

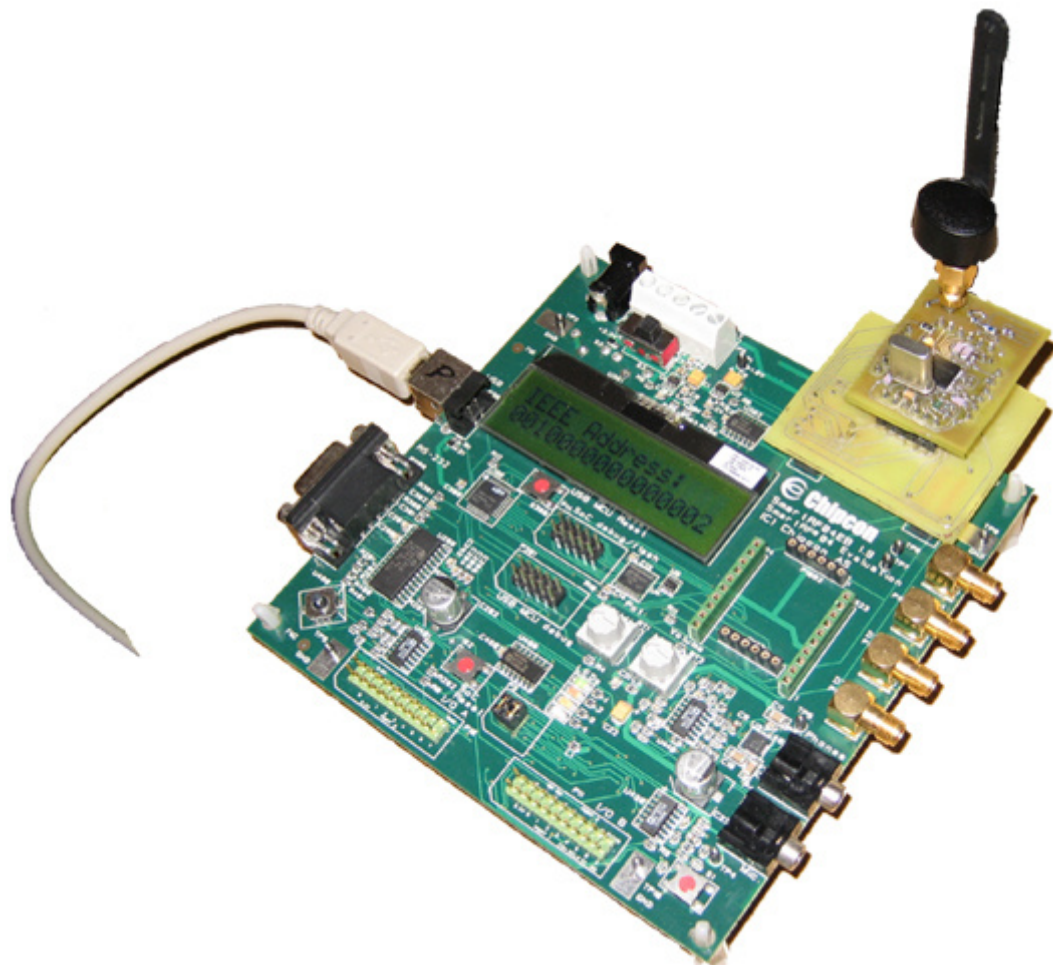


ΑΤΕΙ ΧΑΝΙΩΝ

ΤΜΗΜΑ: ΗΛΕΚΤΡΟΝΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΘΕΜΑ: «ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΣΩ ZIGBEE»



ΥΛΟΠΟΙΗΣΗ: Παπαθεοδώρου Τηλέμαχος

ΕΠΙΒΛΕΠΩΝ: Δρ. Χατζάκης Ιωάννης
Επίκουρος Καθηγητής

Χανιά 2009

Περιεχόμενα

Κεφάλαιο 1^ο

ΠΡΩΤΟΚΟΛΛΑ ΑΣΥΡΜΑΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

1.1 Wi-Fi.....	8
1.2 WiMAX.....	11
1.3 BLUETOOTH.....	12
1.4 ZIGBEE.....	13

Κεφάλαιο 2^ο

ΠΡΩΤΟΚΟΛΛΟ ZIGBEE

2.1 Έννοιες του πρωτοκόλλου.....	15
2.1.1 Services.....	15
2.1.2 Primitives.....	15
2.1.3 Constants & Attributes.....	16
2.1.4 Binding.....	16
2.1.5 Energy Detection (ED).....	16
2.1.6 Carrier Sense (CS).....	17
2.1.7 Link Quality Indicator (LQI).....	17
2.1.8 Clear Channel Assessment (CCA).....	17
2.1.9 Beacon.....	18
2.1.10 Superframe.....	18
2.1.11 Route Discovery.....	18
2.1.12 Device Discovery.....	18
2.2 Τα επίπεδα του ZigBee.....	19
2.2.1 Physical Layer.....	19
2.2.1.1 PHY Services.....	20
2.2.1.2 PPDU.....	21
2.2.2 MAC Layer.....	22
2.2.2.1 MAC Services.....	22
2.2.2.2 MPDU.....	26
2.2.3 Network Layer.....	27
2.2.2.1 NWK Services.....	27
2.2.3.2 Unicast.....	30

2.2.3.3 Multicast.....	30
2.2.3.4 Broadcast.....	31
2.2.3.5 NWK PDU.....	31
2.2.4 Application Layer	33
2.2.4.1 Application Framework	33
2.2.4.2 ZDO	34
2.2.4.3 APL Services - APS.....	34
2.2.4.4 APL PDU	36

Κεφάλαιο 3^ο

ZIGBEE ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

3.1 ZigBee Transceivers	38
3.1.1 Atmel	38
3.1.2 Freescale.....	39
3.1.3 MaxStream	40
3.1.4 Microchip.....	40
3.1.6 Texas Instruments	42
3.2 SoC CC2430.....	42
3.2.1 DMA.....	43
3.2.2 WATCHDOG TIMER.....	43
3.3.3 8051 CPU	43
3.3.4 MEMORY ARBITRATOR.....	44
3.3.5 USARTs.....	44
3.3.6 TIMERS.....	44
3.3.7 ADC.....	44
3.3.8 AES.....	44
3.3.9 ON-CHIP VOLTAGE REGULATOR.....	45
3.3.10 TRANSCEIVER.....	45

Κεφάλαιο 4^ο

ΣΧΕΔΙΑΣΗ ΚΑΙ ΑΝΑΠΤΥΞΗ

4.1 Κύκλωμα πομποδέκτη.....	46
4.2 BALUNs	47
4.2.1 Microstrip Balun	47
4.2.2 Chip Balun.....	48

4.2.3 Discrete components balun.....	48
4.3 Κεραίες για εφαρμογές ZigBee	49
4.3.1 Folded Dipole.....	49
4.3.2 IFA.....	49
4.3.3 Chip Antennas	50
4.4 Προγραμματισμός.....	50
Παράρτημα Α.....	52
Παράρτημα Β.....	55
Βιβλιογραφία	62
Δικτυακοί τόποι.....	62

Οργάνωση

Στο κεφάλαιο 1 περιγράφονται περιληπτικά ορισμένα πρωτόκολλα ασύρματης επικοινωνίας. Σκοπός είναι να γίνει εμφανές ότι κάθε πρωτόκολλο είναι κατάλληλο για συγκεκριμένες εφαρμογές. Αυτός είναι και ο λόγος που δημιουργήθηκε το ZigBee.

Στο κεφάλαιο 2 παρουσιάζεται το ZigBee πρωτόκολλο με τις βασικές έννοιες και τον τρόπο με τον οποίο επικοινωνούν τα επίπεδα μεταξύ τους. Το κεφάλαιο αυτό περιέχει πολλά ακρωνύμια και ο αναγνώστης παροτρύνεται να ανατρέξει στο παράρτημα Α.

Ορισμένα από τα προϊόντα που υπάρχουν στην αγορά για την κατασκευή ενός ZigBee πομποδέκτη καθώς και η περιγραφή του ολοκληρωμένου που χρησιμοποιήθηκε για τα κυκλώματα της πτυχιακής εργασίας, είναι το θέμα του 3^{ου} κεφαλαίου.

Κλείνοντας στο κεφάλαιο 4 αναλύεται το κύκλωμα που κατασκευάστηκε και οι εναλλακτικοί μέθοδοι με τις οποίες μπορούν να σχεδιαστούν κάποιες βαθμίδες του.

Ευχαριστίες

Καταρχήν θα ήθελα να ευχαριστήσω τον κ. Χατζάκη Ιωάννη εισηγητή αυτής της πτυχιακής εργασίας για την πολύτιμη συμβολή και στήριξή του κατά την εκπόνησή της και τον κ. Ρηγάκη Ηρακλή για τις σημαντικές συμβουλές του.

Επίσης θα ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξη κατά την διάρκεια των σπουδών μου, τον αδερφό μου που παρά την απόσταση είναι πάντα δίπλα μου, καθώς και τον πολύ καλό μου φίλο Βαγγέλη Περρή που με βοήθησε να έρθω ξανά σε επαφή με την επιστήμη της ηλεκτρονικής.

Abstract

Wireless technologies based on a protocol for networks implementation, are becoming part of our everyday life. Except engineers, 15-years ago no one was worried about these technologies. Nowadays everyone is carrying a cell phone, a Bluetooth headset, or is getting access to the web through a Wi-Fi hotspot. But this is just the beginning. The advancement of technology in the field of electronics is fast and new sophisticated high integration methods combined with programming techniques for embedded systems, are bringing to us more powerful and small electronic devices. The next step is the “invasion” of wireless in the fields of home automation, monitoring, industrial control, medical applications etc. Here it comes ZigBee, a new wireless protocol suitable for these applications. ZigBee is a technology combining high reliability with low power consumption that will extend battery life for years, and has also the ability to connect a practically infinite number of devices through its flexible network topologies.

This project thesis is dedicated entirely to ZigBee, answering questions like “why to develop this new wireless technology while many others exists?”, “what should I use for my application?” and “which considerations should I take while designing a ZigBee module?”.

Πρόλογος

Οι ασύρματες τεχνολογίες δημιουργίας δικτύων βάσει πρωτοκόλλου γίνονται ολοένα και περισσότερο μέρος της καθημερινής μας ζωής. Πριν από 15 χρόνια οι τεχνολογίες αυτές αφορούσαν μόνο τους μηχανικούς που ασχολούνταν με την ανάπτυξή τους. Σήμερα ο καθένας έχει μια φορητή συσκευή κινητής τηλεφωνίας, ή Bluetooth ακουστικά ή μπορεί να χρησιμοποιεί ένα Wi-Fi hotspot για να αποκτήσει πρόσβαση στο διαδίκτυο. Με την ραγδαία εξέλιξη της τεχνολογίας στον τομέα της ηλεκτρονικής, έχουν αναπτυχθεί νέες μέθοδοι για την υψηλή ολοκλήρωση που σε συνδυασμό με τεχνικές προγραμματισμού για embedded συστήματα οδηγούν στην παραγωγή συσκευών μικρότερου όγκου και περισσότερων δυνατοτήτων. Το επόμενο βήμα είναι η «εισβολή» των ασύρματων τεχνολογιών στους τομείς των αυτοματισμών σε σπίτια, της παρακολούθησης, του βιομηχανικού ελέγχου, των ιατρικών εφαρμογών κτλ. Στο σημείο αυτό έρχεται να δώσει λύσεις το ZigBee, ένα ασύρματο πρωτόκολλο κατάλληλο για τις παραπάνω εφαρμογές. Το ZigBee συνδυάζει την υψηλή αξιοπιστία με την χαμηλή κατανάλωση ενέργειας, που αυξάνει τη διάρκεια ζωής της μπαταρίας για χρόνια, και παρέχει επίσης τη δυνατότητα διασύνδεσης πρακτικά άπειρου αριθμού συσκευών μέσω ευέλικτων μεθόδων δικτύωσης.

Η παρούσα πτυχιακή εργασία είναι αφιερωμένη στην περιγραφή του ZigBee και απαντά σε ερωτήματα όπως «ποιος ο λόγος ανάπτυξης μιας ακόμη ασύρματης τεχνολογίας από τι στιγμή που ήδη υπάρχουν αρκετές;», «τι μπορεί να χρησιμοποιήσει κανείς για την εφαρμογή του;» και «τι θα πρέπει να λάβει κανείς υπόψη κατά το σχεδιασμό ενός ZigBee module;»

Κεφάλαιο 1^ο

ΠΡΩΤΟΚΟΛΛΑ ΑΣΥΡΜΑΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

1.1 Wi-Fi

Wi-Fi είναι η εμπορική ονομασία του πρωτοκόλλου 802.11x της IEEE. Το Wi-Fi δίνει τη δυνατότητα για δημιουργία ασύρματων τοπικών δικτύων (WLANs). Χρησιμοποιείται ευρέως για την πρόσβαση στο διαδίκτυο με πλεονεκτήματα ότι παρακάμπτει την ανάγκη καλωδίωσης των κτιρίων και προσφέρει κάλυψη οπουδήποτε, ακόμα και σε εξωτερικούς χώρους. Πλέον όλοι οι φορητοί υπολογιστές διαθέτουν μια μονάδα που υλοποιεί το 802.11x και για όσους Η/Υ δεν διαθέτουν ενσωματωμένη μονάδα υπάρχει ένα πλήθος προσαρμογέων σε μορφή καρτών PCI, PCMCIA και σε USB περιφερειακό.

Σε πολλά κεντρικά σημεία μιας πόλης είναι δυνατή η σύνδεση στο διαδίκτυο από οποιονδήποτε φέρει μια φορητή συσκευή με τις ανάλογες δυνατότητες και το κατάλληλο λειτουργικό. Αυτό συμβαίνει για το λόγο ότι μεγάλα ξενοδοχεία, εμπορικά κέντρα, διάφορες επιχειρήσεις ή ακόμα και δημόσιες υπηρεσίες διαθέτουν ασύρματο δίκτυο στο οποίο επιτρέπουν ελεύθερη πρόσβαση. Τα σημεία αυτά συναντώνται στην Αγγλική ορολογία ως «Access Points» ή «Hot spots». Η χρήση του Wi-Fi είναι ευρέως διαδεδομένη και στα πανεπιστήμια. Βέβαια, στην περίπτωση αυτή η πρόσβαση είναι περιορισμένη και προορίζεται για τους εκπαιδευτικούς και τους φοιτητές στους οποίους το ίδρυμα παρέχει τους απαραίτητους κωδικούς για τη σύνδεση.

Το σύστημα κρυπτογράφησης που χρησιμοποιείται για την ασφάλεια των Wi-Fi δικτύων είναι το WPA. Το WPA διαδέχθηκε το WEP το οποίο είχε αποδειχθεί χαμηλής ασφάλειας. Με τη σειρά του το WPA θα αντικατασταθεί από το WPA2 που χρησιμοποιεί το πιο εξελιγμένο σύστημα κρυπτογράφησης AES.

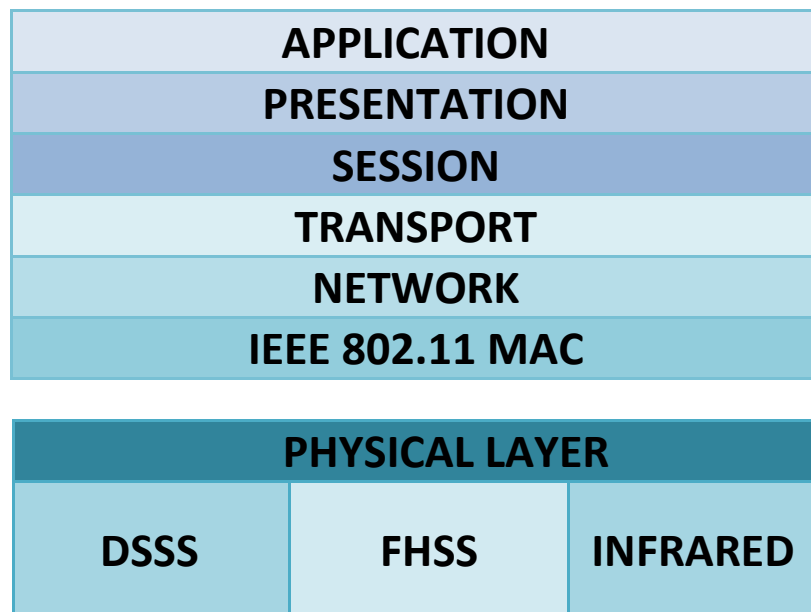
Η ονομασία Wi-Fi στην οποία έγινε αναφορά, δόθηκε από την Wi-Fi Alliance που αποτελεί μια μη κερδοσκοπικού χαρακτήρα συνεταιριστική κίνηση από κατασκευάστριες εταιρίες στο χώρο του ηλεκτρονικού εξοπλισμού. Η Wi-Fi Alliance ιδρύθηκε το 1999 με σκοπό να οδηγήσει στην υιοθέτηση ενός ενιαίου προτύπου για τα ασύρματα τοπικά δίκτυα. Σήμερα αποτελείται από 300 εταιρίες-μέλη. Η προσπάθεια της επικεντρώνεται στον έλεγχο των νέων συσκευών που παράγονται και που υλοποιούν το 802.11 με στόχο την εξασφάλιση της συμβατότητας με τα υπόλοιπα προϊόντα της ίδιας κατηγορίας. Κάθε συσκευή που πληρεί τους κανόνες και τις προϋποθέσεις που θέτει η Wi-Fi Alliance πέραν τον έλεγχο με επιτυχία και λαμβάνει πιστοποίηση.



Σχήμα 1.1
Λογότυπο πιστοποιημένου Wi-Fi προϊόντος

Επίπεδα του πρωτοκόλλου

Στο σχήμα που ακολουθεί φαίνεται ο διαχωρισμός του πρωτοκόλλου σε επίπεδα.



Σχήμα 1.2 Διαστρωμάτωση OSI του Wi-Fi

Τα δυο τελευταία επίπεδα PHY και MAC ορίζονται από την IEEE. Παρατηρώντας το φυσικό επίπεδο στο σχήμα 1.2 διακρίνονται οι τεχνικές κατανομής του χώρου σε ένα διαθέσιμο κανάλι, οι DSSS και FHSS.

Στην τεχνική DSSS κάθε bit πληροφορίας διαμορφώνεται με μια ψευδοτυχαία ακολουθία από 11 ή περισσότερα bits. Στη νέα ακολουθία που προκύπτει εφαρμόζεται ψηφιακή διαμόρφωση διαφορικής ολίσθησης φάσης DPSK και γίνεται εκπομπή του σήματος. Η DSSS αυξάνει σε μεγάλο βαθμό τον αριθμό των bits του σήματος που πρόκειται να σταλεί και αυτό έχει σαν συνέπεια μεγαλύτερες απαιτήσεις σε εύρος ζώνης και σε χωρητικότητα του καναλιού. Το μεγάλο πλεονέκτημα της DSSS είναι ότι σε περίπτωση αλλοίωσης των bits κατά την αποστολή, ο δέκτης μπορεί να ανακτήσει την χαμένη ακολουθία από bits με μεθόδους στατιστικής αποφεύγοντας έτσι την ανάγκη για επαναμετάδοση που θα μείωνε την ταχύτητα επικοινωνίας.

Στην τεχνική FHSS το σήμα πληροφορίας διαμορφώνεται με μια φέρουσα στενής ζώνης η οποία κάνει συνεχείς μεταβάσεις από μια συχνότητα σε μια άλλη βάσει μιας προκαθορισμένης ακολουθίας. Ο δέκτης σχετίζεται με την ακολουθία μεταβάσεων του πομπού και μπορεί να αναγνωρίσει το σήμα, ενώ οποιαδήποτε άλλη συσκευή το βλέπει σαν θόρυβο.

Δικτύωση

Σε ένα δίκτυο Wi-Fi θεωρούμε ότι μπορούν να υπάρξουν δυο τύποι στοιχείων ο σταθμός και το Access Point (AP). Σαν σταθμός ορίζεται ο Η/Υ του τελικού χρήστη ο οποίος έχει μια μονάδα που υλοποιεί το 802.11. Το AP είναι συνήθως μια συσκευή που περιλαμβάνει ένα πομποδέκτη 802.11 και μια κάρτα δικτύου που υλοποιεί το 802.3 Ethernet. Για την δημιουργία δικτύου μεταξύ αυτών των στοιχείων το 802.11 χρησιμοποιεί τις ακόλουθες τοπολογίες διασύνδεσης:

- Infrastructure mode
- Ad-hoc mode
- mesh mode

Infrastructure mode

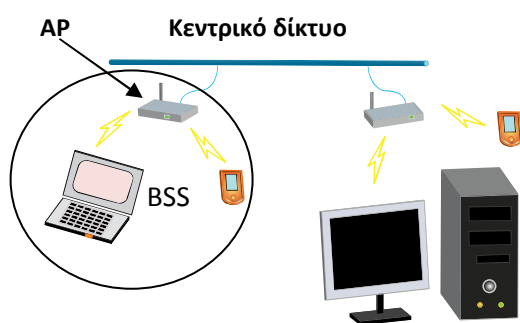
Το mode αυτό περιλαμβάνει τουλάχιστον ένα ασύρματο δίκτυο μεταξύ ενός AP και ενός συνόλου από σταθμούς. Το AP είναι συνδεδεμένο μέσω Ethernet με ένα κεντρικό δίκτυο το οποίο ανήκει σε κάποιον οργανισμό παροχής τηλεπικοινωνιακών υπηρεσιών. Οι σταθμοί αποκτούν πρόσβαση στις υπηρεσίες του κεντρικού δικτύου μέσω του AP. Αυτός ο τρόπος δικτύωσης λέγεται σύνολο βασικών υπηρεσιών (BSS). Περισσότερα από ένα BSS όπως στο σχήμα 1.3 δίνουν μια ολοκληρωμένη εικόνα για το Infrastructure mode.

Ad-Hoc mode

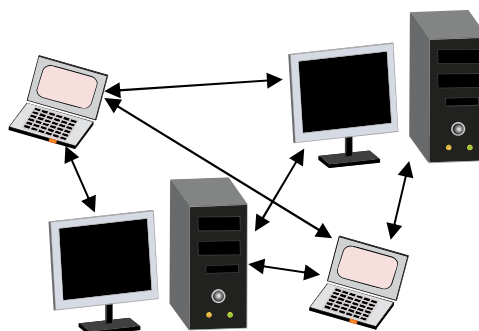
Στην περίπτωση του Ad-Hoc οι σταθμοί σχηματίζουν ασύρματο δίκτυο μεταξύ τους χωρίς τη χρήση AP ή κεντρικού δικτύου. Κάθε σταθμός έχει τη δυνατότητα να επικοινωνήσει με κάθε άλλο σταθμό που ανήκει στο ίδιο δίκτυο. Η δικτύωση αυτή λέγεται ανεξάρτητο σύνολο βασικών υπηρεσιών (IBSS).

Mesh mode

Στο Mesh mode η δημιουργία ασύρματης δικτύωσης γίνεται με το συνδυασμό των Infrastructure και Ad-Hoc modes.



Σχήμα 1.3 Infrastructure mode



Σχήμα 1.4 Ad-Hoc mode

Στον πίνακα αναγράφονται οι παραλλαγές του 802.11 με μια σύντομη περιγραφή

802.11a	Πρότυπο για τη δημιουργία WLAN	5 GHz	54Mbps
802.11b	Πρότυπο για τη δημιουργία WLAN	2.4 GHz	11Mbps
802.11d	Αναλύονται οι απαιτήσεις του 802.11 ώστε να λειτουργήσει σε χώρες στις οποίες δεν χρησιμοποιείται ακόμα		
802.11e	Βελτίωση του MAC για την αύξηση του QoS, ώστε να είναι δυνατή η αξιόπιστη μετάδοση φωνής και βίντεο μέσω του 802.11		
802.11f	Εξασφάλιση συμβατότητας μεταξύ συσκευών APs		
802.11g	Πρότυπο για τη δημιουργία WLAN υψηλής ταχύτητας	2.4 GHz	20Mbps
802.11h	Βελτίωση του 802.11 MAC και του 802.11a PHY	5 GHz	
802.11i	Βελτίωση της ασφάλειας των δικτύων του 802.11		
802.11n	Νέο πρότυπο για τη δημιουργία WLAN	2.4/5GHz	100Mbps
802.11X	Αύξηση της ασφάλειας των δικτύων του 802.11b		

1.2 WiMAX

Οι μέθοδοι που έχουμε γνωρίσει έως σήμερα για την απόκτηση πρόσβασης στο διαδίκτυο είναι μέσω σύνδεσης Dial-up, γραμμής DSL, με Wi-Fi από κάποιο AP και από εταιρείες κινητής τηλεφωνίας μέσω 3G. Όλοι αυτοί οι τρόποι παρουσιάζουν κάποιες αδυναμίες. Η Dial-up έχει πολύ χαμηλές ταχύτητες μεταφοράς δεδομένων ενώ την ώρα λειτουργίας της η τηλεφωνική γραμμή παραμένει κατειλημμένη. Η DSL προσφέρει υψηλές επιδόσεις άλλα το κόστος συντήρησης και κατασκευής της καλωδιακής υποδομής είναι επίσης υψηλό. Αυτό καθιστά δύσκολη την κάλυψη απομακρυσμένων περιοχών. Το Wi-Fi παρέχει αρκετά μεγάλους ρυθμούς μετάδοσης δεδομένων άλλα έχει περιορισμένη εμβέλεια. Τέλος το 3G υπόσχεται ταχύτητες που αδυνατεί να προσφέρει ενώ το κόστος του παραμένει σε υψηλά επίπεδα για τους χρήστες.

Στο σημείο αυτό έρχεται το IEEE 802.16 γνωστό ως WiMAX για να φέρει την επανάσταση στον τρόπο παροχής των διαδικτυακών υπηρεσιών. Το WiMAX μπορεί να καλύψει μια απόσταση 50 Km αν υπάρχει οπτική επαφή με ρυθμό διαμεταγωγής της τάξης των 72 Mbps, ενώ δίχως οπτική επαφή φτάνει τα 6 Km. Με το IEEE 802.16 δεν αναφερόμαστε πλέον σε τοπικά δίκτυα άλλα σε μητροπολιτικά δίκτυα (MAN). Αυτό σημαίνει ότι ολόκληρες πόλεις θα καλύπτονται από το ασύρματο δίκτυο επιτρέποντας πρόσβαση σε κάθε κάτοικο. Η κάλυψη όσο αφορά τις απομακρυσμένες περιοχές μπορεί να γίνει με την προσθήκη αναμεταδοτών και αυτό είναι πολύ πιο εύκολο και πιο οικονομικό σε σχέση με την επέκταση της καλωδιακής υποδομής. Από τη στιγμή που το WiMAX έχει πολλές δυνατότητες εκ των οποίων και η αξιόπιστη μετάδοση φωνής και εικόνας, είναι πιθανό να αντικαταστήσει ορισμένες από τις παλαιότερες τεχνολογίες. Για παράδειγμα οι δυνατότητες των φορητών

συσκευών έχουν αυξηθεί τόσο ώστε να μπορούν να υποστηρίξουν ακόμη και λειτουργικά συστήματα. Αυτό σημαίνει ότι σε ένα κινητό τηλέφωνο μπορεί να εγκατασταθεί μια εφαρμογή VoIP. Αν υποθέσουμε τώρα ότι το WiMAX έχει φτάσει σε σημείο ώστε να παρέχει πρόσβαση στο διαδίκτυο σε οποιαδήποτε περιοχή, τότε ο χρήστης της φορητής συσκευής θα μπορεί να καλεί οποιονδήποτε τηλεφωνικό αριθμό μέσω VoIP παρακάμπτοντας έτσι τις υπηρεσίες των εταιρειών κινητής τηλεφωνίας. Όλα δείχνουν πως το 802.16 είναι μια τεχνολογία που θα αλλάξει τα σημερινά δεδομένα στον τομέα των τηλεπικοινωνιών.

Επίπεδα του 802.16

Το 802.16 αναφέρεται στα επίπεδα PHY και MAC στα οποία κρύβεται η δύναμη του WiMAX. Το PHY επίπεδο είναι ευέλικτο και χρησιμοποιεί ένα πλήθος από μεθόδους κατανομής του ραδιοφάσματος και από τεχνικές διαμόρφωσης ώστε να ανταποκρίνεται εξίσου καλά σε κάθε περίπτωση. Οι μέθοδοι είναι οι OFDM, TDD, και FDD ενώ για την διαμόρφωση οι QPSK και QAM. Με την OFDM δίνεται η δυνατότητα μεταφοράς του σήματος σε μακρινές αποστάσεις, για το λόγο ότι αυτή η τεχνική είναι ιδιαίτερα ανθεκτική στο θόρυβο.

Δικτύωση

Στα WiMAX δίκτυα διακρίνονται δύο στοιχεία, ο σταθμός βάσης (BS) και ο σταθμός συνδρομητή (SS). Οι τοπολογίες διασύνδεσης μεταξύ αυτών είναι η PTP από ένα σημείο εκπομπής σε ένα σημείο λήψης και η PMP από ένα σημείο εκπομπής προς πολλαπλά σημεία λήψης.

1.3 BLUETOOTH

Ίσως είναι το δημοφιλέστερο πρωτόκολλο από τη στιγμή που πλέον συναντάται σε κάθε κινητό τηλέφωνο. Δημιουργήθηκε αρχικά από την Ericsson και στη συνέχεια κέρδισε το ενδιαφέρον άλλων εταιρειών μεταξύ των οποίων οι IBM, Intel, Nokia και Toshiba. Η Ericsson σε συνεργασία με τις εταιρείες αυτές ίδρυσε το SIG, που αποτελεί μια κίνηση για την βελτιστοποίηση του Bluetooth και την προώθησή του στην αγορά.

Το Bluetooth αποσκοπεί στη δημιουργία περιφερειακών συσκευών όπως εκτυπωτές, πληκτρολόγια, ποντίκια, ακουστικά κ.α. που θα επικοινωνούν χωρίς τη χρήση καλωδίων. Βέβαια προκύπτει η ανάγκη για τροφοδοσία από συστοιχίες μπαταριών ακόμα και σε συσκευές οι οποίες συνήθως δεν την χρειάζονται. Για παράδειγμα τα συνηθισμένα ακουστικά δεν έχουν ανάγκη για τροφοδοσία αφού το ζεύγος μεγαφώνων που διαθέτουν οδηγείται από την ισχύ του αναλογικού σήματος εισόδου. Αντίθετα στα ακουστικά Bluetooth

χρειαζόμαστε τροφοδοσία για το κύκλωμα του πομποδέκτη και για την βαθμίδα που ενισχύει το σήμα πληροφορίας και οδηγεί τα μεγάφωνα.

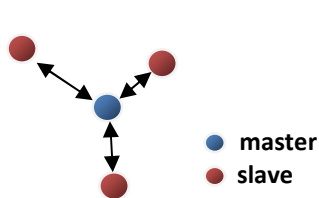
Το Bluetooth χωρίζεται στις ακόλουθες τάξεις ανάλογα με την ισχύ εκπομπής:

- Τάξη 1: Ισχύς εξόδου 100mW μέγιστη απόσταση άνω των 100m
- Τάξη 2: Ισχύς εξόδου 2.5mW μέγιστη απόσταση 10m
- Τάξη 3: Ισχύς εξόδου 1mW μέγιστη απόσταση 1m

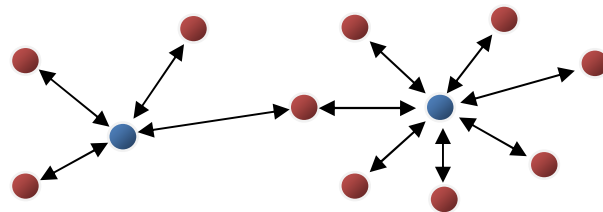
Στο σημείο αυτό θα πρέπει να τονίσουμε ότι οι αποστάσεις που έχουν αναφερθεί σχετικά με την ακτίνα κάλυψης κάθε πρωτοκόλλου είναι ενδεικτικές και μεταβάλλονται ανάλογα με το περιβάλλον στο οποίο πραγματοποιείται η ασύρματη μετάδοση, αφού εξαρτώνται και από εξωτερικούς παράγοντες όπως το θόρυβο, την απορρόφηση και τυχόν εμπόδια.

Δικτύωση

Για το σχηματισμό δικτύων στο Bluetooth έχουμε τη λογική master-slave όπου μια συσκευή ορίζεται ως master ενώ οι υπόλοιπες ως slaves. Όσες έχουν οριστεί σε slave δεν μπορούν να επικοινωνήσουν απευθείας μεταξύ τους, αλλά μόνο με το στοιχείο που είναι master, το οποίο βέβαια έχει τη δυνατότητα να επικοινωνεί με κάθε συσκευή του δικτύου του. Ένα δίκτυο τέτοιου τύπου ονομάζεται piconet και ο master μπορεί να υποστηρίξει μέχρι 7 συσκευές. Σε περίπτωση που κάποιο στοιχείο ανήκει σε ένα piconet ενώ συγχρόνως αποτελεί μέρος και άλλου piconet, τότε σχηματίζεται ένα ευρύτερο δίκτυο που λέγεται scatternet.



Σχήμα 1.5 Piconet



Σχήμα 1.6 Scatternet

1.4 ZIGBEE

Η τεχνολογία ZigBee είναι το κύριο θέμα αυτής της εργασίας και θα μας απασχολήσει σε όλη την υπόλοιπη έκτασή της. Όπως και το Bluetooth προορίζεται για ασύρματα προσωπικά δίκτυα. Οι συχνότητες λειτουργίας του είναι στα 868 MHz, 915 MHz και στην ISM ζώνη των 2.4 GHz. Αυτό που το κάνει ξεχωριστό είναι η εξαιρετικά χαμηλή κατανάλωση ισχύος η οποία και απαιτείται σε πολλές σύγχρονες εφαρμογές. Το ZigBee αναπτύχθηκε από την ZigBee Alliance που παρομοίως με την Wi-Fi Alliance και το SIG που αναφέραμε στις προηγούμενες ενότητες, αποτελεί επίσης μια συνεργασία μεταξύ εταιρειών παραγωγής ηλεκτρονικού εξοπλισμού και ημιαγωγών, για την προώθηση της τεχνολογίας αυτής. Η ZigBee Alliance ανέπτυξε τα ανώτερα επίπεδα του πρωτοκόλλου ενώ για τα PHY και MAC στηρίχθηκε πάνω

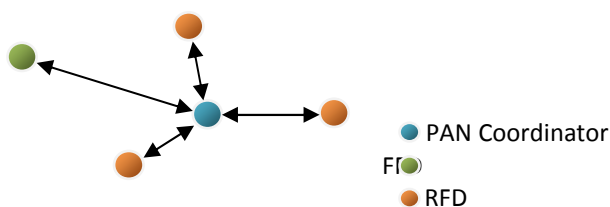
στο IEEE 802.15.4. Το πρωτόκολλο χαρακτηρίζεται ως WPAN-LR γιατί ο μέγιστος ρυθμός μετάδοσης δεδομένων που δύναται να επιτευχθεί είναι μόλις 250Kbps. Για τον ίδιο λόγο δεν προορίζεται για υψηλής ποιότητας μετάδοση φωνής ή εικόνας, άλλα ενδείκνυται περισσότερο για σήματα με χαμηλότερη ποσότητα πληροφορίας όπως για παράδειγμα οι μετρήσεις ενός αισθητηρίου.

Ανακεφαλαιώνοντας σε εφαρμογές όπου απαιτούνται ελάχιστη κατανάλωση ισχύος, ασύρματη διασύνδεση υπέρμετρου αριθμού συσκευών και χαμηλό κόστος κατασκευής, ενώ παράλληλα δεν υπάρχει ανάγκη για υψηλές ταχύτητες μετάδοσης, το ZigBee αποτελεί την τέλεια λύση.

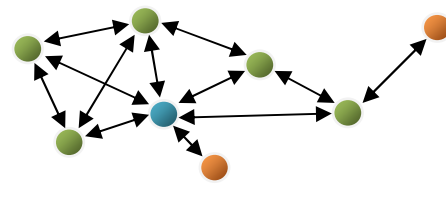
Δικτύωση

Οι συσκευές ZigBee διακρίνονται σε συσκευές με πλήρεις λειτουργίες FFD και σε συσκευές με περιορισμένες λειτουργίες RFD. Τα στοιχεία που έχουμε σε ένα ZigBee δίκτυο είναι ο κεντρικός διαχειριστής (PAN Coordinator), ο απλός διαχειριστής ή δρομολογητής (Router) και η τερματική συσκευή (End Device). Τα PAN Coordinator και Router θα πρέπει να είναι οπωσδήποτε FFD ενώ το End Device μπορεί να είναι οτιδήποτε (συνήθως RFD).

Οι τοπολογίες δικτύωσης είναι σε αστέρα και σε πλέγμα. Η τοπολογία αστέρα περιλαμβάνει ένα κεντρικό διαχειριστή και ένα πλήθος στοιχείων τα οποία μπορούν να επικοινωνούν αποκλειστικά μαζί του. Στην τοπολογία πλέγματος όλα τα FFD στοιχεία έχουν τη δυνατότητα να επικοινωνούν το ένα με το άλλο, ενώ τα RFD αλληλεπιδρούν μόνο με το κοντινότερο σε αυτά FFD.



Σχήμα 1.7 Τοπολογία Αστέρα



Σχήμα 1.8 Τοπολογία Πλέγματος

Στον παρακάτω πίνακα συγκεντρώνονται τα σημαντικότερα χαρακτηριστικά των τεσσάρων προτύπων που συζητήθηκαν στο κεφάλαιο αυτό.

Πρότυπο	Συχνότητα λειτουργίας (GHz)	Ρυθμός μετ. δεδομένων (Mbps)	Τυπική Εμβέλεια (m)	Κατανάλωση ισχύος	Τύπος δικτύου
Wi-Fi	2.4, 5	11 – 54	100	*υψηλή	WLAN
WiMAX	2-11, 10-66	έως 72	50000	*υψηλή	WMAN
Bluetooth	2.4	1-3	10	Χαμηλή	WPAN-MR
ZigBee	0.868, 0.915, 2.4	0.02, 0.04, 0.25	100	Πολύ χαμηλή	WPAN-LR

*Η κατανάλωση ισχύος θεωρείται υψηλή όσο αφορά τις **φορητές** συσκευές. Για παράδειγμα ας υποθέσουμε ένα κινητό τηλέφωνο με ενσωματωμένο Wi-Fi. Κατά τις περιόδους που το Wi-Fi θα είναι ενεργό, η διάρκεια ζωής της μπαταρίας του θα μειωθεί σημαντικά.

Κεφάλαιο 2^ο

ΠΡΩΤΟΚΟΛΛΟ ZIGBEE

2.1 Έννοιες του πρωτοκόλλου

Για την περιγραφή του πρωτοκόλλου είναι αναγκαίο να γίνει αναφορά σε κάποιες καινούριες έννοιες που επεξηγούνται στην ενότητα αυτή. Αυτό θα βοηθήσει και τους αναγνώστες που επιθυμούν να εμβαθύνουν διαβάζοντας το ZigBee Specification.

2.1.1 Services

Κάθε επίπεδο παρέχει μια σειρά από υπηρεσίες (Services) που εκτελούνται συνήθως για λογαριασμό του μόλις ανώτερου επιπέδου. Όλες οι υπηρεσίες πραγματοποιούνται από το Management Entity εκτός από την μεταφορά δεδομένων που γίνεται από το Data Entity. Ένα υψηλότερο επίπεδο αποκτά πρόσβαση στις υπηρεσίες του χαμηλότερου σε αυτό επιπέδου, με τη βοήθεια των Service Access Points (SAP). Για παράδειγμα αν θέλουμε να ενεργοποιήσουμε το πομποδέκτη μας, θα πρέπει το MAC επίπεδο να χρησιμοποιήσει μέσω του PD-SAP το PHY data service το οποίο θα επιτρέψει την αποστολή και λήψη των PDUs.

2.1.2 Primitives

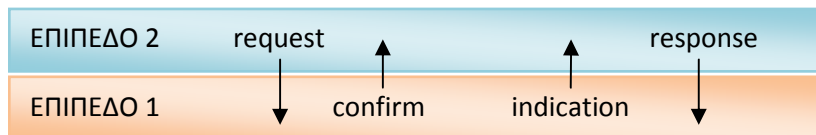
Κάθε Service αποτελείται από μια σειρά εντολών που ονομάζονται Primitives. Όλα τα primitive έχουν τις παρακάτω λειτουργίες ή ορισμένες από αυτές:

- Request
- Confirm
- Indication
- Response

Το όνομα του primitive υποδεικνύει συνήθως το επίπεδο στο οποίο ανήκει καθώς και τη χρήση του. Η σύνταξη ενός primitive που περιλαμβάνει κάποια λειτουργία γίνεται ως εξής, *όνομα_primitive . τύπος λειτουργίας*, π.χ. όταν το φυσικό επίπεδο ολοκληρώσει ένα CCA το αντίστοιχο primitive γράφεται *PLME-CCA.confirm* .

Στο σχήμα 2.1.1 φαίνεται η ακολουθία ανταλλαγής πληροφοριών μεταξύ δυο επιπέδων μέσω ενός primitive. Θεωρούμε τα επίπεδα 1 και 2 όπου το 2 είναι υψηλότερο από το 1. Όταν το επίπεδο 2 θέλει να κάνει χρήση μιας υπηρεσίας απαιτείται πρώτα να κάνει request (αίτηση) στο επίπεδο 1. Στη συνέχεια θα πρέπει το επίπεδο 1 να πληροφορήσει το 2 αν η υπηρεσία ολοκληρώθηκε με επιτυχία ή όχι με το confirm δηλαδή την επιβεβαίωση. Το indication (ένδειξη) χρησιμοποιείται από

το επίπεδο 1 όταν θέλει να αναφέρει ένα συμβάν στο 2. Αν στο indication ζητείται απάντηση τότε το επίπεδο 2 θα πρέπει να στείλει response (απόκριση) στο 1.



Σχήμα 2.1 Εκτέλεση των primitives

2.1.3 Constants & Attributes

Τα constants (σταθερές) εκφράζουν κάποιες καθορισμένες τιμές όπως το μέγεθος ενός πακέτου. Στα επίπεδα PHY και MAC τα constants παίρνουν το πρόθεμα **-a-** ενώ για τα επίπεδα εφαρμογής και δικτύου τα **-apsc-** και **-nwkc-** αντίστοιχα.

Τα attributes (χαρακτηριστικά) είναι μεταβλητές και μπορούν να αλλάξουν εν ώρα λειτουργίας. Κάθε επίπεδο έχει attributes στην PIB την βάση δεδομένων του. Κάποια από τα attributes είναι μόνο για ανάγνωση που σημαίνει ότι μπορούν προσπελαστούν από κάθε επίπεδο αλλά η τιμή τους μπορεί να μεταβληθεί μόνο από εκείνο στο οποίο ανήκουν.

2.1.4 Binding

Οι συσκευές που συσχετίζονται μεταξύ τους λέμε ότι είναι λογικά συνδεδεμένες και ως Binding ορίζεται η διαδικασία δημιουργίας αυτών των «λογικών» διασυνδέσεων. Για παράδειγμα σε ένα ασύρματο σύστημα συναγερμού η μονάδα ZigBee του αισθητηρίου κίνησης είναι λογικά συνδεδεμένη με την μονάδα ZigBee του κεντρικού πίνακα του συναγερμού. Οι πληροφορίες σχετικά με τις λογικές διασυνδέσεις αποθηκεύονται σε έναν πίνακα ο οποίος ονομάζεται Binding table και δημιουργείται στο επίπεδο εφαρμογής. Οι λογικά συνδεδεμένες συσκευές λέγονται Bound devices.

2.1.5 Energy Detection (ED)

Το ED είναι ένας μηχανισμός ο οποίος κάνει μια εκτίμηση όσο αφορά τα επίπεδα ενέργειας των σημάτων που μπορεί να υπάρχουν σε ένα συγκεκριμένο κανάλι. Ωστόσο αν εντοπίσει κάποιο σήμα δεν δύναται να ξεχωρίσει για τι είδος πρόκειται.

2.1.6 Carrier Sense (CS)

Το CS αποτελεί επίσης μια μέθοδος για την ανίχνευση σήματος σε ένα ράδιο-κανάλι. Η διαφορά του με το ED είναι ότι αν εντοπίσει κάποιο σήμα το αποδιαμορφώνει και ελέγχει τι τύπου είναι.

2.1.7 Link Quality Indicator (LQI)

Το LQI είναι η ένδειξη της ποιότητας του λαμβανόμενου σήματος. Οι παράγοντες που καθορίζουν την ποιότητα είναι ο SNR και το RSS. Ο SNR είναι ο λόγος σήματος προς θόρυβο. Όταν έχει μεγάλη τιμή, το ωφέλιμο σήμα επηρεάζεται δύσκολα από το σήμα θορύβου και επομένως έχουμε λιγότερες πιθανότητες σφάλματος. Όσο μεγαλύτερο είναι το SNR τόσο καλύτερη θεωρείται και η ποιότητα σήματος. Ως RSS ορίζεται η συνολική ισχύς του ληφθέντος σήματος.

2.1.8 Clear Channel Assessment (CCA)

Στο 802.15.4 χρησιμοποιείται η τεχνική CSMA-CA. Για την αποφυγή συγκρούσεων μεταξύ των πακέτων εφαρμόζει το CCA, έναν έλεγχο για να διαπιστωθεί η διαθεσιμότητα του καναλιού. Το CCA κάνει χρήση των ED και CS για να καθορίσει αν το κανάλι είναι ελεύθερο και έχει τις εξής καταστάσεις λειτουργίας:

- **Κατάσταση 1** Γίνεται χρήση μόνο του ED και μόλις το επίπεδο ενέργειας που ανιχνεύεται πέσει κάτω από την τιμή κατώφλιου που έχει οριστεί από τον κατασκευαστή τότε το κανάλι θεωρείται ελεύθερο.
- **Κατάσταση 2** Γίνεται χρήση μόνο του CS και το κανάλι θεωρείται κατειλημμένο μόνο αν το επίπεδο ενέργειας που ανιχνεύεται προέρχεται από σήμα ίδιου τύπου με εκείνο του πομπού που κάνει τον έλεγχο.
- **Κατάσταση 3** Χρησιμοποιούνται οι παρακάτω συνδυασμοί των ED και CS με τις λογικές πράξεις **ΚΑΙ** και **Η΄**.
 - Αν το επίπεδο ενέργειας είναι υψηλότερο από το κατώφλι **ΚΑΙ** αν το σήμα είναι ίδιου τύπου με εκείνο του πομπού το κανάλι θεωρείται κατειλημμένο.
 - Αν το επίπεδο ενέργειας είναι υψηλότερο από το κατώφλι **Η΄** αν το σήμα είναι ίδιου τύπου με εκείνο του πομπού το κανάλι θεωρείται κατειλημμένο.

2.1.9 Beacon

Το Beacon είναι ένα σήμα που αποστέλλεται από τον PAN coordinator για να συγχρονίσει όλες τις συσκευές που ανήκουν στο δίκτυο και να μπορέσει να παραχωρήσει ένα GTS. Το GTS δίνεται σε μια συσκευή για να αποκτήσει πρόσβαση στο κανάλι χωρίς τη χρήση του CSMA-CA.

2.1.10 Superframe

Όταν γίνεται χρήση Beacon σε ένα δίκτυο η πρόσβαση στο κανάλι γίνεται μέσω των superframes. Κάθε superframe περικλείεται από δύο Beacons και αποτελείται από τρεις περιόδους. Την περίοδο CAP, την CFP και την ανενεργή περίοδο. Κατά τη διάρκεια της CAP η συσκευή που θέλει να εκπέμψει δεν μπορεί να χρησιμοποιήσει ένα κανάλι μόλις το χρειαστεί, γιατί ο μόνος τρόπος για να αποκτήσει πρόσβαση σε αυτό είναι μέσω του μηχανισμού CSMA-CA. Κατά την CFP δεν γίνεται χρήση του CSMA-CA, αλλά δίνεται ένα GTS σε μια συσκευή για να ξεκινήσει τη μετάδοσή της. Αυτός ο τρόπος είναι πολύ χρήσιμος σε εφαρμογές όπου ο χρόνος είναι κρίσιμος και μια συσκευή δεν μπορεί να περιμένει να ελευθερωθεί ένα κανάλι για να μπορέσει να κάνει εκπομπή. Τα CAP και CFP μαζί αποτελούν την ενεργή περίοδο. Στην διάρκεια της ανενεργούς περιόδου η συσκευή μπαίνει σε κατάσταση χαμηλής κατανάλωσης ισχύος για εξοικονόμηση ενέργειας.

2.1.11 Route Discovery

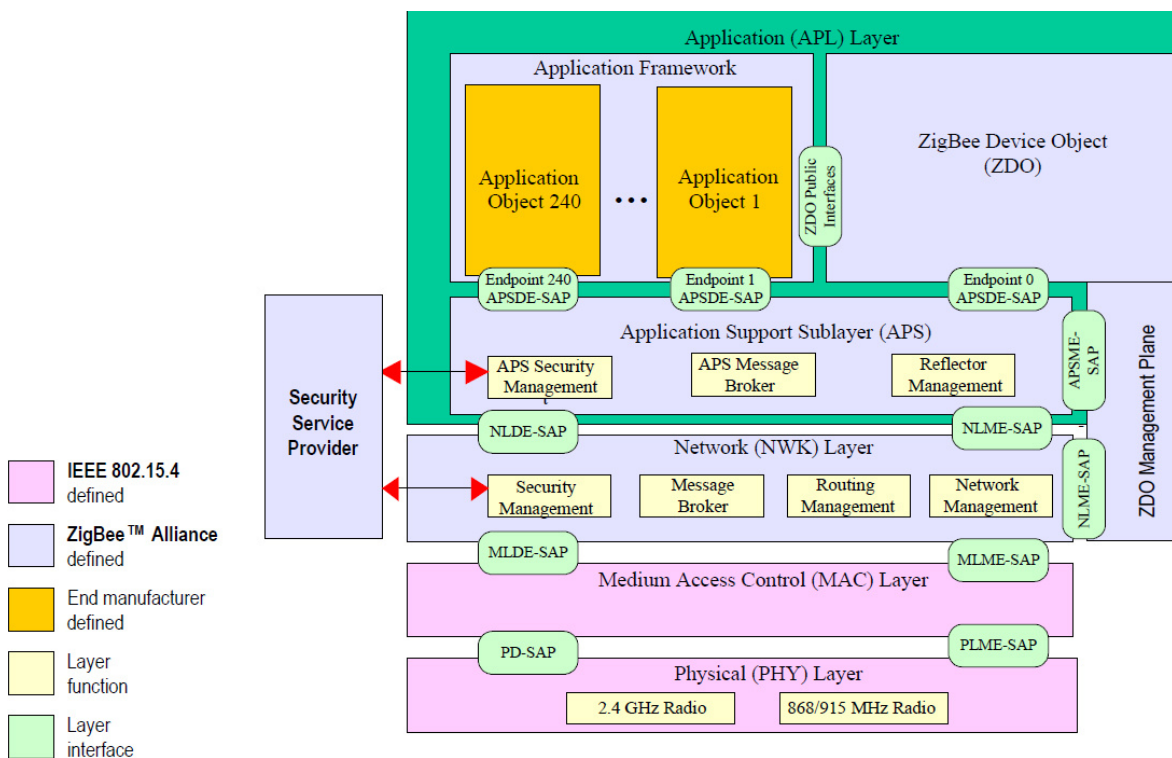
Σε ένα ZigBee δίκτυο οι συσκευές συνεργάζονται για να βρουν τις πιο σύντομες διαδρομές (routes) που μπορούν να εξασφαλίσουν την μεταξύ τους επικοινωνία. Αυτή η μέθοδος είναι το Route Discovery.

2.1.12 Device Discovery

Το Device Discovery είναι η διαδικασία κατά την οποία μια ZigBee συσκευή ανιχνεύει άλλες ZigBee συσκευές στο δίκτυο της.

2.2 Τα επίπεδα του ZigBee

Το ZigBee πρότυπο ακολουθεί τη διαστρωμάτωση κατά OSI άλλα εν αντιθέσει με τα εφτά επίπεδα που προβλέπονται, έχει μόνο τέσσερα. Τα δύο πρώτα επίπεδα PHY και MAC δημιουργήθηκαν από την IEEE και αποτελούν όπως είδαμε το 802.15.4. Η ZigBee Alliance στηριζόμενη πάνω σε αυτό το πρωτόκολλο πρόσθεσε άλλα δύο επίπεδα, τα δικτύου (NWK) και εφαρμογής (APL). Το σχήμα 2.2 δείχνει σε λεπτομέρεια τα επίπεδα και τα υπό-επίπεδα τα οποία και αναλύονται στη συνέχεια της ενότητας αυτής.



Σχήμα 2.2 Τα επίπεδα του ZigBee. Πηγή «TSC-ZigBee-Specification»

2.2.1 Physical Layer

Το επίπεδο PHY είναι εκείνο που συσχετίζεται άμεσα με το κανάλι μετάδοσης και κάνει εφικτή την αποστολή και λήψη των πακέτων που δημιουργήθηκαν στα ανώτερα επίπεδα. Οι αρμοδιότητές του είναι οι ακόλουθες:

- Ενεργοποίηση και απενεργοποίηση του πομποδέκτη
- Εκτέλεση του ED

- Πραγματοποίηση του LQI
- Εκτέλεση του CCA
- Επιλογή της ακριβούς συχνότητας του καναλιού
- Αποστολή και λήψη δεδομένων

Είναι χωρισμένο σε δύο πομποδέκτες, ο ένας στη συχνότητα λειτουργίας των 2.4 GHz και ο άλλος στα 868/915 MHz. Ένα σύνολο 27 καναλιών αριθμημένα από το 0 έως το 26 είναι διαθέσιμα για τις τρεις αυτές συχνότητες. Ένα κανάλι αντιστοιχεί στα 868MHz, 10 κανάλια στα 915 MHz και 16 στα 2.4 GHz. Θεωρώντας ως k τον αριθμό των καναλιών υπολογίζονται οι κεντρικές τους συχνότητες και είναι $F_c = 868.3$ MHz για $k = 0$, $F_c = 906 + 2(k - 1)$ MHz για $k = 1, 2, \dots, 10$ και $F_c = 2405 + 5(k - 11)$ MHz για $k = 11, 12, \dots, 26$.

2.2.1.1 PHY Services

Στο PHY έχουμε τις υπηρεσίες δεδομένων και τις υπηρεσίες διαχείρισης. Η πρόσβαση σε αυτές γίνεται με τα PD-SAP και PLME-SAP αντίστοιχα. Η υπηρεσία δεδομένων περιλαμβάνει ένα Primitive, το PD-Data. Το PD-Data.request καλείται από το MAC για να ζητήσει την αποστολή ενός MPDU. Το PHY ενεργοποιεί τον πομπό και στη συνέχεια δημιουργεί ένα PSDU και το στέλνει. Μόλις ολοκληρωθεί η αποστολή, το PHY στέλνει το PD-Data.confirm στο MAC για να αναφέρει ότι η αποστολή ήταν επιτυχής. Αν το PD-Data.request σταλεί την ώρα που ο πομποδέκτης είναι ήδη απασχολημένος, θα επιστραφεί ένα PD-Data.confirm το οποίο θα περιγράφει την κατάσταση του πομποδέκτη, ουσιαστικά τον λόγο για το οποίο δεν γίνεται να εκτελεσθεί το request. Το PD-Data.indication παράγεται όταν γίνεται μεταφορά πακέτων από το PHY στο MAC.

Η υπηρεσία διαχείρισης αποτελείται από τα παρακάτω primitives:

- **PLME-CCA** Το PLME-CCA.request εμφανίζεται όταν ο CSMA-CA αλγόριθμος απαιτεί από το PLME την πραγματοποίηση ενός CCA. Μετά την ολοκλήρωση του CCA επιστρέφεται το PLME-CCA.confirm το οποίο μπορεί να έχει μια από τις τιμές «BUSY» (κανάλι κατειλημμένο) ή «IDLE» (κανάλι ελεύθερο) ανάλογα με την κατάσταση του καναλιού. Αν ο πομποδέκτης είναι απενεργοποιημένος τότε η τιμή του PLME-CCA.confirm θα είναι «TRX_OFF» ενώ αν βρίσκεται ήδη σε λειτουργία θα είναι «TX_ON». Στις δύο τελευταίες περιπτώσεις έχουμε αποτυχία εκτέλεσης του CCA.
- **PLME-ED** Το ED ζητείται με το PLME-ED.request. Με την αποπεράτωση των μετρήσεων παράγεται το PLME-ED.confirm με την τιμή «SUCCESS» και μια ένδειξη για το ενεργειακό επίπεδο που ανιχνευτικό, η οποία κυμαίνεται μεταξύ 0x00 και 0xff. Το PLME-ED.confirm φέρει ένα μήνυμα σφάλματος με

την τιμή «TRX_OFF» όταν ο πομποδέκτης είναι ανενεργός ή την «TX_ON» όταν ο πομπός είναι απασχολημένος.

- **PLME-GET** Το PLME_GET.request χρησιμοποιείται όταν το MAC «θέλει» να αντλήσει πληροφορίες από κάποιο attribute που βρίσκετε στην PIB του PHY. Αν το attribute που αναζητείται στη βάση δεδομένων βρεθεί τότε στέλνεται το PLME-GET.confirm με την τιμή «SUCCESS», ενώ αν δεν βρεθεί επιστρέφει την τιμή UNSUPPORTED_ATTRIBUTE.
- **PLME-SET-TRX-STATE** Αν χρειαστεί να αλλάξει κατάσταση ο πομποδέκτης, στέλνεται το PLME-SET-TRX-STATE.request . Οι καταστάσεις στις οποίες μπορεί να βρεθεί είναι οι παρακάτω:
 - πομποδέκτης απενεργοποιημένος (TRX_OFF)
 - πομπός ενεργός (TX_ON)
 - δέκτης ενεργός (RX_ON)

Αν ο πομποδέκτης δύναται να τεθεί στην ζητούμενη κατάσταση τότε επιστρέφεται το PLME-SET-TRX-STATE.confirm στην τιμή «SUCCESS». Σε περίπτωση που ο πομπός βρίσκεται σε λειτουργία και την ίδια στιγμή φτάσει μια αίτηση για αλλαγή κατάστασης σε TRX_OFF ή σε RX_ON τότε αγνοείτε και επιστρέφεται η τιμή «BUSY_TX». Παρομοίως όταν ο δέκτης είναι απασχολημένος δεν δέχεται τις αιτήσεις για TRX_OFF ή TX_ON και στέλνει το PLME-SET-TRX-STATE.confirm με την τιμή «BUSY_RX».

- **PLME-SET** Το PLME-SET.request χρησιμοποιείται για να αλλαχθεί η τιμή ενός συγκεκριμένου attribute από την PIB του PHY. Όταν βρεθεί το ζητούμενο attribute και η τιμή του μεταβληθεί επιτυχώς τότε στέλνεται το PLME-SET.confirm σε κατάσταση «SUCCESS». Η νέα τιμή που δίδεται θα πρέπει να βρίσκεται σε ένα πεδίο τιμών που να θεωρείτε έγκυρο για το υπό επεξεργασία attribute, διαφορετικά το αποτέλεσμα του PLME-SET.confirm θα είναι το INVALID_PARAMETER. Αν το attribute δεν βρεθεί επιστρέφεται σε τιμή UNSUPPORTED_ATTRIBUTE.

2.2.1.2 PPDU

Η Δομή ενός πακέτου όπως διαμορφώνεται στο φυσικό επίπεδο φαίνεται στο σχήμα 2.3 . Κάθε PPDU αποτελείται από τρία μέρη, την επικεφαλίδα συγχρονισμού SHR, την επικεφαλίδα φυσικού επιπέδου PHR και το ωφέλιμο φορτίο Payload. Το SHR χωρίζεται στο «Preamble» που χρησιμοποιείται για τον συγχρονισμό των πομποδεκτών και στο «SFD» που δηλώνει το τέλος του πεδίου συγχρονισμού και την αρχή του πακέτου δεδομένων. Το PHR προσδιορίζει το

μέγεθος του πακέτου. Τέλος το Payload είναι το PSDU το οποίο αποτελείται από τα πακέτα που προστέθηκαν από κάθε επίπεδο.

SHR		PHR		PHY PAYLOAD
Preamble	SFD	Frame length	Reserved	

Σχήμα 2.3 PPDU

2.2.2 MAC Layer

Το MAC εξασφαλίζει την διασύνδεση των ανώτερων επιπέδων με το φυσικό. Είναι το επίπεδο που ελέγχει άμεσα το PHY. Οι αρμοδιότητές του είναι:

- Παραγωγή των beacons
- Συγχρονισμός των συσκευών στο εισερχόμενο beacon
- Να επιτρέπει την σύνδεση και την αποσύνδεση μεταξύ των συσκευών στα ZigBee δίκτυα
- Να υποστηρίζει τις παραμέτρους ασφαλείας του πρωτοκόλλου
- Να χρησιμοποιεί τη CSMA-CA για να επιτρέψει την πρόσβαση στο κανάλι
- Παραχώρηση των GTS

2.2.2.1 MAC Services

Το MAC όπως και το PHY περιλαμβάνει την υπηρεσία δεδομένων και την υπηρεσία διαχείρισης. Η πρόσβαση σε αυτές γίνεται με το MCPS-SAP και το MLME-SAP αντίστοιχα. Το MAC data service έχει τα παρακάτω δύο primitives.

- **MCPS-DATA** Το MCPS-DATA.request ζητάει από το MAC να στείλει ένα MSDU. Αν η εντολή ολοκληρωθεί με επιτυχία παράγεται το MCPS-DATA.confirm σε κατάσταση «SUCCESS». Σε περίπτωση σφάλματος, το MCPS-DATA.confirm ορίζεται σε μια από τις εξής καταστάσεις:
 - **INVALID_GTS** όταν η αποστολή γίνεται με χρήση GTS και δεν βρεθεί κάποιο έγκυρο timeslot.
 - **TRANSACTION_OVERFLOW** προκύπτει αν η χωρητικότητα της λίστας αναμονής, στην οποία κρατούνται οι μεταβάσεις πριν εκτελεστούν, είναι πλήρης.

- **TRANSACTION_EXPIRED** εμφανίζεται όταν η μετάβαση αποθηκευθεί στη λίστα αναμονής και ξεπεράσει το χρονικό όριο παραμονής της σε αυτή.
 - **UNAVAILABLE_KEY** όταν ζητηθεί να προστεθεί ασφάλεια στο πακέτο άλλα δεν υπάρχει κανένας έγκυρος κωδικός στη MAC PIB.
 - **FRAME_TOO_LONG** επιστρέφεται από τη στιγμή που το μέγεθος του πακέτου είναι τόσο μεγάλο ώστε να υπερβαίνει την τιμή που ορίζεται από τη σταθερά aMaxMACFrameSize.
 - **FAILED_SECURITY_CHECK** σε περίπτωση που προκύψει οποιοδήποτε άλλο σφάλμα σχετικά με τις παραμέτρους ασφαλείας.
 - **CHANNEL_ACCESS_FAILURE** όταν χρησιμοποιείται η CSMA-CA και δεν επιτευχθεί πρόσβαση στο κανάλι.
 - **NO_ACK** όταν δεν σταλεί σήμα επιβεβαίωσης.
- **MCPS-PURGE** Το MCPS-PURGE.request χρησιμοποιείται για να αφαιρεθεί κάποιο MSDU από τις μεταβάσεις που βρίσκονται σε αναμονή. Αν το MSDU αφαιρεθεί επιστρέφεται το MCPS-PURGE.confirm σε κατάσταση «SUCCESS», διαφορετικά τίθεται σε «INVALID_HANDLE».

Τα Primitives της υπηρεσίας διαχείρισης είναι τα ακόλουθα:

- **MLME-ASSOCIATE** Το MLME-ASSOCIATE.request παράγεται με σκοπό η εν λόγω συσκευή να συνδεθεί με τον Coordinator του ZigBee δικτύου. Μόλις η διαδικασία ολοκληρωθεί επιτυχώς δημιουργείται το MLME-ASSOCIATE.confirm σε κατάσταση «SUCCESS». Αν προκύψει σφάλμα και η σύνδεση δεν είναι εφικτή το MLME-ASSOCIATE.confirm τίθεται στις καταστάσεις:
 - **UNAVAILABLE_KEY** όταν ζητηθεί να προστεθεί ασφάλεια στο πακέτο άλλα δεν υπάρχει κανένας έγκυρος κωδικός στη MAC PIB.
 - **FAILED_SECURITY_CHECK** σε περίπτωση που προκύψει οποιοδήποτε άλλο σφάλμα σχετικά με τις παραμέτρους ασφαλείας.
 - **CHANNEL_ACCESS_FAILURE** όταν χρησιμοποιείται η CSMA-CA και δεν επιτευχθεί πρόσβαση στο κανάλι.
 - **NO_ACK** όταν δεν σταλεί σήμα επιβεβαίωσης.
 - **NO_DATA** όταν η συσκευή που ζητά να συνδεθεί δεν λάβει απόκριση από τον Coordinator.
 - **INVALID_PARAMETER** αν οποιαδήποτε παράμετρος του MLME-ASSOCIATE.request δεν είναι έγκυρη ή βρίσκεται εκτός του πεδίου τιμών που έχει οριστεί.

Το MLME-ASSOCIATE.indication παράγεται από το MLME του Coordinator και στέλνεται στο NWK layer δείχνοντας ότι έχει ληφθεί μια αίτηση σύνδεσης. Όταν ο Coordinator αποφασίσει για το αν θα επιτρέψει τη σύνδεση στη συσκευή ZigBee (που έκανε την αίτηση) στέλνει το MLME-ASSOCIATE.response με την ανάλογη απόφαση.

- **MLME-DISASSOCIATE** Με το MLME-DISASSOCIATE.request μια συσκευή μπορεί να αποσυνδεθεί από ένα PAN στο οποίο ανήκει ή να την αποσυνδέσει ο Coordinator που διαχειρίζεται το PAN αυτό. Όταν πετύχει η αποσύνδεση στέλνεται το MLME-DISASSOCIATE.confirm σε «SUCCESS», αλλιώς παίρνει τις καταστάσεις:
 - **TRANSACTION_OVERFLOW** προκύπτει αν η χωρητικότητα της λίστας αναμονής, στην οποία κρατούνται οι μεταβάσεις πριν εκτελεστούν, είναι πλήρης.
 - **TRANSACTION_EXPIRED** εμφανίζεται όταν η μετάβαση αποθηκευθεί στη λίστα αναμονής και ξεπεράσει το χρονικό όριο παραμονής της σε αυτή.
 - **UNAVAILABLE_KEY** όταν ζητηθεί να προστεθεί ασφάλεια στο πακέτο αλλά δεν υπάρχει κανένας έγκυρος κωδικός στη MAC PIB.
 - **FAILED_SECURITY_CHECK** σε περίπτωση που προκύψει οποιοδήποτε άλλο σφάλμα σχετικά με τις παραμέτρους ασφαλείας.
 - **CHANNEL_ACCESS_FAILURE** όταν χρησιμοποιείται η CSMA-CA και δεν επιτευχθεί πρόσβαση στο κανάλι.
 - **NO_ACK** όταν δεν σταλεί σήμα επιβεβαίωσης.
 - **INVALID_PARAMETER** αν οποιαδήποτε παράμετρος δεν είναι έγκυρη ή βρίσκεται εκτός του πεδίου τιμών που έχει οριστεί.

Το MLME-DISASSOCIATE.indication χρησιμοποιείται για να δείξει ότι έχει ληφθεί μια εντολή αποσύνδεσης.

- **MLME-BEACON-NOTIFY** Το MLME-BEACON-NOTIFY.indication μεταφέρει στο NWK κάποιες παραμέτρους που βρίσκονται σε ένα Beacon που παραλήφθηκε από το MAC.
- **MLME-GET** Λειτουργεί όπως το PLME_GET με τη διαφορά ότι επεξεργάζεται τα στοιχεία της MAC PIB.
- **MLME-GTS** Το MLME-GTS.request παράγεται για να ζητήσει να διανεμηθεί ένα νέο GTS ή για να αφαιρεθεί ένα υπάρχον αφιερωμένο timeslot. Το MLME-GTS.confirm σε κατάσταση «SUCCESS» δείχνει ότι η αίτηση έγινε δεκτή, διαφορετικά επιστρέφει σε μια από τις εξής καταστάσεις:

- **UNAVAILABLE_KEY** όταν δεν υπάρχει κανένας έγκυρος κωδικός στη MAC PIB.
- **NO_SHORT_ADDRESS** όταν το macShortAddress ισούται με 0xffff ή 0xffff.
- **FAILED_SECURITY_CHECK** σε περίπτωση που προκύψει οποιοδήποτε άλλο σφάλμα σχετικά με τις παραμέτρους ασφαλείας.
- **CHANNEL_ACCESS_FAILURE** όταν χρησιμοποιείται η CSMA-CA και δεν επιτευχθεί πρόσβαση στο κανάλι.
- **NO_ACK** όταν δεν σταλεί σήμα επιβεβαίωσης.
- **INVALID_PARAMETER** αν οποιαδήποτε παράμετρος του MLME-GTS.request δεν είναι έγκυρη ή βρίσκεται εκτός του πεδίου τιμών που έχει οριστεί.

Το MLME-GTS.indication δείχνει ότι έγινε η διανομή ενός νέου GTS ή ότι αφαιρέθηκε ένα από τα GTS που ήδη υπήρχαν.

- **MLME-ORPHAN** Το MLME-ORPHAN.indication παράγεται από το MLME ενός Coordinator και υποδεικνύει (στο NWK) την ύπαρξη μιας συσκευής που άνηκε παλαιότερα στο δίκτυο που διαχειρίζεται ο Coordinator αυτός. Μια τέτοια συσκευή χαρακτηρίζεται ως «ορφανή».
- **MLME-RESET** Το MLME-RESET.request δημιουργείται από το NWK για να επαναφέρει το MAC στις αρχικές του ρυθμίσεις, κάνοντας reset σε όλα τα attributes που βρίσκονται στην MAC PIB. Αν το reset ολοκληρωθεί με επιτυχία το MLME-RESET.confirm τίθεται σε «SUCCESS», διαφορετικά η κατάστασή του γίνεται DISABLE_TRX_FAILURE.
- **MLME-RX-ENABLE** Το MLME-RX-ENABLE.request θέτει τον δέκτη σε λειτουργία για ένα ορισμένο χρονικό διάστημα. Το MLME-RX-ENABLE.confirm παράγεται και αφού ο δέκτης τεθεί σε λειτουργία ορίζεται σε «SUCCESS». Αν δεν ενεργοποιηθεί ο δέκτης οι δυνατές καταστάσεις είναι η «TX_ACTIVE» όταν ο πομπός είναι ενεργός και η «INVALID_PARAMETER» για οποιοδήποτε άλλο σφάλμα.
- **MLME-SCAN** Το MLME-SCAN.request χρησιμοποιείται για σάρωση του καναλιού πραγματοποιώντας ένα ED για να καθοριστεί ο βαθμός χρήσης του καναλιού ή εντοπίζοντας πληροφορίες σχετικά με το δίκτυο προέλευσής τους. Το MLME-SCAN.confirm θα είναι σε κατάσταση «SUCCESS» όταν η σάρωση ολοκληρωθεί με επιτυχία, διαφορετικά αν δεν εντοπίσει κανένα beacon τίθεται σε «NO_BEACON».
- **MLME-COMM-STATUS** Το MLME-COMM-STATUS.indication παράγεται για να ενημερώσει το NWK για την κατάσταση κάποιας μετάδοσης που βρίσκεται σε εξέλιξη ή για να πληροφορήσει το NWK για κάποιο σφάλμα που προέκυψε κατά τον έλεγχο των παραμέτρων ασφαλείας ενός εισερχόμενου πακέτου.

- **MLME-SET** Λειτουργεί όπως το PLME-SET με τη διαφορά ότι επεξεργάζεται τα στοιχεία της MAC PIB.
- **MLME-SYNC** Το MLME-SYNC.request ζητά τον συγχρονισμό με τον Coordinator και την ανίχνευση των beacons που εκπέμπει.
- **MLME-SYNC-LOSS** MLME-SYNC-LOSS.indication επισημαίνει ότι χάθηκε ο συγχρονισμός μιας συσκευής ZigBee με τον Coordinator του PAN στο οποίο ανήκει.
- **MLME-POLL** Το MLME-POLL.request παροτρύνει τη ZigBee συσκευή να ζητήσει δεδομένα από τον Coordinator. Όταν παραληφθεί ένα πακέτο με δεδομένα από τον Coordinator το MLME-POLL.confirm λαμβάνει την τιμή «SUCCESS» ενώ σε περίπτωση σφάλματος μια από τις παρακάτω καταστάσεις:
 - **UNAVAILABLE_KEY** όταν ζητηθεί να προστεθεί ασφάλεια στο πακέτο άλλα δεν υπάρχει κανένας έγκυρος κωδικός στη MAC PIB.
 - **FAILED_SECURITY_CHECK** σε περίπτωση που προκύψει οποιοδήποτε σφάλμα σχετικά με τις παραμέτρους ασφαλείας.
 - **CHANNEL_ACCESS_FAILURE** όταν χρησιμοποιείται η CSMA-CA και δεν επιτευχθεί πρόσβαση στο κανάλι.
 - **NO_ACK** όταν δεν σταλεί σήμα επιβεβαίωσης.
 - **NO_DATA** όταν παραληφθεί ένα πακέτο από τον Coordinator με μηδενικό μήκος.
 - **INVALID_PARAMETER** αν οποιαδήποτε παράμετρος του MLME-POLL.request δεν είναι έγκυρη ή βρίσκεται εκτός του πεδίου τιμών που έχει οριστεί.

2.2.2.2 MPDU

Το πακέτο του MAC το MPDU αποτελείται από την επικεφαλίδα MHR , το ωφέλιμο φορτίο MAC PAYLOAD και το πλαίσιο τέλους MFR. Το MHR περιλαμβάνει τη σηματοδότηση για τον έλεγχο του πακέτου, τις πληροφορίες αναγνώρισης και τα στοιχεία διευθυνσιοδότησης αποστολέα και παραλήπτη. Το MFR περιέχει το FCS, μια ακολουθία 16 bit για τον έλεγχο λαθών.

MHR						MAC PAYLOAD	MFR
Frame Control	Sequence number	Destination PAN Identifier	Destination Address	Source PAN Identifier	Source Address	Frame Payload	FCS

Σχήμα 2.4 MPDU

2.2.3 Network Layer

Το επίπεδο δικτύου εξασφαλίζει τη λειτουργικότητα του 802.15.4 ελέγχοντας το επίπεδο MAC με τη βοήθεια των primitives που είδαμε στην προηγούμενη ενότητα. Το NWK μεσολαβεί για την επικοινωνία του APL με τα χαμηλότερα επίπεδα. Αυτό γίνεται με το NLDE-SAP που επιτρέπει στο APL πρόσβαση στις υπηρεσίες δεδομένων του και με το NLME-SAP που δίνει πρόσβαση στις υπηρεσίες διαχείρισης. Το NWK διατηρεί επίσης μια βάση δεδομένων, την NIB. Οι αρμοδιότητες του είναι:

- Να καθορίζει το ρόλο μιας νέας συσκευής.
- Να δημιουργεί ένα νέο δίκτυο.
- Να επιτρέπει τη σύνδεση ή την αποχώρηση από ένα υπάρχον δίκτυο.
- Αν πρόκειται για το NWK ενός Coordinator, να ορίζει τις διευθύνσεις κάθε συσκευής που εισέρχεται στο δίκτυο του.
- Να ανακαλύπτει τις γειτονικές συσκευές δηλαδή εκείνες με τις οποίες μπορεί να επικοινωνήσει με μια μόνο μετάβαση.
- Να ανακαλύπτει και να συντηρεί τις πιο σύντομες διαδρομές (Routes) για να έρθει σε επαφή με άλλες συσκευές.
- Να αλλάζει το μηχανισμό δρομολόγησης των δεδομένων.

2.2.2.1 NWK Services

Η υπηρεσία δεδομένων του NWK έχει ένα μόνο primitive, το NLDE-DATA. Το NLDE-DATA.request ζητά την αποστολή ενός NSDU. Όταν η αποστολή ολοκληρωθεί με επιτυχία το NLDE-DATA.confirm τίθεται σε «SUCCESS», ενώ σε αντίθετη περίπτωση μπαίνει σε κατάσταση σφάλματος. Το NLDE-DATA.indication δείχνει τη μεταφορά ενός PDU από το NWK στο MAC. Για το NLME, την υπηρεσία διαχείρισης, τα primitives είναι τα ακόλουθα:

- **NLME-NETWORK-DISCOVERY** Το NLME-NETWORK-DISCOVERY.request χρησιμοποιείται για την εύρεση εν ενεργεία δικτύων στην περιοχή λειτουργίας (POS) της συσκευής. Επιστρέφεται το NLME-NETWORK-DISCOVERY.confirm φέροντας πληροφορίες για τα δίκτυα που βρέθηκαν μέσω της κατάστασης στην οποία έχει τεθεί. Η κατάσταση αυτή είναι πάντα ίδια με εκείνη του NLME-SCAN.confirm .
- **NLME-NETWORK-FORMATION** Το NLME-NETWORK-FORMATION.request παράγεται όταν επιθυμούμαι η εν λόγω συσκευή να δημιουργήσει ένα νέο δίκτυο ως Coordinator. Όταν η συσκευή δεν δύναται να γίνει Coordinator η κατάσταση του NLME-NETWORK-FORMATION.confirm ορίζεται ως

«INVALID_REQUEST». Αν η συσκευή μπορεί να λειτουργήσει ως Coordinator τότε το NLME παράγει το MLME-SCAN.request για να βρεθεί ένα διαθέσιμο κανάλι. Αν το MLME-SCAN.confirm επιστρέψει σε «SUCCESS», το NLME επιλέγει το κατάλληλο κανάλι από τα διαθέσιμα. Στη συνέχεια το NWK θα πρέπει να επιλέξει ένα κωδικό αναγνώρισης για το δίκτυο (PAN Identifier) που να μην χρησιμοποιείται ήδη. Αν δεν βρεθεί κατάλληλο κανάλι ή PAN Identifier τότε το δίκτυο δε γίνεται να σχηματιστεί και το NLME-NETWORK-FORMATION.confirm γίνεται «STARTUP_FAILURE». Αν δεν προκύψουν σφάλματα και το δίκτυο σχηματιστεί, επιστρέφεται το NLME-NETWORK-FORMATION.confirm σε «SUCCESS».

- **NLME-PERMIT-JOINING** Το NLME-PERMIT-JOINING.request χρησιμοποιείται όταν θέλουμε ο Coordinator να επιτρέπει τη σύνδεση άλλων στοιχείων στο δίκτυό του για ένα συγκεκριμένο χρονικό διάστημα ίσο με την παράμετρο PermitDuration. Αν η συσκευή στην οποία γίνεται το request δεν είναι Coordinator ή Router τότε το NLME-PERMIT-JOINING.confirm μπαίνει σε κατάσταση «INVALID_REQUEST». Αν η συσκευή είναι Coordinator ή Router το NLME-PERMIT-JOINING.confirm θα είναι ίδιο με το MLME-SET.confirm, η κατάσταση του οποίου εξαρτάται από την τιμή του PermitDuration.
- **NLME-START-ROUTER** Το NLME-START-ROUTER.request παράγεται ώστε ο Router να αρχίσει να εκτελεί μια σειρά από εργασίες που βρίσκονται υπό την αρμοδιότητά του. Οι εργασίες αυτές είναι η αποδοχή αιτήσεων από άλλες συσκευές που θέλουν να συνδεθούν στο δίκτυό του, η δρομολόγηση των Data Frames και η λειτουργία Route Discovery. Αν η συσκευή δεν είναι Router το NLME-START-ROUTER.confirm γίνεται «INVALID_REQUEST». Σε οποιαδήποτε άλλη περίπτωση η κατάστασή του γίνεται ίση με εκείνη του MLME-START.confirm. Ο Router θα αρχίσει να εκτελεί τις εργασίες μόνον σε περίπτωση που το MLME-START.confirm επιστρέφει σε κατάσταση «SUCCESS».
- **NLME-ED-SCAN** Το επίπεδο εφαρμογής δημιουργεί το NLME-ED-SCAN.request για να γίνουν οι απαραίτητες μετρήσεις των επιπέδων ενέργειας στα γειτονικά κανάλια. Για να γίνει αυτό το NWK κάνει χρήση του MLME-SCAN.request. Κατά συνέπεια τα αποτελέσματα του NLME-ED-SCAN.confirm προκύπτουν από την κατάσταση του MLME-SCAN.confirm.
- **NLME-JOIN** Χρήση του NLME-JOIN.request γίνεται για να ζητηθούν η σύνδεση ή η επανασύνδεση της συσκευής σε ένα δίκτυο και η αλλαγή του καναλιού μετάδοσης. Όταν το request στέλνεται σε μια συσκευή που βρίσκεται ήδη σε δίκτυο ενώ η παράμετρος RejoinNetwork είναι ίση με 0x00 (δηλαδή δεν ζητείται επανασύνδεση) τότε παράγεται το NLME-JOIN.confirm σε κατάσταση «INVALID_REQUEST». Αν το primitive στέλνεται με σκοπό να αλλάξει το κανάλι μετάδοσης τότε το NLME-JOIN.confirm επιστρέφει σε «SUCCESS» όταν η αλλαγή είναι επιτυχής, όμως αν η συσκευή δεν

υποστηρίζει το attribute `phyCurrentChannel`, η μετάβαση από ένα ράδιο-κανάλι σε ένα άλλο δε μπορεί να επιτευχθεί και το `NLME-JOIN.confirm` τίθεται σε «`UNSUPPORTED_ATTRIBUTE`». Το `NLME-JOIN.indication` παράγεται σε ένα Coordinator ή σε ένα Router για να δείξει ότι κάποια άλλη συσκευή συνδέθηκε στο δίκτυό του.

- **NLME-DIRECT-JOIN** Το `NLME-DIRECT-JOIN.request` δημιουργείται σε ένα Coordinator ή Router ώστε να συνδέσει άμεσα μια συσκευή στο δίκτυό του. Αν προσθέσει μια συσκευή στο δίκτυό του, παράγεται το `NLME-DIRECT-JOIN.confirm` σε «`SUCCESS`». Στην κατάσταση «`ALREADY_PRESENT`» θα βρεθεί όταν η συσκευή ήταν ήδη στο δίκτυο και σε «`NEIGHBOOR_TABLE`» όταν ο πίνακας που περιέχει τα συνδεδεμένα στοιχεία είναι πλήρης.
- **NLME-LEAVE** Όταν μια συσκευή θέλει να εγκαταλείψει ένα δίκτυο ή να υποχρεώσει (αν είναι Coordinator ή Router) κάποια άλλη συσκευή να αποχωρήσει από αυτό, παράγει το `NLME-LEAVE.request`. Αν ληφθεί από το NWK μιας συσκευής που δεν ανήκει σε δίκτυο τότε επιστρέφεται το `NLME-LEAVE.confirm` σε «`INVALID_REQUEST`». Σε κατάσταση `UNKNOWN_DEVICE` εισέρχεται, όταν η συσκευή δεν υπάρχει. Σε κάθε άλλη περίπτωση γίνεται ίδιο με το `MCPS-DATA.confirm`. Το `NLME-LEAVE.indication` δείχνει αν η συσκευή που το παρήγαγε εγκατέλειψε το δίκτυο ή αν ανάγκασε μια άλλη συσκευή να αποσυνδεθεί.
- **NLME-RESET** Το `NLME-RESET.request` επαναφέρει το NWK στην αρχική του κατάσταση. Αν το `reset` ολοκληρωθεί με επιτυχία το `NLME-RESET.confirm` τίθεται σε «`SUCCESS`», διαφορετικά η κατάστασή του γίνεται `DISABLE_TRX_FAILURE`.
- **NLME-SYNC** Το `NLME-SYNC.request` ζητά τον συγχρονισμό με τον Coordinator ή τη λήψη δεδομένων από αυτόν. Το `NLME-SYNC.request` περιλαμβάνει την παράμετρο `TRACK` η οποία παίρνει τις Boolean τιμές `TRUE` και `FALSE` δείχνοντας αν ο συγχρονισμός θα διατηρηθεί ή όχι στα επόμενα beacons. Όταν η παράμετρος `TRACK` είναι `FALSE` και το δίκτυο δουλεύει χωρίς τη χρήση beacons, τότε το NLME παράγει το `MLME-POLL.request`. Μετά την εκτέλεση του `MLME-POLL.request` η κατάσταση του `NLME-SYNC.confirm` θα είναι ίδια με εκείνη που επιστρέφεται από το `MLME-POLL.confirm`. Αν το `TRACK` είναι `TRUE` και το δίκτυο δουλεύει χωρίς τη χρήση beacons τότε το `NLME-SYNC.confirm` παίρνει την κατάσταση «`INVALID_PARAMETER`». Για `TRACK FALSE/TRUE` και δίκτυο με ενεργοποιημένα beacons το NLME ορίζει την τιμή του `macAutoRequest` σε `TRUE` με τη βοήθεια του `MLME-SET.request`. Στη συνέχεια παράγει το `MLME-SYNC.request` με την παράμετρο `TrackBeacon` σε `FALSE/TRUE`. Το `NLME-SYNC.confirm` επιστρέφεται σε κατάσταση «`SUCCESS`».
- **NLME-SYNC-LOSS** Το `NLME-SYNC-LOSS.indication` δείχνει την απώλεια συγχρονισμού στο APL.

- **NLME-GET** Λειτουργεί όπως τα PLME-GET και MLME-GET με τη διαφορά ότι επεξεργάζεται τα δεδομένα της NWK PIB.
- **NLME-SET** Λειτουργεί όπως τα PLME-GET και MLME-GET με τη διαφορά ότι επεξεργάζεται τα δεδομένα της NWK PIB.
- **NLME-NWK-STATUS** Δείχνει στο APL τα σφάλματα που παρουσιάζονται στο ZigBee δίκτυο.
- **NLME-ROUTE-DISCOVERY** Το NLME-ROUTE-DISCOVERY.request ζητά την εκκίνηση του Route Discovery από ένα Coordinator ή Router. Το NLME-ROUTE-DISCOVERY.confirm θα μπει σε κατάσταση «SUCCESS» όταν το Route Discovery ολοκληρωθεί με επιτυχία και η παράμετρος DstAddrMode πάρει την τιμή 0x00. Αν η συσκευή στην οποία γίνεται το request, δεν είναι Coordinator ή Router τότε το NLME-ROUTE-DISCOVERY.confirm επιστρέφει σε «INVALID_REQUEST».

2.2.3.2 Unicast

Για την αποστολή δεδομένων από μια συσκευή χρησιμοποιούνται τρεις διαφορετικοί μηχανισμοί, το Unicast, το Multicast και το Broadcast. Στο Unicast τα δεδομένα στέλνονται προς μια μόνο συσκευή με συγκεκριμένη διεύθυνση. Αυτός είναι ο προεπιλεγμένος τρόπος μετάδοσης.

2.2.3.3 Multicast

Στην μετάδοση κατά Multicast τα πακέτα στέλνονται σε ένα σύνολο στοιχείων που βρίσκονται στο ίδιο δίκτυο. Το σύνολο συσκευών αναγνωρίζεται από μια 16 bit ακολουθία που λέγεται multicast group ID. Τα στοιχεία που αποτελούν μέρος του ίδιου συνόλου ονομάζονται group members. Κάθε συσκευή έχει έναν πίνακα τον multicast table, στον οποίο καταχωρεί σε ποια group ανήκει (η συσκευή μπορεί να ανήκει σε περισσότερα από ένα group) μεταβάλλοντας το attribute nwkGroupIDTable. Μια συσκευή μπορεί να μην ανήκει σε κανένα σύνολο, ωστόσο έχει τη δυνατότητα να κάνει Multicast μετάδοση προς ένα group. Αυτό είναι το non-member mode. Στο member mode η συσκευή που δίνει αρχή στη Multicast μετάδοση πρέπει να είναι μέλος του συνόλου στο οποίο πρόκειται να στείλει τα δεδομένα.

2.2.3.4 Broadcast

Στο broadcast τα μεταδιδόμενα πακέτα σε ένα κανάλι λαμβάνονται από όλες τις συσκευές που λειτουργούν στο κανάλι αυτό, αδιαφορώντας για τις διευθύνσεις τους. Κάθε συσκευή αφού λάβει τα πακέτα, ελέγχει την διεύθυνση προορισμού τους για να διαπιστώσει αν όντως τα πακέτα αυτά προορίζονταν για την ίδια. Όταν μια συσκευή επιθυμεί να ξεκινήσει μια broadcast μετάδοση πρέπει το APS να χρησιμοποιήσει τα services του NWK. Οι συσκευές που είναι ZigBee Coordinators ή Routers διατηρούν έναν πίνακα τον BTT στον οποίο αποθηκεύουν κάθε broadcast μετάδοση που έχουν πραγματοποιήσει. Κάθε καταχώρηση ονομάζεται BTR και περιέχει την αριθμητική ακολουθία και την διεύθυνση του πακέτου. Ένα Router έχει τη δυνατότητα να κρατήσει τουλάχιστον ένα πακέτο στο επίπεδο δικτύου. Το BTR παραμένει αποθηκευμένο για ένα χρονικό διάστημα ίσο με το attribute `nwkNetworkBroadcastDeliveryTime`.

2.2.3.5 NWK PDU

Το πακέτο του επιπέδου δικτύου αποτελείται από την επικεφαλίδα NWK Header και το ωφέλιμο φορτίο NWK Payload. Τα ακόλουθα στοιχεία συνθέτουν το NWK Header:

- **Frame Control** Αποτελείται από 16 bit και περιέχει σήματα ελέγχου, πληροφορίες για το είδος του πακέτου και για την διευθυνσιοδότηση.
- **Destination Address** Είναι η 16 bit διεύθυνση της συσκευής για την οποία προορίζονται τα πακέτα.
- **Source Address** Είναι η 16 bit διεύθυνση της συσκευής που εκπέμπει τα πακέτα.
- **Radius** Είναι ο αριθμός των επιτρεπόμενων μεταβάσεων κατά τη διάρκεια μιας μετάδοσης. Έχει μήκος 1 byte και μετά από κάθε μετάβαση του πακέτου σε άλλη συσκευή μειώνεται κατά 1.
- **Sequence Number** Κάθε φορά που εκπέμπεται ένα νέο πακέτο αυξάνεται κατά 1.
- **Destination IEEE Address** Περιλαμβάνει την 64 bit IEEE διεύθυνση που αντιστοιχεί στην 16 bit διεύθυνση δικτύου που περιέχεται στο Destination Address του NWK Header.

- **Source IEEE Address** Περιλαμβάνει την 64 bit IEEE διεύθυνση που αντιστοιχεί στην 16 bit διεύθυνση δικτύου που περιέχεται στο Source Address του NWK Header.
- **Multicast Control** Εμφανίζεται στο πακέτο μόνο αν η τιμή του πεδίου *Multicast Flag* του **Frame Control** είναι ίση με 1. Το πλαίσιο Multicast αποτελείται από τα εξής στοιχεία:
 - **Multicast Mode** Ορίζει τον τύπο του *Multicast* που πρόκειται να χρησιμοποιηθεί και μπορεί να τεθεί σε member mode ή σε non member mode.
 - **NonmemberRadius** Είναι η εμβέλεια σε member mode multicast που ελέγχεται από συσκευές που δεν αποτελούν members κάποιου Destination Group.
 - **MaxNonmemberRadius** Υποδεικνύει την μέγιστη τιμή που μπορεί να πάρει το NonmemberRadius.
- **Source Route Subframe** Συναντάται στο πακέτο μόνο αν η τιμή του πεδίου *source route* του **Frame Control** είναι ίση με 1. Το Source Route Subframe αποτελείται από τα εξής:
 - **Relay Count**
 - **Relay Index**
 - **Relay List**

Στο NWK Payload συναντάμε το Frame Payload που περιλαμβάνει το APDU και πληροφορίες για το είδος του πακέτου προσδιορίζοντας αν είναι πακέτο δεδομένων ή εντολών.

NWK HEADER									NWK PAYLOAD
Frame Control	Destination Address	Source Address	Radius	Sequence Number	Destination IEEE Address	Source IEEE Address	Multicast control	Source Route	Frame Payload

Σχήμα 2.5 NPDU

2.2.4 Application Layer

Το APL είναι το ανώτερο επίπεδο του πρωτοκόλλου. Τα Application Support Sub-layer, ZDO και Application Framework είναι τα υπό-επίπεδα που συνθέτουν το APL. Οι αρμοδιότητες του επιπέδου εφαρμογής είναι:

- Η συντήρηση του Binding πίνακα
- Η προώθηση μηνυμάτων μεταξύ των Bound Devices
- Η διαχείριση των διευθύνσεων
- Η αξιόπιστη μεταφορά δεδομένων
- Να ορίζει τον ρόλο της συσκευής μέσα στο δίκτυο
- Να ανιχνεύει τις ZigBee συσκευές στο δίκτυο

2.2.4.1 Application Framework

Το Application Framework είναι το υπό-επίπεδο στο οποίο ο σχεδιαστής καθορίζει τη λειτουργία της συσκευής. Αυτό γίνεται μέσω των Application Objects ή Endpoints. Υπάρχουν 256 Application Objects από 0 – 255. Το 0 προορίζεται για το ZDO, από 1 – 240 είναι εκείνα που χρησιμοποιεί ο κατασκευαστής, τα 241 – 254 έχουν μείνει αδέσμευτα για μελλοντική χρήση και το 255 είναι το Application Object που μεσολαβεί για τη μεταφορά δεδομένων από και προς τα Application Objects 1 – 240.

Για την εξασφάλιση της συμβατότητας μεταξύ των εφαρμογών που αναπτύσσονται από διαφορετικούς κατασκευαστές, το ZigBee, δίνει τη δυνατότητα να δημιουργηθούν κάποια πρότυπα που μπορούν να καλύψουν ένα σύνολο από εφαρμογές. Τα πρότυπα αυτά λέγονται Application Profiles. Τα Profiles που έχουν αναπτυχθεί έως τώρα είναι τα εξής:

- Home Automation
- Commercial Building Automation
- Industrial Plant Monitoring
- Telecommunications Applications
- Automatic Metering Initiative
- Personal Home and Health Care

Για παράδειγμα το Home Automation με τις ανάλογες μετατροπές στο κώδικά του μπορεί να καλύψει εφαρμογές όπως τον έλεγχο φωτισμού, την ενεργοποίηση και απενεργοποίηση ενός συστήματος ψύξης ανάλογα με τις μετρήσεις ενός αισθητηρίου θερμότητας κτλ. Ας υποθέσουμε μια εφαρμογή κατά την οποία θέλουμε το άνοιγμα των παραθύρων ενός κτιρίου, να εξαρτάται από τον εσωτερικό

φωτισμό του. Οπότε χρειαζόμαστε μια συσκευή (Coordinator) συνδεδεμένη με ένα αισθητήριο φως και ένα σύνολο συσκευών (End Devices) που θα ελέγχουν το μηχανισμό που έχουν τα παράθυρα ανάλογα με τις εντολές που θα δέχονται από τον Coordinator. Αν όλες αυτές οι συσκευές χρησιμοποιούν το ίδιο Application Profile, τότε μπορούν να δουλέψουν σωστά μεταξύ τους ακόμα και αν προέρχονται από διαφορετικές εταιρείες και διαφορετικούς κατασκευαστές. Αυτή είναι και η σπουδαιότητα των Application Profiles.

Ένα Application Profile αποτελείται από τα Clusters και τα device descriptions. Το Cluster είναι ένα σύνολο χαρακτηριστικών που υπάγονται στην ίδια κατηγορία. Κάθε Cluster αναγνωρίζεται και γίνεται προσβάσιμο με μια μοναδική ακολουθία 16 bit, το cluster Identifier. Το device descriptions παρέχει πληροφορίες για την συσκευή, όπως την συχνότητα λειτουργίας, το κανάλι εκπομπής, το ρόλο της συσκευής στο δίκτυο και την εναπομένουσα διάρκεια της μπαταρίας (αν υπάρχει).

2.2.4.2 ZDO

Το ZDO όπως είδαμε αποτελεί ένα ειδικό application object με διεύθυνση 0. Είναι υπεύθυνο για την αρχικοποίηση του APS, του επιπέδου δικτύου και των υπηρεσιών ασφαλείας. Όπως τα Objects έχουν Profiles έτσι και το ZDO έχει το ZigBee Device Profile. Το ZDP περιλαμβάνει clusters και device descriptions και παρέχει τις υπηρεσίες Device Discovery και Service Discovery.

2.2.4.3 APL Services - APS

Παρομοίως με τα χαμηλότερα επίπεδα που περιγράψαμε έως τώρα, το APL περιλαμβάνει επίσης υπηρεσίες δεδομένων και διαχείρισης. Οι υπηρεσίες παρέχονται από το υπό-επίπεδο APS μέσω των οντοτήτων APSDE για τα δεδομένα και APSME για την διαχείριση. Η πρόσβαση γίνεται με τα APSDE-SAP και APSME-SAP αντίστοιχα.

Το APSDE έχει μόνο ένα primitive το APSDE-DATA. Το APSDE-DATA.request παράγεται όταν ζητηθεί από το ανώτερο υπό-επίπεδο η αποστολή ενός ASDU. Οι καταστάσεις στις οποίες επιστρέφει το APSDE-DATA.confirm είναι:

- **SUCCESS** Όταν το ASDU μεταφέρεται επιτυχώς στο προορισμό του.
- **NO_BOUND_DEVICE** Αν δεν υπάρχουν στοιχεία στον Binding πίνακα.
- **NOT_SUPPORTED** Αν το primitive σταλεί σε μια συσκευή που δεν υποστηρίζει Binding πίνακα.

- **SECURITY_FAIL** Όταν η προσθήκη ασφάλειας στο πακέτο δεν είναι εφικτή ενώ απαιτείται από την παράμετρο TxOptions .
- **ASDU_TOO_LONG** Όταν το ASDU έχει μεγάλο μήκος και δεν γίνεται να χωριστεί σε μικρότερα τμήματα.

Το APSDE-DATA.indication δείχνει ότι ολοκληρώθηκε η μεταφορά ενός ASDU.

Τα primitive του APSME είναι τα ακόλουθα:

- **APSME-BIND** Το APSME-BIND.request ζητάει να συνδεθούν «λογικά» δυο συσκευές μεταξύ τους. Η διασύνδεση καταγράφεται στον Binding πίνακα. Όταν υπάρχει χώρος στον Binding πίνακα η λογική σύνδεση είναι εφικτή γιατί μπορεί να καταγραφεί με αποτέλεσμα το APSME-BIND.confirm να επιστρέψει σε κατάσταση «SUCCESS». Η κατάστασή του τίθεται σε «TABLE_FULL» όταν ο πίνακας είναι πλήρης και επομένως δεν γίνεται η σύνδεση Bind. Αν το primitive σταλεί σε μια συσκευή που δεν βρίσκεται σε κάποιο δίκτυο ή σε μια συσκευή που δεν υποστηρίζει Binding πίνακα τότε το APSME-BIND.confirm γίνεται «ILLEGAL_REQUEST».
- **APSME-UNBIND** Το APSME-UNBIND.request χρησιμοποιείται για να αποσυνδεθούν συσκευές που είναι λογικά συνδεδεμένες μεταξύ τους, αφαιρώντας την καταχώρηση που είχε τοποθετηθεί στο Binding πίνακα. Η καταχώρηση διαγράφεται εφόσον υπάρχει και οι συσκευές δεν θα είναι πλέον bound devices. Συνεπώς το APSME-UNBIND.confirm γίνεται «SUCCESS». Αν η καταχώρηση δεν υπάρχει το APSME-UNBIND.confirm θα τεθεί σε «INVALID_BINDING» ενώ η κατάστασή του θα γίνει «ILLEGAL_REQUEST» αν η εν λόγω συσκευή δεν βρίσκεται σε κάποιο δίκτυο ή δεν υποστηρίζει Binding πίνακα.
- **APSME-GET** Λειτουργεί όπως τα PLME-GET, MLME-GET και NLME-GET με τη διαφορά ότι επεξεργάζεται τα δεδομένα της AIB.
- **APSME-SET** Λειτουργεί όπως τα PLME-SET, MLME-SET και NLME-SET με τη διαφορά ότι επεξεργάζεται τα δεδομένα της AIB.
- **APSME-ADD-GROUP** Το APSME-ADD-GROUP.request δημιουργείται όταν θέλουμε να προσθέσουμε ένα Endpoint σε ένα σύνολο στοιχείων ώστε οι πληροφορίες που προορίζονται για το σύνολο αυτό να καταλήγουν και στο συγκεκριμένο Endpoint. Όταν το request ολοκληρωθεί με επιτυχία η κατάσταση του APSME-ADD-GROUP.confirm γίνεται «SUCCESS». Αν η τιμή της παραμέτρου GroupAddress βρεθεί εκτός του κανονικού της πεδίου, που είναι από 0x0000 ως 0xFFFF, τότε επιστρέφεται το APSME-ADD-GROUP.confirm σε «INVALID_PARAMETER».

- **APSME-REMOVE-GROUP** Το APSME-REMOVE-GROUP.request παράγεται για να αφαιρεθεί ένα Endpoint από ένα σύνολο στοιχείων ώστε τα πακέτα που προορίζονται για το σύνολο αυτό να μην καταλήγουν πλέον στο συγκεκριμένο Endpoint. Όταν ο αποκλεισμός του Endpoint γίνει με επιτυχία η κατάσταση του APSME-REMOVE-GROUP.confirm γίνεται «SUCCESS». Αν η τιμή της παραμέτρου GroupAddress βρεθεί εκτός του κανονικού της πεδίου, τότε επιστρέφεται το APSME-REMOVE-GROUP.confirm σε «INVALID_PARAMETER».
- **APSME-REMOVE-ALL-GROUPS** Το APSME-REMOVE-ALL-GROUPS.request χρησιμοποιείται για να αφαιρεθεί το Endpoint από όλα τα σύνολα στοιχείων. Όταν το Endpoint αφαιρεθεί με επιτυχία η κατάσταση του APSME-REMOVE-GROUP.confirm γίνεται «SUCCESS». Αν η τιμή της παραμέτρου Endpoint βρεθεί εκτός του κανονικού της πεδίου, που είναι από 0x01 ως 0xF0, τότε επιστρέφεται το APSME-REMOVE-GROUP.confirm σε «INVALID_PARAMETER».

2.2.4.4 APL PDU

Στο σχήμα 2.6 απεικονίζεται η δομή του πακέτου που παράγεται από το επίπεδο εφαρμογής, με την επικεφαλίδα και το ωφέλιμο φορτίο. Το APS header αποτελείται από τα ακόλουθα πλαίσια:

- **Frame Control** Αποτελείται από 8 bit και περιλαμβάνει πληροφορίες για τον τύπο του πακέτου, για τις ρυθμίσεις ασφαλείας και τα πλαίσια διευθυνσιοδότησης.
- **Destination Endpoint** Έχει μήκος 8 bits και δείχνει για ποιο Endpoint του τελικού αποδέκτη προορίζεται το πακέτο. Αν το destination endpoint έχει τιμή 0x00 τότε το πακέτο προορίζεται για το ZDO ενώ αν η τιμή του είναι μια από τις τότε 0x01 – 0xf0 τότε θα πηγαίνει στο αντίστοιχο application object από 1 – 240.
- **Group Address** Το Group Address είναι 16 bits και περιέχει τη διεύθυνση του συνόλου συσκευών για το οποίο προορίζεται το πακέτο.
- **Cluster Identifier** Έχει μέγεθος 16 bits και επισημαίνει με ποιο cluster συσχετίζεται το πακέτο.
- **Profile Identifier** Αυτό το πλαίσιο αποτελείται από 16 bits και δείχνει το profile για το οποίο προορίζεται το πακέτο.
- **Source Endpoint** Είναι 8 bits και δείχνει το endpoint από το οποίο προήλθε το πακέτο.

- **APS Counter** Έχει μήκος 8 bits και χρησιμοποιείται για να αποτρέψει τη λήψη του ίδιου πακέτου πάνω από μια φορά. Για κάθε νέα εκπομπή που γίνεται η τιμή του αυξάνεται κατά ένα.
- **Extended header** Αποτελείται από τα ακόλουθα πλαίσια
 - **Extended frame control** Έχει μήκος 8 bits και περιέχει πληροφορίες όσο αφορά το Fragmentation δηλαδή το διαχωρισμό του πακέτου σε μικρότερα τμήματα.
 - **Block number** Είναι 8 bits και ελέγχει το fragmentation.
 - **ACK bitfield** Είναι σήμα επιβεβαίωσης που δείχνει ποια τμήματα του πακέτου παραλήφθηκαν με επιτυχία.

APS HEADER								APS PAYLOAD
Frame Control	Destination Endpoint	Group Address	Cluster ID	Profile ID	Source Endpoint	APS counter	Extended header	Frame Payload

Σχήμα 2.5 APDU

Κεφάλαιο 3°

ZIGBEE ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

3.1 ZigBee Transceivers

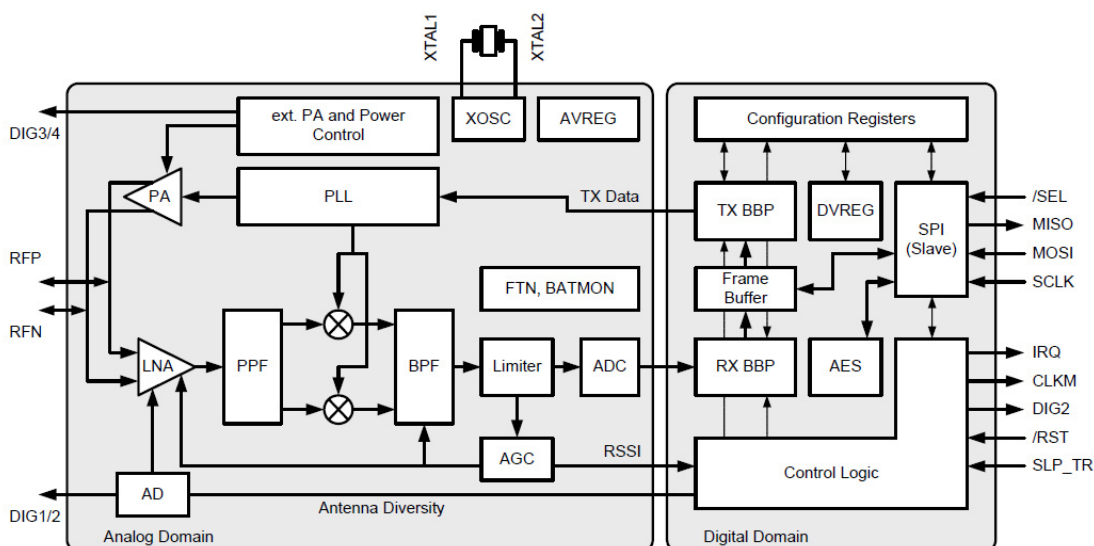
Πολλές εταιρείες μέλη της ZigBee Alliance αναπτύσσουν ολοκληρωμένα κυκλώματα και μονάδες (modules) που υλοποιούν το ZigBee πρωτόκολλο όπως θα δούμε στις υποενότητες που ακολουθούν. Συνεχώς βγαίνουν νέα προϊόντα για να καλύψουν πιο απαιτητικές εφαρμογές ή για να διευκολύνουν τους μηχανικούς κατά την υλοποίηση. Στην ενότητα 1.4 αναφέραμε ότι η ZigBee Alliance στηρίχθηκε στα επίπεδα PHY και MAC του IEEE 802.15.4 για να δημιουργήσει το ZigBee προσθέτοντας τα APL και NWK. Με τον ίδιο τρόπο ορισμένες εταιρείες για να απλοποιήσουν τα πράγματα περισσότερο, ανέπτυξαν δικά τους «μικρά» πρωτόκολλα. Για παράδειγμα η Texas Instruments έχει το SimpliciTI, η Freescale το SMAC και η Microchip το MiWi.

3.1.1 Atmel

Το AT86RF231 αποτελείται από μια βαθμίδα πομποδέκτη και μια βαθμίδα που εξασφαλίζει την διασύνδεση του IC με έναν εξωτερικό Μίκρο-ελεγκτή μέσω SPI. Η ισχύς εκπομπής προγραμματίζεται από -17 dBm έως +3 dBm. Η τάση τροφοδοσίας του κυμαίνεται από 1.8V έως 3.6V. Η κατανάλωση ρεύματος μεταβάλλεται ανάλογα με την κατάσταση λειτουργίας του ολοκληρωμένου και συγκεκριμένα:

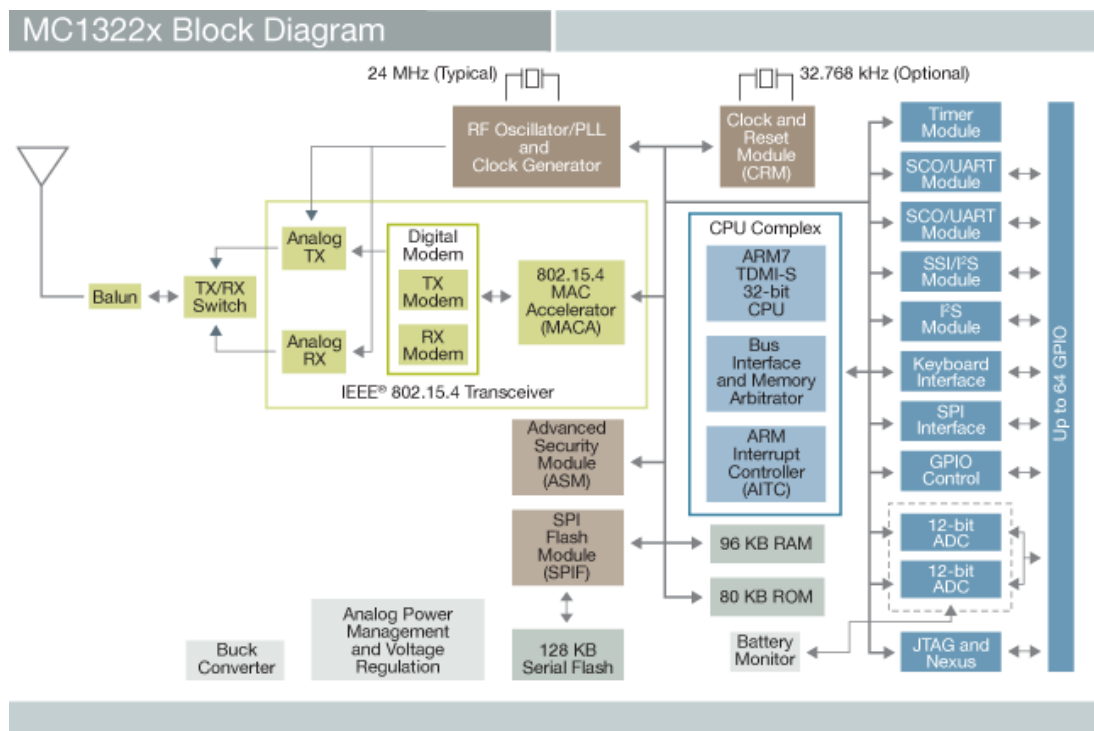
- SLEEP = 0.02A
- TRX_OFF = 0.4 mA
- RX_ON = 12.3 mA
- BUSY_TX = 14mA (max at +3 dBm)

Στο σχήμα 3.1 φαίνονται όλα τα στοιχεία που συνθέτουν τις δύο βαθμίδες.



3.1.2 Freescale

Το νέο προϊόν της, είναι το MC13224V ZigBee τρίτης γενιάς. Το ολοκληρωμένο χαρακτηρίζεται ως PiP και περιλαμβάνει χαμηλής ισχύος πομποδέκτη στα 2.4 GHz, Μίκρο-ελεγκτή με πυρήνα ARM7 στα 32 bit, balun για την προσαρμογή της κεραίας με την έξοδο του πομποδέκτη, μνήμη Flash 128 KB, RAM 96 KB, ROM 80 KB και τα περιφερειακά που φαίνονται στο μπλοκ διάγραμμα του σχήματος 3.2. Όλα σε ένα LGA κέλυφος 9.5mm x 9.5mm 99 ακροδεκτών.



Σχήμα 3.2

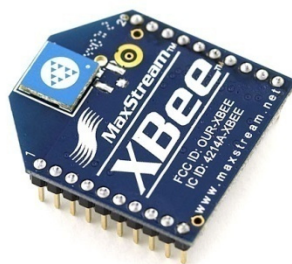
Η ισχύς εκπομπής προγραμματίζεται από -30 dBm έως +4 dBm. Η τάση τροφοδοσίας του κυμαίνεται από 2.0V έως 3.6V. Η κατανάλωση ρεύματος μεταβάλλεται ανάλογα με την κατάσταση λειτουργίας του ολοκληρωμένου και συγκεκριμένα:

- TRX_ON = 29 mA
- RX_ON = 22 mA
- Radio off MCU active = 3.3 mA
- Radio off MCU idle = 0.8 mA
- Radio off MCU off = 0.4 μ A (max)

Το IC περιέχει και όλους τους απαραίτητους πυκνωτές απόζευξης.

3.1.3 MaxStream

Η MaxStream έχει τα modules XBEE και XBEE PRO (σχήμα 3.3). Αποτελούν πλήρης μονάδες πομποδεκτών με δυνατότητα σύνδεσης σε Μίκρο-ελεγκτή και υποστηρίζουν τις απαιτήσεις του 802.15.4 . Τα modules αυτά προγραμματίζονται με AT Commands. Το XBEE έχει εμβέλεια 30m σε εσωτερικούς χώρους και 100m σε εξωτερικούς. Η κατανάλωσή του κατά την εκπομπή είναι 45 mA και κατά τη λήψη 50 mA. Το XBEE PRO έχει εμβέλεια 100m σε εσωτερικούς χώρους και 1500m σε εξωτερικούς. Η κατανάλωσή του κατά την εκπομπή είναι 215 mA και κατά τη λήψη 55 mA. Οι μονάδες τροφοδοτούνται με τάση 3.3V και η τυπική τιμή της ισχύος που εκπέμπουν είναι 0 dBm.



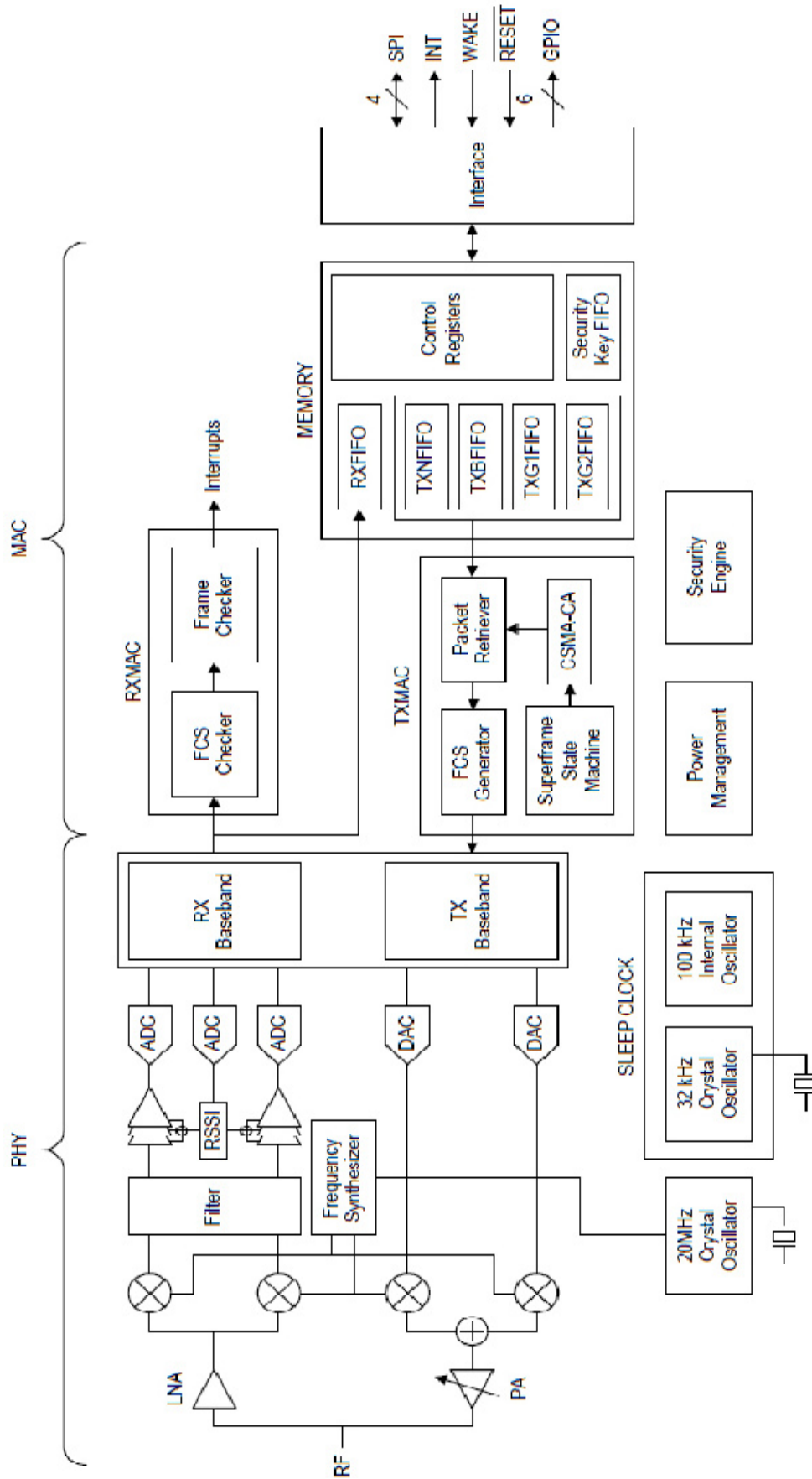
Σχήμα 3.3

3.1.4 Microchip

Το MRF24J40 είναι το ολοκληρωμένο κύκλωμα ZigBee πομποδέκτη της Microchip. Συνδέεται με εξωτερικό Μίκρο-ελεγκτή μέσω SPI. Μπορεί να φτάσει μια μέγιστη ταχύτητα εκπομπής στα 625 kbps και η τυπική τιμή ισχύος είναι 0 dBm. Η κατανάλωση ρεύματος είναι ανάλογη με τις εξής καταστάσεις:

- RX mode = 19 mA
- TX mode = 23 mA
- Sleep mode = 2 μ A

Όλες οι βαθμίδες του IC φαίνονται λεπτομερώς στο σχήμα 3.4



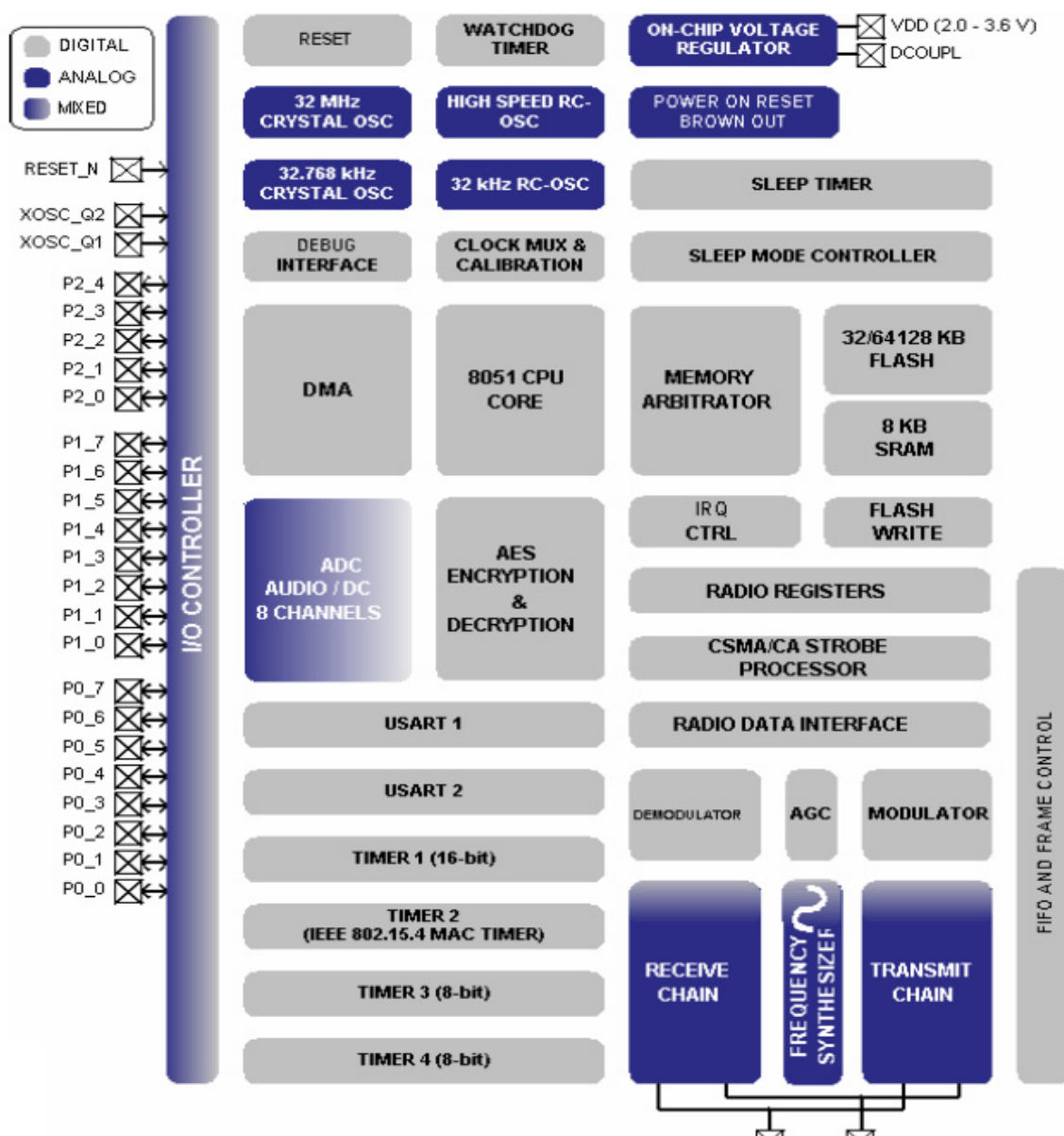
Σχήμα 3.4 MRF24J40 μπλοκ διάγραμμα

3.1.6 Texas Instruments

Η TI αναπτύσσει διάφορα ολοκληρωμένα για την υλοποίηση του ZigBee. Εκείνο που θα μας απασχολήσει όμως είναι το CC2430, γιατί είναι αυτό που επιλέχθηκε για να κατασκευαστεί η μονάδα ZigBee αυτής της πτυχιακής εργασίας. Ο λόγος για την επιλογή αυτή ήταν ότι η μονάδα έπρεπε να είναι όσο το δυνατόν μικρότερη και τότε το CC2430 ήταν το μοναδικό IC που συμπεριλάμβανε Μικροελεγκτή και πομποδέκτη μαζί. Η επόμενη ενότητα είναι αφιερωμένη σε αυτό το εκπληκτικό ολοκληρωμένο το οποίο έχει μέσα του ένα πλήρες ηλεκτρονικό σύστημα σε ένα κέλυφος μόλις 7mm x 7mm. Το SoC τροφοδοτείται με 2.0V – 3.6V. Η κατανάλωση ρεύματος κατά την εκπομπή και λήψη είναι 27 mA, σε powerdown mode όπου μπορεί να τεθεί ξανά σε λειτουργία από εξωτερικά interrupts ή από το RTC είναι 0.5 μ A και σε stand-by mode όπου μπορεί να τεθεί σε λειτουργία μόνο από εξωτερικά interrupts είναι 0.3 μ A.

3.2 SoC CC2430

Στο σχήμα 3.5 φαίνεται το αναλυτικό μπλοκ διάγραμμα του CC2430. Στη συνέχεια περιγράφεται κάθε βαθμίδα του.



3.2.1 DMA

Το DMA είναι μια τεχνική για την απευθείας μεταφορά δεδομένων μεταξύ δύο διατάξεων στο ίδιο hardware. Για να γίνει αυτό ο επεξεργαστής παρέχει στο DMA controller τις διευθύνσεις (των διατάξεων) του αποστολέα και του παραλήπτη, καθώς και το συνολικό αριθμό των bytes που πρόκειται να σταλούν. Το DMA αρχίζει τη μεταφορά των δεδομένων και κάθε φορά που παραδίδει ένα byte μειώνει την τιμή του συνολικού αριθμού των bytes κατά ένα. Όταν ο συνολικός αριθμός των bytes γίνει 0 τότε ενημερώνει τον επεξεργαστή με ένα interrupt ότι η αποστολή ολοκληρώθηκε. Αν δεν υπάρχει DMA συσκευή, για να γίνει η μεταφορά, ο επεξεργαστής θα πρέπει να διαβάσει τα δεδομένα από τη μια διάταξη και να τα γράψει στην άλλη byte ανά byte. Επομένως όταν μεταφέρεται μεγάλος όγκος δεδομένων ή όταν υπάρχει συχνά η ανάγκη για μετακινήσεις δεδομένων ο επεξεργαστής θα είναι συνεχώς απασχολημένος με αποτέλεσμα να μην μπορεί να εκτελέσει άλλες κρίσιμες λειτουργίες του λογισμικού. Εν ολίγοις το DMA αυξάνει την ταχύτητα του συστήματος.

3.2.2 WATCHDOG TIMER

Το Watchdog timer προστατεύει το λογισμικό αποτρέποντάς το από την πιθανότητα να κολλήσει. Αυτός ο timer αρχίζει αντίστροφη μέτρηση από έναν μεγάλο αριθμό. Το λογισμικό έχει προγραμματιστεί ώστε ανά τακτά χρονικά διαστήματα να τον επαναφέρει στην αρχική του τιμή. Σε περίπτωση που ο Watchdog timer μηδενιστεί σημαίνει ότι το λογισμικό δεν μπόρεσε να τον επαναφέρει. Από τη στιγμή που η επαναφορά είναι μια από τις λειτουργίες που το λογισμικό θα έπρεπε να εκτελεί, υπό κανονικές συνθήκες, τότε ο Watchdog timer αντιλαμβάνεται ότι το λογισμικό κόλλησε και κάνει reset τον επεξεργαστή ώστε να γίνει η επανεκκίνησή του.

3.3.3 8051 CPU

Ο ενσωματωμένος Μίκρο-ελεγκτής είναι αρχιτεκτονικής 8051 στα 8 bit. Έχει δυο ολόκληρα I/O PORTS τα P0 και P1 και ένα των 5 bits το P2. Χρησιμοποιεί το τυποποιημένο σύνολο εντολών του 8051 και κάθε εντολή εκτελείται σε διάρκεια ενός κύκλου λειτουργίας. Η CPU περιλαμβάνει τις ακόλουθες μνήμες:

- **CODE** Έχει μέγεθος 64 KB και είναι μόνο για ανάγνωση.
- **DATA** Μπορεί προσπελαστεί έμμεσα ή άμεσα με μεγάλη ταχύτητα αφού απαιτείται μόνο ένας κύκλος λειτουργίας. Το συνολικό της μέγεθος είναι 256 bytes. Από αυτά τα 128 είναι προσβάσιμα και έμμεσα και άμεσα ενώ τα άλλα 128 μόνο με έμμεση διευθυνσιοδότηση.

- **XDATA** Για να προσπελαστεί χρειάζονται 4-5 κύκλοι εργασίας. Το μεγεθός της είναι 64 KB.
- **SFR** Εδώ βρίσκονται οι καταχωρητές ειδική χρήσης που είναι άμεσα προσβάσιμοι με ένα κύκλο λειτουργίας. Ορισμένοι από αυτούς είναι bit addressable που σημαίνει ότι μπορούμε να επέμβουμε σε κάθε ένα από τα 8 bit από τα οποία αποτελούνται ξεχωριστά.

Για ταχύτερη επικοινωνία με εξωτερικές μνήμες περιλαμβάνει δύο Data pointers, το DPTR0 και DPTR1. Έχει συνολικά 19 interrupts.

3.3.4 MEMORY ARBITRATOR

Χειρίζεται την πρόσβαση της MCU και του DMA σε κάθε μνήμη του συστήματος.

3.3.5 USARTs

Το CC2430 έχει δύο σειριακές την USART 1 και USART 2 για να επικοινωνεί με εξωτερικά περιφερειακά.

3.3.6 TIMERS

Ο TIMER 1 στα 16 bit και οι TIMERS 3 & 4 στα 8 bit είναι χρονιστές γενικής χρήσεως. Ο TIMER 2 παρέχει τον απαραίτητο χρονισμό για τον αλγόριθμο CSMA-CA στο MAC 802.15.4 . Ο ορίζει τις χρονικές περιόδους κατά τις οποίες το σύστημα βρίσκεται σε κατάσταση χαμηλής κατανάλωσης

3.3.7 ADC

Το ADC είναι 12-bit μετατροπέας αναλογικού σε ψηφιακό. Ως είσοδο χρησιμοποιεί την πόρτα P0. Αποθηκεύει τα αποτελέσματα από τις μετατροπές στη μνήμη μέσω του DMA.

3.3.8 AES

Ο AES επεξεργαστής είναι υπεύθυνος για την κρυπτογράφηση των δεδομένων. Με την ύπαρξή του αποσυμφορίζεται η CPU αφού δεν χρειάζεται να τρέξει η ίδια τους αλγόριθμους κρυπτογράφησης.

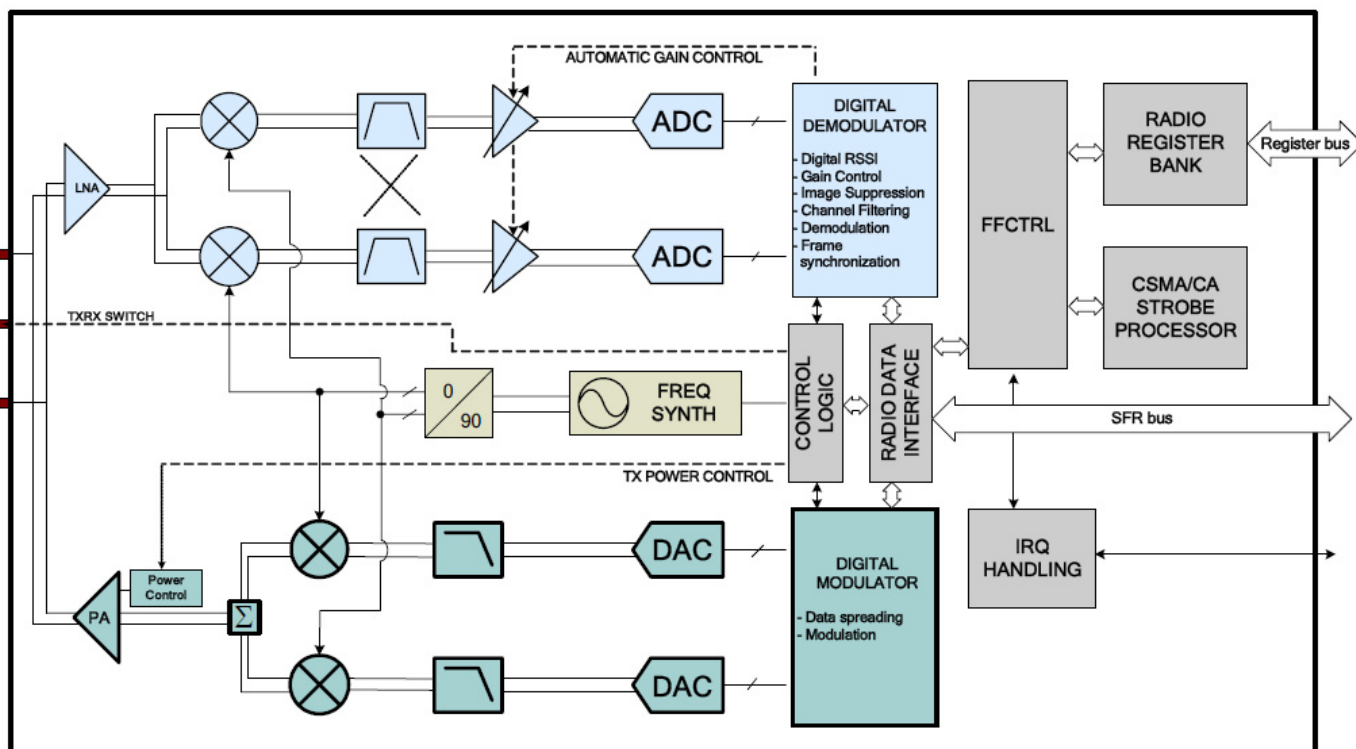
3.3.9 ON-CHIP VOLTAGE REGULATOR

Το CC2430 έχει δύο ρυθμιστές τάσεως, έναν για τις ψηφιακές και έναν για τις αναλογικές βαθμίδες του ολοκληρωμένου και παρέχουν σταθερή έξοδο στα 1.8 V. Ο ρυθμιστής για την αναλογική τροφοδοσία παίρνει είσοδο από 2.0 – 3.6 V από το pin AVDD_RREG. Η έξοδός του είναι στο pin RREG_OUT και συνδέεται στα pins 25, 27-31 και 35-40. Η είσοδος του regulator για την ψηφιακή τροφοδοσία είναι στο pin AVDD_DREG και κυμαίνεται πάλι στα 2.0 – 3.6 V. Η έξοδός του συνδέεται εσωτερικά με τα ψηφιακά μέρη του.

3.3.10 TRANSCEIVER

Τα μπλόκ RADIO REGISTERS, RADIO DATA INTERFACE, RECEIVE CHAIN, TRANSMIT CHAIN, FREQUENCY SYNTHESIZER, CSMA-CA STROBE PROCESSOR, AGC, DEMODULATOR και MODULATOR αποτελούν την βαθμίδα του πομποδέκτη. Στο σχήμα 3.6 απεικονίζεται η βαθμίδα του πομποδέκτη με μεγαλύτερη λεπτομέρεια.

Κατά την εκπομπή το σήμα διαμορφώνεται από τον digital modulator με O-QPSK και στη συνέχεια ενισχύεται από τον Power Amplifier (PA). Κατά την λήψη το λαμβανόμενο σήμα ενισχύεται από το LNA και αποδιαμορφώνεται από τον digital demodulator. Το TxRx Switch είναι ο διακόπτης που κάνει την εναλλαγή μεταξύ των κυκλωμάτων πομπού-δέκτη.



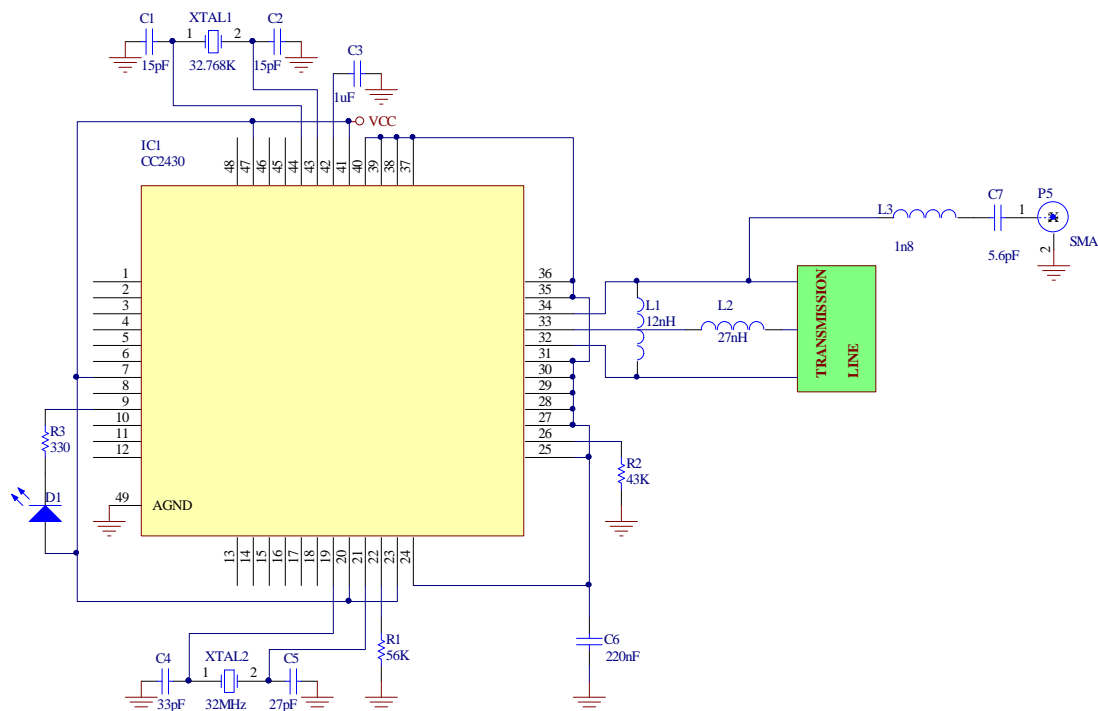
Σχήμα 3.6 Διάγραμμα του πομποδέκτη Πηγή «CC2430 datasheet»

Κεφάλαιο 4^ο

ΣΧΕΔΙΑΣΗ ΚΑΙ ΑΝΑΠΤΥΞΗ

4.1 Κύκλωμα πομποδέκτη

Το σχηματικό διάγραμμα του κυκλώματος είναι απλό και αποτελείται από λίγα εξωτερικά εξαρτήματα, αφού το ολοκληρωμένο όπως είδαμε έχει ενσωματωμένα σχεδόν όλα τα απαραίτητα στοιχεία.



Σχήμα 4.1 Το διάγραμμα της μονάδας

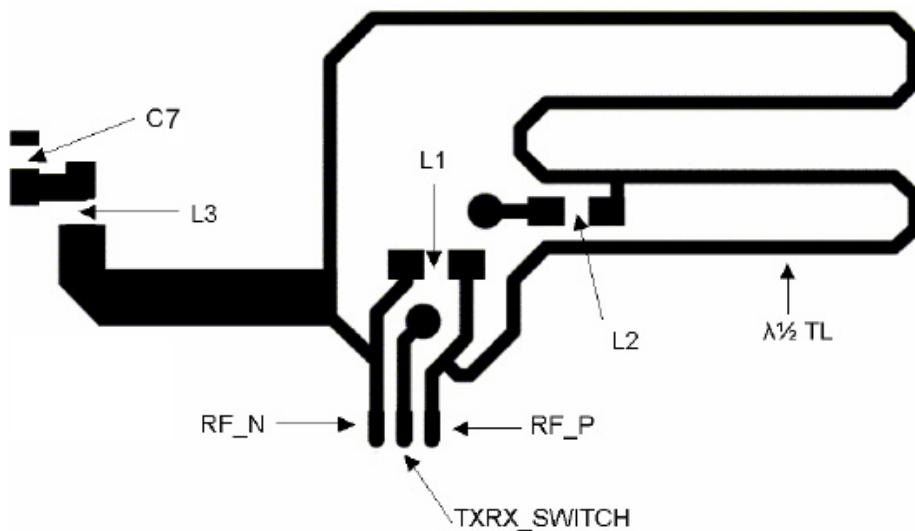
Τα C1, C2 και XTAL1 σχηματίζουν τον ταλαντωτή στα 32.768 KHz ενώ τα C4, C5, και XTAL τον ταλαντωτή των 32 MHz. Η R1 και R2 είναι αντιστάσεις πόλωσης. Η R1 ρυθμίζει το ρεύμα στην κατάλληλη τιμή για τον ταλαντωτή των 32 MHz. Η R2 ρυθμίζει το ρεύμα στις RF βαθμίδες. Ο πυκνωτής C3 την τάση για τα ψηφιακά κυκλώματα. Ο πυκνωτής C6 συνδέεται με τον ρυθμιστή τάσης του IC για την παραγωγή των 1.8 V που τροφοδοτούν τα αναλογικά μέρη του ολοκληρωμένου. Τα πηνία L1, L2 και L3, το Transmission Line και ο C7 αποτελούν το BALUN, δηλαδή το κύκλωμα προσαρμογής της διαφορικής εισόδου/εξόδου των RF_N και RF_P προς την 50 ohm μονή είσοδο/έξοδο της κεραίας. Στο I/O P1.0 προστέθηκε μια LED καθώς και η αντίσταση R3 για να περιορίσει το ρεύμα που την διαρρέει.

4.2 BALUNS

Η σωστή προσαρμογή της τελικής βαθμίδας με την κεραία είναι πολύ κρίσιμη και καθορίζει την απόδοση του συστήματος κατά την εκπομπή και λήψη. Ακολουθούν ορισμένες από τις τεχνικές που χρησιμοποιούνται για την προσαρμογή.

4.2.1 Microstrip Balun

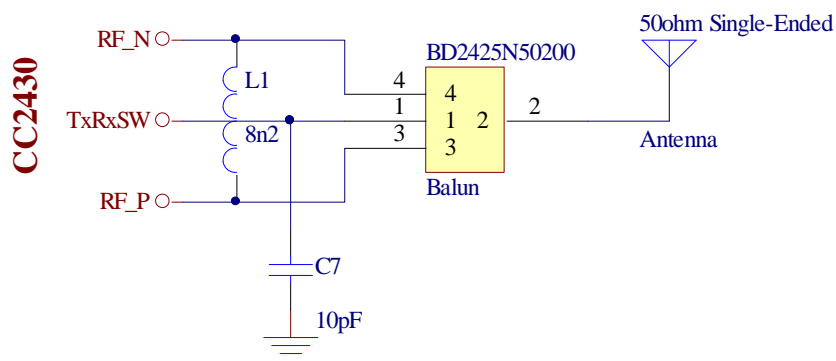
Το balun αυτό αναπτύχθηκε από την TI για το CC2430 και γενικά για όλα τα ZigBee transceiver ολοκληρωμένα της. Αποτελείται από τρία πηνία, έναν πυκνωτή και μια γραμμή μεταφοράς (όπως είδαμε κατά την περιγραφή του κυκλώματος) μήκους $\lambda/2$ που σχεδιάζεται στο τυπωμένο. Τα L1, L3 μαζί με τη γραμμή μεταφοράς κάνουν την προσαρμογή. Το L2 είναι πηνίο στραγγαλισμού και αποκόπτει το RF σήμα, για να μην εισβάλει στο διακόπτη εκπομπής-λήψης. Τέλος, ο πυκνωτής C7 σταματάει τη ροή συνεχούς ρεύματος προς την κεραία. Η TI παρέχει το σχέδιο της γραμμής μεταφοράς μαζί με όλες τις διαστάσεις των αγωγών δίνοντας την δυνατότητα σε οποιονδήποτε να το σχεδιάσει με ακρίβεια στο δικό του PCB. Αυτό το balun χρησιμοποιήθηκε για τις μονάδες ZigBee που αναπτύχθηκαν στα πλαίσια της παρούσας πτυχιακής εργασίας.



Σχήμα 4.2 Η γραμμή μεταφοράς σχεδιασμένη σε τυπωμένο. Πηγή: «TI Application Note swra098d»

4.2.2 Chip Balun

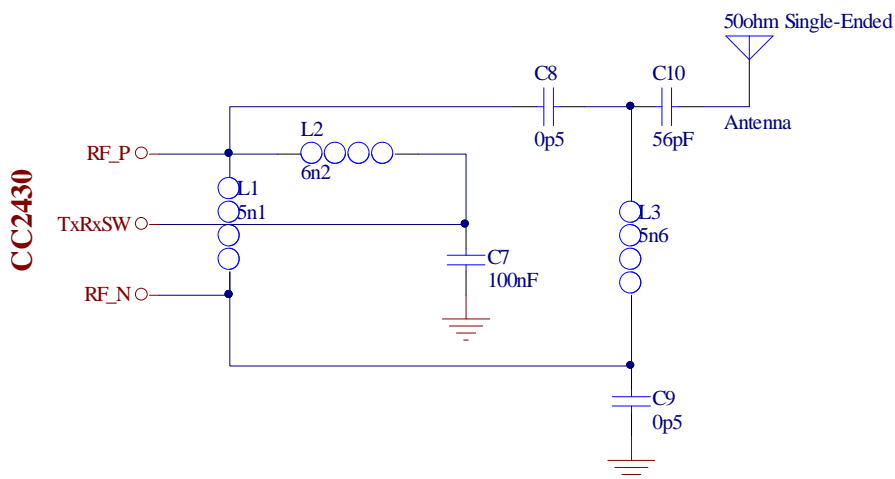
Η λύση της Anaren για να καλύψει τις ανάγκες προσαρμογής είναι το BD2425N50200A00, το οποίο αποτελεί μετασχηματιστή σε μορφή ολοκληρωμένου με μέγεθος μόλις ένα τετραγωνικό χιλιοστό. Το εξάρτημα συνδέεται με τη διαφορική είσοδο/έξοδο στα 200 Ω και καταλήγει στην μονή είσοδο/έξοδο των 50 Ω. Για να λειτουργήσει σωστά χρειάζεται μόνο ένα πηνίο και ένα πυκνωτή επιπλέον. Ο χώρος που καταλαμβάνεται στην πλακέτα μειώνεται αισθητά σε σχέση με το balun που είδαμε προηγουμένως του οποίου η γραμμή μεταφοράς χρειάζεται ένα συνολικό εμβαδόν 12mm x 8 mm.



Σχήμα 4.3 Σύνδεση του BD2425N50200A00 με το CC2430.

4.2.3 Discrete components balun

Το balun μπορεί να υλοποιηθεί και με διακριτά εξαρτήματα όπως στο σχήμα 4.4. Ο C10 δεν αφήνει τη διέλευση DC ρεύματος προς την κεραία. Τα υπόλοιπα εξαρτήματα πραγματοποιούν την προσαρμογή.



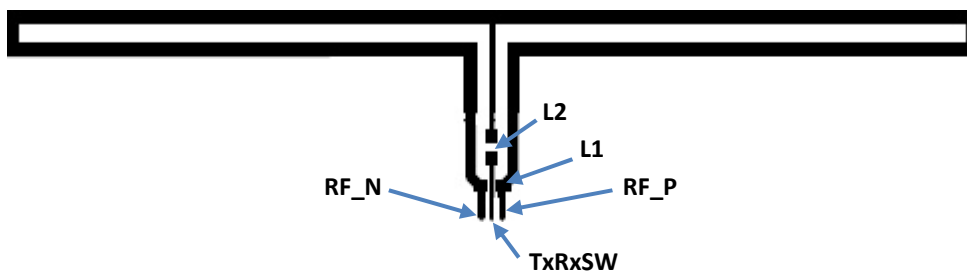
Σχήμα 4.4 Balun διακριτών στοιχείων

4.3 Κεραίες για εφαρμογές ZigBee

Ένα άλλο βασικό στοιχείο στο οποίο πρέπει να δοθεί προσοχή κατά τη σχεδίαση του πομποδέκτη είναι η κεραία. Από αυτήν εξαρτάται αν το balun θα χρειαστεί ή όχι. Η κεραία μπορεί να είναι σε μορφή ολοκληρωμένου κυκλώματος, σχεδιασμένη πάνω στο τυπωμένο ή να αποτελεί εξωτερικό εξάρτημα που συνδέεται πάνω στην πλακέτα. Οι κεραίες που ενδείκνυνται περισσότερο για ZigBee εφαρμογές είναι το αναδιπλωμένο δίπολο και η κεραία τύπου F.

4.3.1 Folded Dipole

Το αναδιπλωμένο δίπολο δεν χρειάζεται balun καθώς έχει διαφορετική είσοδο και μέσω του L2 παρέχει τη διαδρομή ώστε το TxRxSW να τροφοδοτηθεί με 1.8V τα RF pins. Το στραγγαλιστικό πηνίο L2 τοποθετήθηκε για να εμποδίσει το RF σήμα να εισχωρήσει στο TxRxSW. Το διάγραμμα ακτινοβολίας της κεραίας είναι σχεδόν όμοιο-κατευθυντικό.



Σχήμα 4.5 Το σχέδιο του δίπολου καθώς και πως συνδέεται με το CC2430

4.3.2 IFA

Η ανεστραμμένη κεραία τύπου F είναι μια κεραία υψηλών επιδόσεων με κέρδος +3.3 dB. Έχει σχεδιαστεί ώστε να προσαρμόζεται άμεσα σε μια 50 Ω πηγή. Εκπέμπει όμοιο-κατευθυντικά στο επίπεδο της πλακέτας και δεν είναι αναγκαίο να τοποθετηθεί σε συγκεκριμένο σημείο του PCB. Το μέγεθός της είναι 25.7 x 7.5 mm. Αν ο χώρος στην πλακέτα είναι περιορισμένος η IFA μπορεί να αντικατασταθεί με την IFA τύπου μαιάνδρου που χρειάζεται 15.2 x 5.7 mm.



Σχήμα 4.6 PCB σχέδιο IFA. Πηγή: «swru120b»



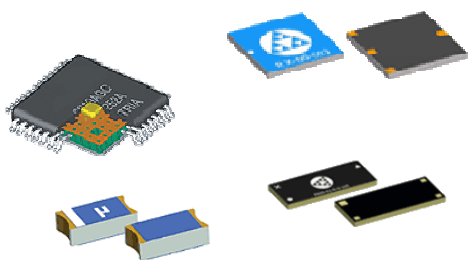
Σχήμα 4.7 IFA μαιάνδρου. Πηγή: «swru117d»

4.3.3 Chip Antennas

Στην αγορά κυκλοφορούν πολλά είδη κεραιών σε ολοκληρωμένη μορφή. Το πλεονέκτημά τους είναι ότι καταλαμβάνουν μικρότερο χώρο πάνω στην πλακέτα. Όμως η μεγάλη ολοκλήρωση και η τεχνητή αύξηση του συντελεστή ποιότητας Q έχει τα εξής αρνητικά επακόλουθα:

- Μείωση της απόδοσης
- Μείωση του ωφέλιμου bandwidth
- Μεγαλύτερη ευαισθησία σε εξωτερικούς παράγοντες
- Μικρότερη εμβέλεια

Οι εξωτερικές και οι κεραιές που σχεδιάζονται σε PCB έχουν καλύτερη απόδοση και αν γίνεται, είναι προτιμητέο να χρησιμοποιούνται στη θέση των chip antennas.



Σχήμα 4.8 Διάφορα chip antennas της Fractus.



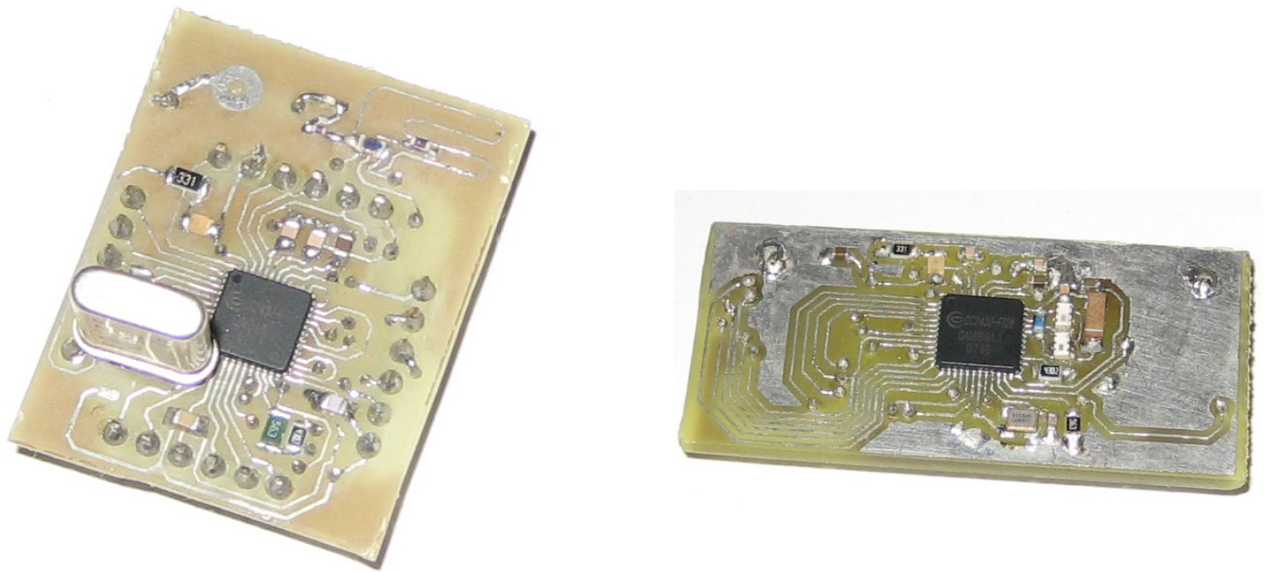
Σχήμα 4.9 Εξωτερική κεραία με SMA connector.

4.4 Προγραμματισμός

Όταν ο πομποδέκτης κατασκευαστεί σύμφωνα με το σχηματικό διάγραμμα (σχήμα 4.1) και με τις προδιαγραφές που ορίστηκαν για τα κρίσιμα RF μέρη του κυκλώματος, το μόνο που απομένει για να λειτουργήσει η μονάδα είναι να προγραμματιστεί η CPU του ολοκληρωμένου.

Η TI ανέπτυξε το Z-Stack, ένα Firmware που περιέχει κώδικα για κάθε επίπεδο του ZigBee και για όλες τις λειτουργίες του. Το Z-Stack έχει εγκριθεί από την ZigBee Alliance ως συμβατό με το πρωτόκολλο αφού πληρεί όλες τις προδιαγραφές του. Το Firmware διατίθεται δωρεάν για download από την ιστοσελίδα της Texas Instruments και περιέχει το Home Automation profile. Η σπουδαιότητα της Z-Stack είναι ότι ο σχεδιαστής δεν χρειάζεται να γράψει από την αρχή έναν εκτενή κώδικα που να υλοποιεί όλες τις τυποποιημένες ανάγκες του

πρωτοκόλλου. Αυτό είναι ήδη έτοιμο, και επομένως ο μηχανικός που αναπτύσσει την εφαρμογή μπορεί απλώς να προσθέσει κώδικα στο επίπεδο εφαρμογής και αν είναι απαραίτητο να κάνει αλλαγές και στα υπόλοιπα επίπεδα. Το Firmware έχει αναπτυχθεί σε ένα compiler της IAR ειδικά για το CC2430 και είναι συμβατό μόνο με αυτόν. Πριν από τον προγραμματισμό του CC2430 είναι απαραίτητο να δώσουμε μια IEEE address στο ολοκληρωμένο. Αυτό γίνεται με το πρόγραμμα της TI SmartRF04 Flash Programmer.



Σχήμα 4.10 Οι μονάδες ZigBee που κατασκευάστηκαν κατά την εκπόνηση της πτυχιακής εργασίας

ΑΚΡΩΝΥΜΙΑ

ACL	Access Control List
AES	Advanced Encryption System
AIB	APS Information Base
AP	Access Point
APL	Application Layer
APS	Application Support sub-layer
APSDE	Application Support sub-layer Data Entity
APSME	Application Support Sub-layer Management Entity
BS	Base Station
BSS	Basic Service Set
BTR	Broadcast Transaction Record
BTT	Broadcast Transaction Table
CAP	Contention Access Period
CFP	Contention Free Period
CCA	Clear Channel Assessment
CPU	Central Processing Unit
CS	Carrier Sense
CSMA-CA	Carrier Sense Multiple Access – Collision Avoidance
DC	Direct Current
DPSK	Differential Phase Shift Keying
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
FCS	Frame Check Sequence
FDD	Frequency Division Duplex
FFD	Full Functions Device
FHSS	Frequency Hopping Spread Spectrum
GTS	Guaranteed Time Slot
IBSS	Independent Basic Service Set
IC	Integrated Circuit
IEEE	Institute of Electrical & Electronics Engineers
IFA	Inverted F Antenna
I/O	Input/Output
IP	Internet Protocol
ISM	Industrial Scientific Medical
LIFS	Long InterFrame Spacing
LNA	Low Noise Amplifier
LQI	Link Quality Indicator
MAC	Medium Access Control Layer
MAN	Metropolitan Area Network
MCPS	MAC Common Part Sub-layer

MCU	MicroController Unit
MFR	MAC Footer
MHR	MAC Header
MLME	MAC Layer Management Entity
MPDU	MAC layer PDU
MSDU	MAC layer Service Data Unit
NIB	Network Information Base
NLDE	Network Layer Data Entity
NLME	Network Layer Management Entity
NWK	Network Layer
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
PA	Power Amplifier
PAN	Personal Area Network
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PD-SAP	PHY Data SAP
PDU	Protocol Data Unit
PHR	PHY Header
PHY	Physical Layer
PIB	PAN Information Base
PiP	Platform in Package
PLME	PHY Layer Management Entity
PMP	Point-to-Multipoint
POS	Personal Operating Space
PPDU	Physical layer PDU
PSDU	PHY Service Data Unit
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RFD	Reduced Functions Device
RSS	Received Signal Strength
RTC	Real Time Clock
RX	Receiver
SAP	Service Access Point
SFD	Start of Frame Delimiter
SFR	Special Function Registers
SHR	Synchronization Header
SIFS	Short InterFrame Spacing
SIG	Senior Interest Group
SNR	Signal-to-Noise Ratio
SoC	System on Chip
SS	Subscriber Station
SW	Switch

TDD	Time Division Duplex
TRX	Transceiver
TX	Transmitter
USART	Universal Synchronous Asynchronous Receive Transmit
USB	Universal Serial Bus
VoIP	Voice over IP
WEP	Wired Equivalent Protocol
Wi Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	Wireless Protected Access
WPAN-LR	Wireless Personal Area Network – Low data Rate
WPAN-MR	Wireless Personal Area Network – Medium data Rate
ZDO	ZigBee Device Object
ZDP	ZigBee Device Profile

ATTRIBUTES ΚΑΙ CONSTANTS ΤΩΝ ΕΠΙΠΕΔΩΝ ΤΟΥ ZIGBEE

PHY Attributes

phyCurrentChannel Δείχνει ποίο από τα 27 ράδιο-κανάλια χρησιμοποιείται εκείνη τη στιγμή ακολουθώντας την αρίθμηση από 0-26.

phyChannelsSupported Αποτελείται από 32 bits και επισημαίνει ποια από τα κανάλια είναι διαθέσιμα και ποια όχι. Τα πρώτα 5 bits είναι μηδέν 0, τα 27 που ακολουθούν αντιστοιχούν στα έγκυρα ράδιο-κανάλια. Όσα είναι στον άσσο 1 συμβολίζουν τα διαθέσιμα κανάλια ενώ αυτά που είναι μηδέν 0 τα μη διαθέσιμα κανάλια. Για παράδειγμα από την ακολουθία 000000000000000000001000011111111111 συμπεραίνουμε ότι τα κανάλια από 0 έως 10 και το 15 είναι ελεύθερα ενώ τα υπόλοιπα είναι κατειλημμένα.

phyTransmitPower Υποδεικνύει την εκπεμπόμενη ισχύ μέσω ενός πεδίου τιμών από 0x00 έως 0xbf. Τα 2 σημαντικότερα bits δείχνουν την απόκλιση από την εκπεμπόμενη ισχύ. Έτσι έχουμε για 00 = ±1 dB, για 01 = ±3 dB και για 10 = ±6 dB. Τα υπόλοιπα 6 bits αποτελούν την τιμή της εκπεμπόμενης ισχύος σε dBm.

phyCCAMode Δείχνει σε ποια από τις τρεις καταστάσεις λειτουργίας βρίσκεται το CCA.

PHY Constants

aMaxPHYPacketSize Είναι το μέγιστο επιτρεπόμενο μέγεθος ενός πακέτου PPDU και ισούται με 127 bytes.

aTurnaroundTime Ο χρόνος που χρειάζεται για αλλαγή από RX σε TX και από TX σε RX.

MAC Attributes

macAckWaitDuration Το μέγιστο χρονικό περιθώριο μετρημένο σε αριθμό συμβόλων κατά το οποίο ο δέκτης θα περιμένει για να λάβει το πακέτο επιβεβαίωσης

macAssociationPermit Δείχνει αν ο Coordinator πρόκειται να επιτρέψει μια σύνδεση παίρνοντας τις τιμές TRUE ή FALSE.

macAutoRequest Δείχνει αν μια συσκευή κάνει αίτηση για να λάβει δεδομένα παίρνοντας τις τιμές TRUE ή FALSE.

macBattLifeExt Αποτελεί ένδειξη για το αν ο Coordinator υποχρεωθεί να περιορίσει τις μεταδόσεις ώστε να παραταθεί η διάρκεια ζωής της μπαταρίας, παίρνοντας τις τιμές TRUE ή FALSE.

macBattLifeExtPeriods Ο αριθμός των περιόδων που κατά τη διάρκειά τους ο δέκτης παραμένει ενεργός όταν βρίσκεται σε κατάσταση μειωμένης κατανάλωσης ισχύος.

macBeaconPayload Περιλαμβάνει τα περιεχόμενα του ωφέλιμου φορτίου ενός Beacon.

macBeaconPayloadLength Είναι το μήκος σε bytes του ωφέλιμου φορτίου ενός Beacon και κυμαίνεται από 0 έως aMaxBeaconPayloadLength.

macBeaconOrder Δείχνει πόσο συχνά εκπέμπεται κάποιο Beacon από ένα Coordinator.

macBeaconTxTime Ο χρόνος κατά τον οποίο μια συσκευή εξέπεμψε το τελευταίο Beacon σε περιόδους συμβόλων.

macBSN Η ακολουθία αριθμών που προστίθεται στο εκπεμπόμενο Beacon

macCoordExtendedAddress Είναι η 64 bit διεύθυνση του Coordinator με τον οποίο σχετίζεται η εν λόγω συσκευή.

macCoordShortAddress Η 16 bit διεύθυνση του Coordinator με τον οποίο σχετίζεται η εν λόγω συσκευή.

macDSN Η ακολουθία αριθμών που προστίθεται στο εκπεμπόμενο πακέτο δεδομένων.

macGTSPermit Δείχνει αν ο PAN Coordinator θα δεχθεί τις αιτήσεις για την παραχώρηση GTS με τις τιμές TRUE ή FALSE.

macMaxCSMABackoffs Ο μέγιστος αριθμός από προσπάθειες για απόκτηση πρόσβασης στο κανάλι που θα επιχειρήσει ο αλγόριθμος CSMA-CA μέχρι να το θεωρήσει κατελημμένο.

macPANId Ο 16 bit κωδικός αναγνώρισης του PAN στο οποίο εργάζεται η εν λόγω συσκευή.

macPromiscuousMode Δείχνει αν το MAC έχει τεθεί σε κατάσταση να δέχεται όλα τα πακέτα του PHY ή όχι, παίρνοντας τις τιμές TRUE ή FALSE.

macRxOnWhenIdle Δείχνει αν το MAC έχει οριστεί ώστε να ενεργοποιεί το κύκλωμα του δέκτη όταν συσκευή είναι ανενεργή παίρνοντας τις τιμές TRUE ή FALSE.

macShortAddress Ο 16 bit κωδικός που χρησιμοποιεί η συσκευή ως αναγνωριστικό στοιχείο στο PAN δίκτυο στο οποίο ανήκει.

macSuperframeOrder Διευκρινίζει το μήκος του Superframe.

macTransactionPersistenceTime Ο μέγιστος χρόνος κατά τον οποίο μια μετάβαση παραμένει αποθηκευμένη στον Coordinator.

macACLEntryDescriptorSet Περιλαμβάνει μια σειρά από στοιχεία που αφορούν παραμέτρους ασφαλείας και περιέχονται στην ACL.

macACLEntryDescriptorSetSize Ο αριθμός των στοιχείων που περιέχονται στην ACL.

macDefaultSecurity Δείχνει αν η συσκευή επιτρέπει την ανταλλαγή δεδομένων με άλλες συσκευές που δεν βρίσκονται στην ACL.

macDefaultSecurityMaterialLength Ο αριθμός των bytes που περιέχονται στην ACLSecurityMaterial.

macDefaultSecurityMaterial Είναι το υλικό που χρησιμοποιείται για προστασία από συσκευές που δεν βρίσκονται στην ACL.

macSecurityMode Δείχνει τον επιλεγμένο τύπο ασφάλειας. Παρακάτω φαίνονται οι τιμές που παίρνει και ο τύπος ασφάλειας στον οποίο ανήκει η καθεμία.

- 0x00 = Unsecured Mode
- 0x01 = ACL Mode
- 0x02 = Secured Mode

MAC Constants

aBaseSlotDuration Ο αριθμός των συμβόλων που συνθέτουν ένα Superframe slot.

aBaseSuperframeDuration Ο αριθμός των συμβόλων που συνθέτουν ένα Superframe.

aExtendedAddress Η 64 bit διεύθυνση της συσκευής.

aMaxBeaconOverhead Ο μέγιστος αριθμός των bytes που προσθέτει το MAC στο ωφέλιμο φορτίο κάθε Beacon.

aMaxBeaconPayloadLength Το μέγιστο μέγεθος του ωφέλιμου φορτίου ενός Beacon σε bytes.

aMaxFrameOverhead Ο μέγιστος αριθμός των bytes που προσθέτει το MAC στο ωφέλιμο φορτίο του χωρίς τη χρήση παραμέτρων ασφαλείας.

aMaxFrameRetries Ο μέγιστος αριθμός προσπαθειών εκπομπής μετά από αποτυχία μετάδοσης.

aMaxLostBeacons Όταν ο αριθμός των συνεχόμενων απολεσθέντων Beacon φθάσει την τιμή της σταθεράς αυτής, η συσκευή λήψης θεωρεί ότι έχασε το συγχρονισμό της με τον αποστολέα.

aMaxMACFrameSize Ο μέγιστος αριθμός των bytes που μπορούν να εκπεμφθούν με το ωφέλιμο φορτίο ενός πακέτου από το MAC.

aMaxSIFSFrameSize Το μέγιστο μέγεθος σε bytes ενός MPDU που μπορεί να συνοδευτεί από ένα SIFS.

aMinCAPLength Ο ελάχιστος αριθμός συμβόλων για το σχηματισμό ενός CAP.

aMinLIFSPeriod Ο ελάχιστος αριθμός συμβόλων για το σχηματισμό μιας LIFS περιόδου

aMinSIFSPeriod Ο ελάχιστος αριθμός συμβόλων για το σχηματισμό μιας SIFS περιόδου.

aNumSuperframeSlots Ο αριθμός των Slots που περιέχονται σε κάθε Superframe.

aUnitBackoffPeriod Ο αριθμός των συμβόλων που αποτελούν το χρονικό διάστημα που χρησιμοποιείται από τον CSMA-CA αλγόριθμο.

NWK Attributes

nwkSequenceNumber Η αριθμητική ακολουθία για την αναγνώριση των εξερχόμενων πακέτων.

nwkPassiveAckTimeout Ο μέγιστος χρόνος σε ms κατά τον οποίο επιτρέπεται επαναμετάδοση δεδομένων που στάλθηκαν μέσω Broadcast

nwkMaxBroadcastRetries Ο μέγιστος αριθμός των προσπαθειών επανεκπομπής που μπορούν να γίνουν μετά από αποτυχημένη μετάδοση.

nwkNeighborTable Οι τρέχουσες καταχωρήσεις στον πίνακα NeighborTable

nwkNetworkBroadcastDeliveryTime Ο χρόνος που απαιτείται ώστε ένα πακέτο που στάλθηκε κατά Broadcast να διασχίσει ολόκληρο το δίκτυο.

nwkReportConstantCost

nwkRouteDiscoveryRetriesPermitted Μετά από μια αποτυχημένη προσπάθεια για Route Discovery, το Attributes αυτό δείχνει πόσες προσπάθειες μπορούν να γίνουν ξανά.

nwkRouteTable Οι τρέχουσες καταχωρήσεις στον πίνακα όπου αποθηκεύονται οι διαδρομές επικοινωνίας (Routes) μεταξύ των συσκευών ενός δικτύου.

nwkMaxSourceRoute Ο μέγιστος αριθμός μεταβάσεων σε μια διαδρομή επικοινωνίας.

nwkUpdateId Ανακαλύπτει τις ρυθμίσεις λειτουργίας του δικτύου.

nwkTransactionPersistenceTime Ο μέγιστος χρόνος κατά τον οποίο παραμένει αποθηκευμένη μια μετάδοση.

nwkNetworkAddress Η διεύθυνση που έχει μια συσκευή για να επικοινωνεί με το δίκτυό της.

nwkStackProfile Ο αριθμός αναγνώρισης του Profile που χρησιμοποιείται στην συσκευή.

nwkBroadcastTransactionTable Οι τρέχουσες καταχωρήσεις στο Broadcast Transaction Table.

nwkGroupIDTable Διατηρεί τον πίνακα με το σύνολο των ID (αριθμών ταυτοποίησης) των Group στα οποία ανήκει η συσκευή.

nwkExtendedPANID Ο αριθμός PAN ID του δικτύου στο οποίο ανήκει η πτυχιακή.

nwkPANId Αυτό το attribute παίρνει την ίδια τιμή με το macPANId.

nwkTxTotal Δείχνει το σύνολο των μεταδόσεων που έχουν γίνει. Για κάθε νέα μετάδοση αυξάνεται κατά 1.

NWK Constants

nwkCoordinatorCapable Δείχνει αν η συσκευή μπορεί να γίνει coordinator.

nwkDefaultSecurityLevel Ο προεπιλεγμένος βαθμός ασφαλείας.

nwkDiscoveryRetryLimit Ο μέγιστος αριθμός των Route Discovery που μπορούν να ξανά γίνουν.

nwkMinHeaderOverhead Ο ελάχιστος αριθμός των bytes που μπορεί να προστεθεί από το επίπεδο δικτύου στο NSDU.

nwkProtocolVersion Η έκδοση του ZigBee πρωτοκόλλου στη συσκευή.

nwkRouteDiscoveryTime Ο χρόνος σε ms μέχρι να τελειώσει το Route Discovery.

nwkMACFrameOverhead Το μέγεθος του MAC header που χρησιμοποιείται από το NWK.

APS Attributes

apsBindingTable Το σύνολο των καταχωρήσεων στον πίνακα Binding.

apsDesignatedCoordinator Είναι Boolean τιμή και γίνεται TRUE αν η συσκευή πρόκειται να γίνει Coordinator και FALSE αν όχι.

apsUseExtendedPANID Η 64-bit διεύθυνση ενός δικτύου.

apsGroupTable Το σύνολο των καταχωρήσεων στον πίνακα με τα Group συσκευών.

apsNonmemberRadius Η τιμή της παραμέτρου NonmemberRadius όταν γίνεται χρήση της μετάδοσης κατά Multicast.

apsInterframeDelay Όταν ένα πακέτο έχει πολύ μεγάλο μήκος τότε χωρίζεται σε τμήματα τα οποία μεταδίδονται το ένα μετά το άλλο. Όταν σταλεί ένα τμήμα ακολουθεί μια χρονική καθυστέρηση και στη συνέχεια στέλνεται ένα άλλο. Αυτή η χρονική καθυστέρηση μεταξύ των μεταδόσεων είναι το apsInterframeDelay.

apsLastChannelEnergy Οι μετρήσεις για τα επίπεδα ενέργειας στο κανάλι.

apsLastChannelFailureRate Το ποσοστό αποτυχημένων μεταδόσεων σε ένα κανάλι.

APS Constants

apscMaxFrameRetries Ο μέγιστος αριθμός από επιτρεπόμενες προσπάθειες επανεκπομπής.

apscAckWaitDuration Ο μέγιστος χρόνος αναμονής μέχρι να φτάσει το σήμα επιβεβαίωσης.

apscInterframeDelay Η χρονική καθυστέρηση μεταξύ των τμημάτων ενός πακέτου κατά την αποστολή τους.

apscMinHeaderOverhead Ο ελάχιστος αριθμός των bytes που προσθέτει το APS στο ASDU.

Βιβλιογραφία

802.15.4 [Εγγραφο] / συντάκτης IEEE. - [s.l.] : IEEE, 2003.

Hands-on Zigbee [Βιβλίο] / συγγραφέας Eady Fread. - [s.l.] : Newnes, 2007.

Programming Embedded Systems in C & C++ [Βιβλίο] / συγγραφέας BARR MICHAEL. - [s.l.] : O'REILLY, 1999.

WiFi Handbook [Βιβλίο] / συγγραφείς Frank Ohrtman, Konrad Roeder. - [s.l.] : McGraw Hill, 2003.

WI-FI, BLUETOOTH, ZIGBEE and WiMAX [Βιβλίο] / συγγραφείς H. LABIOD, H. AFIFI, C. DE SANTIS. - [s.l.] : Springer, 2007.

WiMAX HANDBOOK [Βιβλίο] / συγγραφέας OHRTMAN FRANK. - [s.l.] : McGraw HILL, 2005.

Zigbee Specification [Εγγραφο] / συντάκτης Alliance ZigBee. - [s.l.] : ZigBee Alliance, 2007.

ZIGBEE WIRELESS NETWORKING [Βιβλίο] / συγγραφέας Gislason Drew. - [s.l.] : Newnes, 2008.

ZIGBEE WIRELESS NETWORKS AND TRANSCEIVERS [Βιβλίο] / συγγραφέας Farahani Shahin. - [s.l.] : Newnes, 2008.

Δικτυακοί τόποι

- www.zigbee.org
- www.ti.com
- www.fractus.com
- www.anaren.com
- www.freescale.com
- www.atmel.com
- www.microchip.com
- www.maxstream.fr