Α.Τ.Ε.Ι. ΠΕΙΡΑΙΑ

Μ.Η.Υ.Σ

Καθηγητής: Σ. ΑΛΑΤΣΑΘΙΑΝΟΣ

Εφαρμογές του ZigBee

Μπελόκας Ανδρέας ΑΜ:40443

Αθήνα, Ιούνιος 2014

Περιεχόμενα

Εισαγωγη.....σελ.3

1.Πρωτοκόλλο ZigBee.....σελ.5

1.1 Έννοιες του πρωτοκόλλου.....σελ.5
1.1.1 Services.....σελ.5
1.1.2 Primitives.....σελ.5
1.1.3 Constants & Attributes.....σελ.6
1.1.4 Binding.....σελ.6
1.1.5 Energy Detection (ED).....σελ.6
1.1.6 Carrier Sense (CS).....σελ.6
1.1.7 Link Quality Indicator (LQI).....σελ.7
1.1.8 Clear Channel Assessment (CCA).....σελ.7
1.1.9 Beacon.....σελ.7
1.1.10 Superframe.....σελ.8
1.1.11 Route Discovery.....σελ.8
1.1.12 Device Discovery.....σελ.8
1.2 Τα επίπεδα του ZigBee.....σελ.8
1.2.1 Physical Layer.....σελ.9
1.2.1.1 PHY Services.....σελ.10
1.2.1.2 PPDU.....σελ.11
1.2.2 MAC Layer.....σελ.11
1.2.2.1 MAC Services.....σελ.11
1.2.2.2 MPDU.....σελ.15
1.2.3 Network Layer.....σελ.15
1.2.3.1 NWK Services.....σελ.16
1.2.3.2 Unicast.....σελ.18
1.2.3.3 Multicast.....σελ.18
1.2.3.4 Broadcast.....σελ.19
1.2.3.5 NWK PDU.....σελ.19
1.2.4 Application Layer.....σελ.20
1.2.4.1 Application Framework.....σελ.21
1.2.4.2 ZDO.....σελ.22
1.2.4.3 APL Services - APS.....σελ.22
1.2.4.4 APL PDU.....σελ.24

2. ZIGBEE ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ.....σελ.25
2.1 ZigBee Transceivers.....σελ.25
2.1.1 Atmel.....σελ.25
2.1.2 Freescale.....σελ.26
2.1.3 MaxStream.....σελ.27
2.1.4 Microchip.....σελ.27
2.1.5 Texas Instruments.....σελ.28
2.2 SoC CC2430.....σελ.29
2.2.1 DMA.....σελ.29
2.2.2 WATCHDOG TIMER.....σελ.29
2.2.3 8051 CPU.....σελ.30
2.2.4 MEMORY ARBITRATOR.....σελ.30

2.2.5 USARTs....σελ.30
2.2.6 TIMERs....σελ.31
2.2.7 ADC....σελ.31
2.2.8 AES....σελ.31
2.2.9 ON-CHIP VOLTAGE REGULATOR....σελ.31
2.2.10 TRANSCEIVER....σελ.32

3. ZigBee....σελ.33
3.1 Η στοίβα πρωτοκόλλων του ZigBee....σελ.33
3.2 Τύποι συσκευών....σελ.34
3.3 Τοπολογίες δικτύων....σελ.34
3.4 Φυσικό επίπεδο (Physical layer, PHY)....σελ.36
3.4.1 Χαρακτηριστικά καναλιών και διαμορφωσης....σελ.36
3.4.2 Πρόσβαση στο κάναλι....σελ.36
3.4.3 Υπηρεσίες δεδομένων....σελ.37
3.5 Επίπεδο ελέγχου πρόσβασης στο μέσο (Medium access control layer, MAC)....σελ.37
3.5.1 Υπηρεσίες δεδομένων....σελ.38
3.5.2 Πλαίσια MAC....σελ.38
3.5.2.1. Πεδίο έλεγχου πλαισίου....σελ.39
3.5.2.2. Πεδίο αριθμού ακολουθίας....σελ.39
3.5.2.3. Πεδία διευθύνσεων....σελ.39
3.5.2.4. Ακολουθία ελέγχου πλαισίου (FCS)....σελ.40
3.5.2.5. Ωφέλιμο φορτίο MAC....σελ.40
3.5.3 Λειτουργίες επιπέδου MAC....σελ.40

3.6 Επίπεδο δικτύου (Network layer, NWK)....σελ.41
3.6.1 Πλαίσια επιπέδου δικτύου....σελ.41
3.6.2 Πίνακες γειτόνων....σελ.43
3.6.3 Σύνδεση σε ένα δίκτυο και αποχώρηση από αυτό....σελ.43
3.6.4. Δημιουργία ενός δικτύου....σελ.44
3.6.5. Δρομολόγηση πλαισίων....σελ.45
3.6.6. Ασφάλεια....σελ.46
3.7 Επίπεδο εφαρμογών (Application layer, APL)....σελ.47
3.7.1. Υποεπίπεδο υποστήριξης εφαρμογών (Application support sublayer, APS)....σελ.48
3.7.1.1.Υπηρεσίες δεδομένων υποεπιπέδου APS....σελ.48
3.7.1.2. Υπηρεσίες διαχείρισης υποεπιπέδου APS....σελ.49
3.7.1.3. Πλαίσια υποεπιπέδου APS....σελ.49
3.7.1.4.Μετάδοση, παραλαβή και επιβεβαίωση πλαισίων....σελ.50
3.7.1.5.Ασφάλεια στο υποεπίπεδο APS....σελ.52
3.7.2. Πλαίσιο εφαρμογών (Application framework, AF)....σελ.52
3.7.2.1. Τα προφίλ του ZigBee....σελ.53
3.7.2.2.Πλαίσια εντολών AF (Application framework)....σελ.53
3.7.3. Αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO)....σελ.54

ΕΙΣΑΓΩΓΗ

Το πρωτόκολλο αυτό δημιουργήθηκε από έναν οργανισμό γνωστό ως Zigbee Alliance που αποτελείται από μεγάλες εταιρίες και βιομηχανίες του χώρου που το υποστηρίζουν, ως ένα πρότυπο πολύ χαμηλού κόστους, πολύ χαμηλής κατανάλωσης, αμφίδρομο, ασύρματης επικοινωνίας.
Σημαντικότερες χρήσεις του θα είναι σε ηλεκτρικές και ηλεκτρονικές συσκευές, αυτοματισμούς, εργοστασιακό έλεγχο, περιφερειακά υπολογιστών, εφαρμογές ιατρικών αισθητήρων, παιχνίδια κ.α.
Το Zigbee είναι σχεδιασμένο έτσι ώστε να μπορεί να ενσωματωθεί σε ένα πλήθος συσκευών στο σπίτι ή το γραφείο, για παράδειγμα σε φωτισμούς, διακόπτες, εισόδους και ηλεκτρικές συσκευές. Αυτές οι συσκευές μπορούν να αλληλεπιδράσουν χωρίς την χρήση καλωδιώσεων και μπορούν να ελεγχθούν από μία και μόνη συσκευή η οποία μπορεί να είναι ένα κινητό τηλέφωνο ή ένα τηλεχειριστήριο. Παρά το γεγονός ότι η τεχνολογία που εισάγει δεν είναι επαναστατική, προχωράει ένα βήμα παραπέρα από τις παραδοσιακές ασύρματες επικοινωνίες όπως ο απλός τηλεχειρισμός για το άνοιγμα της γκαραζόπορτας ή το άναμμα του φωτισμού. Το σημείο που διαφοροποιείται από αυτές τις εφαρμογές είναι το γεγονός ότι το πρωτόκολλο 802.15.4 επιτρέπει την επικοινωνία δύο δρόμων μεταξύ όλων των συσκευών στις οποίες ενσωματώνεται, δηλαδή τα φώτα, τους διακόπτες, τους θερμοστάτες, τον κλιματισμό και λοιπά.
Μπορεί να καλύψει μεγάλους χώρους, λόγω της αυξημένης εμβέλειάς του και μπορεί να διαχειριστεί πολλούς αισθητήρες που εκτελούν διαφορετικές εργασίες ταυτόχρονα.
Το Zigbee έχει σχεδιαστεί για να μεταδίδει δεδομένα σε χαμηλές ταχύτητες και έτσι είναι λιγότερο ενεργοβόρο. Ανάλογα με την εφαρμογή και τον τύπο της μπαταρίας που θα χρησιμοποιηθεί, η αυτονομία ενός συστήματος με ασύρματη δικτύωση που κάνει χρήση αυτού του πρωτοκόλλου μπορεί να φτάσει ακόμη και τα 10 χρόνια.
Ένα δίκτυο βασισμένο στο Zigbee χρησιμοποιεί ψηφιακούς πομπούς για να επικοινωνήσει μεταξύ των διαφορετικών συσκευών που βρίσκονται διάσπαρτες στον χώρο. Μία από τις συσκευές πρέπει να λειτουργεί ως συντονιστής (coordinator) για να γνωρίζει όλους τους κόμβους του δικτύου και να διαχειρίζεται την πληροφορία που ανταλλάσσεται μεταξύ των κόμβων και του δικτύου συνολικά. Σε ένα δίκτυο Zigbee εκτός από τον συντονιστή, άλλες συσκευές δρουν ως δρομολογητές και άλλες ως οι συσκευές που αλληλεπιδρούν με τον φυσικό κόσμο.
Τα δίκτυα Zigbee μπορούν να λειτουργήσουν είτε σε λειτουργία περιοδικής εκπομπής ενός σήματος συντονισμού, είτε σε λειτουργία μη εκπομπής. Στην πρώτη περίπτωση ένα σήμα αποστέλλεται περιοδικά από το συντονιστή, το οποίο σαν επακόλουθο έχει να «ξυπνά» όλες τις συσκευές του δικτύου οι οποίες πρέπει να ενημερώσουν τον συντονιστή αν έχουν κάποιο μήνυμα να αποστείλουν. Εάν όχι, τότε η κάθε συσκευή επιστρέφει σε κατάσταση αναμονής. Στην άλλη περίπτωση, όταν δεν υπάρχει αυτή η περιοδική εκπομπή του σήματος από τον συντονιστή, το δίκτυο το οποίο δημιουργείται είναι λιγότερο συντονισμένο, καθώς η κάθε τερματική συσκευή εκπέμπει ένα σήμα το οποίο θα πρέπει να φτάσει στο συντονιστή περνώντας από όλους τους ενδιάμεσους κόμβους του δικτύου. Σε αυτή την περίπτωση, ο συντονιστής θα πρέπει να είναι συνεχώς σε λειτουργία για να είναι έτοιμος σε κάθε σήμα που μπορεί να ληφθεί, καταναλώνοντας έτσι μεγαλύτερα ποσά ενέργειας.

Σε κάθε περίπτωση όμως, ένα δίκτυο αποτελούμενο από συσκευές που ενσωματώνουν τοπρωτόκολλο IEEE802.15.4 διατηρεί την κατανάλωση ισχύος σε χαμηλά επίπεδα διότι η πλειοψηφία των συσκευών του δικτύου παραμένουν ανενεργές για μεγάλα χρονικά διαστήματα.
Σύγκριση του πρωτοκόλλου ZigBee IEEE802.15.4 με άλλα ασύρματα πρωτόκολλα, στον πίνακα παρακάτω.

Χαρακτηριστικά ασυρμάτων πρωτοκολλών για δίκτυα WPAN

	ZigBee	802.11 (Wi-Fi)	Bluetooth	UWB	Wireless USB	IR Wireless
Data Rate	20, 40, και 250 Kbps	11 & 54 Mbps	1 Mbps	100-500 Mbps	62.5 Kbps	20-40 Kbps 115 Kbps 4 & 16 Mbps
Εμβέλεια	10-100 μέτρα	50-100 μέτρα	10 μέτρα	<10 μέτρα	10 μέτρα	<10 μέτρα (οπτική επαφή)
Τοπολογία δικτύου	Ad-hoc, peer to peer, star, ή mesh	Point to hub	Ad-hoc, πολύ μικρά δίκτυα	Point to point	Point to point	Point to point
Συχνότητα λειτουργίας	868 MHz (Ευρώπη) 900-928 MHz (Β.Α.), 2.4 GHz (παγκόσμια)	2.4 και 5 GHz	2.4 GHz	3.1-10.6 GHz	2.4 GHz	800-900 nm
Πολυπλοκότητα	Χαμηλή	Υψηλή	Υψηλή	Μέση	Χαμηλή	Χαμηλή
Κατανάλωση ισχύος	Πολύ χαμηλή (στόχος η χαμηλή κατανάλωση)	Υψηλή	Μέση	Χαμηλή	Χαμηλή	Χαμηλή
Ασφάλεια	128 AES και application layer security		64, 128bit encyption			
Άλλες πληροφορίες	Οι συσκευές μπορούν να ενταχθούν στο δίκτυο σε λιγότερο από 30ms	Οι συσκευές συνδέονται σε 3-5 sec	Η σύνδεση μια συσκευής απαιτεί έως 10 sec			
Τυπικές εφαρμογές	Βιομηχανικός έλεγχος, δίκτυα αισθητήρων, αυτοματισμοί κτιρίων, οικιακοί αυτοματισμοί, παιχνίδια	Wireless LAN, ευρυζωνική σύνδεση στο Internet	Ασύρματα δίκτυα μεταξύ συσκευών όπως τηλέφωνα, PDA, laptops, ακουστικά	Μετάδοση βίντεο, υπηρεσίες οικιακής νυχαγωγίας	Σύνδεση περιφερειακών υπολογιστών	Τηλεχειρισμοί, PC, PDA, τηλέφωνα

Ιστορικά Στοιχεία:
Δίκτυα παρόμοιας μορφής με το ZigBee ξεκίνησαν να προτείνονται από το 1998, όταν έγινε αντιληπτό ότι το WiFi και το Bluetooth δεν μπορούν να χρησιμοποιηθούν σε αρκετές εφαρμογές. Υπήρχε η ανάγκη για αυτοοργανωτικό επί τούτω (ad-hoc) ασύρματο δίκτυο. Το IEEE 802.15.4 πρότυπο ολοκληρώθηκε τον Μάιο του 2003. Οι ZigBee προδιαγραφές επικυρώθηκαν στις 14 Δεκεμβρίου 2004. Η διαθεσιμότητα του πρωτοκόλλου 1.0 στο κοινό έγινε στις 13 Ιουνίου 2005 με την ονομασία "Προδιαγραφή ZigBee 2004". Η ZigBee Alliance, ανακοίνωσε ότι τον Οκτώβριο του 2004 τα μέλη της είχαν διπλασιαστεί με πάνω από 100 εταιρίες σε 22 χώρες. Τον Απρίλιο του 2005 είχε 150 μέλη και τον Δεκέμβριο 200. Τον Οκτώβριο του 2006 ανακοινώθηκε και δόθηκε το βελτιωμένο πρότυπο με την ονομασία "Προδιαγραφή ZigBee 2006".
Στις 19 Οκτωβρίου του 2007, ολοκληρώθηκαν οι βελτιωμένες προδιαγραφές του ZigBee με όνομα "Προδιαγραφή ZigBee 2006" και "ZigBee PRO".

Κεφάλαιο 1ο

ΠΡΩΤΟΚΟΛΛΟ ZIGBEE

1.1 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.

1.1.1 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.

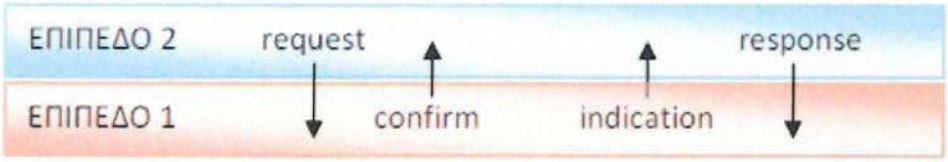
1.1.2 Primitives

Κάθε Service αποτελείτε 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 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 1.1 Εκτέλεση των primitives

1.1.3 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 άλλα η τιμή τους μπορεί να μεταβληθεί μόνο από εκείνο στο οποίο ανήκουν.

1.1.4 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.

1.1.5 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.

1.1.6 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.

1.1.7 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.

1.1.8 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 κατωφλίου που έχει οριστεί από τον κατασκευαστή τότε το κανάλι θεωρείτε ελεύθερο.
- Κατάσταση 2 Γίνεται χρήση μόνο του CS και το κανάλι θεωρείτε 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 ιδίου τύπου με εκείνο του πομπού το κανάλι θεωρείτε κατειλημμένο.
    - ❖ Αν το επίπεδο ενέργειας είναι υψηλότερο από το κατώφλι **Η΄** αν το σήμα είναι ιδίου τύπου με εκείνο του πομπού το κανάλι θεωρείτε κατειλημμένο.

1.1.9 Beacon

Το Beacon είναι ένα σήμα που αποστέλλεται από τον PAN coordinator για να συγχρονίσει όλες τι 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.

1.1.10 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 τρείς 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, άλλα 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.

1.1.11 Route Discovery

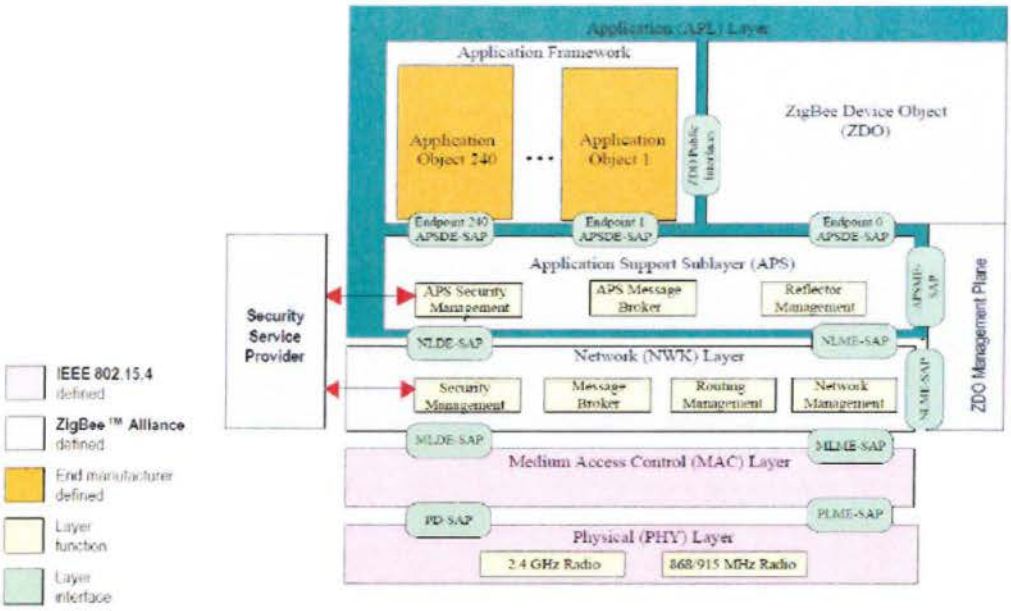
Σε ένα ZigBee δίκτυο οι συσκευές συνεργάζονται για να βρουν τις πιο σύντομες διαδρομές (routes) που μπορούν να εξασφαλίσουν την μεταξύ τους επικοινωνία. Αυτή η μέθοδος είναι το Route Discovery.

1.1.12 Device Discovery

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

1.2 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 1.2 δείχνει σε λεπτομέρεια τα επίπεδα και τα υπό-επίπεδα τα οποία και αναλύονται στη συνέχεια της ενότητας αυτής.



Σχήμα 1.2 Τα επίπεδα του ZigBee. Πηγή «TSC-ZigBee-Specification»

1.2.1 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 τρείς 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 Fc = 868.3 MHz για k = 0, Fc = 906 + 2(k - 1) MHz για k = 1, 2,…, 10 και Fc = 2405 + 5(k - 11) MHz για k = 11, 12,..., 26.

1.2.1.1 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 καλείτε 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 ανιχνευτικέ, 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.

1.2.1.2 PPDU

Η Δομή ενός πακέτου όπως διαμορφώνεται στο φυσικό επίπεδο φαίνεται στο σχήμα 1.3 . 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 1.3 PPDU

1.2.2 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

1.2.2.1 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 MLMESAP 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 MCPSDATA. 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 λόγο συσκευή να συνδεθεί με τον Coordinator του ZigBee δικτύου. Μόλις η διαδικασία ολοκληρωθεί επιτυχώς δημιουργείται το MLMEASSOCIATE.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 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.
  - **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 0xfffe 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-RXENABLE. 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 MLMEPOLL.request δεν είναι έγκυρη ή βρίσκεται εκτός του πεδίου τιμών που έχει οριστεί.

1.2.2.2 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 σηματοδοσία 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 1.4 MPDU

1.2.3 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.

1.2.3.1 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-NETWORKDISCOVERY.confirm φέροντας πληροφορίες για τα δίκτυα που βρέθηκαν μέσω της κατάστασης στην οποία έχει τεθεί. Η κατάσταση αυτή είναι πάντα ίδια με εκείνη του MLME-SCAN.confirm .
- **NLME-NETWORK-FORMATION** Το NLME-NETWORK-FORMATION.request παράγεται όταν επιθυμούμαι η εν λόγο 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-NETWORKFORMATION.
  confirm γίνεται «STARTUP_FAILURE». Αν δεν προκύψουν σφάλματα και το δίκτυο σχηματιστεί, επιστρέφεται το NLME-NETWORKFORMATION.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-EDSCAN. 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-EDSCAN.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 NLMELEAVE.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 κατάσταση 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 NLMESYNC. confirm θα είναι ίδια με εκείνη που επιστρέφεται από το MLMEPOLL. 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 MLMESYNC.request με την παράμετρο TrackBeacon σε FALSE/TRUE. Το NLMESYNC.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 NLMEROUTE- 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».

1.2.3.2 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.

1.2.3.3 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 nonmember 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.

1.2.3.4 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.

1.2.3.5 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 1.5 NPDU

1.2.4 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

1.2.4.1 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 φωτός 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).

1.2.4.2 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.

1.2.4.3 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 λόγο 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-ADDGROUP.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».

1.2.4.4 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 1.5 APDU

Κεφάλαιο 2°

ZIGBEE ΤΕΧΝΟΛΟΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

2.1 ZigBee Transceivers

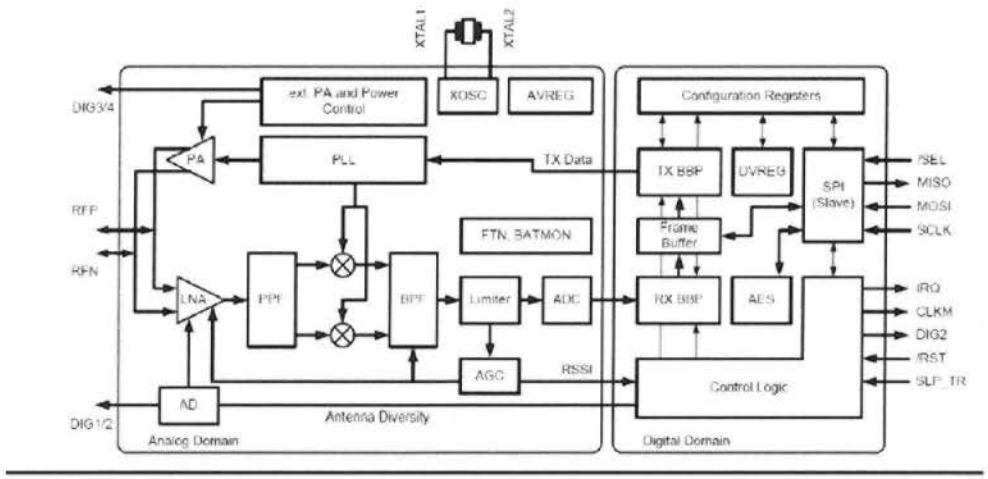
Πολλές εταιρείες μέλη της ZigBee Alliance αναπτύσσουν ολοκληρωμένα κυκλώματα και μονάδες (modules) που υλοποιούν το ZigBee πρωτόκολλο όπως θα δούμε στις υποενότητες που ακολουθούν. Συνεχώς βγαίνουν νέα προϊόντα για να καλύψουν πιο απαιτητικές εφαρμογές ή για να διευκολύνουν τους μηχανικούς κατά την υλοποίηση. 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.

2.1.1 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:

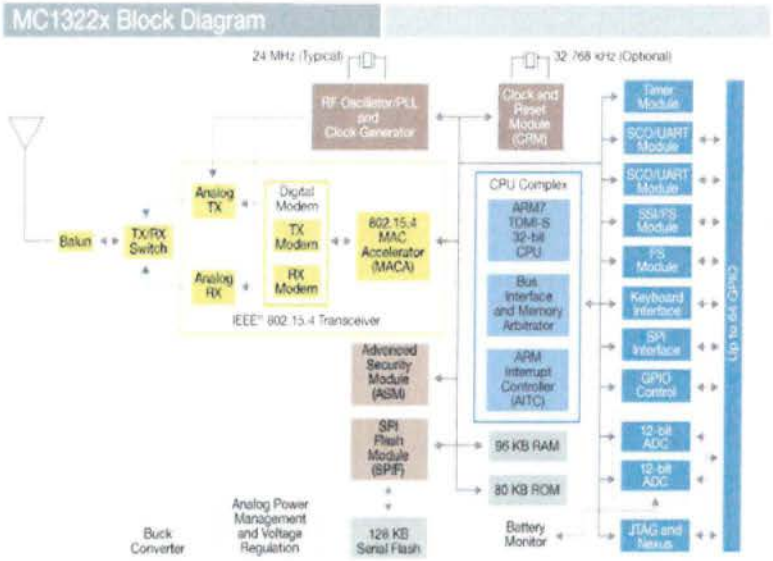
- SLEEP = 0.02A
- TRX_OFF = 0.4 mA
- RX_ON = 12.3 mA
- BUSY_TX = 14mA (max at +3 dBm)

Στο σχήμα 2.1 φαίνονται όλα τα στοιχεία που συνθέτουν τις δύο βαθμίδες.



2.1.2 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 2.2 . Όλα σε ένα LGA κέλυφος 9.5mm x 9.5mm 99 ακροδεκτών.



Σχήμα 2.2

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 μA (max)

Το IC περιέχει και όλους τους απαραίτητους πυκνωτές απόζευξης.

2.1.3 MaxStream

Η MaxStream έχει τα modules XBEE και XBEE PRO (σχήμα 2.3). 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.

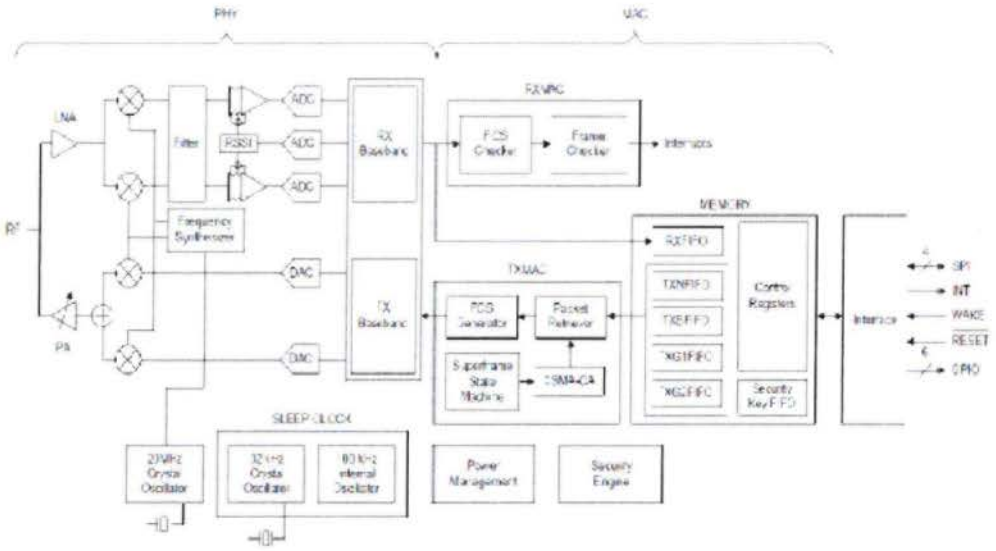
Σχήμα 2.3

2.1.4 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 μA

Όλες οι βαθμίδες του IC φαίνονται λεπτομερώς στο σχήμα 2.4

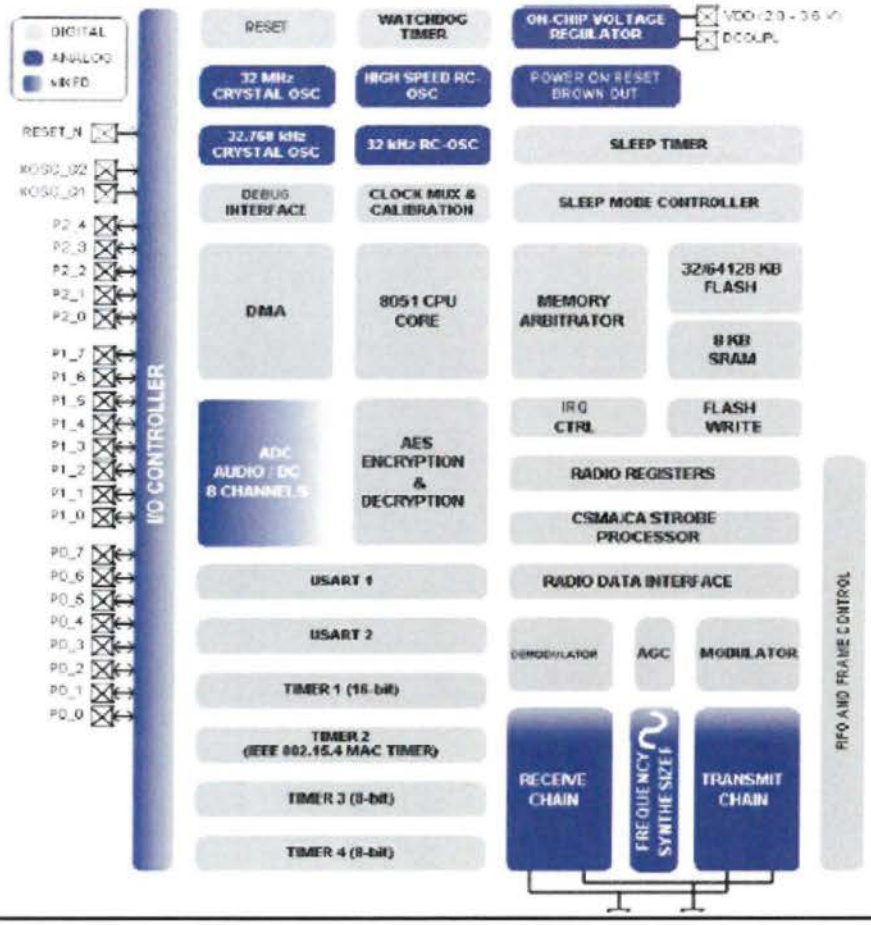


2.1.5 Texas Instruments

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 Μίκρο-ελεγκτή 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 μA και σε stand-by mode όπου μπορεί να τεθεί σε λειτουργία μόνο από εξωτερικά interrupts είναι 0.3 μA.

2.2 SoC CC2430

Στο σχήμα 2.5 φαίνεται το αναλυτικό μπλοκ διάγραμμα του CC2430. Στη συνέχεια περιγράφεται κάθε βαθμίδα του.



2.2.1 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.

2.2.2 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.

2.2.3 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.

2.2.4 MEMORY ARBITRATOR

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

2.2.5 USARTs

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

2.2.6 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.

2.2.7 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.

2.2.8 AES

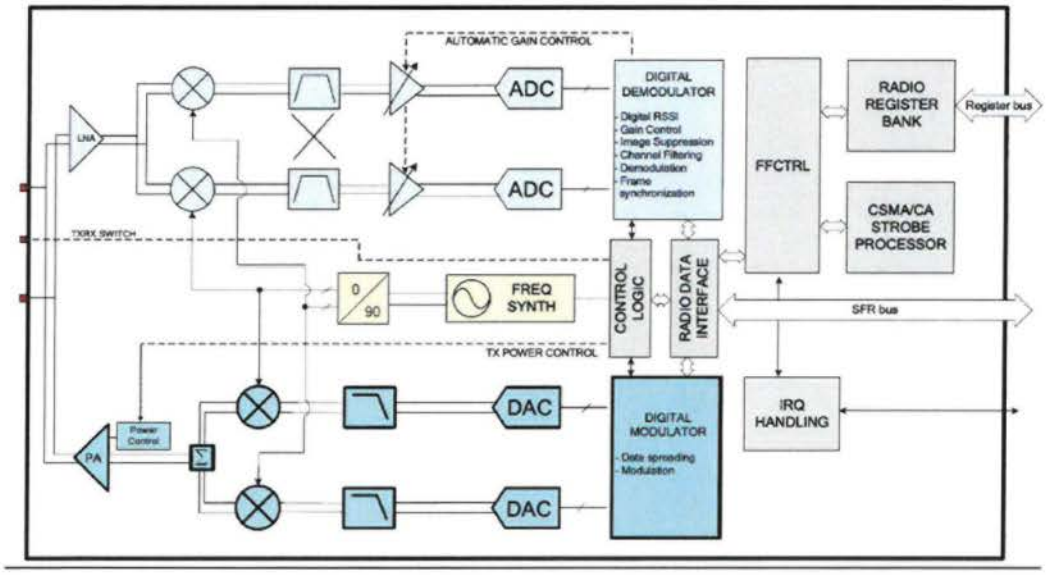
Ο AES επεξεργαστής είναι υπεύθυνος για την κρυπτογράφηση των δεδομένων. Με την ύπαρξή του αποσυμφορίζεται η CPU αφού δεν χρειάζεται να τρέξει η ίδια τους αλγόριθμους κρυπτογράφησης.

2.2.9 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.

2.2.10 TRANSCEIVER

Τα μπλόκ RADIO REGISTERS, RADIO DATA INTERFACE, RECEIVE CHAIN, TRANSMIT CHAIN, FREQUENCY SYNTHESIZER, CSMA-CA STROBE PROCCESSOR, AGC, DEMODULATOR και MODULATOR αποτελούν την Βαθμίδα του πομποδέκτη. Στο σχήμα 2.6 απεικονίζεται η βαθμίδα του πομποδέκτη με μεγαλύτερη λεπτομέρεια. Κατά την εκπομπή το σήμα διαμορφώνεται από τον digital modulator με OQPSK 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 2.6 Διάγραμμα του πομποδέκτη Πηγή «CC2430 datasheet»

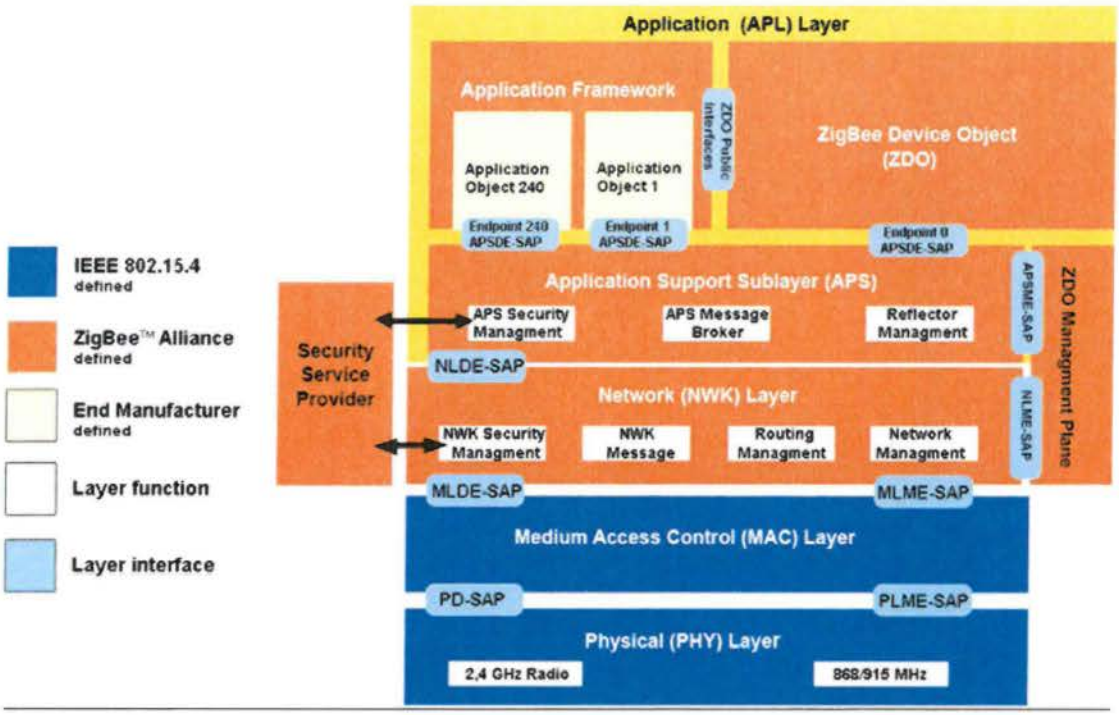
Κεφάλαιο 3ο

ZigBee

3.1 Η στοίβα πρωτοκόλλων του ZigBee

Η στοίβα πρωτοκόλλων του ZigBee αποτελείται από 4 επίπεδα. Κάθε επίπεδο εκτελεί ένα συγκεκριμένο σύνολο λειτουργιών και παρέχει τις υπηρεσίες του στο ανώτερο επίπεδο μέσω μιας διεπαφής που ονομάζεται σημείο πρόσβασης υπηρεσιών (service access point, SAP). Τα 4 επίπεδα της στοίβας πρωτοκόλλων του ZigBee (σχήμα 3.1.1) είναι τα παρακάτω:

- Το φυσικό επίπεδο (Physical layer, PHY) που είναι υπεύθυνο για την ενεργοποίηση και απενεργοποίηση του πομποδέκτη, τη μετάδοση και λήψη δεδομένων, την ανίχνευση ενέργειας στο κανάλι, την εκτίμηση της κατάστασης των καναλιών για την πολλαπλή πρόσβαση με ανίχνευση φέροντος και με αποφυγή συγκρούσεων (CSMA-CA) και τη μέτρηση της ποιότητας των λαμβανομένων πακέτων.
- Το επίπεδο ελέγχου πρόσβασης στο μέσο (Medium access control layer, MAC) που παρέχει υπηρεσίες μεταφοράς δεδομένων και διαχείρισης. Είναι υπεύθυνο για την πρόσβαση στο κανάλι, για τη διαχείριση των χρονοσχισμών και για την παροχή μιας αξιόπιστης σύνδεσης μεταξύ δύο επιπέδων MAC. Επιπρόσθετα παρέχει τα μέσα για την εφαρμογή διαφόρων μηχανισμών ασφάλειας. Το επίπεδο δικτύου (Network layer, NWK) που είναι υπεύθυνο για τη δημιουργία του δικτύου, για την είσοδο και την έξοδο μία συσκευής από ένα δίκτυο, για την ασφάλεια και για τη δρομολόγηση των μεταδιδόμενων πακέτων.
- Το επίπεδο εφαρμογών (Application layer, APL) που περιλαμβάνει το υποεπίπεδο υποστήριξης εφαρμογών (Application support sublayer, APS), το πλαίσιο εφαρμογών (Application framework, AF), τα αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO) και τις καθορισμένες από τον κατασκευαστή εφαρμογές. Το υποεπίπεδο APS είναι υπεύθυνο για τη σύνδεση δύο συσκευών βάση των αναγκών και των υπηρεσιών τους και για την αποστολή δεδομένων μεταξύ τους. Τα ZDO είναι αυτά που καθορίζουν το ρόλο της κάθε συσκευής στο δίκτυο και το επίπεδο ασφάλειας. Επίσης συμβάλλουν στην ανίχνευση των συσκευών σε ένα δίκτυο και στον προσδιορισμό των υπηρεσιών που αυτές παρέχουν. Το πλαίσιο εφαρμογών είναι το περιβάλλον στο οποίο φιλοξενούνται οι εφαρμογές μέσα σε μία συσκευή ZigBee.



Σχήμα 3.1.1: Η στοίβα πρωτοκόλλων του ZigBee

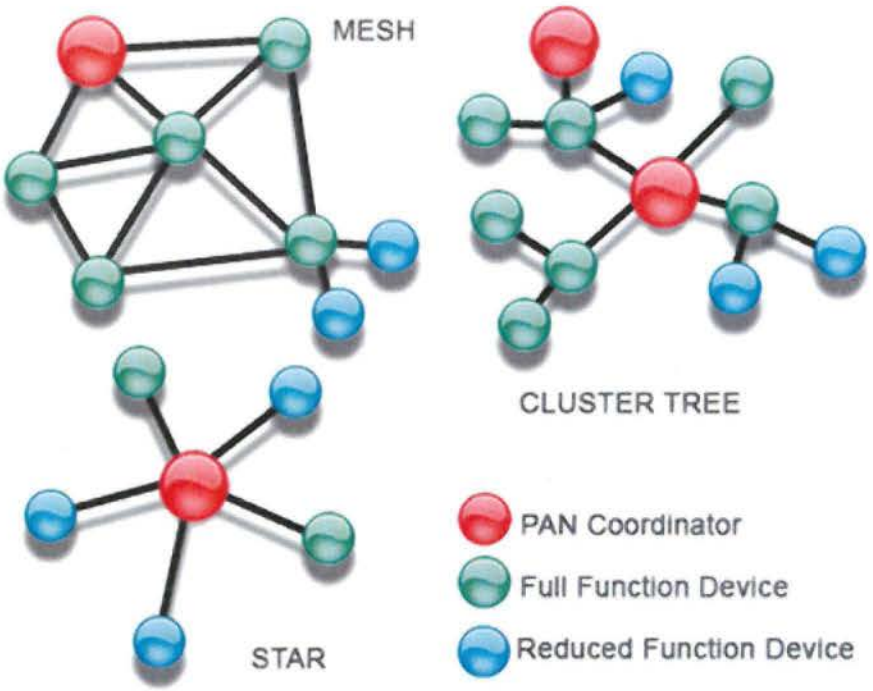
3.2 Τύποι συσκευών

Σε ένα δίκτυο που λειτουργεί με βάση τη στοίβα πρωτοκόλλων του ZigBee, οι συσκευές μπορούν να διακριθούν σε πλήρους λειτουργίας (full-function device , FFD) και μειωμένης λειτουργίας (reduced-function device, RFD). Σε κάθε δίκτυο υπάρχει πάντοτε μία FFD που έχει το ρόλο του συντονιστή του δικτύου (PAN coordinator). Οι FFDs μπορούν να επικοινωνήσουν με όλες τις άλλες συσκευές, ενώ οι RFDs μόνο με μία FFD. Οι RFDs χρησιμοποιούνται σε πολύ απλές εφαρμογές.

3.3 Τοπολογίες δικτύων

Ανάλογα με τις απαιτήσεις των εφαρμογών, το ZigBee μπορεί να υποστηρίξει δύο τοπολογίες δικτύων (σχήμα 3.3.1). Ανεξαρτήτως τοπολογίας, κάθε συσκευή έχει μία μοναδική διεύθυνση με μήκος 64 bits. Αυτή μπορεί να χρησιμοποιηθεί για την επικοινωνία μέσα σε ένα δίκτυο ή να χρησιμοποιηθεί από το συντονιστή για να χορηγήσει μία συντομευμένη διεύθυνση (16 bits) στη συσκευή. Για κάθε δίκτυο που δημιουργείται, ο συντονιστής επιλέγει μία ταυτότητα (16 bits) που προσδιορίζει μοναδικά το συγκεκριμένο δίκτυο. Ο συνδυασμός ταυτότητας δικτύου και διεύθυνσης συσκευής επιτρέπει την επικοινωνία μεταξύ συσκευών. Κάθε δίκτυο μπορεί να έχει μέχρι και 255 συσκευές. Οι τοπολογίες αυτές είναι:

- Τοπολογία σε σχήμα αστεριού(star): Σε αυτή υπάρχει ο συντονιστής(pan coordinator) του δικτύου, ο οποίος εγκαθιστά συνδέσεις σημείου προς σημείο με άλλες συσκευές. Επίσης ο συντονιστής λειτουργεί και ως δρομολογητής για τη μεταφορά των δεδομένων μεταξύ των άλλων συσκευών, αφού αυτές δεν μπορούν να επικοινωνήσουν απευθείας.



Σχήμα 3.3.1: Τοπολογίες δικτύων

- Τοπολογία σημείου προς σημείο: Κάθε συσκευή εγκαθιστά συνδέσεις σημείου προς σημείο με άλλες συσκευές που βρίσκονται μέσα στην εμβέλεια της. Με αυτό τον τρόπο δημιουργούνται δίκτυα που έχουν τη μορφή δένδρου(cluster tree) ή πλέγματος(mesh). Με τη βοήθεια αλγορίθμων δρομολόγησης, όλες οι συσκευές μπορούν να επικοινωνήσουν μεταξύ τους. Πολλά τέτοια δίκτυα μπορούν να ενωθούν μεταξύ τους και να σχηματίσουν ένα μεγαλύτερο. Στο μεγαλύτερο δίκτυο υπάρχει μόνο ένας συντονιστής δικτύου(pan coordinator), ενώ κάθε μικρότερο δίκτυο έχει από ένα δρομολογητή.

3.4 Φυσικό επίπεδο (Physical layer, PHY)

Το φυσικό επίπεδο παρέχει δύο ειδών υπηρεσίες, δεδομένων και διαχείρισης, στο επίπεδο MAC. Η πρόσβαση σε αυτές επιτυγχάνεται μέσω δύο διαφορετικών σημείων πρόσβασης υπηρεσιών (SAPs), των PHY dataSAP (PD-SAP) και PLME-SAP. Επίσης στο επίπεδο αυτό υπάρχει και μία βάση δεδομένων (PHY PIB) που περιέχει πληροφορίες σχετικές με τη λειτουργία του (κανάλι που χρησιμοποιείται, κανάλια που υποστηρίζονται, εκπεμπόμενη ισχύς, τρόπος ανίχνευσης ελεύθερου καναλιού).

3.4.1 Χαρακτηριστικά καναλιών και διαμόρφωσης

Προσφέρονται συνολικά 27 κανάλια, αριθμημένα από 0 ως 26 και είναι διαθέσιμα σε 3 ζώνες συχνοτήτων. Ένα κανάλι υπάρχει μεταξύ 868 και 868,6 MHz, 10 κανάλια μεταξύ 902 και 928 MHz και 16 κανάλια μεταξύ 2,4 και 2,4835 GHz. Κάθε συσκευή θα πρέπει να υποστηρίζει όλα τα κανάλια, εκτός και αν κάποια από αυτά δεν είναι ελεύθερα στην περιοχή που λειτουργεί. Ο πομπός, και στις 3 ζώνες συχνοτήτων, έχει ελάχιστη ισχύ εκπομπής ίση με -3 dBm, ενώ η μέγιστη περιορίζεται από τη νομοθεσία κάθε περιοχής. Ο κάθε πομπός έχει τη δυνατότητα να ρυθμίζει την ισχύ εκπομπής του, έτσι ώστε να εκπέμπει πάντοτε με την ελάχιστη απαιτούμενη. Η ευαισθησία του δέκτη είναι -85 dBm ή καλύτερη στη ζώνη μεταξύ 2,4-2,4835 GHz και -92 dBm ή καλύτερη στις άλλες δύο. Η ευαισθησία ορίζεται ως η ελάχιστη απαιτούμενη ισχύς για να έχουμε ποσοστό λανθασμένων πλαισίων μικρότερο του 1% για πλαίσια με 20 bytes ωφέλιμο φορτίο.

3.4.2 Πρόσβαση στο κανάλι

Οι μεταδόσεις σε κάθε κανάλι μπορούν να γίνουν με δύο τρόπους. Στον πρώτο τρόπο χρησιμοποιείται ο μηχανισμός πολλαπλής πρόσβασης με ανίχνευση φέροντος, αποφυγή συγκρούσεων και χωρίς χρονοσχισμές (unslotted CSMA-CA). Κάθε συσκευή πριν να μεταδώσει, ανιχνεύει το κανάλι. Αν είναι αδρανές, αρχίζει να μεταδίδει. Αν είναι κατειλημμένο, ο αποστολέας αναβάλλει τη μετάδοση μέχρι το κανάλι να γίνει αδρανές.

Στο δεύτερο τρόπο χρησιμοποιείται το υπερπλαίσιο, το οποίο οριοθετείται από τα αναγνωριστικά σήματα και χωρίζεται σε 16 χρονοσχισμές ίσης διάρκειας. Το αναγνωριστικό σήμα στέλνεται πάντοτε στην πρώτη χρονοσχισμή. Τα σήματα αυτά χρησιμοποιούνται για να περιγράψουν τη δομή του υπερπλαισίου, για το συγχρονισμό των συσκευών του δικτύου και για τον προσδιορισμό του δικτύου.Το υπερπλαίσιο μπορεί να έχει ένα ενεργό και ένα μη ενεργό μέρος. Κατά τη διάρκεια του μη ενεργού μέρους, ο συντονιστής δεν αλληλεπιδρά με το δίκτυο του και λειτουργεί με χαμηλή κατανάλωση ισχύος. Το ενεργό μέρος αποτελείται από την περίοδο πρόσβασης με ανταγωνισμό (CAP) και από την περίοδο χωρίς ανταγωνισμό (CFP). Στην CAP κάθε συσκευή που μεταδίδει χρησιμοποιεί το μηχανισμό πολλαπλής

πρόσβασης με ανίχνευση φέροντος, αποφυγή συγκρούσεων και χρονοσχισμές (slotted CSMA-CA). Αυτό είναι το ίδιο με το unslotted CSMA-CA, με τη διαφορά ότι οι μεταδόσεις ξεκινούν πάντοτε στην αρχή κάποιας χρονοσχισμής και σε περίπτωση κατειλημμένου καναλιού, ο αποστολέας αναβάλλει τη μετάδοση για τυχαίο αριθμό χρονοσχισμών. Όταν ένα κανάλι είναι αδρανές, η μετάδοση πραγματοποιείται μόνο αν υπάρχει αρκετός χρόνος για να ολοκληρωθεί πριν τη λήξη της CAP. Η CFP περιέχει κρατημένες χρονοσχισμές και βρίσκεται ακριβώς πριν το μη ενεργό μέρος. Οι χρονοσχισμές αυτές μπορούν να χρησιμοποιηθούν για την εξυπηρέτηση εφαρμογών που απαιτούν συγκεκριμένο εύρος ζώνης.

3.4.3 Υπηρεσίες δεδομένων

Το σημείο πρόσβασης υπηρεσιών για δεδομένα (PD-SAP) υποστηρίζει τη μεταφορά των μονάδων δεδομένων πρωτοκόλλου του επιπέδου MAC (MPDUs). Για την πραγματοποίηση της μεταφοράς αυτής ορίζονται τρεις στοιχειώδεις υπηρεσίες:

- PD-DATA.request: Το επίπεδο MAC ζητά από το φυσικό επίπεδο την αποστολή μίας MPDU.
- PD-DATA.confirm: Το φυσικό επίπεδο επιβεβαιώνει, θετικά ή αρνητικά, στο επίπεδο MAC την αποστολή μίας MPDU.
- PD-DATA.indication: Το επίπεδο MAC ενημερώνεται από το φυσικό επίπεδο για την άφιξη δεδομένων.

Η μεταφορά των MPDUs γίνεται με τα πακέτα φυσικού επιπέδου. Το κάθε πακέτο αποτελείται από τα πεδία επικεφαλίδα συγχρονισμού (SHR, synchronization header), επικεφαλίδα φυσικού επιπέδου (PHR, PHY header) και ωφέλιμο φορτίο φυσικού επιπέδου (PHY payload). Η επικεφαλίδα συγχρονισμού χρησιμοποιείται για το συγχρονισμό του δέκτη και για να προσδιορίζει την έναρξη των δεδομένων. Η επικεφαλίδα φυσικού επιπέδου προσδιορίζει το μήκος του ωφέλιμου φορτίου, ενώ το πεδίο ωφέλιμο φορτίο φυσικού επιπέδου περιέχει την MPDU.

3.5 Επίπεδο ελέγχου πρόσβασης στο μέσο (Medium access control layer, MAC)

Το επίπεδο MAC παρέχει τις υπηρεσίες του στο επίπεδο δικτύου. Η πρόσβαση στις υπηρεσίες δεδομένων γίνεται μέσω του MLDE-SAP, ενώ για τις υπηρεσίες διαχείρισης υπάρχει το MLME-SAP. Επίσης στο επίπεδο αυτό υπάρχει και μία βάση δεδομένων (MAC PIB) που περιέχει πληροφορίες σχετικές με τη λειτουργία του.

3.5.1 Υπηρεσίες δεδομένων

Το σημείο πρόσβασης υπηρεσιών για τα δεδομένα (MLDE-SAP) υποστηρίζει τη μεταφορά των μονάδων δεδομένων πρωτοκόλλου του επιπέδου δικτύου (NPDUs). Για την πραγματοποίηση της μεταφοράς αυτής ορίζονται οι παρακάτω στοιχειώδεις υπηρεσίες:

- MLDE-DATA.request: Το επίπεδο δικτύου ζητά από το επίπεδο MAC την αποστολή μίας NPDU.
- MLDE-DATA.confirm: Το επίπεδο MAC επιβεβαιώνει, θετικά ή αρνητικά, στο επίπεδο δικτύου την αποστολή μίας NPDU.
- MLDE-DATA.indication: Το επίπεδο δικτύου ενημερώνεται από το επίπεδο MAC για την άφιξη δεδομένων.
- MLDE-PURGE.request: Χρησιμοποιείται όταν το επίπεδο δικτύου θέλει να διαγράψει ένα μήνυμά του από την ουρά αναμονής του MAC.
- MLDE-PURGE.confirm: Απαντάει στην προηγούμενη αίτηση.

3.5.2 Πλαίσια MAC

Ορίζονται τέσσερις διαφορετικοί τύποι πλαισίων, τα δεδομένα, οι επιβεβαιώσεις, οι εντολές και τα αναγνωριστικά σήματα. Η γενική δομή ενός πλαισίου MAC φαίνεται στο σχήμα 3.5.1. Αποτελείται από τα πεδία επικεφαλίδας MAC (MHR), ωφέλιμου φορτίου MAC και υποσημείωσης MAC (MFR). Το MHR περιέχει τα πεδία έλεγχου πλαισίου, αριθμού ακολουθίας και διευθύνσεων. Το πεδίο ωφέλιμου φορτίου MAC περιέχει διάφορες πληροφορίες ανάλογα με τον τύπο του πλαισίου. Το MFR περιέχει την ακολουθία ελέγχου του πλαισίου (FCS). Το συνολικό μήκος του πλαισίου δεν πρέπει να ξεπερνά τα 127 bytes (μέγιστο μήκος ωφέλιμου φορτίου του πακέτου φυσικού επιπέδου).

<table>
<tr><td>Octets: 2</td><td>1</td><td>0/2</td><td>0/2/8</td><td>0/2</td><td>0/2/8</td><td>variable</td><td>2</td></tr>
<tr><td rowspan="2">Frame control</td><td rowspan="2">Sequence number</td><td>Destination PAN identifier</td><td>Destination address</td><td>Source PAN identifier</td><td>Source address</td><td rowspan="2">Frame payload</td><td rowspan="2">FCS</td></tr>
<tr><td colspan="5">Addressing fields</td></tr>
<tr><td colspan="6">MHR</td><td>MAC payload</td><td>MFR</td></tr>
</table>

Σχήμα 3.5.1: Γενική δομή πλαισίου MAC

3.5.2.1. Πεδίο έλεγχου πλαισίου

Έχει μήκος 2 bytes και η δομή του φαίνεται στο σχήμα και αποτελείται από τα παρακάτω υποπεδία:

- Τύπος πλαισίου (frame type) που καθορίζει τον τύπο του πλαισίου (δεδομένα, επιβεβαίωση, εντολή ή αναγνωριστικό σήμα).
- Ασφάλεια (security enabled) που καθορίζει αν το πλαίσιο είναι κρυπτογραφημένο.
- Πλαίσιο που εκκρεμεί (frame pending) που καθορίζει εάν ο αποστολέας έχει και άλλα δεδομένα να στείλει στον παραλήπτη.
- Αίτημα επιβεβαίωσης (acknowledgment request) που καθορίζει εάν ο αποστολέας θέλει να λάβει επιβεβαίωση για το πλαίσιο.
- Intra-PAN που καθορίζει εάν το πλαίσιο θα σταλεί μέσα στο ίδιο PAN ή σε διαφορετικό.
- Μορφή διεύθυνσης προορισμού (destination addressing mode) που καθορίζει τον τύπο, την ύπαρξη και το μέγεθος των υποπεδίων προορισμού στα πεδία διευθύνσεων.
- Μορφή διεύθυνσης πηγής (source addressing mode) που καθορίζει τον τύπο, την ύπαρξη και το μέγεθος των υποπεδίων πηγής στα πεδία διευθύνσεων.

Υπάρχουν συνολικά και 5 bits κρατημένα για μελλοντική χρήση, 3 μετά το Intra-PAN και 2 μετά τη μορφή διεύθυνσης προορισμού.

3.5.2.2. Πεδίο αριθμού ακολουθίας

Έχει μήκος 8 bits και παίρνει μία τυχαία τιμή. Χρησιμοποιείται για να αντιστοιχίζεται ένα πλαίσιο επιβεβαίωσης με το πλαίσιο εντολής ή δεδομένων. Έτσι, όταν φθάσει μία επιβεβαίωση, ο παραλήπτης γνωρίζει ότι το πλαίσιο εντολής ή δεδομένων που έχει τον ίδιο αριθμό ακολουθίας με αυτή, έχει φθάσει στον προορισμό του. Στην περίπτωση των αναγνωριστικών σημάτων ο αριθμός ακολουθίας προσδιορίζει ένα συγκεκριμένο σήμα.

3.5.2.3. Πεδία διευθύνσεων

Η ύπαρξη των πεδίων αυτών καθώς και το μήκος τους εξαρτώνται από τον τύπο του πλαισίου. Στα πλαίσια επιβεβαιώσεων δεν υπάρχουν καθόλου. Αποτελούνται από τα παρακάτω υποπεδία:

- Ταυτότητα δικτύου προορισμού (destination PAN identifier) που προσδιορίζει την ταυτότητα του δικτύου στο οποίο ανήκει ο παραλήπτης.
- Διεύθυνση προορισμού (destination address) που προσδιορίζει τη διεύθυνση του παραλήπτη.
- Ταυτότητα δικτύου πηγής (source PAN identifier) που προσδιορίζει την ταυτότητα του δικτύου στο οποίο ανήκει ο δημιουργός του πλαισίου.
- Διεύθυνση πηγής (source address) που προσδιορίζει τη διεύθυνση του δημιουργού του πλαισίου.

3.5.2.4. Ακολουθία ελέγχου πλαισίου (FCS)

Έχει μήκος 2 bytes. Περιέχει κώδικα CRC για ανίχνευση λαθών. Υπολογίζετε για τα πεδία επικεφαλίδα MAC (MHR) και ωφέλιμο φορτίο MAC.

3.5.2.5. Ωφέλιμο φορτίο MAC

Περιέχει διάφορες πληροφορίες ανάλογα με τον τύπο του πλαισίου. Μπορεί να είναι κρυπτογραφημένο. Σε ένα αναγνωριστικό σήμα περιέχει πληροφορίες σχετικά με τη δομή του υπερπλαισίου, σε ένα πλαίσιο δεδομένων περιέχει τα δεδομένα του ανωτέρου επιπέδου, σε μία επιβεβαίωση δεν υπάρχει καθόλου και σε ένα πλαίσιο εντολών περιέχει την εντολή που μεταδίδεται.

3.5.3 Λειτουργίες επιπέδου MAC

Το επίπεδο MAC έχει μία σειρά από λειτουργίες. Δημιουργεί αναγνωριστικά σήματα εάν η συσκευή είναι συντονιστής του δικτύου τα οποία χρησιμοποιούνται για την περιγραφή της δομή του υπερπλαισίου, για το συγχρονισμό των συσκευών του δικτύου και για τον προσδιορισμό του δικτύου.

Επιπλέον υποστηρίζει τη δημιουργία και τη διατήρηση δικτύων. Ζητά από το φυσικό επίπεδο να ανιχνεύσει σε ορισμένα κανάλια και να παραδώσει τα αποτελέσματα στο επίπεδο δικτύου. Έτσι ανιχνεύονται τα αναγνωριστικά σήματα που εκπέμπουν οι συντονιστές των δικτύων και μπορεί να ζητήσει τη σύνδεση σε κάποιο δίκτυο. Επιπλέον, το επίπεδο MAC μπορεί να ζητήσει από το φυσικό επίπεδο και τη μέτρηση της ενέργειας σε ένα σύνολο καναλιών και έτσι να επιλέξει το κατάλληλο κανάλι για τη δημιουργία ενός δικτύου.

Μία ακόμα λειτουργία του είναι η υποστήριξη υπηρεσιών ασφάλειας. Το επίπεδο MAC είναι σε θέση να παρέχει στα ανώτερα του επίπεδα κάποιες βασικές υπηρεσίες ασφαλείας, όπως είναι ο έλεγχος πρόσβασης, η κρυπτογράφηση των δεδομένων και η ακεραιότητα των πλαισίων όταν αυτό του ζητηθεί. Τα κλειδιά και οι λίστες που απαιτούνται για αυτές, του παρέχονται από τα ανώτερα επίπεδα.

3.6. Επίπεδο δικτύου (Network layer, NWK)

Το επίπεδο δικτύου παρέχει τις υπηρεσίες του, δεδομένων και διαχείρισης, στο επίπεδο εφαρμογών και επιπλέον εξασφαλίζει τη σωστή λειτουργία του επιπέδου MAC. Οι υπηρεσίες δεδομένων παρέχονται στο επίπεδο εφαρμογών μέσω του σημείου πρόσβασης υπηρεσιών NLDE (Network Layer Data Entity), ενώ οι υπηρεσίες διαχείρισης μέσω του σημείου πρόσβασης υπηρεσιών NLME (Network Layer Management Entity). Επίσης στο επίπεδο αυτό υπάρχει και μία βάση δεδομένων που περιέχει πληροφορίες σχετικές με τη λειτουργία του.

Οι υπηρεσίες δεδομένων περιλαμβάνουν την παραλαβή των δεδομένων από το ανώτερο επίπεδο, την τοποθέτησή τους σε κατάλληλα πλαίσια και την αποστολή τους στην κατάλληλη συσκευή, είτε απευθείας είτε μέσω κάποιας άλλης. Για την πραγματοποίηση αυτών ορίζονται οι στοιχειώδεις υπηρεσίες, NLDE-DATA.request, NLDE-DATA.confirm και NLDE-DATA.indication.

Οι υπηρεσίες διαχείρισης περιλαμβάνουν τη διαμόρφωση της λειτουργίας μίας συσκευής ανάλογα με το ρόλο της στο δίκτυο, τη δημιουργία ενός δικτύου, τη σύνδεση σε ένα δίκτυο, την αποχώρηση από αυτό, τη διευθυνσιοδότηση των συσκευών του δικτύου, τη δυνατότητα να ανακαλύπτουν γειτονικές συσκευές, τη δυνατότητα να ανακαλύπτουν και να καταγράφουν διαδρομές για την αποτελεσματική αποστολή των μηνυμάτων στο δίκτυο και τη δυνατότητα να ελέγχουν τη λειτουργία του δέκτη.

3.6.1. Πλαίσια επιπέδου δικτύου

Η γενική δομή του πλαισίου φαίνεται στο σχήμα 3.6.1. Κάθε πλαίσιο αποτελείται από τα πεδία επικεφαλίδα (NWK Header) και ωφέλιμο φορτίο (NWK Payload). Η επικεφαλίδα του πλαισίου αποτελείται από το πεδίο έλεγχος πλαισίου (Frame Control) και τα πεδία δρομολόγησης (Routing Fields).

<table>
<tr><td>Octets: 2</td><td>2</td><td>2</td><td>1</td><td>1</td><td>Variable</td></tr>
<tr><td rowspan="2">Frame Con-trol</td><td>Destination Address</td><td>Source Address</td><td>Radius[a]</td><td>Sequence Number[b]</td><td>Frame Payload</td></tr>
<tr><td colspan="4">Routing Fields</td><td></td></tr>
<tr><td colspan="5">NWK Header</td><td>NWK Payload</td></tr>
</table>

Σχήμα 3.6.1: Γενική δομή του πλαισίου επιπέδου δικτύου

Το πεδίο έλεγχου πλαισίου (Frame Control, 2 bytes) έχει τη δομή που φαίνεται στο σχήμα 3.6.2 και αποτελείται από τα παρακάτω υποπεδία:

- Τύπος πλαισίου (Frame type) που προσδιορίζει τον τύπο του πλαισίου (δεδομένα ή εντολή).

- Έκδοση πρωτοκόλλου (Protocol version) που προσδιορίζει την έκδοση του πρωτοκόλλου που χρησιμοποιείται.
- Ανακάλυψη διαδρομής (Discover route) που χρησιμοποιείται για να ελέγχει τις λειτουργίες ανακάλυψης διαδρομής για τη μετάδοση του πλαισίου.
- Ασφάλεια (Security) που δείχνει αν έχουν χρησιμοποιηθεί οι υπηρεσίες ασφάλειας που παρέχει το επίπεδο δικτύου.

Bits: 0-1	2-5	6-7[a]	8	9	10-15
Frame type	Protocol version	Discover route	Reserved	Security	Reserved

Σχήμα 3.6.2: Το πεδίο έλεγχος πλαισίου

Υπάρχουν και 7 bits κρατημένα για μελλοντική χρήση, ένα μετά την ανακάλυψη διαδρομής και έξι μετά την ασφάλεια.

Τα πεδία δρομολόγησης αποτελούνται από τα παρακάτω υποπεδία:

- Διεύθυνση προορισμού (Destination Address) που προσδιορίζει την διεύθυνση προορισμού του πλαισίου.
- Διεύθυνση πηγής (Source Address) που προσδιορίζει την διεύθυνση της συσκευής που δημιούργησε το πλαίσιο.
- Ακτίνα (Radiu) που προσδιορίζει τον αριθμό των βημάτων που ακολούθησε ένα πλαίσιο μέχρι να φθάσει στον προορισμό.
- Αριθμός ακολουθίας (Sequence Number) που είναι ένας μετρητής που αυξάνεται κατά 1 κάθε φορά που δημιουργείται ένα καινούριο πλαίσιο.

Το πεδίο ωφέλιμο φορτίο έχει μεταβλητό μήκος και περιέχει συγκεκριμένες πληροφορίες για κάθε τύπο πλαισίου. Στο πλαίσιο δεδομένων περιέχονται τα δεδομένα που θέλει το ανώτερο επίπεδο να στείλει. Στο πλαίσιο εντολών περιέχεται η ταυτότητα της εντολής (1 byte), που προσδιορίζει τον τύπο της, και το ωφέλιμο φορτίο της εντολής. Στις προδιαγραφές του ZigBee ορίζονται οι παρακάτω τύποι εντολών:

- Route request: Με αυτή μία συσκευή μπορεί να ζητήσει από τις γειτονικές της να ψάξουν για ένα συγκεκριμένο παραλήπτη. Με τις πληροφορίες που παίρνει, μπορεί να επιλέξει κατάλληλα δρομολόγια για τη μετάδοση πλαισίων προς όλες τις συσκευές του δικτύου.
- Route reply: Με αυτή η συσκευή προορισμού ενημερώνει τον αρχικό αποστολέα της Route request ότι έλαβε τη συγκεκριμένη αίτηση. Επίσης επιστρέφει πληροφορίες που αφορούν τη διαδρομή που ακολούθησε η αντίστοιχη αίτηση.
- Route error: Χρησιμοποιείται όταν μία συσκευή δεν μπορεί να προωθήσει ένα πλαίσιο δεδομένων. Με αυτή ενημερώνεται ο αποστολέας ότι το πλαίσιο δεν έφθασε στον προορισμό του.
- Leave: Χρησιμοποιείται από μία συσκευή για να ενημερώσει ότι αποχωρεί από το δίκτυο ή για να ζητήσει από κάποια συσκευή να αποχωρήσει.

3.6.2 Πίνακες γειτόνων

Κάθε συσκευή διατηρεί στη βάση δεδομένων της έναν πίνακα με πληροφορίες για τις συσκευές που βρίσκονται μέσα στην ακτίνα δράσης της. Στον πίνακα αυτό, για κάθε γειτονική συσκευή υπάρχει μία εγγραφή που περιέχει την ταυτότητα του δικτύου της, τον τύπο της, τη διεύθυνση της μέσα στο δίκτυο που ανήκει, τη σχέση που υπάρχει μεταξύ των δύο συσκευών και την εκτεταμένη της διεύθυνση εφόσον οι δύο συσκευές είναι συνδεμένες. Στον πίνακα αυτό μπορεί να υπάρχουν και διάφορες άλλες προαιρετικές πληροφορίες, όπως το πόσο συχνά εκπέμπει αναγνωριστικά σήματα, αν αποδέχεται τις αιτήσεις για σύνδεση, μία εκτίμηση της ποιότητας της ζεύξης, το λογικό κανάλι στο οποίο λειτουργεί και το πόσα βήματα απέχει από το συντονιστή του δικτύου της.

3.6.3. Σύνδεση σε ένα δίκτυο και αποχώρηση από αυτό

Κάθε συσκευή ZigBee έχει τη δυνατότητα να συνδέεται σε ένα δίκτυο και να αποχωρεί από αυτό. Μία σχέση γονέα-παιδιού αναπτύσσεται κάθε φορά που μία συσκευή ενός δικτύου επιτρέπει σε μία άλλη να γίνει μέλος του δικτύου. Η νέα συσκευή είναι το παιδί, ενώ η πρώτη είναι ο γονέας. Ένα παιδί μπορεί να προστεθεί σε ένα δίκτυο με 2 τρόπους.

Στον πρώτο τρόπο, η διαδικασία ξεκινά από τη νέα συσκευή (παιδί). Μία εφαρμογή της ζητά αρχικά να γίνει ανίχνευση κάποιων καναλιών. Η αίτηση αυτή μεταβιβάζεται από το ανώτερο προς τα κατώτερα επίπεδα. Στη συνέχεια, τα αποτελέσματα της ανίχνευσης, τα διαθέσιμα δίκτυα και τα χαρακτηριστικά τους, ακολουθώντας την αντίθετη πορεία παραδίδονται στο επίπεδο εφαρμογών, το οποίο και αποφασίζει σε ποιό από τα διαθέσιμα δίκτυα θέλει να συνδεθεί. Στέλνει μία αίτηση στο επίπεδο δικτύου για σύνδεση με το συγκεκριμένο δίκτυο. Το επίπεδο δικτύου ψάχνει στον πίνακα γειτόνων για μία συσκευή που να ανήκει σε αυτό το δίκτυο και αν αυτή αποδέχεται τις αιτήσεις για σύνδεση τότε χρησιμοποιεί τη διεύθυνση της συσκευής που βρίσκεται στον πίνακα, στέλνει μία αίτηση για σύνδεση και περιμένει για την απάντηση. Αν δεν βρει κάποια κατάλληλη, απαντά ότι η σύνδεση με το συγκεκριμένο δίκτυο δεν επιτρέπεται και το επίπεδο δικτύου ψάχνει για μία δεύτερη κατάλληλη συσκευή και επαναλαμβάνει την αίτηση για σύνδεση. Η διαδικασία συνεχίζεται μέχρι να έρθει κάποια θετική απάντηση ή μέχρι να μη βρίσκει κάποια άλλη κατάλληλη συσκευή, οπότε και το ανώτερο επίπεδο ενημερώνεται για την αδυναμία σύνδεσης στο συγκεκριμένο δίκτυο. Η διαδικασία αυτή μπορεί να ξεκινήσει μόνο από μία συσκευή που δεν ανήκει σε κάποιο δίκτυο.

Στην πλευρά του γονέα ακολουθείται η εξής διαδικασία. Η αίτηση για σύνδεση παραδίδεται ιεραρχικά στο επίπεδο δικτύου. Εκεί απορρίπτεται σε περίπτωση που ο πιθανός γονέας δεν είναι συντονιστής του δικτύου ή δρομολογητής ή αν δεν υπάρχει διαθέσιμη διεύθυνση για να δοθεί στη νέα συσκευή. Εφόσον δεν συντρέχει λόγος απόρριψης, ο πιθανός γονέας ελέγχει μήπως η συσκευή που έστειλε την αίτηση ανήκει ήδη στο δίκτυο. Ο έλεγχος

αυτός γίνεται με σύγκριση της εκτεταμένης διεύθυνσης της συσκευής, που περιέχεται στην αίτηση, με τις διευθύνσεις που υπάρχουν στον πίνακα γειτόνων του. Αν βρεθεί μία εγγραφή, ο γονέας απαντά θετικά στην αίτηση με την διεύθυνση που βρίσκεται στον πίνακα. Σε διαφορετική περίπτωση, διαθέτει μία νέα διεύθυνση, η οποία είναι μοναδική στο δίκτυο, και στη συνέχεια απαντά και πάλι θετικά.

Στο δεύτερο τρόπο, η διαδικασία ξεκινά από τον πιθανό γονέα, ο οποίος θα πρέπει να είναι συντονιστής του δικτύου ή δρομολογητής και να γνωρίζει την εκτεταμένη διεύθυνση της συσκευής, την οποία επιθυμεί να εντάξει στο δίκτυο. Αρχικά το επίπεδο εφαρμογών ζητά από το επίπεδο δικτύου να συνδεθεί με τη συγκεκριμένη συσκευή. Το επίπεδο δικτύου συγκρίνει την εκτεταμένη διεύθυνση που του στάλθηκε με αυτές που υπάρχουν στον πίνακα γειτόνων. Αν βρεθεί στον πίνακα, ενημερώνει το επίπεδο εφαρμογών ότι η συγκεκριμένη συσκευή ανήκει ήδη στο δίκτυο αλλιώς διαθέτει μία νέα διεύθυνση για τη συσκευή και ενημερώνει το επίπεδο εφαρμογών ότι η συσκευή προστέθηκε στο δίκτυο.

Στην πλευρά του παιδιού το επίπεδο εφαρμογών ζητά από το επίπεδο δικτύου να κάνει εκπομπές μηνυμάτων προς όλα τα δίκτυα που λειτουργούν στην γύρω περιοχή. Τα μηνύματα αυτά περιέχουν την εκτεταμένη διεύθυνση της συσκευής, ενώ ως διεύθυνση προορισμού έχουν τη διεύθυνση εκπομπής. Μόλις ένα τέτοιο μήνυμα φθάσει στη συσκευή του πιθανού γονέα, το επίπεδο δικτύου θα καταλάβει ότι πρόκειται για μία συσκευή που ανήκει στο δίκτυο και θα τις στείλει τη διεύθυνση την οποία θα πρέπει να χρησιμοποιεί για τις μεταδόσεις της στο δίκτυο.

Η αποχώρηση μίας συσκευής από ένα δίκτυο μπορεί και αυτή να γίνει με δύο τρόπους. Στον πρώτο τρόπο, το ίδιο το παιδί ζητά από το γονέα να αποχωρήσει. Ο γονέας εγκρίνει και η σύνδεση διακόπτεται. Στην περίπτωση όμως που το παιδί έχει και αυτό άλλα παιδιά, πρέπει πρώτα να ζητήσει από αυτά να φύγουν και στη συνέχεια να διακόψει τη σύνδεση. Στο δεύτερο τρόπο, ο γονέας ζητά από το παιδί να φύγει από το δίκτυο. Μόλις ένα παιδί λάβει αυτή την εντολή, ενεργεί όπως στον πρώτο τρόπο.

3.6.4. Δημιουργία ενός δικτύου

Μόνο συσκευές ZigBee που έχουν τη δυνατότητα να γίνουν συντονιστές δικτύων μπορούν να ξεκινήσουν τη διαδικασία δημιουργίας δικτύου. Αρχικά, το επίπεδο εφαρμογών ζητά από το επίπεδο δικτύου να δημιουργήσει ένα καινούριο δίκτυο με συγκεκριμένα χαρακτηριστικά. Η διαδικασία συνεχίζεται με την εκτέλεση ανίχνευσης ενέργειας σε ένα σύνολο καναλιών. Η ανίχνευση αυτή πραγματοποιείται από το επίπεδο δικτύου, με τη βοήθεια των κατώτερων επιπέδων. Με τη λήψη των αποτελεσμάτων, το επίπεδο δικτύου κατατάσσει τα κανάλια σε μία σειρά, ξεκινώντας από το κανάλι στο οποίο μετρήθηκε η χαμηλότερη ενέργεια. Επίσης απορρίπτει τα κανάλια στα οποία η ενέργεια ξεπερνά ένα αποδεκτό επίπεδο, το οποίο καθορίζεται από την εφαρμογή για την αποφυγή παρεμβολών.

Στη συνέχεια το επίπεδο δικτύου, με τη βοήθεια των κατώτερων, εκτελεί ενεργή ανίχνευση των αποδεκτών καναλιών, ψάχνοντας για συσκευές. Τα αποτελέσματα της ανίχνευσης παραδίδονται στο επίπεδο δικτύου, το οποίο προσδιορίζει τον αριθμό και τις

ταυτότητες των δικτύων που λειτουργούν σε κάθε κανάλι. Ως κανάλι λειτουργίας του δικτύου επιλέγεται εκείνο με το μικρότερο αριθμό δικτύων. Έπειτα επιλέγεται η ταυτότητα του δικτύου. Αυτή έχει μήκος 16 bits, δεν πρέπει να είναι μία από τις κρατημένες για ειδικούς σκοπούς και πρέπει να προσδιορίζει μοναδικά το δίκτυο στη συγκεκριμένη περιοχή. Η αδυναμία εύρεσης κατάλληλου καναλιού ή μοναδικής ταυτότητας, οδηγεί τη διαδικασία σε τερματισμό.

Αφού επιλεγεί η ταυτότητα, το επίπεδο δικτύου του συντονιστή πρέπει να προσδιορίσει τη διεύθυνση του μέσα στο δίκτυο. Αυτή έχει μήκος 16 bits και την τιμή 0. Έπειτα μέσω του σημείου πρόσβασης υπηρεσιών διαχείρισης του επιπέδου MAC (MLME-SAP), το επίπεδο δικτύου διαμορφώνει τη λειτουργία του MAC, ανάλογα με τις απαιτήσεις της εφαρμογής. Τελικά, το επίπεδο εφαρμογών ενημερώνεται για την επιτυχία της αίτησης και ο συντονιστής είναι πλέον έτοιμος να δεχθεί νέες συσκευές στο δίκτυο με τη διαδικασία που περιγράφηκε στην προηγούμενη παράγραφο.

3.6.5. Δρομολόγηση πλαισίων

Κάθε συντονιστής δικτύου και όλοι οι δρομολογητές έχουν από έναν πίνακα δρομολόγησης. Κάθε εγγραφή σε αυτόν περιέχει τη διεύθυνση προορισμού, την κατάσταση της διαδρομής και τη διεύθυνση του επόμενου βήματος. Εκτός του πίνακα δρομολόγησης, στις συσκευές των συντονιστών και των δρομολογητών υπάρχει και ένας πίνακας ανακάλυψης διαδρομής. Αυτός περιέχει την ταυτότητα του αιτήματος διαδρομής, τη διεύθυνση της συσκευής που έκανε την αίτηση, τη διεύθυνση του αποστολέα του αιτήματος, το κόστος της διαδρομής από τη συσκευή που έκανε την αίτηση ως τη συγκεκριμένη συσκευή, το κόστος της διαδρομής από τη συγκεκριμένη συσκευή ως τον τελικό προορισμό και το χρόνο λήξης.

Μόλις το επίπεδο εφαρμογών μιας συσκευής συντονιστή ή δρομολογητή στείλει ένα πλαίσιο για μετάδοση στο επίπεδο δικτύου, τότε αυτό ελέγχει τη διεύθυνση προορισμού του πλαισίου. Αν η συσκευή προορισμού είναι ένα από τα παιδιά του, τότε γίνεται απευθείας μετάδοση. Στην περίπτωση αυτή η διεύθυνση του επόμενου βήματος και η διεύθυνση προορισμού στον πίνακα δρομολόγησης είναι ίδιες. Αν η διεύθυνση προορισμού είναι η διεύθυνση εκπομπής, τότε στο πεδίο διεύθυνση προορισμού της επικεφαλίδας του πλαισίου MAC τοποθετείται η διεύθυνση εκπομπής, ενώ στο πεδίο ταυτότητα δικτύου προορισμού η ταυτότητα του δικτύου στο οποίο ανήκει η συσκευή.

Στην περίπτωση που δεν συμβαίνει κάτι από τα παραπάνω, το επίπεδο δικτύου ψάχνει στον πίνακα δρομολόγησης για μία εγγραφή που να έχει τη συγκεκριμένη διεύθυνση προορισμού. Αν υπάρχει, το πλαίσιο παραδίδεται στο επίπεδο MAC για αποστολή. Στο πεδίο διεύθυνση προορισμού της επικεφαλίδας του πλαισίου MAC τοποθετείται η διεύθυνση του επόμενου βήματος. Το πεδίο διεύθυνση πηγής περιέχει τη διεύθυνση της συσκευής που έστειλε το πλαίσιο.

Στο επόμενο βήμα το πλαίσιο φθάνει σε μία ενδιάμεση συσκευή. Εκεί γίνεται δεκτό από το επίπεδο MAC της συσκευής, αφού έχει ως διεύθυνση προορισμού τη διεύθυνση της

συγκεκριμένης συσκευής. Εφόσον δεν ανιχνευθεί κάποιο λάθος, το πλαίσιο παραδίδεται στο επίπεδο δικτύου. Από το πεδίο διεύθυνση προορισμού της επικεφαλίδας δικτύου (NWK Header), καταλαβαίνει ότι πρόκειται για ένα πλαίσιο που δεν προορίζεται για τη συγκεκριμένη συσκευή. Ψάχνει στον πίνακα δρομολόγησης για μία εγγραφή που να έχει τη συγκεκριμένη διεύθυνση προορισμού. Αν υπάρχει, το πλαίσιο παραδίδεται στο επίπεδο MAC για αποστολή. Στο πεδίο διεύθυνση προορισμού της επικεφαλίδας του πλαισίου MAC τοποθετείται η διεύθυνση του επόμενου βήματος από τον πίνακα δρομολόγησης, ενώ στο πεδίο διεύθυνση πηγής περιέχεται η διεύθυνση της ενδιάμεσης συσκευής. Με αυτά τα διαδοχικά βήματα, το πλαίσιο φθάνει στον τελικό προορισμό του και παραδίδεται στο επίπεδο εφαρμογών.

Υπάρχει βέβαια και το ενδεχόμενο ο πίνακας δρομολόγησης του αποστολέα ή κάποιας ενδιάμεσης συσκευής να μην περιέχει εγγραφή για την συγκεκριμένη διεύθυνση προορισμού. Στην περίπτωση αυτή, το πλαίσιο αποθηκεύεται προσωρινά και ξεκινά η διαδικασία αναζήτησης διαδρομής που περιγράφεται στην επόμενη παράγραφο. Με το τέλος αυτής, συμπληρώνεται ο πίνακας δρομολόγησης και συνεχίζεται η αποστολή του πλαισίου προς τον τελικό προορισμό.

Η παραπάνω διαδικασία ισχύει μόνο όταν η συσκευή έχει δυνατότητες δρομολόγησης. Οι συσκευές που δεν έχουν τέτοιες δυνατότητες, μπορούν να επικοινωνήσουν μόνο με τα παιδιά και το γονέα τους. Τα πλαίσια που έχουν προορισμό είτε το γονέα είτε κάποιο από τα παιδιά, μεταδίδονται απευθείας. Τα πλαίσια με προορισμό μία συσκευή που είναι απόγονος κάποιου από τα παιδιά, μεταδίδονται μέσω του κατάλληλου παιδιού. Όταν ο προορισμός του πλαισίου είναι μία τυχαία συσκευή, η μετάδοση του πλαισίου γίνεται μέσω του γονέα. Αν και αυτός δεν έχει δυνατότητες δρομολόγησης, η μετάδοση συνεχίζεται προς το δικό του γονέα. Η διαδικασία αυτή συνεχίζεται μέχρι το πλαίσιο να φθάσει σε μία συσκευή με δυνατότητες δρομολόγησης, οπότε και μεταδίδεται προς τον τελικό προορισμό.

3.6.6. Ασφάλεια

Για την ασφάλεια των μεταδιδόμενων πλαισίων, το επίπεδο δικτύου χρησιμοποιεί το πλαίσιο που φαίνεται στο σχήμα 3.6.3. Το πλαίσιο αποτελείται από την πλήρη επικεφαλίδα δικτύου (Full NWK header) και από το ασφαλές ωφέλιμο φορτίο δικτύου (Secured NWK payload). Η πλήρης επικεφαλίδα περιέχει την επικεφαλίδα του γενικού πλαισίου δικτύου και τη βοηθητική επικεφαλίδα πλαισίου (Auxiliary frame header).

<table>
<tr><td>Octets: Variable</td><td>14</td><td colspan="2">Variable</td></tr>
<tr><td rowspan="2">Original NWK Header ([B3], Clause 7.1)</td><td rowspan="2">Auxiliary frame header</td><td>Encrypted Payload</td><td>Encrypted Message Integrity Code (MIC)</td></tr>
<tr><td colspan="2">Secure frame payload = Output of CCM*</td></tr>
<tr><td colspan="2">Full NWK header</td><td colspan="2">Secured NWK payload</td></tr>
</table>

Σχήμα 3.6.3: Δομή ασφαλές πλαισίου δικτύου

Η βοηθητική επικεφαλίδα πλαισίου έχει τη δομή του σχήματος 3.6.4. Αποτελείται από τα πεδία έλεγχου ασφάλειας (Security control), μετρητή πλαισίων (Frame Counter), διεύθυνσης πηγής (Source Address) και αριθμού ακολουθίας κλειδιού (Key Sequence Number).

Octets: 1	4	0/8	0/1
Security control	Frame Counter	Source Address	Key Sequence Number

Σχήμα 3.6.4: Δομή βοηθητικής επικεφαλίδας

Το πεδίο έλεγχου ασφάλειας (σχήμα 3.6.5) αποτελείται από τα παρακάτω υποπεδία:

- Επίπεδο ασφάλειας (Security level) που προσδιορίζει τις μεθόδους που έχουν χρησιμοποιηθεί στο πλαίσιο για την παροχή ασφάλειας.
- Ταυτότητα κλειδιού (Key identifier) που προσδιορίζει τον τύπο του κλειδιού κρυπτογράφησης που χρησιμοποιείται.
- Το επόμενο bit (Extended Nonce) δείχνει αν υπάρχει το πεδίο διεύθυνσης πηγής στη βοηθητική επικεφαλίδα.

Τέλος, τα επόμενα 2 bits είναι κρατημένα για μελλοντική χρήση.

Bit: 0-2	3-4	5	6-7
Security level	Key identifier	Extended Nonce	Reserved

Σχήμα 3.6.5: Δομή του πεδίου έλεγχος ασφάλειας

Το πεδίο διεύθυνσης πηγής περιέχει την εκτεταμένη διεύθυνση της συσκευήςπου είναι υπεύθυνη για την ασφάλεια του πακέτου ενώ το πεδίο μετρητή πλαισίων χρησιμοποιείται για την αρίθμηση των πλαισίων. Το πεδίο αριθμού ακολουθίας κλειδιού προσδιορίζει ακριβώς το κλειδί κρυπτογράφησης που χρησιμοποιείται. Τέλος, το πεδίο ασφαλούς ωφέλιμου φορτίου δικτύουυ έχει μεταβλητό μήκος και αποτελείται από το κρυπτογραφημένο ωφέλιμο φορτίο και τον κρυπτογραφημένο κωδικό ακεραιότητας μηνυμάτων.

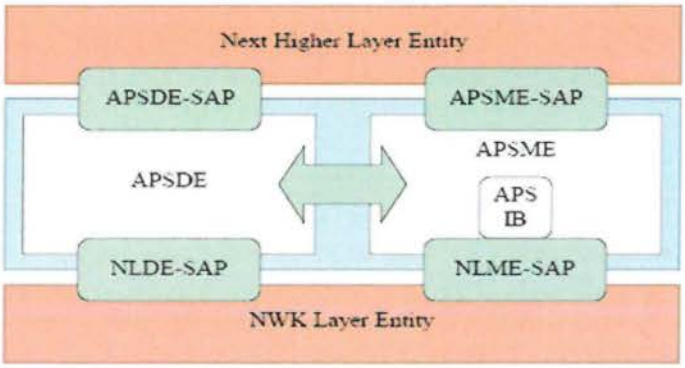
3.7 Επίπεδο εφαρμογών (Application layer, APL)

Το επίπεδο εφαρμογών αποτελείται από το υποεπίπεδο υποστήριξης εφαρμογών (Application support sublayer, APS), το πλαίσιο εφαρμογών (Application framework, AF), τα αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO) και από τις καθορισμένες από τον κατασκευαστή εφαρμογές. Το υποεπίπεδο APS είναι υπεύθυνο για τη μεταφορά των δεδομένων των εφαρμογών σε άλλες συσκευές του δικτύου. Επίσης υποστηρίζει την

ανακάλυψη συσκευών και την εγκατάσταση συνδέσεων με αυτές. Τα ZDO είναι αυτά που καθορίζουν το ρόλο της κάθε συσκευής στο δίκτυο, τον τρόπο λειτουργίας της και παρέχουν τη δυνατότητα για ανακάλυψη υπηρεσιών και συσκευών στις εφαρμογές. Επίσης διαχειρίζονται όλους τους μηχανισμούς που έχουν σχέση με την ασφάλεια. Το πλαίσιο εφαρμογών είναι το περιβάλλον στο οποίο φιλοξενούνται οι εφαρμογές μέσα σε μία συσκευή ZigBee. Σε αυτό μπορούν να υπάρξουν μέχρι και 240 εφαρμογές. Το επίπεδο εφαρμογών έχει φτιαχτεί εξ' ολοκλήρου από τη Zigbee Alliance.

3.7.1. Υποεπίπεδο υποστήριξης εφαρμογών (Application support sublayer, APS)

Το υποεπίπεδο APS χρησιμοποιεί τις υπηρεσίες που του παρέχονται από το επίπεδο δικτύου μέσω των σημείων πρόσβασης υπηρεσιών NLDE (Network Layer Data Entity) και NLME (Network Layer Management Entity), ενώ ταυτόχρονα παρέχει τις υπηρεσίες του στις εφαρμογές και στα ZDO. Αυτές οι υπηρεσίες παρέχονται διαμέσου των οντοτήτων δεδομένων (APSDE) και διαχείρισης (APSME) και των αντίστοιχων σημείων πρόσβασης υπηρεσιών (APSDE-SAP και APSME-SAP). Επίσης στο υποεπίπεδο αυτό υπάρχει και μία βάση δεδομένων (APSIB), που περιέχει πληροφορίες σχετικές με τη λειτουργία του.



Σχήμα 3.7.1: Μοντέλο αναφοράς APS.

3.7.1.1. Υπηρεσίες δεδομένων υποεπιπέδου APS

Η υπηρεσία δεδομένων που παρέχει το υποεπίπεδο APS είναι η δημιουργία των μονάδων δεδομένων πρωτοκόλλου APS (APS-PDUs) από τα δεδομένα των εφαρμογών και η

μεταφορά των δεδομένων από τη μία συσκευή στην άλλη. Οι στοιχειώδεις υπηρεσίες που υποστηρίζει το APSDE-SAP είναι οι:

- APSDE-DATA.request. Με αυτή μία εφαρμογή ενημερώνει το υποεπίπεδο APS ότι έχει δεδομένα για μεταφορά.
- APSDE-DATA.confirm. Με αυτή το υποεπίπεδο APS ενημερώνει την εφαρμογή για την έκβαση της αίτησης.
- APSDE-DATA.indication. Με αυτή το υποεπίπεδο APS ενημερώνει την εφαρμογή ότι έχουν φθάσει δεδομένα από μία άλλη συσκευή.

3.7.1.2. Υπηρεσίες διαχείρισης υποεπιπέδου APS

Οι υπηρεσίες διαχείρισης επιτρέπουν σε μία εφαρμογή να αλληλεπιδρά με τη στοίβα πρωτοκόλλων. Οι υπηρεσίες που παρέχονται είναι η σύνδεση δύο ή και περισσότερων συσκευών του ίδιου δικτύου, η διαχείριση της βάσης δεδομένων και η ασφάλεια των δεδομένων. Οι στοιχειώδεις υπηρεσίες που υποστηρίζει το APSME-SAP είναι οι:

- APSME-BIND. Με τη request, μία εφαρμογή ζητά από το υποεπίπεδο APS να συνδεθεί με μία εφαρμογή μίας άλλης συσκευής. Με την confirm, το υποεπίπεδο APS ενημερώνει την εφαρμογή για την έκβαση της αίτησης.
- APSME-GET. Με τη request, μία εφαρμογή ζητά από το υποεπίπεδο APS να διαβάσει την τιμή μιας ιδιότητας της βάσης δεδομένων. Με την confirm, το υποεπίπεδο APS επιστρέφει την τιμή της ιδιότητας.
- APSME-SET. Με τη request, μία εφαρμογή ζητά από το υποεπίπεδο APS να αλλάξει την τιμή μιας ιδιότητας της βάσης δεδομένων. Με την confirm, το υποεπίπεδο APS ενημερώνει την εφαρμογή για την έκβαση της αίτησης.
- APSME-UNBIND. Με τη request, μία εφαρμογή ζητά από το υποεπίπεδο APS να τερματίσει μία σύνδεση. Με την confirm, το υποεπίπεδο APS ενημερώνει την εφαρμογή για την έκβαση της αίτησης.

3.7.1.3. Πλαίσια υποεπιπέδου APS

Το πλαίσιο του υποεπιπέδου APS (σχήμα 3.7.2) αποτελείται από την επικεφαλίδα APS (APS header) και από το ωφέλιμο φορτίο APS (APS payload). Η επικεφαλίδα περιέχει το πεδίο έλεγχος πλαισίου και τα πεδία διευθύνσεων.

<table>
<tr><td>Octets: 1</td><td>0/1</td><td>0/1</td><td>0/2</td><td>0/1</td><td>Variable</td></tr>
<tr><td rowspan="2">Frame control</td><td>Destination end-point</td><td>Cluster Identifier</td><td>Profile Identifier</td><td>Source endpoint</td><td rowspan="2">Frame payload</td></tr>
<tr><td colspan="4">Addressing fields</td></tr>
<tr><td colspan="5">APS header</td><td>APS payload</td></tr>
</table>

Σχήμα 3.7.2: Πλαίσιο APS

Το πεδίο έλεγχος πλαισίου (σχήμα 3.7.3) αποτελείται από τα παρακάτω υποπεδία:

- Τύπος πλαισίου (Frame type) που προσδιορίζει τον τύπο του πλαισίου.
- Τρόπος παράδοσης (Delivery mode) που καθορίζει τον τρόπο παράδοσης των δεδομένων στις εφαρμογές.
- Τρόπος έμμεσης μετάδοσης (Indirect address mode) που καθορίζει αν υπάρχουν τα υποπεδία σημείο τερματισμού προορισμού και σημείο τερματισμού πηγής στην επικεφαλίδα του πλαισίου.
- Ασφάλεια (Security) που προσδιορίζει αν το πλαίσιο είναι κρυπτογραφημένο.
- Αίτημα επιβεβαίωσης (Ack. Request) που προσδιορίζει αν το συγκεκριμένο πλαίσιο απαιτεί επιβεβαίωση.

Το επόμενο bit είναι κρατημένο για μελλοντική χρήση.

Bits: 0-1	2-3	4	5	6	7
Frame type	Delivery mode	Indirect address mode[3]	Security	Ack. request	Reserved

Σχήμα 3.7.3: Έλεγχος πλαισίου.

Τα πεδία διευθύνσεων αποτελούνται τα παρακάτω υποπεδία:

- Σημείο τερματισμού στον προορισμό (destination endpoint) που προσδιορίζει την εφαρμογή στην οποία πρέπει να παραδοθούν τα δεδομένα.
- Ταυτότητα συμπλέγματος (cluster identifier) που καθορίζει τη μορφή που έχουν τα μεταφερόμενα δεδομένα.
- Ταυτότητα προφίλ (profile identifier) που προσδιορίζει το προφίλ στο οποίο απευθύνεται το πλαίσιο.
- Σημείο τερματισμού στην πηγή (source endpoint) που προσδιορίζει την εφαρμογή που στέλνει τα δεδομένα.

Τα πεδία διευθύνσεων δεν περιέχονται στα πλαίσια εντολών. Σε αυτά οι διευθύνσεις προορισμού και πηγής περιέχονται σε υποπεδία στο ωφέλιμο φορτίο. Το πεδίο ωφέλιμο φορτίο έχει μεταβλητό μήκος και περιέχει συγκεκριμένες πληροφορίες για κάθε τύπο πλαισίου. Στα πλαίσια δεδομένων, περιέχει τα δεδομένα των εφαρμογών. Στα πλαίσια εντολών, περιέχει την ταυτότητα της εντολής και την εντολή ενώ στα πλαίσια επιβεβαιώσεων δεν υπάρχει.

3.7.1.4.Μετάδοση, παραλαβή και επιβεβαίωση πλαισίων

Μία συσκευή μπορεί να μεταδώσει ένα πλαίσιο APS μόνο αν ανήκει στο δικτύου. Η μετάδοση μπορεί να είναι είτε άμεση είτε έμμεση. Στην άμεση, τα πλαίσια περιλαμβάνουν τα υποπεδία σημείο τερματισμού στον προορισμό και σημείο τερματισμού στην πηγή. Όλες οι συσκευές που διαθέτουν πίνακα συνδέσεων κάνουν άμεσες μεταδόσεις πλαισίων προς κάθε προορισμό.

Στην περίπτωση των έμμεσων μεταδόσεων, τα πλαίσια περιλαμβάνουν μόνο ένα από τα παραπάνω υποπεδία και έχουν την τιμή 10 στο υποπεδίο τρόπος παράδοσης. Όλες οι συσκευές που δεν διαθέτουν πίνακα συνδέσεων, όταν κάνουν μία έμμεση μετάδοση θα πρέπει να την κατευθύνουν προς τη συσκευή του συντονιστή που περιέχει τον αντίστοιχο πίνακα. Το συγκεκριμένο πλαίσιο δεν θα περιέχει το υποπεδίο σημείο τερματισμού στον προορισμό. Ο συντονιστής με τη βοήθεια του πίνακα συνδέσεων, θα βρει τη διεύθυνση προορισμού και το αντίστοιχο σημείο τερματισμού. Στη συνέχεια, θα μεταδώσει το πλαίσιο προς τον τελικό προορισμό χωρίς το υποπεδίο σημείο τερματισμού στην πηγή.

Η έμμεση μετάδοση χρησιμοποιείται κυρίως από πολύ απλές συσκευές που δεν έχουν τη δυνατότητα να αποθηκεύουν μεγάλο όγκο δεδομένων. Για μία άμεση μετάδοση, η συσκευή θα πρέπει να γνωρίζει τη διεύθυνση προορισμού, το σημείο τερματισμού στον προορισμό και την ταυτότητα του συμπλέγματος. Σε μία έμμεση μετάδοση, μόνο η ταυτότητα του συμπλέγματος απαιτείται. Και στις δύο περιπτώσεις, έμμεση και άμεση μετάδοση, η μεταφορά του πλαισίου από την πηγή στον προορισμό επιτυγχάνεται μέσω των υπηρεσιών που παρέχουν τα κατώτερα στρώματα.

Στην πλευρά του δέκτη, το υποεπίπεδο APS παραλαμβάνει τα πλαίσια από το επίπεδο δικτύου. Όταν το πλαίσιο περιέχει και τα δύο υποπεδία, το APS το παραδίδει στην εφαρμογή που καθορίζεται από το σημείο τερματισμού στον προορισμό. Στην περίπτωση των έμμεσων μεταδόσεων, όπου το υποπεδίο τρόπος παράδοσης έχει την τιμή 10, ο τρόπος χειρισμού του πλαισίου είναι διαφορετικός. Αν ένα πλαίσιο περιέχει μόνο το υποπεδίο σημείο τερματισμού στην πηγή και φθάσει σε μία συσκευή που διαθέτει πίνακα συνδέσεων, τότε θα βρεθεί στον πίνακα η αντίστοιχη εγγραφή και το πλαίσιο θα αποσταλεί προς τον τελικό του προορισμό χωρίς το υποπεδίο σημείο τερματισμού στην πηγή. Αν η συσκευή δεν διαθέτει πίνακα ή ο πίνακας δεν περιέχει την κατάλληλη εγγραφή, το πλαίσιο θα απορριφθεί. Επίσης, το πλαίσιο θα απορριφθεί και στην περίπτωση που η συσκευή δεν διαθέτει πίνακα και δεν υπάρχει το υποπεδίο σημείο τερματισμού στον προορισμό.

Εκτός από την άμεση και έμμεση μετάδοση, υπάρχει και η εκπομπή προς όλες τις εφαρμογές που περιέχονται σε μία συσκευή. Στην περίπτωση αυτή, το υποπεδίο τρόπος παράδοσης έχει την τιμή 01 και το πλαίσιο APS έχει τα υποπεδία ταυτότητα συμπλέγματος, ταυτότητα προφίλ και σημείο τερματισμού στην πηγή (με τιμή 255). Ως διεύθυνση προορισμού στην επικεφαλίδα δικτύου χρησιμοποιείται η διεύθυνση εκπομπής στο δίκτυο.

Σε κάθε πλαίσιο APS υπάρχει το υποπεδίο αίτημα επιβεβαίωσης (Ack request). Όταν αυτό έχει την τιμή 1, ο δημιουργός του πλαισίου απαιτεί από τον παραλήπτη να του επιβεβαιώσει την ορθή λήψη. Εφόσον η επιβεβαίωση δεν έρθει μέσα σε ένα ορισμένο χρονικό διάστημα, το πλαίσιο μεταδίδεται ξανά. Η παραπάνω διαδικασία επαναλαμβάνεται είτε μέχρι να έρθει μία επιβεβαίωση είτε μέχρι να συμπληρωθεί ο μέγιστος αριθμός επαναμεταδόσεων (3 επαναμεταδόσεις). Στην περίπτωση των έμμεσων μεταδόσεων, η ενδιάμεση συσκευή που αναλαμβάνει να μεταδώσει το πλαίσιο στον τελικό προορισμό, έχει την υποχρέωση να στείλει μία επιβεβαίωση στο δημιουργό του πλαισίου. Στη συνέχεια στέλνει το πλαίσιο προς τον τελικό προορισμό και απαιτεί από αυτόν να της στείλει επιβεβαίωση.

3.7.1.5.Ασφάλεια στο υποεπίπεδο APS

Το υποεπίπεδο APS είναι υπεύθυνο για όλες τις διαδικασίες που απαιτούνται για την εγκαθίδρυση ασφαλών συνδέσεων. Μέσω των υπηρεσιών του επιτυγχάνεται η δημιουργία των διαφόρων κλειδιών, η μεταφορά τους από τη μία συσκευή στην άλλη, η αλλαγή τους και η είσοδος μίας συσκευής σε ένα δίκτυο που παρέχει ασφάλεια. Όλες οι παραπάνω διαδικασίες ξεκινούν κατόπιν εντολής του ZigBee Device Object (ZDO), το οποίο καθορίζει το επίπεδο ασφαλείας που θα χρησιμοποιηθεί και διαχειρίζεται τα κλειδιά.

Για την ασφάλεια των μεταδιδόμενων πλαισίων, το υποεπίπεδο APS χρησιμοποιεί το πλαίσιο του σχήματος 3.7.4. Αποτελείται από την πλήρη επικεφαλίδα APS (Full APS header) και από το ασφαλές ωφέλιμο φορτίο APS (Secured APS payload). Η πλήρης επικεφαλίδα περιέχει την επικεφαλίδα του γενικού πλαισίου APS και τη βοηθητική επικεφαλίδα πλαισίου (Auxiliary frame header).

<table>
<tr><td>Octets: variable</td><td>5 or 6</td><td colspan="2">Variable</td></tr>
<tr><td rowspan="2">Original APS Header
([B7], Clause 7.1)</td><td rowspan="2">Auxiliary frame header</td><td>Encrypted Payload</td><td>Encrypted Message Integrity Code (MIC)</td></tr>
<tr><td colspan="2">Secure frame payload = Output of CCM*</td></tr>
<tr><td colspan="2">Full APS header</td><td colspan="2">Secured APS payload</td></tr>
</table>

Σχήμα 3.7.4: Ασφαλές πλαίσιο APS

Το πεδίο ασφαλές ωφέλιμο φορτίο APS έχει μεταβλητό μήκος και αποτελείται από το κρυπτογραφημένο ωφέλιμο φορτίο και τον κρυπτογραφημένο κωδικό ακεραιότητας μηνυμάτων. Για την κρυπτογράφηση χρησιμοποιείται ο κώδικας CCM.

3.7.2. Πλαίσιο εφαρμογών (Application framework, AF)

Το πλαίσιο εφαρμογών είναι το περιβάλλον μέσα στο οποίο φιλοξενούνται όλες οι εφαρμογές σε μία συσκευή ZigBee. Μέσα σε αυτό στέλνουν και λαμβάνουν δεδομένα διαμέσου του APSDE-SAP. Υπεύθυνα για τον έλεγχο και τη διαχείριση των εφαρμογών είναι τα ZigBee Device Objects (ZDO). Έως και 240 εφαρμογές μπορούν να υπάρξουν στο πλαίσιο εφαρμογών. Για το διαχωρισμό τους, καθεμία έχει το δικό της σημείο τερματισμού (αριθμημένα από 1 ως 240). Το σημείο τερματισμού 0 χρησιμοποιείται για τη μεταφορά δεδομένων προς τα ZDO, ενώ το 255 χρησιμοποιείται για την εκπομπή δεδομένων προς όλες τις εφαρμογές. Τα σημεία τερματισμού 241-254 είναι κρατημένα για μελλοντική χρήση.

3.7.2.1. Τα προφίλ του ZigBee

Κάθε συσκευή ZigBee μπορεί να υποστηρίζει ένα ή και περισσότερα προφίλ. Δύο συσκευές μπορούν να επικοινωνήσουν μόνο αν υποστηρίζουν ένα συγκεκριμένο προφίλ. Το κάθε προφίλ έχει τη δική του ταυτότητα (profile identifier, 2 bytes), η οποία είναι μοναδική. Τα προφίλ καθορίζουν τη φύση των εφαρμογών, τα χαρακτηριστικά των συσκευών και τα συμπλέγματα δεδομένων που χρησιμοποιούνται στην επικοινωνία.

Τα συμπλέγματα δεδομένων έχουν και αυτά τη δική τους ταυτότητα (cluster identifier, 1 byte), η οποία είναι μοναδική μέσα σε ένα συγκεκριμένο προφίλ. Καθορίζουν τις δομές των δεδομένων που χρησιμοποιούνται στην επικοινωνία μεταξύ των σημείων τερματισμού. Κάθε σύμπλεγμα αποτελείται από ιδιότητες. Κάθε ιδιότητα έχει μία μοναδική ταυτότητα (attribute identifier, 2 bytes) μέσα σε ένα συγκεκριμένο σύμπλεγμα.

Τα χαρακτηριστικά των συσκευών ZigBee καθορίζονται από τους παρακάτω περιγραφείς:

- Περιγραφέας κόμβου. Περιέχει πληροφορίες σχετικά με τις συσκευές που υπάρχουν σε αυτόν, τις ζώνες συχνοτήτων που λειτουργεί, τον κωδικό του κατασκευαστή και το μέγιστο μέγεθος των δεδομένων που παραδίδονται στο υποεπίπεδο APS ή παραλαμβάνονται από αυτό.
- Περιγραφέας ισχύος κόμβου. Περιέχει πληροφορίες σχετικά με την κατάσταση λειτουργίας του δέκτη, τις διαθέσιμες πηγές ενέργειας, την πηγή ενέργειας που χρησιμοποιείται και το επίπεδο φόρτισης.
- Απλός περιγραφέας. Περιέχει τον αριθμό του σημείου, την ταυτότητα του προφίλ που υποστηρίζει το συγκεκριμένο σημείο, την ταυτότητα των συσκευών που υποστηρίζονται, τον αριθμό και τη λίστα των εισερχόμενων και εξερχόμενων συμπλεγμάτων δεδομένων που υποστηρίζονται.
- Σύνθετος περιγραφέας. Είναι προαιρετικός και περιέχει πληροφορίες για τη συσκευή, όπως το όνομα του κατασκευαστή, τον αριθμό της και το URL στο οποίο βρίσκονται όλες οι πληροφορίες σχετικά με αυτή.
- Περιγραφέας χρήστη. Είναι και αυτός προαιρετικός και περιέχει το όνομα που δίνει ο χρήστης στη συσκευή.

3.7.2.2.Πλαίσια εντολών AF (Application framework)

Το γενικό πλαίσιο εντολών AF φαίνεται στο σχήμα 3.7.5. και αποτελείται από τα παρακάτω πεδία:

- Μέτρημα συναλλαγών (Transaction count) που καθορίζει τον αριθμό των συναλλαγών που περιέχονται στο πλαίσιο.
- Τύπος πλαισίου (Frame type) που καθορίζει τον τύπο της υπηρεσίας που χρησιμοποιείται.
- Συναλλαγές (Transactions) που αποτελούνται από τον αριθμό ακολουθίας (8 bits) και από το πεδίο των δεδομένων.

Bits: 4	4	Variable	Variable	Variable
Transaction count	Frame type	Transaction 1	...	Transaction *n*

Σχήμα 3.7.5: Πλαίσιο εντολών AF

3.7.3. Αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO)

Τα αντικείμενα συσκευής ZigBee (ZigBee Device Objects, ZDO) βρίσκονται στο επίπεδο εφαρμογών. Επικοινωνούν με το υποεπίπεδο APS και το επίπεδο δικτύου μέσω των APSME-SAP και NLME-SAP αντίστοιχα. Η μεταφορά των δεδομένων σε αυτά γίνεται από το υποεπίπεδο APS μέσω του APSDE-SAP και του σημείου τερματισμού 0. Επικοινωνούν με τις άλλες εφαρμογές της συσκευής μέσω μίας κοινής διεπαφής και επιπλέον μπορούν να επικοινωνήσουν με οποιαδήποτε άλλη συσκευή ZigBee χρησιμοποιώντας το προφίλ συσκευής. Είναι υπεύθυνα για τις παρακάτω διαδικασίες:

- Αρχικοποίηση του υποεπιπέδου APS και του επιπέδου δικτύου.
- Ανακάλυψη της ταυτότητας των άλλων συσκευών του δικτύου.
- Ανακάλυψη υπηρεσιών. Με αυτή, μία συσκευή μπορεί να ανακαλύψει όλες τις εφαρμογές που είναι διαθέσιμες στα σημεία τερματισμού μίας άλλης, να ζητήσει τον περιγραφέα κόμβου ή τον περιγραφέα ισχύος μιας συγκεκριμένης συσκευής ή και τον απλό περιγραφέα ενός συγκεκριμένου σημείου τερματισμού της.
- Διαχείριση ασφάλειας. Τα ZDO είναι υπεύθυνα για την ενεργοποίηση ή όχι της ασφάλειας. Όταν η ασφάλεια είναι ενεργοποιημένη, πρέπει να καθορίσουν το επίπεδο στο οποίο θα εφαρμόζεται, να δημιουργήσουν τα κλειδιά που είναι απαραίτητα για την κρυπτογράφηση των δεδομένων, να φροντίσουν για τη μεταφορά αυτών στις υπόλοιπες συσκευές που συμμετέχουν στην επικοινωνία και να πιστοποιούν την ταυτότητα των συσκευών που στέλνουν τα πλαίσια.

- Διαχείριση δικτύου. Τα ZDO ζητούν από το επίπεδο δικτύου να ανιχνεύσει ένα συγκεκριμένο σύνολο καναλιών, επιλέγουν το κατάλληλο κανάλι για τη δημιουργία ενός δικτύου ή για την ένταξη σε ένα δίκτυο με βάση τα αποτελέσματα των ανιχνεύσεων, ξεκινούν τη διαδικασία για αποχώρηση ή ένταξη σε ένα δίκτυο και επιτρέπουν ή απαγορεύουν σε άλλες συσκευές να συνδεθούν.
- Διαχείριση συνδέσεων μεταξύ σημείων τερματισμού. Τα ZDO διαχειρίζονται τις εγγραφές σε έναν πίνακα συνδέσεων και εξυπηρετούν τις αιτήσεις των εφαρμογών για σύνδεση με κάποια άλλη εφαρμογή σε μία απομακρυσμένη συσκευή.
- Διαχείριση κόμβου. Με αυτή, οι συντονιστές και οι δρομολογητές μπορούν να επιτύχουν τη διαχείριση μιας απομακρυσμένης συσκευής τερματισμού.

Βιβλιογραφία

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

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

Zigbee Specification [Έγγραφο] / 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