4.2 HCCA (HCF Control Channel Access)**

Γενικά, Η HCCA μοιάζει πολύ στην λειτουργία της με την PCF. Παρόλα αυτά στην PCF, στην οποία το διάστημα μετάδοσης δεδομένων χωρίζεται σε δύο περιόδους αυτής του ανταγωνισμού και αυτής της ελεύθερης πρόσβασης, η HCCA επιτρέπει να δημιουργηθούν περίοδοι ελεύθερης πρόσβασης μέσα σε περιόδους ανταγωνισμού. Αυτό το είδος της ελεύθερης πρόσβασης χωρίς ανταγωνισμό ονομάζεται Φάση Ελεγχόμενης Πρόσβασης **CAP (Controlled Access Phase)**. Η φάση αυτή αρχικοποιείται από ένα AP, όποτε θέλει να στείλει ή να λάβει ένα πλαίσιο από κάποιο σταθμό έχοντας ελεύθερη πρόσβαση στο μέσο χωρίς

ανταγωνισμό. Κατά τη διάρκεια της φάσης αυτής, ο συντονιστής **HC (Hybrid Coordinator)** ο οποίος είναι συνήθως το AP, ελέγχει την πρόσβαση στο μέσο. Κατά τη διάρκεια της περιόδου του ανταγωνισμού, όλοι οι σταθμοί λειτουργούν με βάση την EDCA.

Μία άλλη διαφορά με την τεχνική PCF είναι πως ορίζονται κατηγορίες κίνησης. Αυτό σημαίνει πως ο HC δεν περιορίζεται στην χρήση ουρών ανά σταθμό αλλά παρέχει ένα είδος εξυπηρέτησης ανά συνεδρία. Επιπλέον, κάθε σταθμός παρέχει στον HC πληροφορίες σχετικές με τις κατηγορίες κίνησης που έχει κατατάξει τα δεδομένα του. Το σύστημα μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες και να δώσει προτεραιότητα σε έναν σταθμό έναντι κάποιου άλλου. Μια άλλη διαφορά είναι ότι στους σταθμούς έχουν δοθεί TXOP ώστε να μπορούν να στείλουν πολλαπλά πακέτα σε μια σειρά, για μια δεδομένη χρονική στιγμή που επιλέγεται από τον HC.

Ο μηχανισμός HCCA χρησιμοποιεί τον HC και λειτουργεί κάτω από κανόνες που είναι διαφορετικοί από τον PC (point coordinator) της PCF. Ο συντονιστής αυτός χρησιμοποιεί τις υψηλότερες προτεραιότητες πρόσβασης του μέσου για να αρχικοποιήσει την ανταλλαγή πλαισίων και να δεσμεύσει TXOPs για το AP αλλά και για τους άλλους σταθμούς ώστε να παρέχει χρονικά περιορισμένη ελεγχόμενη πρόσβαση για μεταφορά δεδομένων χωρίς συναγωνισμό.

Ο συντονιστής αποκτά τον έλεγχο του ασύρματου μέσου ώστε να στείλει δεδομένα σε σταθμούς του δικτύου αναμένοντας μικρότερο διάστημα μεταξύ των μεταδόσεων από ότι περιμένουν οι σταθμοί που χρησιμοποιούν την EDCA. Όταν ο συντονιστής χρειάζεται πρόσβαση στο μέσο για να ξεκινήσει μια περίοδο χωρίς ανταγωνισμό θα πρέπει πρώτα να ανιχνεύσει το μέσο. Εάν το μέσο είναι αδρανές για διάρκεια ίση με τον PIFS, τότε ο συντονιστής μεταδίδει το πρώτο πλαίσιο με περιορισμό η διάρκεια του να μην ξεπεράσει την διάρκεια της περιόδου χωρίς ανταγωνισμό.

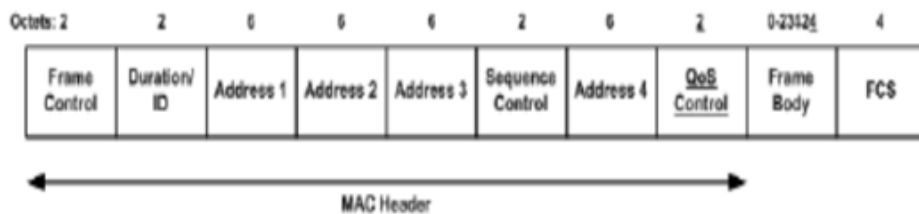
Όταν ένας σταθμός καταλάβει το μέσο αφού του έχει χορηγηθεί ένα TXOP, ξεκινά να στέλνει τα δεδομένα μιας συγκεκριμένης ουράς από το σύνολο της πληροφορίας που χρήζει μετάδοσης. Έπειτα από το τελευταίο πακέτο της ουράς,

ο σταθμός αυτός του περιμένει για διάστημα ίσο με SIFS και στη συνέχεια εκπέμπει το πρώτο πλαίσιο της επόμενης ουράς του. Ο συντονιστής περιμένει τη λήξη του TXOP που χρησιμοποιείται από τον σταθμό ανιχνεύοντας παράλληλα το μέσο και να προχωρήσει στη διαδικασία κατοχής του αφού παρέλθει ένα χρονικό διάστημα ίσο με PIFS εάν φυσικά το μέσο είναι ακόμα αδρανές. Η ελεγχόμενη πρόσβαση στο μέσο θα τελειώσει όταν ο συντονιστής δεν ανακτήσει το μέσο μέχρι το πέρας ενός PIFS από τη λήξη του TXOP.

Η HCCA θεωρείται ως μία από τις πιο πολύπλοκες τεχνικές πρόσβασης στο μέσο, όμως η παροχή της ποιότητας των υπηρεσιών επιτυγχάνεται σε πολύ μεγάλο ποσοστό με τη χρήση της. Όλοι οι σταθμοί που λειτουργούν για την παροχή υπηρεσιών έχουν τη δυνατότητα να ζητήσουν συγκεκριμένες πληροφορίες και παραμέτρους μετάδοσης από το AP ώστε να μπορέσουν να επιτρέψουν στις εφαρμογές του video και της φωνής να λειτουργήσουν πιο αποδοτικά στο ασύρματο δίκτυο.

### 802.11 Frame Format

Η δομή του πλαισίου του 802.11e [46] φαίνεται στην παρακάτω εικόνα και γεγονός αποτελεί πως είναι ελαφρώς τροποποιημένη σε σύγκριση με το αρχικό πλαίσιο που χρησιμοποιείται στο 802.11.



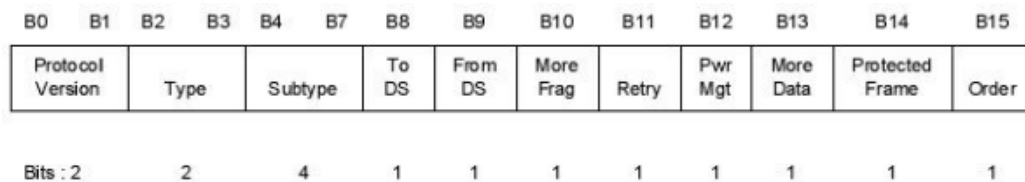
Εικόνα 5.5: Πλαίσιο υποστρώματος MAC του 802.11e

Όπως έχει αναφερθεί, για την πλαισίωση του γενικού πρωτοκόλλου 802.11, κάθε πλαίσιο αποτελείται από τα εξής κύρια στοιχεία :

- Μια επικεφαλίδα MAC που περιλαμβάνει στοιχεία για έλεγχο του πλαισίου όπως είναι η διεύθυνση και οι πληροφορίες ελέγχου για την παροχή ποιότητας υπηρεσιών.
- Ένα μεταβλητού μεγέθους κυρίως σώμα που περιέχει την καθαρή πληροφορία που πρόκειται να μεταδοθεί.
- Ένα FCS πεδίο που χρησιμοποιείται για τον έλεγχο της ακεραιότητας του περιεχόμενου του πλαισίου.

Τα τρία πρώτα πεδία όπως και το τελευταίο (frame control, duration/id, address1 και FCS) συνιστούν την ελάχιστη δομή πλαισίου και είναι παρόντα σε όλα τα πλαίσια ενώ η ύπαρξη ή μη των υπολοίπων εξαρτάται από τον εκάστοτε τύπο πλαισίου που μεταδίδεται. Στο πλαίσιο του 802.11e υποστρώματος MAC υπάρχει ένα επιπλέον και καθοριστικό πεδίο για την παροχή ποιότητας υπηρεσιών, το QoS control.

Το QoS control Field είναι ένα πεδίο από 16bits που ανιχνεύει την κατηγορία κίνησης στην οποία ανήκει το συγκεκριμένο πλαίσιο καθώς και πολλές άλλες πληροφορίες που σχετίζονται με την παροχή QoS. Το QoS control Field υπάρχει σε όλα τα πλαίσια δεδομένων και περιλαμβάνει επιμέρους πεδία τα οποία φαίνονται στην παρακάτω εικόνα:



Εικόνα 5.6: QoS Control Field

- *Protocol Version (2 bits)*: Χρησιμοποιείται για τον καθορισμό του προτύπου. Για το συγκεκριμένο πρότυπο η τιμή του πεδίου είναι «0» ενώ οι υπόλοιπες τιμές είναι δεσμευμένες. Η τιμή του πεδίου θα αυξηθεί όταν ανακοινωθεί καινούργια έκδοση του προτύπου.

- *Type / Subtype (2 bits / 4 bits)*: Τα δύο αυτά πεδία καθορίζουν τον τύπο του πλαισίου που μεταδίδεται. Το πλαίσιο θα μπορούσε να είναι πλαίσιο ελέγχου, διαχείρισης ή δεδομένων.
- *To DS / From DS (από 1 bit)*: Τα δύο αυτά πεδία σε συνδυασμό καθορίζουν τα δίκτυα αποστολής και λήψης των πλαισίων. Πιο συγκεκριμένα, εάν και τα δύο πεδία έχουν μηδενικές τιμές, σημαίνει πως το πλαίσιο μεταδίδεται από έναν σταθμό του δικτύου απευθείας σε ένα άλλο σταθμό του ίδιου δικτύου. Εάν το πεδίο To DS έχει την τιμή «0» και το πεδίο From DS έχει την τιμή «1» σημαίνει πως το πλαίσιο μεταδίδεται από το δικό μας δίκτυο σε κάποιο άλλο. Το αντίθετο στις τιμές των δύο αυτών πεδίων σημαίνει πως κάποιο άλλο δίκτυο στέλνει ένα πλαίσιο δεδομένων στο δικό μας δίκτυο. Τέλος, και τα δύο πεδία δεν μπορούν να έχουν την τιμή «1» μιας και το 802.11e δεν μπορεί να επεξεργαστεί αυτήν την περίπτωση.
- *More fragments (1 bit)*: Το πεδίο αυτό ενημερώνει για τη ροή των δεδομένων που μεταδίδονται. Εάν το πλαίσιο έχει κομματιστεί και αποτελείται από επιμέρους τμήματα, το πεδίο αυτό έχει την τιμή «1» αλλιώς εάν η προς μετάδοση πληροφορία είναι ολόκληρη σε ένα πλαίσιο, η τιμή του πεδίου θα είναι ίση με «0».
- *Retry (1 bit)*: Έχει την τιμή «1» μόνο στην περίπτωση που το πλαίσιο είναι τύπου δεδομένων ή τύπου διαχείρισης και δεν είναι η πρώτη φορά που βρίσκεται σε κατάσταση αποστολής. Σε όλες τις άλλες περιπτώσεις έχει την τιμή «0».
- *Power Management Field (1 bit)*: Το πεδίο αυτό περιγράφει την κατάσταση που βρίσκεται ο σταθμός. Εάν η τιμή του είναι «1» σημαίνει πως ο σταθμός βρίσκεται σε κατάσταση χαμηλής κατανάλωσης ενώ αν είναι «0» σημαίνει πως ο σταθμός είναι ενεργός και λειτουργεί κανονικά.
- *More Data (1 bit)*: Το πεδίο αυτό χρησιμοποιείται για να ενημερώσει ένα σταθμό που βρίσκεται σε κατάσταση χαμηλής κατανάλωσης ενέργειας πως στο AP υπάρχουν πλαίσια που προορίζονται για αυτόν και δεν του έχουν

αποσταλεί λόγω της κατάστασης στην οποία βρίσκεται, στην περίπτωση που έχει την τιμή «1». Στην περίπτωση που έχει την τιμή «0» σημαίνει πως ο σταθμός είτε δεν βρίσκεται σε κατάσταση χαμηλής κατανάλωσης είτε το AP δεν έχει γι' αυτόν αποθηκευμένα πλαίσια.

- *Protected Frame Field (1 bit)*: Το πεδίο αυτό παίρνει την τιμή «1» στην περίπτωση που τα δεδομένα του πλαισίου έχουν υποστεί τη διαδικασία κρυπτογράφησης για την παροχή μεγαλύτερου ποσοστού ασφαλείας. Στην περίπτωση που τα δεδομένα μεταφέρονται ατόφια, η τιμή του πεδίου είναι «0».
- *Order Field (1 bit)*: Το πεδίο αυτό έχει την τιμή «1» για όλους τους σταθμούς που δεν μπορούν να υλοποιήσουν τις τεχνικές παροχής υπηρεσιών ενώ για τους 802.11e σταθμούς το πεδίο αυτό έχει την τιμή «0».

Στα πλαίσια του 802.11e αξίζει να σημειωθεί ότι έχουν προταθεί και κάποιοι επιπλέον μηχανισμοί λειτουργίας που προσδοκείται να προσδώσουν περαιτέρω ευελιξία στην παροχή ποιότητας υπηρεσιών. Σε αυτούς συμπεριλαμβάνονται οι εξής μηχανισμοί:

- **APSD (Automatic Power Save Delivery)**. Ο APSD συνιστά έναν πολύ αποτελεσματικό μηχανισμό διαχείρισης ενέργειας που απευθύνεται κατά κύριο λόγο στις κλήσεις **VoIP (Voice Over IP)**. Στην περίπτωση της μετάδοσης των δεδομένων φωνής, το AP ενεργοποιείται αμέσως για να μεταδώσει τα δεδομένα προς τον προορισμό τους. Έπειτα από την αποστολή η VoIP συσκευή μεταβαίνει σε μία κατάσταση χαμηλής κατανάλωσης ενέργειας ώσπου να σταλούν τα νέα δεδομένα VoIP στο AP.
- **NoAck (No Acknowledgments)**. Ο μηχανισμός NoAck συνιστά μία επιπλέον παράμετρο κατά την παροχή ποιότητας υπηρεσιών. Όταν είναι ενεργή μια υπηρεσία με σημαντικούς ρυθμούς αύξησης φόρτου στο δίκτυο που απαιτεί να τηρούνται κανόνες συγχρονισμού για την αποτελεσματική λειτουργία της, τότε είναι δυνατό ενεργοποιώντας την υπηρεσία NoAck να



απενεργοποιούμε την αποστολή των ACKs γεγονός που μειώνει το φόρτο του μέσου.

- **DLS (Direct Link Setup).** Ο μηχανισμός DLS επιτρέπει να δημιουργείται απευθείας επικοινωνία μεταξύ δύο σταθμών σε ένα BSS χωρίς την μεσολάβηση ενός AP, γεγονός που επιτρέπει την μείωση του φόρτου στο AP όταν εκτελούνται εφαρμογές που δεν απαιτούν απαραίτητα την παρουσία του όπως είναι τα παιχνίδια ή η μεταφορά αρχείων.

## 5.5 802.11n

Το 802.11n [47] είναι μία τροποποίηση του IEEE 802.11 για τη βελτίωση της απόδοσης του δικτύου και βασίζεται πάνω από τα δύο προηγούμενα πρότυπα 802.11a και 802.11g. Οι εργασίες για την ανάπτυξη του ξεκίνησαν το 2002 και το πρότυπο ανακοινώθηκε επτά χρόνια αργότερα, το 2009. Το βασικό χαρακτηριστικό του είναι η σημαντική αύξηση του ανώτατου ρυθμού μετάδοσης δεδομένων από 54 Mbps σε 600 Mbps και του κατώτατου στα 108 Mbps με χρήση τεσσάρων ρευμάτων δεδομένων σε εύρος καναλιού των 40 MHz για το καθένα από αυτά υποστηρίζοντας έτσι τους χρήστες που έχουν αυξημένες απαιτήσεις για το μέγιστο εύρος που μπορούν να χρησιμοποιήσουν στη μετάδοση των δεδομένων τους.

Το πρότυπο αυτό παρουσιάζει καινούργιες τεχνολογίες που βασίζονται στις ήδη υπάρχουσες, όπως είναι η χρήση του φυσικού επιπέδου OFDM και τεχνικές κωδικοποίησης ώστε να μειωθεί το κόστος του και να διατηρηθεί ταυτόχρονα η συμβατότητα με τα παλαιότερα πρότυπα. Η προδιαγραφή του 802.11n όμως διαφέρει από τους προκατόχους του, αφού περιλαμβάνει μία ποικιλία τεχνικών που χρησιμοποιούνται για να επιτύχουν διαφορετικές μέγιστες τιμές στους ρυθμούς μετάδοσης των δεδομένων. Παρόλα αυτά το υλικό που χρησιμοποιείται για να υλοποιηθεί το πρότυπο αυτό δεν χρειάζεται να είναι συμβατό με όλες τις τροποποιήσεις που αυτό προδιαγράφει.

Για να επιτευχθεί η συμβατότητα με τα παλαιότερα πρότυπα, ένα AP που υλοποιεί το 802.11n θα επικοινωνήσει με τις 802.11b/g συσκευές στη συχνότητα των 2.4

GHz ενώ με τις 802.11a συσκευές θα χρησιμοποιήσει τη μπάντα των 5 GHz. Τα κανάλια συχνοτήτων που χρησιμοποιούνται είναι 56 στον αριθμό, με τέσσερα από αυτά να είναι μη επικαλυπτόμενα στην περίπτωση των 5 GHz. Όταν χρησιμοποιείται η μπάντα συχνοτήτων των 2.4 GHz, έχουμε ένα μόνο μη επικαλυπτόμενο κανάλι.

Καθώς οι χρήστες των ασύρματων δικτύων αυξάνονται, οι απαιτήσεις για καλύτερη και γρηγορότερη χρήση των εφαρμογών τους γίνονται όλο και μεγαλύτερες. Το 802.11n προσφέρει καλύτερη απόδοση σε εφαρμογές όπως είναι η μετάδοση φωνής, η μετάδοση βίντεο και τα παιχνίδια.

Τα βασικά χαρακτηριστικά του προτύπου αυτού φαίνονται στον παρακάτω πίνακα.

<b>802.11n</b>	
<b>Έκδοση</b>	2009
<b>Συχνότητα</b>	2.4 / 5 GHz
<b>Μέγιστος Ρυθμός μετάδοσης</b>	320 Mbps (για κανάλια πλάτους 20 MHz) και 600 Mbps (για κανάλια πλάτους 40 MHz)
<b>Φυσικό επίπεδο</b>	OFDM
<b>Εμβέλεια</b>	100 m

*Πίνακας 5.14: Βασικά χαρακτηριστικά του 802.11n*

Προκειμένου να επιτευχθούν οι υψηλότεροι ρυθμοί μετάδοσης, στο 802.11n χρησιμοποιείται η τεχνική πολλαπλών εισόδων και εξόδων **MIMO (Multi-Input Multi-Output)** που υλοποιείται στα ήδη υπάρχοντα 802.11a και 802.11g. Η MIMO βασίζεται στη μέθοδο πολυπλεξίας με διαίρεση χώρου **SDM (Space Division Multiplexing)**. Η ασύρματη συσκευή που πρόκειται να μεταδώσει χωρίζει τη ροή των δεδομένων της σε τμήματα που ονομάζονται χωρικά ρεύματα και μεταδίδει κάθε ένα από αυτά τα ρεύματα μέσω ξεχωριστών κεραιών στις αντίστοιχες κεραιές που χρησιμοποιούνται από τον παραλήπτη. Το τρέχον 802.11n προβλέπει την χρήση μέχρι και τεσσάρων τέτοιων ρευμάτων αν και στην πραγματικότητα οι

συσκευές χρησιμοποιούν λιγότερα από τέσσερα ρεύματα για τη μετάδοση των δεδομένων τους.

Στην τεχνική MIMO, οι πολλαπλές κεραιές ενός σταθμού μετάδοσης εισάγουν τα σήματα στις ραδιοσυχνότητες του μέσου και αντίστοιχα οι πολλαπλές κεραιές του παραλήπτη εξάγουν τα σήματα αυτά από το κανάλι επικοινωνίας. Όταν μεταδίδονται πολλαπλά σήματα στην ίδια συχνότητα και την ίδια χρονική στιγμή, το σήμα που φτάνει στα κεραιές των δεκτών είναι το άθροισμα όλων των μεταδιδόμενων σημάτων. Με άλλα λόγια, οι κεραιές λαμβάνουν ένα συνδυασμό των μεταδιδόμενων αυτών σημάτων. Στην περίπτωση λοιπόν που οι κεραιές ενός σταθμού θα λάβουν διαφορετικούς συνδυασμούς σημάτων, ο σταθμός αυτός είναι σε θέση να καθορίσει ποια σήματα δημιουργούν αυτούς τους συνδυασμούς. Ωστόσο, εάν τα σήματα που λαμβάνονται στις κεραιές λήψης είναι παρόμοια μεταξύ τους, ο δέκτης δεν είναι σε θέση να αντιληφθεί και να ξεχωρίσει τα μεταδιδόμενα σήματα.

Η MIMO λειτουργεί καλύτερα σε περιβάλλοντα όπου το σήμα μεταξύ του AP και του σταθμού που δεν αντανακλάται σε τοίχους ή και σε άλλα φυσικά εμπόδια. Όταν τα σήματα αντανακλούν σε επιφάνειες υπάρχει πολύ μεγάλη πιθανότητα τα μηνύματα που θα φτάσουν στις κεραιές λήψης του δέκτη να είναι αρκετά διαφορετικά από την αρχική τους μορφή.

Στην περίπτωση της τεχνικής MIMO, ο διπλασιασμός του αριθμού των ρευμάτων από ένα σε δύο, διπλασιάζει τον ρυθμό μετάδοσης των δεδομένων. Προκειμένου να διπλασιαστεί ο ρυθμός μετάδοσης των δεδομένων που στο 802.11n χρησιμοποιούνται κανάλια επικοινωνίας μήκους 40MHz γεγονός που περιορίζει κατά πολύ τη διαθεσιμότητα του καναλιού για τους υπόλοιπους σταθμούς του δικτύου. Στην περίπτωση λειτουργίας του δικτύου στα 2.4 GHz, μπορούν να χρησιμοποιηθούν τρία μη επικαλυπτόμενα κανάλια μήκους 20 MHz. Όταν όμως χρησιμοποιούνται κανάλια των 40 MHz δεν έχουν πολλοί σταθμοί τη δυνατότητα να ενταχθούν στο δίκτυο και να μεταδώσουν τα δεδομένα τους. Αυτό σημαίνει πως η διαχείριση των πόρων του δικτύου θα πρέπει να γίνει με τέτοιο τρόπο ώστε να διασφαλιστεί ότι η επιλογή χρήσης καναλιών των 40 MHz βελτιώνει τη συνολική απόδοση του συστήματος εξισορροπώντας τις αυξημένες απαιτήσεις ορισμένων

σταθμών για υψηλούς ρυθμούς μετάδοσης με τις ανάγκες των υπολοίπων σταθμών να παραμείνουν συνδεδεμένοι με το δίκτυο.

Για την βελτίωση της τεχνικής MIMO χρησιμοποιούνται δύο επιπλέον μέθοδοι, ο σχηματισμός των δεσμών δεδομένων (beam-forming) και η διαφορετικότητα (diversity). Η beam-forming είναι μια τεχνική που εστιάζει τα σήματα που μεταδίδονται απευθείας στην κεραία για την οποία προορίζονται, βελτιώνοντας έτσι την απόδοση του δικτύου αφού περιορίζονται τυχόν παρεμβολές. Η διαφορετικότητα εκμεταλλεύεται τις πολλαπλές κεραίες που υποστηρίζονται από αυτό το πρότυπο, χρησιμοποιώντας περισσότερες από αυτές που απαιτούνται για τη λήψη των δεδομένων, γεγονός που με τη σειρά του βοηθάει στην βελτίωση της απόδοσης και της λειτουργικότητας του δικτύου.

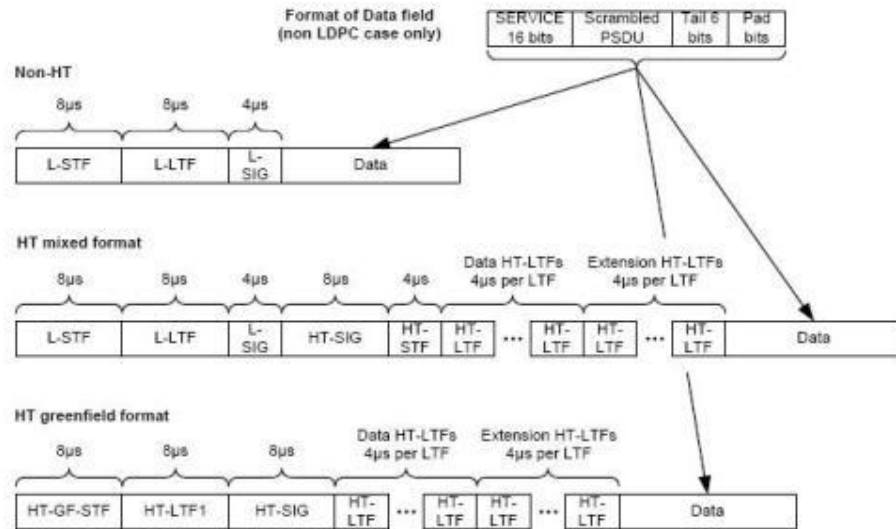
Παρόλα αυτά, υπάρχουν μειονεκτήματα χρήσης αυτής της τεχνικής μιας και απαιτείται αυξημένη κατανάλωση ενέργειας από τους σταθμούς και, σε μικρότερο βαθμό, η αύξηση του κόστους υλοποίησης ενός τέτοιου δικτύου. Οι προδιαγραφές όμως του 802.11n περιλαμβάνουν την κατάσταση χαμηλής κατανάλωσης για τους σταθμούς του δικτύου, η οποία μετριάζει την ενέργεια που καταναλώνεται με τη χρήση πολλαπλών ρευμάτων μόνο στις περιπτώσεις που η επικοινωνία θα επωφεληθεί από την τεχνική αυτή. Η κατάσταση χαμηλής κατανάλωσης ενέργειας είναι μία από τις υποχρεωτικές πρακτικές του 802.11n.

Το πρότυπο 802.11n περιγράφει τρεις τρόπους λειτουργίας, σχετικούς με την επικοινωνία των σταθμών που υλοποιούν παλαιότερα πρότυπα και είναι οι εξής [48]:

- **High Throughput (Greenfield) Mode:** Ένα 802.11n AP όταν χρησιμοποιεί τη λειτουργία υψηλής απόδοσης **HT (High Throughput)**, γνωστή και ως λειτουργία Greenfield, υποθέτει πως δεν υπάρχουν γειτονικοί σταθμοί στην ίδια ζώνη συχνοτήτων που λειτουργούν σε παλαιότερα πρότυπα. Στην περίπτωση που τέτοιοι σταθμοί υπάρχουν στο δίκτυο δε θα μπορέσουν να επικοινωνήσουν με το AP όταν αυτό χρησιμοποιεί τη λειτουργία υψηλής απόδοσης. Η λειτουργία αυτή είναι προαιρετική για τους σταθμούς του 802.11n και χρησιμοποιεί κανάλια συχνοτήτων μήκους 40 MHz.

- **Non HT (legacy) Mode:** Ένα 802.11n AP χρησιμοποιώντας τη λειτουργία αυτή στέλνει όλα τα πλαίσια σύμφωνα με τις προδιαγραφές των 802.11a / g ώστε όλοι οι σταθμοί που απαρτίζουν το δίκτυο και λειτουργούν βάσει παλαιότερων προτύπων να μπορούν να τα καταλάβουν. Το AP θα πρέπει να χρησιμοποιήσει κανάλια μήκους 20 MHz. Όλες οι συσκευές θα πρέπει να υποστηρίζουν αυτή τη λειτουργία προκειμένου να εξασφαλισθεί η συμβατότητα, όμως ένα 802.11n AP όταν χρησιμοποιεί αυτή τη λειτουργία δεν προσφέρει καλύτερη απόδοση στο σύστημα από ό, τι τα αντίστοιχα 802.11a / g APs.
- **HT Mixed Mode:** Η λειτουργία αυτή είναι υποχρεωτική και η πιο κοινή για τα 802.11n APs. Στη μεικτή λειτουργία, οι βελτιώσεις που προσφέρει η λειτουργία υψηλής απόδοσης μπορούν να συνδυαστούν με τους μηχανισμούς προστασίας της ώστε να επιτρέπουν την επικοινωνία μεταξύ των σταθμών που λειτουργούν βάσει παλαιότερων προτύπων και σταθμών που υλοποιούν το 802.11n. Η μεικτή λειτουργία παρέχει συμβατότητα με παλαιότερες εκδόσεις, αλλά οι 802.11n συσκευές εμφανίζουν σημαντικές μειώσεις στην απόδοση του συστήματος σε σύγκριση με την κατάσταση Greenfield.

Τα πλαίσια του υποστρώματος MAC που χρησιμοποιεί κάθε μία από τις παραπάνω λειτουργίες φαίνονται στην παρακάτω εικόνα.



Εικόνα 5.7: Πλαίσια υποστρώματος MAC για το 802.11n

Το 802.11n προκειμένου να μειώσει την πλεονάζουσα πληροφορία που μεταδίδεται ώστε να αυξηθεί η απόδοση του δικτύου, χρησιμοποιεί δύο τεχνικές [49], την συγκέντρωση των πλαισίων σε ένα (**frame aggregation**) και την μείωση των μηνυμάτων θετικής επιβεβαίωσης (**block acknowledgments**) που συνοδεύουν τα πλαίσια αυτά.

Κάθε πλαίσιο που μεταδίδεται από μια συσκευή 802.11 έχει ένα σημαντικό ποσό πλεονάζουσας πληροφορίας, συμπεριλαμβανομένων των κεφαλίδων των πλαισίων, τον μετρητών που χρησιμοποιούνται και των μηνυμάτων θετικής επιβεβαίωσης. Στις περιπτώσεις της μετάδοσης με υψηλούς ρυθμούς, η πληροφορία αυτή μπορεί να καταναλώσει περισσότερο εύρος ζώνης από την καθαρή πληροφορία που μεταδίδεται. Για την αντιμετώπιση αυτού του ζητήματος, το πρότυπο 802.11n ορίζει δύο τύπους πλαισίων συγκέντρωσης, το **MSDU (MAC Service Data Unit)** και το **MPDU (MAC Protocol Data Unit)**. Και οι δύο τύποι ομαδοποιούν έναν αριθμό πλαισίων σε ένα μεγαλύτερο και ενιαίο πλαίσιο. Κατ' αυτόν τον τρόπο η πλεονάζουσα πληροφορία που θα αποστέλλονταν για όλα αυτά τα πλαίσια συνδυάζεται σε μία μόνο αποστολή αυξάνοντας την απόδοση του δικτύου. Ταυτόχρονα, μειώνονται και οι πιθανότητες συγκρούσεων των δεδομένων μιας και τα πλαίσια που μεταδίδονται είναι λιγότερα στον αριθμό αλλά και

μεγαλύτερα από αυτά που χρησιμοποιούνται στα προγενέστερα πρότυπα αυξάνοντας το μέγεθός τους από τα 4 KB στα 64 KB.

Ένας από τους περιορισμούς του συνδυασμού των πλαισίων είναι το γεγονός πως ο αποδέκτης αυτών θα πρέπει να είναι ο ίδιος για όλα τα πλαίσια που ομαδοποιήθηκαν. Στα μειονεκτήματά της συγκαταλέγεται και η χρονική καθυστέρηση που υφίστανται τα μικρότερα από τα πλαίσια που αποτελούν το ενιαίο αφού περιμένουν τα μεγαλύτερα από αυτά να δηλωθούν έτοιμα για μετάδοση.

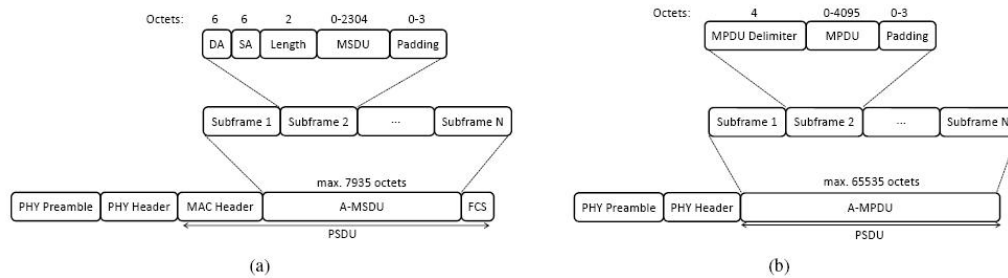
Η MSDU είναι η πιο αποτελεσματική από τις δύο μεθόδους συγκέντρωσης. Στηρίζεται στο γεγονός ότι ένα AP λαμβάνει όλα τα πλαίσια από την ενσύρματη δικτύωσή του (Ethernet frames), τα μεταφράζει σε πλαίσια του πρωτοκόλλου 802.11 και στη συνέχεια τα μεταδίδει στους ασύρματους σταθμούς. Οι κεφαλίδες των πλαισίων είναι αρκετά μικρότερες από αυτές που χρησιμοποιούνται στην τεχνική MPDU με αποτέλεσμα να εμφανίζονται βελτιώσεις στην απόδοση του δικτύου.

Εδώ θα πρέπει να σημειωθεί πως ο περιορισμός της MSDU είναι πως όλα τα πλαίσια που απαρτίζουν το ενιαίο, πρέπει να είναι της ίδιας κατηγορίας με αυτές που χρησιμοποιούνται στο 802.11e για την παροχή της ποιότητας των υπηρεσιών. Δεν επιτρέπεται για παράδειγμα να αναμειγνύονται τα πλαίσια φωνής με αυτά που απαρτίζονται από απλά δεδομένα.

Ο τρόπος λειτουργίας της MPDU είναι ελαφρώς διαφορετικός από την MSDU. Αντί για την αρχική συλλογή πλαισίων τύπου Ethernet, η MPDU μεταφράζει κάθε πλαίσιο τύπου Ethernet στον τύπο του 802.11 και στη συνέχεια συλλέγει όλα τα 802.11 πλαίσια που έχουν κοινό προορισμό για να τα μεταδώσει.

Η αποτελεσματικότητα της μεθόδου MPDU είναι μικρότερη από εκείνη της μεθόδου MSDU για τα μικρά και μεσαίου μεγέθους πλαίσια, λόγω της επιβάρυνσης των επιμέρους 802.11 κεφαλίδων για κάθε πλαίσιο. Και στην τεχνική αυτή, όλα τα πλαίσια που απαρτίζουν το ενιαίο, πρέπει να είναι της ίδιας κατηγορίας με αυτές που χρησιμοποιούνται στο 802.11e για την παροχή της ποιότητας των υπηρεσιών.

Τα πλαίσια που χρησιμοποιούν οι δύο τεχνικές φαίνονται στην παρακάτω εικόνα.



Εικόνα 5.8: Μορφές πλαισίων συνδυασμού για τις MSDU και MPDU.

Για να λειτουργεί αξιόπιστα το υπόστρωμα MAC του 802.11, καθένα από τα πλαίσια που μεταδίδεται σε ένα μόνο παραλήπτη θα πρέπει να επιβεβαιώνεται αμέσως μετά τη λήψη του από αυτόν. Η MSDU δεν απαιτεί τροποποιήσεις σε αυτή τη λειτουργία. Το συνολικό πλαίσιο αναγνωρίζεται, όπως γίνεται σε κάθε πλαίσιο του 802.11. Για την λειτουργία MPDU δεν ισχύει αυτή η πρακτική. Κάθε ένα από τα πλαίσια θα πρέπει να αναγνωρισθεί. Ο μηχανισμός για την αντιμετώπιση αυτής της απαίτησης του 802.11n είναι η απόρριψη των επιμέρους επιβεβαιώσεων για κάθε πλαίσιο. Σύμφωνα με τον αποκλεισμό αυτό, συγκεντρώνονται όλα τα μηνύματα της θετικής επιβεβαίωσης σε ένα ενιαίο πλαίσιο που αποστέλλεται από τον παραλήπτη στον αποστολέα. Αυτή η τεχνική επιτρέπει την επιλεκτική αναμετάδοση των πλαισίων που δεν έχουν αναγνωρισθεί. Σε περιβάλλοντα με υψηλά ποσοστά σφαλμάτων, αυτή η τεχνική επιλεκτικής αναμετάδοσης παρέχει βελτίωση στην απόδοση του δικτύου, μιας και αποστέλλονται εκ νέου λιγότερα πλαίσια από αυτά της τεχνικής MSDU.



## 6. Πρωτόκολλα 802.16 και 802.11

Στο κεφάλαιο αυτό θα γίνει μία σύγκριση στα δύο βασικότερα πρωτόκολλα ασύρματης επικοινωνίας, το 802.11 που σχετίζεται με τα ασύρματα τοπικά δίκτυα (WLANs) και το 802.16 που χρησιμοποιείται για την επέκταση των τοπικών αυτών δικτύων ώστε να παρέχεται σε ένα χρήστη η πρόσβαση στο ασύρματο δίκτυο με εμβέλεια που φτάνει να καλύψει τα όρια μιας πόλης (WMANs).

### 6.1 Πρωτόκολλο 802.16

Οι τεχνολογίες ασύρματης δικτύωσης τα τελευταία χρόνια έχουν γνωρίσει σημαντική εξέλιξη, καθώς από τα πλεονεκτήματά τους επωφελούνται τόσο οι εταιρίες παροχής υπηρεσιών διαδικτύου **ISP (Internet Service Provider)**, όσο και οι ιδιώτες ή οι απλοί χρήστες. Η ευκολία εγκατάστασης ενός ασύρματου δικτύου, οδήγησε στην ανάπτυξη σήμερα εκατομμυρίων δικτύων WiFi σε ολόκληρο τον πλανήτη. Παρόλα αυτά, το WiFi αντιμετωπίζει μειονεκτήματα όπως είναι η μικρή εμβέλεια του δικτύου, που έρχεται να λύσει μια νέα τεχνολογία ασύρματης δικτύωσης, η οποία ακούει στο όνομα **WiMAX (World Interoperability for Microwave Access)** [50].

Το 2003 η IEEE υιοθέτησε το πρότυπο 802.16 γνωστό και σαν WiMAX, ώστε να ικανοποιήσει τις απαιτήσεις για ασύρματη πρόσβαση ευρείας ζώνης **BWA (Broadband Wireless Access)**. Το WiMAX Forum είναι ένας μη κερδοσκοπικός οργανισμός ο οποίος ταυτοποιεί συγκεκριμένο εξοπλισμό υποστηριζόμενος από εταιρίες (Intel, Samsung, Motorola, Cisco) προσπαθώντας να προωθήσει το πρότυπο 802.16 σε κάθε ευρυζωνικής ασύρματης πρόσβασης σύστημα.

Όπως συμβαίνει με τα πρότυπα της σειράς 802.11 για τα ασύρματα τοπικά δίκτυα, έτσι και το 802.16 καθορίζει μια οικογένεια προτύπων με επιλογές για συγκεκριμένες λειτουργίες. Το WiMAX είναι μια τεχνολογία που παρέχει ασύρματη ευρυζωνική πρόσβαση υψηλών ταχυτήτων σε μεγάλες αποστάσεις. Πλέον ένας φορητός υπολογιστής έχει τη δυνατότητα να συνδέεται σε ασύρματα δίκτυα και να

μετακινείται μέσα σε αυτά σχεδόν χωρίς να υπάρχουν περιορισμοί σχετικοί με την απόσταση που μπορεί να καλυφθεί από την εμβέλεια του εν λόγω δικτύου.

Το WiMAX χρησιμοποιεί τις μπάντες συχνοτήτων των 5 και 2.5 GHz. Για σταθερούς σταθμούς που έχουν πρόσβαση στα ασύρματα δίκτυα, οι περισσότερες χώρες έχουν διαθέσει τις ζώνες μεταξύ των 3.4 και 3.6 GHz, με εξαίρεση τις ΗΠΑ, το Μεξικό, τη Βραζιλία και ορισμένα κράτη της νοτιοανατολικής Ασίας που έχουν υιοθετήσει τη ζώνη μεταξύ 2.5 και 2.7 GHz.

Το αρχικό πρότυπο 802.16 σχεδιάστηκε ώστε να λειτουργεί σε μια ευρεία περιοχή συχνοτήτων η οποία εκτείνεται από 10 ως 66 GHz [51]. Το πλεονέκτημα της χρήσης των υψηλών συχνοτήτων είναι πως προσφέρεται μεγαλύτερο εύρος ζώνης στους χρήστες με μικρότερες πιθανότητες παρεμβολής. Στον αντίποδα αυτού, έρχεται ο περιορισμός της χρήσης των υψηλών συχνοτήτων που δεν είναι άλλος από την υποχρεωτική οπτική επαφή του πομπού με τον δέκτη χωρίς να παρεμβάλλονται ενδιάμεσα φυσικά εμπόδια. Για την αντιμετώπιση του περιορισμού αυτού αναπτύχθηκε το πρότυπο 802.16a που χρησιμοποιεί συχνότητες από 2 έως 11 GHz χωρίς να είναι απαραίτητη η οπτική επαφή. Επιπροσθέτως, αναπτύχθηκε και το πρότυπο 802.16b που λειτουργεί στις απαλλαγμένες από άδειες συχνότητες μεταξύ των 5 και 6 GHz και χρησιμοποιείται για τη συνεργασία των ασύρματων δικτύων ευρείας περιοχής.

Οι δύο βασικές επεκτάσεις του IEEE 802.16 έχουν τα εξής χαρακτηριστικά:

- 802.16a, με ρυθμό μετάδοσης δεδομένων στα 280 Kbps για κάθε σταθμό λειτουργώντας σε συχνότητες μεταξύ των 2 και 11 GHz με περιοχή κάλυψης μέχρι και τα 50 χιλιόμετρα.
- 802.16b, που χρησιμοποιείται για την επίτευξη της ποιότητας στην παροχή υπηρεσιών QoS όπως είναι η μετάδοση φωνής και βίντεο.
- 802.16e που χρησιμοποιείται κυρίως για τη συνεργασία των κινούμενων με τους σταθερούς σταθμούς του δικτύου.

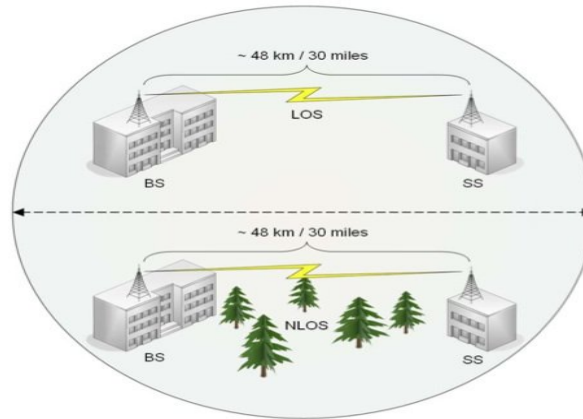
Παρακάτω φαίνονται συνοπτικά τα κύρια χαρακτηριστικά των τριών αυτών βασικών επεκτάσεων.

	<b>802.16</b>	<b>802.16a</b>	<b>802.16e</b>
<b>Spectrum</b>	10 – 66 GHz	2 – 11 GHz	<6 GHz
<b>Configuration</b>	Line of Sight	Non- Line of Sight	Non- Line of Sight
<b>Bit Rate</b>	32 to 134 Mbps (28 MHz Channel)	≤ 70 or 100 Mbps (20 MHz Channel)	Up to 15 Mbps
<b>Modulation</b>	QPSK, 16-QAM, 64-QAM	256 Sub-Carrier OFDM using QPSK, 16-QAM, 64-QAM, 256-QAM	Same as 802.16a
<b>Mobility</b>	Fixed	Fixed	≤75 MPH
<b>Channel Bandwidth</b>	20, 25, 28 MHz	Selectable 1.25 to 20 MHz	5 MHz (Planned)
<b>Typical Cell Radius</b>	1-3 miles	3-5 miles	1-3 miles
<b>Completed</b>	Dec, 2001	Jan, 2003	2nd Half of 2005

Εικόνα 6.1: Βασικά χαρακτηριστικά των επεκτάσεων του 802.16

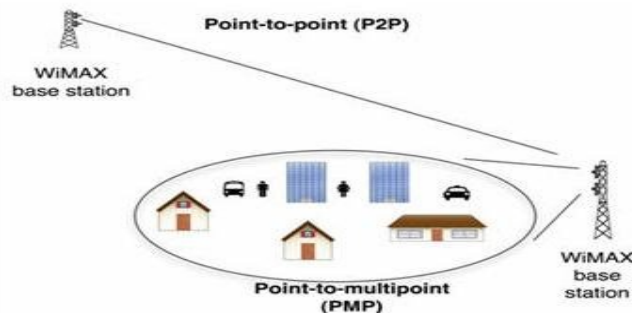
Οι αποστάσεις που μπορούν να καλυφθούν ξεπερνούν θεωρητικά τα 50 χιλιόμετρα σε συνθήκες οπτικής επαφής με ρυθμούς μετάδοσης έως και 75 Mbps. Μια σημαντική διαφορά του προτύπου 802.16 σε σχέση με το 802.11 είναι ότι το πρώτο χρησιμοποιείται και σε συνθήκες μη οπτικής επαφής καλύπτοντας αποστάσεις των 2 χιλιομέτρων με χαμηλότερους βέβαια ρυθμούς μετάδοσης.

Για το πρότυπο 802.16 τα κανάλια ασύρματης επικοινωνίας διαχωρίζονται σε δύο κατηγορίες, αυτά της οπτικής επαφής **LOS (Line of sight)** και στα **NLOS (Non line of sight)** μη οπτικής επαφής. Σε μια σύνδεση LOS ένα σήμα ταξιδεύει σε μία άμεση και χωρίς εμπόδια διαδρομή από το πομπό στο δέκτη. Μια σύνδεση LOS, απαιτεί περισσότερο εύρος ζώνης να μην παρεμποδίζεται από κάτι. Αν δεν ισχύει αυτό, η ισχύς του σήματος ελαττώνεται σημαντικά. Σε μια NLOS σύνδεση ένα σήμα φθάνει στο δέκτη μέσω αντανάκλασεων και διασποράς. Το σήμα που φθάνει στο δέκτη αποτελείται από το σήμα που έφτασε άμεσα από το πομπό και από το σήμα που έφτασε από πολλαπλά μονοπάτια μέσω αντανάκλασης. Οι διαδρομές που ακολουθούνται στις δύο περιπτώσεις φαίνονται καλύτερα στην παρακάτω εικόνα.



Εικόνα 6.2: Διαδρομές LOS και NLOS

Το WiMAX σχεδιάστηκε με τέτοιο τρόπο ώστε να υποστηρίζει τόσο τις τοπολογίες στις οποίες ένα μόνο σημείο συνδέεται με κάποιο άλλο **P2P (Point-To-Point)**, όσο και τις τοπολογίες στις οποίες ένα σημείο συνδέεται με πολλά άλλα σημεία **PMP (Point-to-Multipoint)**. Το WiMAX σχεδιάστηκε κατά βάση ώστε να καλύπτει κυρίως PMP συνδέσεις. Σε μία τέτοια τοπολογία, ένας σταθμός βάσης **BS (Base Station)** διαμοιράζει την κίνηση στους σταθμούς που είναι καταγεγραμμένοι στο δίκτυο **SS (Subscriber Station)**. Για να επιτευχθεί η υψηλή απόδοση του δικτύου, χρησιμοποιούνται προγραμματισμένες μέθοδοι σύμφωνα με τις οποίες κάθε σταθμός βάσης θα μπορέσει να μεταδώσει τα δεδομένα του μόνο σε συγκεκριμένα times slots ώστε να αποφευχθούν οι συγκρούσεις. Υψηλότεροι ρυθμοί μετάδοσης επιτυγχάνονται στις συνδέσεις P2P που αφορούν κυρίως δύο σταθμούς βάσης στην μεταξύ τους επικοινωνία. Στην παρακάτω εικόνα φαίνεται ο συνδυασμός των δύο τοπολογιών.



Εικόνα 6.3: Συνδυασμός τοπολογιών P2P και PMP

Επιπλέον, το WiMAX επιτρέπει και την τοπολογία mesh στην οποία ένας σταθμός μπορεί απευθείας να επικοινωνεί με κάποιον άλλο σταθμό μέσα στο δίκτυο χωρίς να είναι απαραίτητη η μεσολάβηση κάποιου σταθμού βάσης στην μεταξύ τους επικοινωνία.

### 6.1.1 WiMAX Physical Layer

Όπως και στα υπόλοιπα πρότυπα, έτσι και στο 802.16 το φυσικό επίπεδο καθορίζει την συχνότητα μετάδοσης, τις τεχνικές διαμόρφωσης του μεταδιδόμενου σήματος, τις τεχνικές διόρθωσης λαθών, τον συγχρονισμό μεταξύ του πομπού και του δέκτη, τη διαίρεση συχνοτήτων **FDD (Frequency Division Duplexing)** και τέλος τη διαίρεση του χρόνου μετάδοσης **TDD (Time Division Duplexing)** πάντα με τη χρήση μεθόδων πολύπλεξης.

Το αρχικό φυσικό επίπεδο του 802.16 [52] δημιουργήθηκε με προδιαγραφές ώστε να χρησιμοποιούνται οι συχνότητες μεταξύ των 10 και 66 GHz μόνο σε περιπτώσεις που υπήρχε οπτική επαφή. Η επέκτασή του, το 802.16a, χρησιμοποιεί στο φυσικό του επίπεδο συχνότητες μεταξύ των 2 και 11 GHz χωρίς να απαιτείται οπτική επαφή κάνοντας το πρότυπο περισσότερο ευέλικτο αλλά και το ίδιο το δίκτυο πιο αποδοτικό.

Στο φυσικό επίπεδο της οικογενείας του 802.16 χρησιμοποιούνται δύο τεχνικές διαμόρφωσης, οι OFDM και OFDMA, που αντιμετωπίζονται ως δύο ξεχωριστά φυσικά επίπεδα.

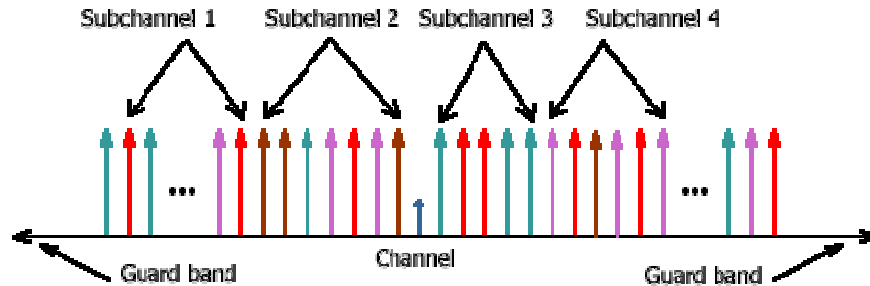
Η OFDM όπως αναφέρθηκε και σε προηγούμενο κεφάλαιο, είναι μία μέθοδος ψηφιακής διαμόρφωσης σύμφωνα με την οποία το σήμα για να μεταδοθεί διαχωρίζεται σε μικρής συχνότητας κανάλια. Μόλις το σήμα διαχωριστεί στα επιμέρους αυτά κανάλια θα μεταδοθεί ταυτόχρονα στον αποδέκτη.

Το επίπεδο αυτό, υποστηρίζει τον διαχωρισμό των δεδομένων σε κανάλια κατά τη μεταφορά τους από τον απλό σταθμό στο σταθμό βάσης (uplink). Για το uplink συγκεκριμένα χρησιμοποιούνται 16 επιμέρους κανάλια. Σαν τεχνικές πολύπλεξης υποστηρίζονται οι TDD για τον χρόνο και η FDD για τις συχνότητες για όλους τους

σταθμούς του δικτύου. Η διαίρεση χρόνου TDD έχει την έννοια της τοποθέτησης δύο ροών δεδομένων μέσα σε ένα σήμα χωρίζοντας το σήμα σε επιμέρους τμήματα με το καθένα να έχει πολύ μικρή διάρκεια. Τα τμήματα αυτά όταν ολοκληρωθεί η μετάδοσή τους, συγκεντρώνονται και ανακατασκευάζονται στον δέκτη. Η διαίρεση συχνότητας FDD αναφέρεται στη μέθοδο εκείνη όπου δύο διαφορετικά σήματα συνδυάζονται όταν είναι να μεταδοθούν μέσω ενός καναλιού επικοινωνίας. Τέλος, το OFDM επίπεδο υποστηρίζει επίσης και τον διαχωρισμό των δεδομένων από το σταθμό βάσης στον εκάστοτε απλό σταθμό του δικτύου (downlink).

Όπως η OFDM, έτσι και η OFDMA [53] χρησιμοποιεί πολλαπλά κανάλια σημάτων που βρίσκονται σε συχνότητες πολύ κοντά το ένα από το άλλο για τη μεταφορά της πληροφορίας. Στην τεχνική αυτή, τα υποκανάλια που δημιουργούνται ομαδοποιούνται και αποστέλλονται σε συχνότητες που δεν παρουσιάζουν κενά μεταξύ τους. Χαρακτηριστικό αυτής της τεχνικής είναι πως για τις downlink συνδέσεις, τα σήματα που συνθέτουν ένα υποκανάλι δεν είναι απαραίτητο να προορίζονται για τον ίδιο παραλήπτη. Στις uplink συνδέσεις, ένας πομπός μπορεί να χρησιμοποιήσει περισσότερα του ενός υποκανάλια για να μεταφέρει την πληροφορία του.

Η ομαδοποίηση των φορέων του σήματος σε υποκανάλια γίνεται με τέτοιο τρόπο ώστε κάθε ένας από τους καταγεγραμμένους σταθμούς του δικτύου να έχει στην κατοχή του έναν αριθμό από υποκανάλια ανάλογα με τις απαιτήσεις που υπάρχουν και είναι σχετικές με τους ρυθμούς μετάδοσης των δεδομένων. Επίσης, η ομαδοποίηση αυτή δίνει τη δυνατότητα στους σταθμούς της βάσης να διαθέσουν περισσότερη ισχύ στους εγγεγραμμένους σταθμούς που είναι συνδεδεμένοι σε σταθερά δίκτυα εσωτερικών χώρων, προσφέροντας έτσι μεγαλύτερη κάλυψη στο δίκτυο. Στην παρακάτω εικόνα φαίνεται ο τρόπος καταχώρησης των υποκαναλιών στους χρήστες του δικτύου.



Εικόνα 6.4: Καταχώρηση υποκαναλιών από την OFDMA στους χρήστες

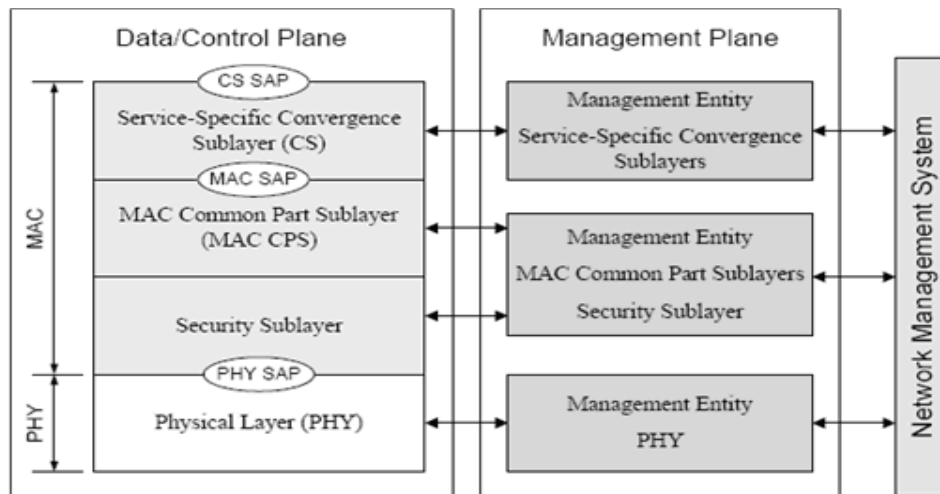
### 6.1.2 WiMAX MAC Layer

Το MAC επίπεδο του WiMAX [54] υποστηρίζει κυρίως τις τοπολογίες PMP όπου ένα σημείο συνδέεται με πολλά και προαιρετικά τις τοπολογίες πλέγματος (mesh). Είναι δομημένο με τέτοιο τρόπο ώστε να μπορεί να υποστηρίξει διάφορες υλοποιήσεις φυσικών επιπέδων, όπως είναι η χρήση της μπάντας των 10-66 GHz που απαιτεί οπτική επαφή μεταξύ των σταθμών, αλλά και του φυσικού επιπέδου που χρησιμοποιεί συχνότητες κάτω των 11 GHz χωρίς να απαιτείται οπτική επαφή με χρήση των μεθόδων OFDM και OFDMA.

Ένα από τα κύρια καθήκοντα του επιπέδου MAC είναι η μεταφορά των δεδομένων μεταξύ των διαφόρων στρωμάτων. Κατά την αποστολή των δεδομένων, λαμβάνονται τα MSDUs από τα υψηλότερα στρώματα και εν συνεχεία συγκεντρώνονται και ενσωματώνονται σε πλαίσια τύπου MPDU προκειμένου να μεταδοθούν από το φυσικό επίπεδο. Όσον αφορά τη λήψη των δεδομένων, το MAC επίπεδο παίρνει τα MPDUs από το φυσικό επίπεδο, τα μετατρέπει σε MSDUs και στη συνέχεια τα διαβιβάζει στα ανώτερα στρώματα.

Το επίπεδο MAC του WiMAX αποτελείται από τρία επιμέρους υποστρώματα, το **CS (Service-specific Convergence Sublayer)**, το **CPS (MAC Common Part Sublayer)** και το **SS (Security Sublayer)**. Στις επεκτάσεις του WiMAX, το CS υπόστρωμα χρησιμοποιείται ως μεσολαβητής μεταξύ του MAC στρώματος και των υπολοίπων πρωτοκόλλων των ανώτερων στρωμάτων όπως είναι το Ethernet, το IP κτλ. Το CPS ή αλλιώς κοινό MAC, χρησιμοποιείται για την ενθυλάκωση των πλαισίων δεδομένων, για τον τεμαχισμό της ροής των δεδομένων όπου αυτό

κρίνεται απαραίτητο και τέλος για την παροχή ποιότητας σε υπηρεσίες όπως είναι η μετάδοση της φωνής και του βίντεο. Το τρίτο και τελευταίο υπόστρωμα, ονόματι SS χρησιμοποιείται για την παροχή ασφάλειας στη μετάδοση των δεδομένων αλλά και στην εξουσιοδοτημένη είσοδο των χρηστών στο σύστημα. Οι υπηρεσίες που λαμβάνουν χώρα σε αυτό το υπόστρωμα ασχολούνται κυρίως με την αυθεντικοποίηση των χρηστών, την ανταλλαγή των κωδικών για πρόσβαση στο σύστημα αλλά και την κρυπτογράφηση των μεταδιδόμενων δεδομένων. Η στοίβα πρωτοκόλλου για το 802.16 φαίνεται στην παρακάτω εικόνα.



Εικόνα 6.5: Στοίβα πρωτοκόλλων για το 802.16

Προκειμένου να γίνει περισσότερο ανταγωνιστικό αλλά και παράλληλα αποδοτικό, το WiMAX χρησιμοποιεί και ορισμένες τεχνολογίες, τα βασικά χαρακτηριστικά των οποίων είναι τα εξής:

- Κατευθυντικές κεραιές: Οι κατευθυντικές κεραιές στα σταθερά ασύρματα συστήματα που ακτινοβολούν σε ένα συγκεκριμένο σημείο, παρουσιάζουν πλεονεκτήματα έναντι των κεραιών που ακτινοβολούν προς όλες τις κατευθύνσεις, διότι είναι περισσότερο ισχυρές στην λήψη των μεταδιδόμενων σημάτων.
- Εκπομπή και λήψη δεδομένων: Το WiMAX μπορεί να χρησιμοποιήσει προαιρετικά τους ίδιους αλγορίθμους πολλαπλής εισόδου και εξόδου, όπως το MIMO, για να καταστήσει το σύστημα πιο αποδοτικό.



- Επιλογή τρόπου διαμόρφωσης: Το WiMAX δίνει τη δυνατότητα στον αποστολέα των δεδομένων να επιλέξει τον τρόπο διαμόρφωσης της πληροφορίας λαμβάνοντας υπόψη παράγοντες όπως είναι ο λόγος του σήματος προς τον θόρυβο **SNR (Signal to Noise Ratio)** προκειμένου να επιτευχθεί μεγαλύτερη απόδοση στη μετάδοση της πληροφορίας.
- Τεχνικές διόρθωσης σφαλμάτων: Χρησιμοποιούνται τεχνικές όπως είναι η Reed Solomon FEC και η ARQ (Automatic Repeat Request), κυρίως για να ανακτηθούν πλαίσια που χάθηκαν στην διαδικασία επιλογής και χρήσης διαφορετικών συχνοτήτων.
- Έλεγχος κατανάλωσης ενέργειας: Ένας σταθμός βάσης μπορεί να ελέγξει την κατανάλωση της ενέργειας των σταθμών του δικτύου, στέλνοντάς τους κώδικες αλγορίθμων που ρυθμίζουν το ποσοστό κατανάλωσης.
- Ασφάλεια: Το WiMAX επιτρέπει την πρόσβαση στο δίκτυο με τη χρήση δημοσίων κλειδιών εξασφαλίζοντας έτσι την αυθεντικοποίηση των χρηστών του. Επίσης, χρησιμοποιούνται αλγόριθμοι κρυπτογράφησης για τη μεταφορά των δεδομένων ώστε να εξασφαλιστεί η εμπιστευτικότητα του περιεχομένου του πλαισίου.

Συνοπτικά, θα μπορούσαμε να πούμε ότι η ασύρματη δικτύωση συστημάτων με τοπολογία πλέγματος, η πιο εξέχουσα περίπτωση χρήσης του WiMAX, προκαλεί σημαντικό ενδιαφέρον τόσο από τις επιχειρήσεις, όσο και από τους απλούς χρήστες ή και τις ομάδες δημιουργίας προτύπων. Με αρκετά θετικά χαρακτηριστικά όπως είναι δυναμική οργάνωση και ρύθμιση ενός τέτοιου συστήματος, η εύκολη διαχείρισή του, η υψηλή επεκτασιμότητα και οι αξιόπιστες υπηρεσίες που προσφέρει, το WiMAX αποτελεί μία επιτυχημένη προσπάθεια στην δικτύωση με κάλυψη μεγάλων αποστάσεων. Το κόστος υλοποίησης και συντήρησης ενός συστήματος WiMAX είναι τέτοιο ώστε να ισοσταθμίζεται με τις υπηρεσίες που παρέχει για επίτευξη υψηλών ρυθμών μετάδοσης σε ευρυζωνικές συνδέσεις.

## 6.2 Σύγκριση WiMAX με WiFi

Έχοντας αναπτύξει τους τρόπους λειτουργίας και των υπηρεσιών που παρέχουν τα δύο αυτά πρότυπα, θα προσπαθήσουμε να κάνουμε μια σύγκριση μεταξύ τους αν και θα πρέπει να λάβουμε υπόψη πως ο σχεδιασμός τους είχε στόχο να υλοποιήσει διαφορετικούς στόχους. Γεγονός αποτελεί πως και τα δύο πρότυπα μοιράζονται κάποια θεμελιώδη χαρακτηριστικά, όμως προσεγγίζουν το θέμα της ασύρματης δικτύωσης από δύο διαφορετικές οπτικές [55].

Ένα βασικό μέτρο σύγκρισης μεταξύ των δύο αυτών τεχνολογιών είναι η εμβέλεια του δικτύου, που είναι σημαντικά μεγαλύτερη στην περίπτωση του WiMAX. Πιο συγκεκριμένα, η εμβέλεια ενός δικτύου WiMAX μπορεί να φτάσει και τα 50 χιλιόμετρα σε περιπτώσεις οπτικής επαφής χωρίς να μεσολαβούν φυσικά εμπόδια, ενώ το WiFi περιορίζεται μόνο σε περιορισμένους εσωτερικούς χώρους όπως είναι ένα σπίτι ή μία μικρή επιχείρηση παρέχοντας εμβέλεια μέχρι και 100 μέτρα.

Οι κεραιές που χρησιμοποιούνται στη λειτουργία του WiMAX με οπτική επαφή μπορούν να φτάσουν σε συχνότητες των 60 MHz, ενώ αυτές που δεν χρησιμοποιούν οπτική επαφή λειτουργούν στις ίδιες συχνότητες με αυτές που θα χρησιμοποιούσε το πρότυπο 802.11. Κατ' αυτόν τον τρόπο, παρέχεται η δυνατότητα μεγαλύτερης αποδοτικότητας του συστήματος σε περιπτώσεις όπου οι συνθήκες το επιτρέπουν, όταν δηλαδή δε μεσολαβούν φυσικά εμπόδια, σε σύγκριση με το 802.11 που δεν προβλέπει διαφορετικό τρόπο αντιμετώπισης αυτής της περίπτωσης.

Επίσης σε σύγκριση με το πρότυπο 802.11, το 802.16 παρέχει σαφώς υψηλότερου επιπέδου **ποιότητα υπηρεσίας**. Το επίπεδο MAC του προτύπου 802.16 είναι σχεδιασμένο με τέτοιο τρόπο ώστε να παρέχει στους τελικούς χρήστες, κατόπιν δικής τους επιθυμίας, εγγυημένο ρυθμό μετάδοσης στην αποστολή των δεδομένων παρέχοντας υψηλή ποιότητα υπηρεσίας, κάτι που το πρότυπο 802.11 δεν ήταν σε θέση να εξασφαλίσει. Οι σταθμοί αυτοί θα πρέπει να καλύπτονται από το ίδιο σταθμό βάσης. Αυτό σημαίνει πως, αν θεωρήσουμε ότι

δύο χρήστες καλύπτονται από τον ίδιο σταθμό βάσης, είναι δυνατόν ο ένας χρήστης να έχει σταθερή και εξασφαλισμένη ποιότητα υπηρεσίας μεταδίδοντας δεδομένα φωνής ή βίντεο, ενώ ο δεύτερος χρήστης να δέχεται και να στέλνει απλής μορφής δεδομένα. Στο 802.11, όσοι χρήστες βρίσκονταν στην κάλυψη ενός AP έχουν την ίδια ποιότητα υπηρεσίας, με εξαίρεση την χρήση των δύο τελευταίων προτύπων της οικογενείας, 802.11e και 802.11n που προσφέρουν πλέον ποιότητα υπηρεσιών.

Μία από τις σημαντικότερες διαφορές μεταξύ των δύο αυτών τεχνολογιών είναι το κόστος, το οποίο και τελικά καθορίζει την επιλογή μεταξύ 802.11 και 802.16. Το κόστος υλοποίησης ενός δικτύου 802.16 είναι σαφώς μεγαλύτερο έναντι του κόστους για το 802.11. Δεν πρέπει φυσικά να ξεχνάμε ότι το WiFi είναι μια τεχνολογία για τοπική δικτύωση και σχεδιάστηκε για να δώσει μια κινητικότητα σε ιδιωτικά ενσύρματα τοπικά δίκτυα ενώ το WiMAX σχεδιάστηκε για να παρέχει ευρυζωνική ασύρματη πρόσβαση. Μπορούμε λοιπόν να οδηγηθούμε στο συμπέρασμα πως για την ανάπτυξη ενός μικρού ασύρματου δικτύου το κόστος του WiMAX είναι απαγορευτικό. Επίσης, το 802.11 δεν μπορεί να καλύψει μεγάλης εμβέλειας περιοχές άρα μοιραία οδηγούμαστε στη χρήση του 802.16 που έχει ένα εύλογο κόστος για τις υπηρεσίες που παρέχει σε τόσο μεγάλες αποστάσεις.

Στη σύγκριση των δύο προτύπων, υπάρχουν αρκετές διαφορές στη ραδιοτεχνολογία που τα διακρίνουν. Όλες οι υλοποιήσεις του WiFi χρησιμοποιούν μη αδειοδοτημένες μπάντες συχνοτήτων, ενώ το WiMAX δουλεύει σε νόμιμες και μη μπάντες γεγονός που κάνει πιο εύκολο τον έλεγχο της μετάδοσης και παράλληλα βελτιώνει την ποιότητα των μεταδιδόμενων σημάτων.

Επίσης τα πρότυπα WiFi και WiMAX έχουν και μία σημαντική διαφορά στο εύρος ζώνης των καναλιών. Το WiFi καθορίζει ένα σταθερό εύρος ζώνης καναλιού 25 MHz για το πρότυπο 802.11b και 20 MHz για τα πρότυπα 802.11a και 802.11g. Αντίθετα στο WiMAX, το εύρος ζώνης του καναλιού είναι προσαρμοστικό και κυμαίνεται από το 1.25MHz μέχρι τα 20MHz, γεγονός που το κάνει ιδιαίτερα σημαντικό στις περιπτώσεις που η μπάντα συχνοτήτων που χρησιμοποιείται είναι αδειοδοτημένη.

Επιπροσθέτως, παρατηρείται σημαντική διαφορά στις ταχύτητες μετάδοσης των δεδομένων. Το WiMAX προσφέρει υψηλές ταχύτητες στη χρήση του διαδικτύου ως σύστημα ευρυζωνικής πρόσβασης που χρησιμοποιείται και από τους παρόχους υπηρεσιών διαδικτύου ISPs ενώ παράλληλα μεταφέρονται αρκετά πιο γρήγορα τα δεδομένα φωνής και βίντεο σε σύγκριση με το αρχικό πρότυπο 802.11 που δεν προβλέπει ποιότητα σε τέτοιου είδους υπηρεσίες.

Διαφορές επίσης παρατηρούνται και στον τρόπο λειτουργίας του επιπέδου MAC των δύο πρωτοκόλλων. Στο MAC επίπεδο του WiFi οι σταθμοί συμπεριφέρονται ανταγωνιστικά ως προς τον τρόπο πρόσβασης στο κοινόχρηστο μέσο. Όλοι οι σταθμοί που θέλουν να μεταφέρουν δεδομένα ανταγωνίζονται για την κατοχή του μέσου, με αποτέλεσμα να μειώνεται η απόδοση του δικτύου ειδικά στις περιπτώσεις που εμφανίζονται τα προβλήματα των κρυμμένων αλλά και των εκτεθειμένων σταθμών. Αντίθετα, το MAC επίπεδο του 802.16 χρησιμοποιεί έναν αλγόριθμο σύμφωνα με τον οποίο κάθε σταθμός έχει πρόσβαση ανά πάσα στιγμή αφού βέβαια προηγηθεί η εγγραφή του στο εν λόγω δίκτυο. Από εκεί και πέρα, οι σταθμοί βάσης είναι υπεύθυνοι για τον καθορισμό του τρόπου πρόσβασης κάθε σταθμού. Ένα ακόμα πλεονέκτημα της χρήσης αυτής της τεχνικής είναι πως ο αλγόριθμος που χρησιμοποιείται έχει προβλέψει και την περίπτωση υπερφόρτωσης του δικτύου μετατρέποντας τη μεταφορά των δεδομένων ως ικανοποιητική, αυξάνοντας κατά πολύ τον μέγιστο αριθμό που μπορεί να εξυπηρετήσει το δίκτυο σε σύγκριση με το 802.11 που ο αριθμός των χρηστών είναι αρκετά περιορισμένος.

Τέλος, το WiMAX προσφέρει τη δυνατότητα ταυτόχρονης αποστολής και λήψης δεδομένων μεταξύ των σταθμών. Σε αντίθεση με το WiFi που οι σταθμοί ήταν υποχρεωμένοι να περιμένουν τη μετάδοση των δεδομένων από τον σταθμό με τον οποίο επικοινωνούν για να αποστείλουν και αυτοί με τη σειρά τους τα δικά τους δεδομένα, στο WiMAX οι δύο πλευρές μπορούν παράλληλα να λαμβάνουν αλλά και να στέλνουν τα δεδομένα τους, γεγονός που αυξάνει κατά πολύ την απόδοση του δικτύου και την εξυπηρέτηση των χρηστών.

Στον παρακάτω πίνακα παρουσιάζονται οι βασικές διαφορές μεταξύ των βασικότερων προτύπων των οικογενειών 802.16 και 802.11.

Feature	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
<b>Primary Application</b>	Broadband Wireless Access	Wireless LAN	Wireless LAN
<b>Frequency Band</b>	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
<b>Channel Bandwidth</b>	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
<b>Half/Full Duplex</b>	Full	Half	Half
<b>Radio Technology</b>	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
<b>Bandwidth Efficiency</b>	<=5 bps/Hz	<=0.44 bps/Hz	<=2.7 bps/Hz
<b>Modulation</b>	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
<b>FEC</b>	Convolutional Code Reed-Solomon	None	Convolutional Code
<b>Encryption</b>	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
<b>Mobility</b>	Mobile WiMax (802.16e)	In development	In development
<b>Mesh</b>	Yes	Vendor Proprietary	Vendor Proprietary
<b>Access Protocol</b>	Request/Grant	CSMA/CA	CSMA/CA

Εικόνα 6.6: Σύγκριση προτύπων 802.16 και 802.11.

Συμπερασματικά, η σύγκριση των δύο πρωτοκόλλων ουσιαστικά δεν μπορεί να συμβεί αφού αναφέρονται τεχνολογίες που χρησιμοποιούνται για να εξυπηρετήσουν διαφορετικούς σκοπούς. Μερικά μόνο σημεία μπορούν να συγκριθούν όπως είναι οι ρυθμοί μετάδοσης, το κόστος και η παροχή υπηρεσιών, όταν οι δύο τεχνολογίες θα χρησιμοποιηθούν για να υλοποιήσουν ένα ασύρματο τοπικό δίκτυο που είναι η μόνη κοινή υλοποίησή τους. Σαφώς, για ευρυζωνικές συνδέσεις και καλύψεις μερικών χιλιομέτρων το WiMAX έχει γνωρίσει μεγάλης απήχησης και παρουσιάζεται ως πολλά υποσχόμενο. Από την άλλη, όσον αφορά τα ασύρματα τοπικά δίκτυα, η τεχνολογία WiFi δεν έχει βρει ακόμα αντικαταστάτη μιας και το WiMAX έχει αυξημένο κόστος και μικρότερους ρυθμούς μετάδοσης σε τέτοιου είδους χρήση.

## ΑΝΑΦΟΡΕΣ

- [1] Anonymous, (2008), “wireless LAN (WLAN or Wireless Local Area Network)”, <http://searchmobilecomputing.techtarget.com/definition/wireless-LAN>
- [2] Anonymous, (2009), “Wireless LAN History Wireless Local Networks“, <http://www.tech-ware-tips-startup-internet-business.com/Wireless-LAN.html>
- [3] Anonymous, (2012), “Mobile ad-hoc network”, [http://en.wikipedia.org/wiki/Mobile\\_ad-hoc\\_networks](http://en.wikipedia.org/wiki/Mobile_ad-hoc_networks)
- [4] Anonymous, (2007), “Basic Service Set”, [http://it.toolbox.com/wiki/index.php/Basic\\_Service\\_Set](http://it.toolbox.com/wiki/index.php/Basic_Service_Set)
- [5] Martz Christine, (2011), “ESS - Extended Service Set”, [http://www.birds-eye.net/definition/e/ess-extended\\_service\\_set.shtml](http://www.birds-eye.net/definition/e/ess-extended_service_set.shtml)
- [6] Anonymous, (2012), “Multi-BSS environments: virtual APs“, <http://sourcedaddy.com/networking/multi-bss-environments-virtual-aps.html>
- [7] Anonymous, (2010), “The 7 Layers of the OSI Model“, [http://www.webopedia.com/quick\\_ref/OSI\\_Layers.asp](http://www.webopedia.com/quick_ref/OSI_Layers.asp)
- [8] Khan Jakhanzeb, Khwaja Anis, (2003), *Building secure wireless networks with 802.11*, Publisher: Wiley
- [9] Petri Daniel, (2009), “OSI Model Concepts“, [http://www.petri.co.il/osi\\_concepts.htm](http://www.petri.co.il/osi_concepts.htm)
- [10] Παπαπέτρου Ευάγγελος, (2012), “Ασύρματα Τοπικά Δίκτυα”, <http://www.cs.uoi.gr/~epap/asurmata/downloads/lect6.pdf>
- [11] Roshan Pejman, Leary Jonathan, (2003), *802.11 Wireless LAN Fundamentals*, Publisher: Cisco Press
- [12] Boer Jan, (1993), *Direct Sequence Spread Spectrum Physical Layer Specification IEEE 802.11*, Document: IEEE P802.11-96/49E
- [13] Khan Jakhanzeb, Khwaja Anis, (2003), *Building secure wireless networks with 802.11*, Publisher: Wiley

- [14] Chayat Naftali, (1996), Frequency Hopping Spread Spectrum PHY of the 802.11 Wireless LAN Standard, Document: IEEE P802.11-96/49D
- [15] Anonymous, (2012), “Spread Spectrum”,  
[http://www-cs-faculty.stanford.edu/~eroberts/courses/soco/projects/2003-04/wireless-computing/int\\_ss.shtml](http://www-cs-faculty.stanford.edu/~eroberts/courses/soco/projects/2003-04/wireless-computing/int_ss.shtml)
- [16] Anonymous, (2012), “Frequency Hopping Spread Spectrum“, <http://www.tech-faq.com/frequency-hopping-spread-spectrum.html>
- [17] Anonymous, (2012), “IR Physical Medium Dependent (PMD) Sublayer”,  
<http://www.wireless-center.net/WLANs-WPANs/1483.html>
- [18] Geier Jim, (2003), “Infrared WLAN“,  
<http://www.wi-fiplanet.com/tutorials/article.php/2110301>
- [19] Schwartz Sorin, (2012), “Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA)and Wireless LAN (WLAN)”,  
[http://sorin-schwartz.com/white\\_papers/fhvsds.pdf](http://sorin-schwartz.com/white_papers/fhvsds.pdf)
- [20] Perahia Eldad, Stacey Robert, (2008), *Next Generation Wireless LANs*, Publisher: Cambridge Press
- [21] Zheng Pei et al., (2008), *Wireless Networking Complete*, Publisher: Elsevier
- [22] Roshan Pejman, Leary Jonathan, (2003), *802.11 Wireless LAN Fundamentals*, Publisher: Cisco Press
- [23] Darchis Nicolas, (2012), “802.11 frames: A starter guide to learn wireless sniffer traces“,  
<https://supportforums.cisco.com/docs/DOC-13664>
- [24] Tanenbaum Andrew, (2003), *Computer networking*, Publisher: Prentice Hall
- [25] Bianchi G. ,(2000), “Performance analysis of the IEEE 802.11 distributed coordination function“,  
<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=840210&userType=inst>
- [26] Anonymous, (2012), “CSMA/CA”,  
[http://www.cs.clemson.edu/~westall/851/802.11/802\\_CSMA\\_CA.pdf](http://www.cs.clemson.edu/~westall/851/802.11/802_CSMA_CA.pdf)
- [27] Gast M., (2005), *Wireless networks the definitive guide*, Publisher: O’Reilly

- [28] Geier Jim, (2002), “802.11 Beacons Revealed“, <http://www.wi-fiplanet.com/tutorials/article.php/1492071>
- [29] Tanenbaum Andrew, (2003), *Computer networks 4rth edition*, Publisher: Prentice Hall
- [30] Jahanzeb Khan, Anis Khwaza, (2003), *Building secure wireless networks with 802.11*, Publisher: Wiley
- [31] Anonymous, (2004), “Complementary Code Keying (CCK)”, <http://searchmobilecomputing.techtarget.com/definition/Complementary-Code-Keying>
- [32] Mustafa Ergen, (2002), “IEEE Tutorial”, <http://www.scribd.com/doc/54133075/66/DSSS-Packet-Binary-Convolutional-Coding>
- [33] Anonymous, (2006), “WEP (wired equivalent privacy)”, <http://www.networkworld.com/details/715.html>
- [34] Anonymous, (2012), “IEEE 802.11b-1999”, [http://en.wikipedia.org/wiki/IEEE\\_802.11b-1999](http://en.wikipedia.org/wiki/IEEE_802.11b-1999)
- [35] Pejman Roshan, Jonathan Leary, (2003), *Wireless Lan Fundamentals*, Publisher: Cisco Press
- [36] Jahanzeb Khan, Anis Khwaza, (2003), *Building secure wireless networks with 802.11*, Publisher: Wiley
- [37] Cisco Systems, (2009), “Voice over Wireless LAN 4.1 Design Guide”, [http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan\\_ch3.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan_ch3.html)
- [38] Anonymous, (2012), “OFDM”, <http://www.mobileisgood.com/ofdm.php>
- [39] Dimitris Vassis et al., (2005), “The IEEE 802.11g Standard for High Data Rate WLANs”, [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1453395&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D1453395](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1453395&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D1453395)
- [40] Cisco Systems, (2012), “Capacity Coverage & Deployment Considerations for IEEE 802.11g”, [http://www.cisco.com/en/US/products/hw/wireless/ps4570/products\\_white\\_paper09186a00801d61a3.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_white_paper09186a00801d61a3.shtml)



- [41] Dimitris Vassis et al., (2005), “The IEEE 802.11g Standard for High Data Rate WLANs”,  
[http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1453395&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D1453395](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1453395&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D1453395)
- [42] Gast M., (2005), *Wireless networks the definitive guide*, Publisher: O’Reilly
- [43] Yang Xiao, Yi Pan, (2009), *Emerging wireless lans wireless pans and wireless mans*, Publisher: Wiley
- [44] VonNagy Andrew, (2010), “Wireless QoS Part 2 - IEEE 802.11e Principles”,  
<http://revolutionwifi.blogspot.com/2010/08/wireless-qos-part-2-80211e-principles.html>
- [45] Stefan Mangold et al., “ieee 802.11e wireless lan for quality of service”,  
[http://webstaff.itn.liu.se/~davqu/tnk087/802\\_11\\_e.pdf](http://webstaff.itn.liu.se/~davqu/tnk087/802_11_e.pdf)
- [46] Sunghyun Choi, (2008), “IEEE 802.11 Wireless LANs”,  
<http://www.scribd.com/doc/58671771/45/QoS-Control-Field-QoS-Control-Field>
- [47] Zheng Pei et al., (2008), *Wireless Networking Complete*, Publisher: Elsevier
- [48] Airmagnet, (2008), *802.11n Primer*, Publisher: AirMagnet
- [49] Cisco Systems, (2011), “802.11n: The Next Generation of Wireless Performance”,  
[http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white\\_paper\\_c11-427843\\_v1.pdf](http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns348/ns767/white_paper_c11-427843_v1.pdf)
- [50] Yang Xiao, Yi Pan, (2009), *Emerging wireless lans wireless pans and wireless mans*, Publisher: Wiley
- [51] Pei Zheng et al., (2004), *wireless networking complete*, Publisher: Elsevier
- [52] Amitabh Mishra, (2008), *Security and quality of service in ad hoc wireless networks*, Publisher: Cambridge University Press
- [53] Anonymous, (2009), “Introduction to FDM, OFDM, OFDMA, SOFDMA”,  
<http://www.conniq.com/WiMAX/fdm-ofdm-ofdma-sofdma-02.htm>
- [54] Syed Ahson, Mohammad Ilyas, (2008), *WiMAX Technologies, Performance Analysis, and QoS*, Publisher: CRC Press
- [55] Finneran Michael, (2004), “Wimax versus Wifi A comparison of technologies, markets and business plans”,  
<http://media.techtarget.com/searchMobileComputing/downloads/Finneran.pdf>

## ΒΙΒΛΙΟΓΡΑΦΙΑ

Αλεξόπουλος Α., Λαγογιάννης Γ., (2003), *Τηλεπικοινωνίες και δίκτυα υπολογιστών*, Εκδόσεις: Παπασωτηρίου

Γεωργίου Γεώργιος, (2007), “Τεχνολογίες ασύρματων τοπικών δικτύων και η χρήση τους σε περιβάλλοντα γραφείου”, <http://www.scribd.com/doc/55759089/>

Δρεμούση Ευγενία και Ιωαννίδης Γεώργιος, (2004), “Αξιολόγηση απόδοσης ασύρματων μητροπολιτικών δικτύων”, <http://www.scribd.com/doc/55886140/>

Κωνσταντίνος Γεωργακόπουλος, (2007), “Τεχνολογίες σύγχρονων ασύρματων δικτύων δεδομένων”,  
[http://de.teikav.edu.gr/telematics/pdf/3o\\_Meros\\_Asymmata\\_thlematikh.pdf](http://de.teikav.edu.gr/telematics/pdf/3o_Meros_Asymmata_thlematikh.pdf)

Anonymous, (2011), “Τι χρειάζεται να γνωρίζετε για τα ασύρματα δίκτυα”,  
[http://www.cisco.com/web/GR/solutions/smb/products/wireless/wireless\\_primer.html](http://www.cisco.com/web/GR/solutions/smb/products/wireless/wireless_primer.html)

Anonymous, (2012), “Carrier Sense multiple access with collision avoidance”,  
[http://en.wikipedia.org/wiki/Carrier\\_sense\\_multiple\\_access\\_with\\_collision\\_avoidance](http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance)

Anonymous, (2012), “contention window optimization for 802.11 dcf access control”, [http://www.vocal.com/network/802\\_11\\_dcf.html](http://www.vocal.com/network/802_11_dcf.html)

Anonymous, (2010), “History of OFDMA and How it Works“,  
[http://www.webopedia.com/DidYouKnow/Computer\\_Science/2005/OFDMA.asp](http://www.webopedia.com/DidYouKnow/Computer_Science/2005/OFDMA.asp)

Anonymous, (2012), “IEEE 802.11 RTS/CTS”,  
[http://en.wikipedia.org/wiki/IEEE\\_802.11\\_RTS/CTS](http://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS)

Anonymous, (2012), “IEEE 802.11a-1999”,  
[http://en.wikipedia.org/wiki/IEEE\\_802.11a-1999](http://en.wikipedia.org/wiki/IEEE_802.11a-1999)

Anonymous, (2012), “IEEE 802.11g The New Mainstream Wireless LAN Standard”,  
[http://www.dell.com/downloads/global/shared/broadcom\\_802\\_11\\_g.pdf](http://www.dell.com/downloads/global/shared/broadcom_802_11_g.pdf)

Anonymous, (2010), “OFDM Tutorial”,  
<http://www.wave-report.com/blog/?p=72>

Anonymous, (2012), “Orthogonal frequency division multiplexing”,  
[http://en.wikipedia.org/wiki/Orthogonal\\_frequency-division\\_multiplexing](http://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing)

Anonymous, (2009), “open system interconnection”,  
[http://docwiki.cisco.com/wiki/Open\\_System\\_Interconnection\\_Protocols#OSI\\_Network\\_Layer](http://docwiki.cisco.com/wiki/Open_System_Interconnection_Protocols#OSI_Network_Layer)

Anonymous, (2012), “open system interconnection (OSI)”,  
<http://www.techabulary.com/o/osi/>

Anonymous, (2012), “WiMAX MAC Layer“,  
<http://www.radio-electronics.com/info/wireless/wimax/mac-layer.php>

Anonymous, (2012), “WiFi and WiMax Comparison“,  
<http://itsallabouttechnology.com/wifi/wifi-vs-wimax.html>

Anonymous, (2012), “Wimax Vs WiFi - Comparison between WiFi and Wimax“,  
<http://www.wifinotes.com/wimax/wimax-vs-wifi.html>

Anonymous, (2012), “Wimax Vs WiFi - Comparison of Wimax and WiFi“,  
<http://freewimaxinfo.com/wimax-vs-wifi-comparison.html>

Anonymous, (2011), “Wired Vs Wireless home networks“,  
<http://www.wifinotes.com/wired-vs-wireless-home-networks.html>

Anonymous, (2008), “WLAN - 802.11 a,b,g and n“,  
<http://zone.ni.com/devzone/cda/tut/p/id/7131>

Anonymous, (2012), “802.11a Wireless LAN“,  
[http://www.vocal.com/redirect/802\\_11a.html](http://www.vocal.com/redirect/802_11a.html)

Anonymous, (2012), “802.11g Wireless Turbo White Paper“,  
<http://www.usr.com/download/whitepapers/80211g-wp.pdf>

Bradley Mitchell, (2011), “Wired vs. Wireless Networking“,  
<http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm>

Bradley Mitchell, (2012), “WPA - Wi-Fi Protected Access“,  
[http://compnetworking.about.com/cs/wirelesssecurity/g/bldef\\_wpa.htm](http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm)

Brenner Pablo, (1997), “a technical tutorial on the ieee 802.11 protocol“,  
[http://www.sss-mag.com/pdf/802\\_11tut.pdf](http://www.sss-mag.com/pdf/802_11tut.pdf)

Burton M., (2009), “802.11 Arbitration“,  
[http://www.cwnp.com/pdf/802.11\\_arbitration.pdf](http://www.cwnp.com/pdf/802.11_arbitration.pdf)

Calgary A., (2000), “Spread Spectrum Wireless Technology“,  
[http://www.old.optivera.ru/products/Wilan/whitepaper\\_mcdsss.pdf](http://www.old.optivera.ru/products/Wilan/whitepaper_mcdsss.pdf)

Chandra A., et al, (2000) “Wireless Medium Access Control Protocols”, IEEE Communications Society,  
[http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5340799&tag=1](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5340799&tag=1)

- Charan Langton, (2004), "OFDM tutorial"  
<http://www.complextoreal.com/chapters/ofdm2.pdf>
- Duong M., (2012), "802.16 MAC layer: structure and QoS support",  
[http://uet.vnu.edu.vn/~tantd/Chi\\_doan/MAC%20layer\\_structure%20and%20QoS%20support.pdf](http://uet.vnu.edu.vn/~tantd/Chi_doan/MAC%20layer_structure%20and%20QoS%20support.pdf)
- Eldad Perahia and Robert Stacey, (2008), *Next generation wireless lans*, Publisher: Cambridge Publishing
- Garetto M. and Chiasserini F., (2011), "Performance Analysis of the 802.11 Distributed Coordination Function under Sporadic Traffic",  
<http://www.telematics.polito.it/oldsite/garetto/papers/sporadictechrep.pdf>
- Gast M., (2005), *Wireless networks the definitive guide*, Publisher: O'Reilly
- Geier J., (2000), "IEEE 802.11 Standard overview",  
<http://www.informit.com/articles/article.aspx?p=19825&seqNum=4>
- Geier J., (2003), "802.11a Physical Layer Revealed",  
<http://www.wi-fiplanet.com/tutorials/article.php/2109881>
- IEEE Committee, (2007), "IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications",  
<http://standards.ieee.org/getieee802/download/802.11-2007.pdf>
- IEEE Committee, (2003), "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band",  
<http://standards.ieee.org/getieee802/download/802.11a-1999.pdf>
- Khan J. and Khwaja A., (2003), *Building secure wireless networks with 802.11*, Publisher: Wiley
- Marks Roger et al., (2001), "The 802.16 WirelessMAN™ MAC: It's Done, but What Is It?",  
[http://ieee802.org/16/docs/01/80216-01\\_58r1.pdf](http://ieee802.org/16/docs/01/80216-01_58r1.pdf)
- Pei Zheng et al., (2004), *wireless networking complete*, Publisher: Elsevier
- Pejman Roshan and Jonathan Leary, (2003), *802.11 wireless lan fundamentals*, Publisher: Cisco Press
- Schwartz Sorin, (2011), "Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN)",  
[http://sorin-schwartz.com/white\\_papers/fhvsds.pdf](http://sorin-schwartz.com/white_papers/fhvsds.pdf)
- Umrani F., (2011), "Spread Spectrum Communication",  
<http://www.scribd.com/doc/55080451/36/Benefits-of-FHSS>

University of Washington, (2011), “The OSI model”,  
[http://www.washington.edu/lst/help/computing\\_fundamentals/networking/osi](http://www.washington.edu/lst/help/computing_fundamentals/networking/osi)

Wave Report, (2010), “OFDM tutorial”, <http://www.wave-report.com/blog/?p=72>

Youssef M. and Miller R., (2002), “Analyzing the Point Coordination Function of the IEEE 802.11 WLAN protocol using a system of communication machines specification”, [http://www.cs.umd.edu/~moustafa/papers/pcf\\_tr.pdf](http://www.cs.umd.edu/~moustafa/papers/pcf_tr.pdf)