Α.Τ.Ε.Ι ΠΕΛΟΠΟΝΝΗΣΟΥ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«Οικογένεια πρωτοκόλλων 802.11 σε Ασύρματο Δίκτυο Υπολογιστών (WLAN) και σύγκριση πρωτοκόλλων 802.11g *vs* 802.11n»

Καρούτσος Χρήστος – Α.Μ. 2008135

Επιβλέπων καθηγητής: κ. Ψαρράς Δημήτριος

Σπάρτη 2014

Πίνακας Περιεχομένων

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου για την στήριξη τους όλα αυτά τα χρόνια.

Επίσης θα ήθελα να ευχαριστήσω τον καθηγητή μου, για την σημαντική βοήθειά του στην διάρκεια της πτυχιακής μου εργασίας.

Πρόλογος

Στο μάθημα της Μετάδοσης Δεδομένων και Δικτύων Υπολογιστών μαθαίνουμε ότι «Τηλεπικοινωνία είναι η επικοινωνία μεταξύ ανθρώπων (ή και μηχανών), που βρίσκονται σε απόσταση μεταξύ τους και συνίσταται στη μετάδοση πληροφοριών που επιτυγχάνει ένας πομπός προς έναν δεκτή». Από τα αρχαία χρόνια οι άνθρωποι έβρισκαν τρόπους να επικοινωνούν από απόσταση. Ξεκινώντας από τους αγγελιοφόρους, δρομείς δηλαδή, που έκαναν τη μεταφορά προφορικών και γραπτών μηνυμάτων, περνώντας στις φρυκτωρίες που ήταν ένα σύστημα μεταβίβασης φωτεινών σημάτων με διαδοχικό άναμμα φωτιάς στις κορυφές βουνών και που χρησιμοποιήθηκαν για στρατιωτικούς κυρίως σκοπούς από την εποχή του τρωικού πόλεμου, έως τους βυζαντινούς χρόνους από τους Έλληνες, και στις πυρσίες που ήταν ο πρώτος οπτικός τηλέγραφος που αναφέρεται στην ιστορία, μέχρι τα ταχυδρομικά περιστέρια και τα τύμπανα των αφρικανικών φυλών και τα σήματα καπνού των ινδιάνων, φτάσαμε τελικά στο πρώτο πραγματικά ασύρματο τρόπο επικοινωνίας σύμφωνα με τον ορισμό που χρησιμοποιούμε και σήμερα. Ήταν ο ασύρματος του Μαρκόνι, ο οποίος άρχισε να πειραματίζεται με τον ηλεκτρομαγνητισμό το 1894 και πέτυχε την πρώτη μετάδοση μηνύματος χωρίς την χρήση συρμάτων. Αυτή του η εφεύρεση χρησιμοποιήθηκε στα πλοία και χρησιμοποιούταν ακόμα και πριν από λίγα χρόνια. Συχνά δε τον ασυρματιστή του πλοίου τον αποκαλούσαν Μαρκόνι.

Τον περασμένο αιώνα, έγινε ένα μεγάλο άλμα τις τηλεπικοινωνίες. Κι αυτό έγινε με τη χρήση δορυφόρων που επέτρεψε την εύκολη διασύνδεση απομακρυσμένων περιοχών της υδρογείου και κατήργησε την ανάγκη χρήσης συρμάτινων αγωγών τεράστιου μήκους ή την χρήση πολλών και ισχυρών επίγειων αναμεταδοτών. Ο πρώτος τηλεπικοινωνιακός δορυφόρος εκτοξεύτηκε από τη NASA στις 12 Αυγούστου 1960. Η ασύρματη επικοινωνία χρησιμοποιεί τα ηλεκτρομαγνητικά κύματα, τα οποία μεταδίδονται στη γήινη ατμόσφαιρα ή στο διάστημα. Έτσι για παράδειγμα, τα ραδιοκύματα (με συχνότητες από 3KHz μέχρι 300MHz), χρησιμοποιούνται στα ασύρματα τηλέφωνα, στην κινητή τηλεφωνία, στη ραδιοεπικοινωνία, τη ραδιοφωνική και τηλεοπτική μετάδοση. Τα μικροκύματα (με συχνότητες από 300MHz μέχρι 300GHz) χρησιμοποιούνται στη ραδιοφωνική και τηλεοπτική μετάδοση και σε διάφορες μικροκυματικές ζεύξεις. Ακόμα και υπέρυθρη ακτινοβολία χρησιμοποιείται για ψηφιακή επικοινωνία σε δίκτυα περιορισμένης γεωγραφικής εμβέλειας. Με την δημιουργία των πρώτων δικτύων ηλεκτρονικών υπολογιστών, παράλληλα με τις μεθόδους που αναπτύχθηκαν για ενσύρματη σύνδεση των κόμβων, είχαμε και την προσπάθεια δημιουργίας ασύρματων τοπικών δικτύων που θα αποδέσμευε την επικοινωνία από τα ενσύρματα μέσα.

Σήμερα τα ασύρματα τοπικά δίκτυα υπολογιστών, υλοποιούνται βασισμένα στις προδιαγραφές που ορίζει η οικογένεια πρωτοκόλλων του IEEE 802.11 και που

στην ουσία είναι τον πρότυπο Ethernet και το CSMA/SA, δηλαδή το πρωτόκολλο πολλαπλής πρόσβασης με ανίχνευση φέροντος και αποφυγή συγκρούσεων. Ενδεικτικά αναφέρουμε το 802.11b, που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 11Mbps και το 802.11g που είναι τεχνολογία ασύρματης μετάδοσης που επιτρέπει ταχύτητες μέχρι 54Mbps. Η κάρτα δικτύου που χρησιμοποιείται στην υλοποίηση, κάνοντας χρήση της ασύρματης τεχνολογίας επιτυγχάνει την ίδια δικτύωση με μια κλασσική κάρτα δικτύου, αλλά χωρίς καλώδια. Μια ειδική περίπτωση που μας ενδιαφέρει ιδιαίτερα, είναι το hotspot, το οποίο είναι το ασύρματο δίκτυο, στο οποίο ο χρήστης μπορεί να έχει πρόσβαση στο internet.

Εισαγωγή

Τα ασύρματα δίκτυα είναι κομμάτι της παγκόσμιας καθημερινότητας μας. Τα παλαιοτέρα χρόνια η ιδέα της ασύρματης επικοινωνίας δεν ήταν ιδιαίτερα γνωστή, όμως τα τελευταία χρόνια έχει αρχίσει να εξαπλώνεται με ταχύ ρυθμό. Με αυτό τον τρόπο τα ασύρματα δίκτυα άρχισαν να ενσωματώνονται στις ζωές των ανθρώπων, στο σπίτι, στο γραφείο, στα νοσοκομεία, στα σχολεία.

Η ασύρματη ψηφιακή μετάδοση έκανε τα πρώτα βήματα της χάρη στον φυσικό Guglielmo Marconi, ο οποίος έκανε πειράματα με ραδιοκύματα. Το 1896 ίδρυσε μια εταιρεία την Wireless Telegraph and Signal Company, η οποία ήταν η πρώτη εταιρεία στο είδος της παγκοσμίως. Μερικά χρόνια αργότερα το 1901, έκανε μια επίδειξη μέσω ενός τηλεγράφου για επικοινωνία πλοίου με την ακτή, μέσω του κώδικα Morse. Στη συνέχεια, η ασύρματη τεχνολογία άρχισε να χρησιμοποιείται και από το στρατό, δηλαδή μετέδιδαν τις πληροφορίες κρυπτογραφημένες με αποτέλεσμα να είναι αρκετά πολύπλοκο να αποκρυπτογραφηθούν. Αυτό βοήθησε πολύ στον 2ο παγκόσμιο πόλεμο. Στην αρχή της δεκαετίας του 50, έγινε διαθέσιμο το πρώτο εμπορικό δίκτυο ραδιοτηλεφωνίας στους πελάτες από την εταιρεία Bell Telephone Company. Το πρόβλημα που δημιουργήθηκε είναι ο μειωμένος αριθμός των χρηστών που μπορούσε να είναι συνδεδεμένοι το ίδιο χρονικό διάστημα. Όλο και περισσότερο εξελισσόταν και αναπτυσσόταν το δίκτυο για να μπορεί να εξυπηρετήσει περισσότερους χρήστες και να είναι πιο αξιόπιστο. Το 1981, αναπτύχτηκε από τους ερευνητές του πανεπιστήμιου της Hawaii το οποίο πήρε το όνομα ALOHA net.

Στην παρούσα πτυχιακή εργασία θα ασχοληθούμε με και θα αναφέρουμε στο πως ξεκίνησαν τα ασύρματα δίκτυα, τα διάφορα είδη τους και τις κύριες εφαρμογές τους.

Κεφάλαιο 1

Τύποι και τοπολογίες ασύρματων δικτύων

1.1 Τύποι Ασύρματων Δικτύων

Υπάρχουν διάφορα είδη ασύρματων δικτύων, τα οποία παρουσιάζονται συνοπτικά παρακάτω :

1. **Ασύρματο Τοπικό Δίκτυο (Wireless LAN):** Το wireless LAN είναι ένα είδος ασύρματου δικτύου, όπως γίνεται εύκολα αντιληπτό και από το όνομα του. Όπως και στα άλλα ασύρματα δίκτυα, χρησιμοποιεί τα ραδιοκύματα αντί των αγωγών στην μετάδοση δεδομένων μεταξύ των υπολογιστών του ίδιου δικτύου , όπως στην περίπτωση του ALOHNET.

2. **Global System for Mobile Communication (GSM):** Το GSM είναι ένα άλλο είδος ασύρματου δικτύου, το οποίο αποτελείται από τρία βασικά συστήματα:
   a) **Switching System**
   b) **Base Station System**
   c) **Operation and Support System**

   Το κυψελωτό (κινητό) συνδέεται στο σταθμό βάσης του συστήματος (base station system). Στη συνέχεια συνδέεται στο σταθμό μεταγωγής (switching station) όπου η κλήση μεταφέρεται στον προορισμό της, ο οποίος συνδέεται με τη σειρά του στο σταθμό λειτουργίας και υποστήριξης (Operation and Support System) και τέλος συνδέεται στο switching station όπου η κλήση μεταφέρεται στον προορισμό της. Χρησιμοποιείται για τα κυψελωτά τηλέφωνα και είναι το πιο διαδεδομένο πρωτόκολλο που χρησιμοποιείται από τις περισσότερες εταιρείες παροχής υπηρεσιών.

3. **Personal Communication Service (PCS):** Το PCS αναφέρεται στην ζώνη ραδιοσυχνοτήτων που μπορεί να χρησιμοποιηθεί από τα κινητά τηλέφωνα στην Βόρεια Αμερική

4. **Digital Advanced Mobile Phone Service (D-AMPS)**: Το D-AMPS είναι μια αναβαθμισμένη έκδοση του AMPS, αλλά έχει αποσυρθεί σταδιακά λόγω της εξέλιξης της τεχνολογίας. Τα νεότερα GSM δίκτυα αντικαθιστούν τα παλιότερα συστήματα.

5. **Fixed Wireless Data**: Είναι ένα είδος ασύρματου δικτύου πληροφοριών, το οποίο μπορεί να χρησιμοποιηθεί για τη σύνδεση δυο ή περισσότερων κτιρίων, καθώς και για την επέκταση ή την χρήση κοινής ζώνης συχνοτήτων, χωρίς τη χρήση καλωδίωσης.

1.2 Τοπολογίες

Οι βασικές μονάδες που αποτελούν τα ασύρματα δίκτυα 802.11 είναι :

- **Το σημείο πρόσβασης (Access Point – AP):** Το AP παίζει τον ρόλο της γέφυρας μεταξύ του ασύρματου και του ενσύρματου δικτύου μετατρέποντας κατάλληλα τα πακέτα που ανταλλάσσονται μεταξύ τους.

Σχήμα 1.1: Wireless Access Point εμπορίου

Σχήμα 1.2: Wireless Access Point τροποποιημένο για υδατοστεγή εξωτερική χρήση

Για εσωτερικό οικιακό ασύρματο δίκτυο χρησιμοποιούνται κυρίως PCI ασύρματες κάρτες για οικονομικούς κυρίως λόγους.

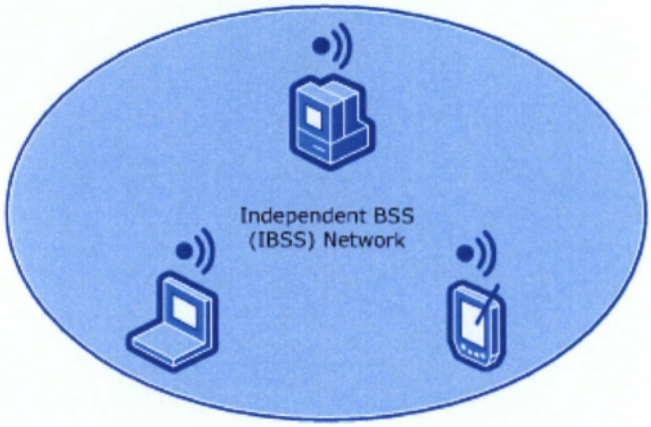
Σχήμα 1.3: PCI κάρτα δικτύου

- **Το σύστημα διανομής (distribution system – DS):** Το DS ενώνει τα διάφορα APs που ανήκουν στο ίδιο δίκτυο επιτρέποντας την ανταλλαγή πλαισίων. Το 802.11 δεν προσδιορίζει τον τρόπο που θα γίνεται αυτό, έτσι μπορεί να είναι ένα ενσύρματο δίκτυο Ethernet 802.3
- **Το ασύρματο μέσο μετάδοσης (wireless medium – WM):** Έχουν οριστεί διάφορα φυσικά στρώματα που χρησιμοποιούν είτε ραδιοσυχνότητες είτε υπέρυθρες ακτίνες για τη μετάδοση των πλαισίων μεταξύ των σταθμών του ασύρματου δικτύου.
- **Οι σταθμοί (stations – STA):** Οι σταθμοί που ανταλλάσσουν πληροφορίες μέσω του ασύρματου δικτύου και είναι συνήθως φορητές συσκευές , όπως για παράδειγμα υπολογιστές παλάμης (PDAs) ή φορητοί υπολογιστές (laptops), χωρίς όμως αυτό να είναι απαραίτητο

Η βασική μονάδα κάθε 802.11 δικτύου αποκαλείται **βασική μονάδα υπηρεσιών** (basic service set – BSS) και αποτελείται από μια ομάδα σταθμών οι οποίοι επικοινωνούν μεταξύ τους. Τα όρια του BSS ορίζονται από την περιοχή ραδιοκάλυψης που ονομάζεται **βασική περιοχή υπηρεσιών** (basic service area – BSA). Με αυτό τον τρόπο ένας σταθμός σε ένα BSS μπορεί να επικοινωνεί με οποιονδήποτε άλλο σταθμό στο ίδιο BSS. Τα ασύρματα δίκτυα εμφανίζονται με δυο τοπολογίες, **των ανεξάρτητων δικτύων** (independent networks) και **των δικτύων υποδομής** (infrastructure networks) .

1.2.1 Τοπολογία ανεξάρτητου δικτύου/ Ad-Hoc

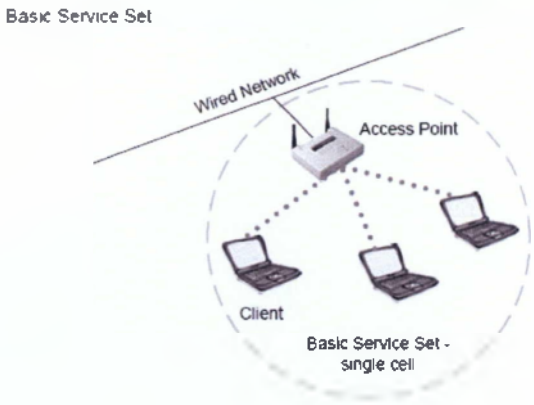
Στο **ανεξάρτητο δίκτυο** κάθε σταθμός επικοινωνεί απευθείας με όλους τους υπόλοιπους και αποτελεί τον πιο απλό τύπο ασύρματου δικτύου. Το BSS σε αυτή την τοπολογία ονομάζεται IBSS (independent BSS), ενώ πολλές φορές αναφέρεται και ως ad hoc δίκτυο ή ad hoc BSS. Σε αυτή την τοπολογία πρέπει όλοι οι σταθμοί να βρίσκονται στην περιοχή ραδιοκάλυψης με τους υπόλοιπους ώστε να υπάρχει επικοινωνία μεταξύ τους. Το IBSS αποτελείται τουλάχιστον από δυο σταθμούς και είναι προσωρινό, μέχρι να επιτελέσει το σκοπό του, καθώς μετά σταματά να υφίσταται. Το BSS το σύνολο από ίδια STAs τα οποία λειτουργούν κάτω από το ίδιο πρωτόκολλο.



Σχήμα 1.4: Τοπολογία IBSS (Ad-Hoc)

1.2.2 Τοπολογία δικτύου υποδομής

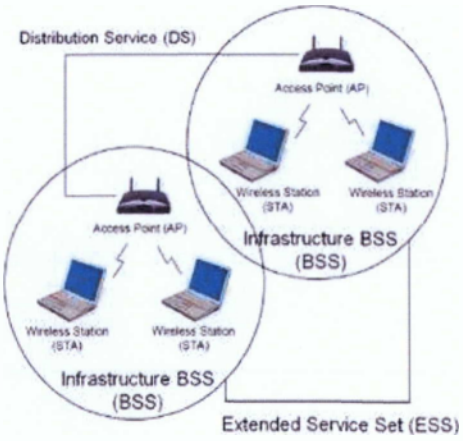
Σε ένα **δίκτυο υποδομής** διακρίνεται στο BSS η παρουσία ενός AP. Το AP που συνδέει το BSS με το ενσύρματο δίκτυο είναι υπεύθυνο για την ανταλλαγή πλαισίων μεταξύ των σταθμών καθώς και για τον κεντρικό έλεγχο της λειτουργίας του BSS. Όταν ένας σταθμός θέλει να αποστείλει ένα πλαίσιο σε έναν άλλο σταθμό, αρχικά το πλαίσιο αποστέλλεται στο AP και αυτό το στέλνει στον τελικό προορισμό του. Η BSA σε αυτή την τοπολογία είναι η περιοχή όπου υπάρχει ραδιοκάλυψη από το AP. Σε αντίθεση με το IBSS, όπου όλοι οι σταθμοί πρέπει να βρίσκονται στην περιοχή ραδιοκάλυψης των υπολοίπων, για να έχουν επικοινωνία με αυτούς, σε αυτή την περίπτωση αρκεί να βρίσκονται στην περιοχή ραδιοκάλυψης του AP, χωρίς να παίζει ρόλο η μεταξύ τους απόσταση. Για να μπορέσει να συμμετάσχει ένας σταθμός στο BSS θα πρέπει να ακολουθήσει την διαδικασία του association με το AP. Η διαδικασία αυτή πάντα αρχίζει με την πρωτοβουλία του σταθμού και είναι απόφαση του AP αν θα γίνει τελικά δεκτός ο σταθμός στο BSS.



Σχήμα 1.4: Τοπολογία δικτύου υποδομής (infrastructure BSS)

1.2.3 Τοπολογία ESS

Η τοπολογία αυτή αποτελείται από έναν αριθμό κυψελών. Η κάθε κυψέλη μπορεί να εξυπηρετείται από ένα σημείο πρόσβασης (AP) και όλα τα AP μπορούν να είναι συνδεδεμένα μεταξύ τους με μια δομή δικτύου μετάδοσης. Με βάση αυτή την τοπολογία μεγαλώνει και η εμβέλεια της ασύρματης κάλυψης. Σε περίπτωση που υπάρχει μόνο ένα AP δεν μπορεί να καλύψει μια ολόκληρη περιοχή ή την καλύπτει αλλά όχι στον μέγιστο βαθμό που επιθυμούμε τότε εγκαθιστούμε έναν αριθμό από AP σε διάφορα σημεία , για να έχουμε την κάλυψη ικανοποιητικά όλους τους χώρους και έπειτα συνδέουμε τα AP μεταξύ τους. Στην κυψελοειδή αυτή δομή του δικτύου ο κάθε ασύρματος σταθμός μπορεί να μετακινηθεί από την μια κυψέλη σε μια άλλη, χωρίς να χάνεται η σύνδεση του.



Σχήμα 1.5: Τοπολογία ESS

1.3 Εφαρμογές

Κατά την αρχική περίοδο της ανάπτυξης τους τα ασύρματα δίκτυα προορίζονταν ως αντικαταστάτες των ενσύρματων. Σήμερα αυτό έχει αλλάξει. Τα ενσύρματα δίκτυα προσφέροντας πολύ μεγαλύτερους ρυθμούς μετάδοσης , μεγαλύτερη ασφάλεια αλλά και ευκολία στην εγκατάσταση (τα σύγχρονα κτίρια διαθέτουν σχεδόν πάντα την καλωδίωση για την ενσύρματη δικτύωση) δεν πρόκειται να αντικατασταθούν εξολοκλήρου. Σήμερα τα ασύρματα δίκτυα έχουν τέσσερις βασικές εφαρμογές :

- **Επέκταση των ενσύρματων LAN:** Τα ενσύρματα δίκτυα χρησιμοποιούνται για τη διασύνδεση των χρηστών με το βασικό κορμό (backbone) του ασύρματου δικτύου. Έτσι, δεν απαιτείται η ύπαρξη καλωδίωσης μέχρι τον τελικό χρήστη, που μπορεί να είναι δύσκολο και οικονομικά ασύμφορο να εγκατασταθεί.
- **Διασύνδεση μεταξύ κτιρίων:** Είναι εφικτό με την τεχνολογία των ασύρματων δικτύων να κατασκευαστούν ζεύξεις μεταξύ κτιρίων. Οι συσκευές που συνδέονται στα δυο άκρα της ζεύξης είναι συνήθως δρομολογητές (routers) ή γέφυρες (bridges).
- **Σποραδική πρόσβαση στο δίκτυο:** Ασύρματα δίκτυα μπορούν να εγκατασταθούν σε χώρους όπου οι χρήστες κινούνται ελεύθερα, όπως για παράδειγμα σε βιβλιοθήκες, εκπαιδευτικά ιδρύματα ή χώρους εργασίας, για να προσφέρουν πρόσβαση στο ενσύρματο δίκτυο του κάθε οργανισμού. Το πιο σημαντικό θέμα σε αυτή την περίπτωση είναι φυσικά η ασφάλεια των δεδομένων.
- **Δημιουργία Ad-Hoc δικτύων:** Τα δίκτυα Ad-Hoc είναι peer-to-peer δίκτυα, που χρησιμοποιούνται συνήθως για την κάλυψη άμεσα συγκεκριμένων αναγκών. Τέτοια δίκτυα μπορούν να χρησιμοποιηθούν για παράδειγμα σε εργασιακούς χώρους ή σε αίθουσες διδασκαλίας, οπότε οι συμμετέχοντες μπορούν να ανταλλάσουν δεδομένα μέσω του προσωρινού ασύρματου δικτύου, χωρίς να έχει γίνει εκ των προτέρων διαμόρφωση του χώρου.

Κεφάλαιο 2

Η οικογένεια 802.11

2.1 Πρωτόκολλα Ασύρματων Δικτύων

Το Wi-Fi είναι το πρώτο ασύρματο πρωτόκολλο που εντάχτηκε δυναμικά στο χώρο της δικτύωσης, όπου οι αλλαγές και οι επαναστάσεις είναι ελάχιστες. Το πιο διαδεδομένο πρότυπο είναι το 802.11 και είναι σχεδιασμένο για να υλοποιεί μεγάλα ασύρματα τοπικά δίκτυα. Το πρωτόκολλο 802.11 είναι ορισμός του Media Access Control (MAC) Layer, καθώς και των τριών διαφορετικών και ασύμβατων physicalLayers του μοντέλου OSI. Στο πρωτόκολλο 802.11, έχουμε 2 τρόπους κωδικοποίησης τον **FHSS** και τον **DSSS**.

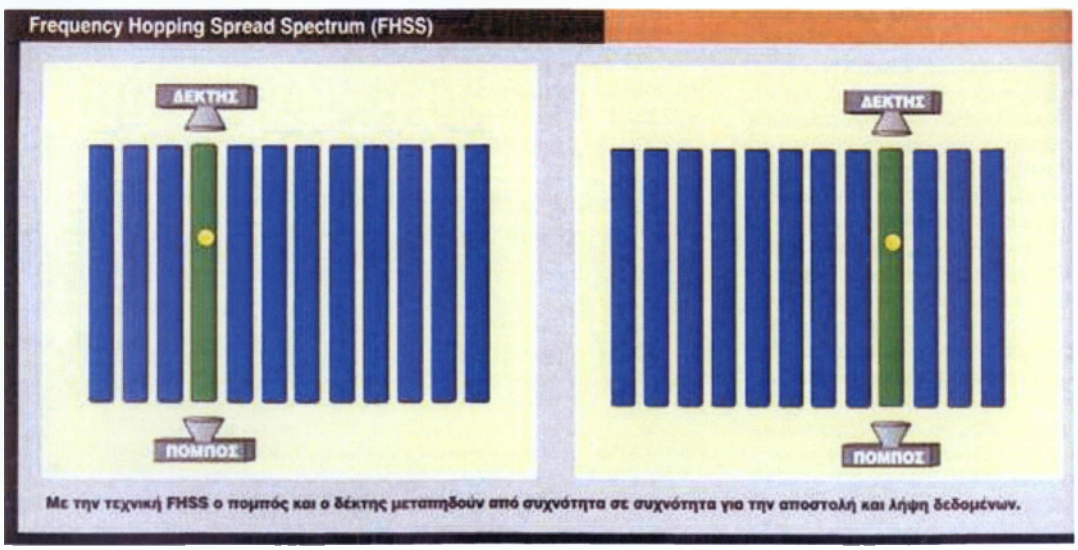
2.1.1 Η τεχνική Απλωμένου Φάσματος και Αναπήδησης Συχνότητας FHSS (Frequency Hopping Spread Spectrum)

Η τεχνική αναπήδησης συχνότητας χρησιμοποιήθηκε ευρέως σε εμπορικά προϊόντα. Όσον αναφορά τη μετάδοση. Η τεχνική αυτή βασίζεται στην ιδέα της αλλαγής της φέρουσας ενός σήματος μέσα σε ένα μεγάλο εύρος συχνοτήτων και σύμφωνα με το σχέδιο αναπήδησης. Μοιάζει με την κλασική FDMA (Frequency Division Multiple Access), με τη διαφορά ότι ο κάθε χρήστης χρησιμοποιεί κάθε φορά διάφορες φέρουσες ανάλογα με το σχέδιο αναπήδησης του. Για να επιτευχθεί επικοινωνία μεταξύ του πομπού και του δέκτη, πρέπει ο δέκτης να γνωρίζει το σχέδιο αναπήδησης του πομπού και να υπάρχει καλός συγχρονισμός μεταξύ τους. Τα πλεονεκτήματα της συγκεκριμένης τεχνικής έναντι της ευθείας ακολουθίας (DSSS) φυσικού στρώματος, είναι τα απλούστερα και φθηνότερα ηλεκτρονικά για την υλοποίηση των ανάλογων συσκευών, η χαμηλότερη κατανάλωση ενέργειας και η δυνατότητα συνύπαρξης πολλών τέτοιων δικτύων στην ίδια περιοχή χωρίς να επηρεάζεται η συνολική διέλευση. Άλλο ένα πλεονέκτημα της τεχνικής αυτής είναι η δυνατότητα συνύπαρξης διαφορετικών ασύρματων δικτύων, με τη μόνη προϋπόθεση ότι τα σχέδια αναπήδησης τους θα πρέπει να είναι διαφορετικά. Πιο συγκεκριμένα, σε κάθε χρονική στιγμή το κάθε σύστημα πρέπει να μεταδίδει σε διαφορετική φέρουσα και τα σχέδια αναπήδησης ονομάζονται ορθογώνια με τη συνολική διέλευση να μεγιστοποιείται. Το τρίτο και τελευταίο πλεονέκτημα είναι η δυνατότητα συνύπαρξης με χρήστες που εκπέμπουν σήματα στενής ζώνης. Αν η εκπομπή γίνεται με μεγάλη ισχύ από ένα σύστημα αναπήδησης συχνότητας (FH) η παρεμβολή που θα έχουν οι χρήστες είναι αμελητέα εφόσον μπλοκάρουν μια μόνο φέρουσα από όσες αυτό χρησιμοποιεί. Το φυσικό στρώμα FHSS στο πρότυπο 802.11 διαιρεί την ISM ζώνη των 2,4 GHz στα κανάλια εύρους ζώνης 1 MHz με το πρώτο κανάλι, δηλαδή το κανάλι 0 να έχει τη κεντρική του συχνότητα στα 2,4 GHz. Έχει οριστεί ότι το 99% της ενέργειας του εκπεμπόμενου σήματος, πρέπει να βρίσκεται μέσα στο κανάλι. Επίσης, υπάρχει αυστηρή προδιαγραφή τόσο ο χρόνος

εκπομπής μέσα σε ένα κανάλι (dwell time) που είναι ίσος περίπου με 0,4 δευτερόλεπτα, όσο και οι λεπτομέρειες της μεταπήδησης του από κανάλι σε κανάλι ανάλογα με το σχέδιο αναπήδησης. Όσο αναφορά την επίδοση του FH φυσικού στρώματος παρουσία θορύβου και παρεμβολών στενής ζώνης είναι ικανοποιητική και μειώνεται γραμμικά, όσο οι παρεμβολές αυξάνονται. Οι μεγάλες παρεμβολές σε ένα από τα χρησιμοποιούμενα κανάλια δεν προκαλούν μεγάλες αποκλίσεις στην απόδοση του αλλά όσο ο αριθμός των καναλιών που επηρεάζονται από τις παρεμβολές αυξάνεται, τόσο η μείωση της απόδοσης αρχίζει να γίνεται αισθητή.

Περιοχή και Υπεύθυνη Αρχή	Επιτρεπόμενα Κανάλια
ΗΠΑ, Καναδάς, IC	2 έως 79(2,402 – 2,479 GHz)
Ευρώπη εκτός Γαλλίας και Ισπανίας, ETSI	2 έως 79(2,402 – 2,479 GHz)
Γαλλία	48 έως 82 (2,448 – 2,482 GHz)
Ισπανία	47 έως 73 (2,447 – 2,473 GHz)
Ιαπωνία, MKK	73 έως 95 (2,473 – 2,495 GHz)

Πίνακας 2.1: Διαθέσιμα κανάλια FHSS στο 802.11



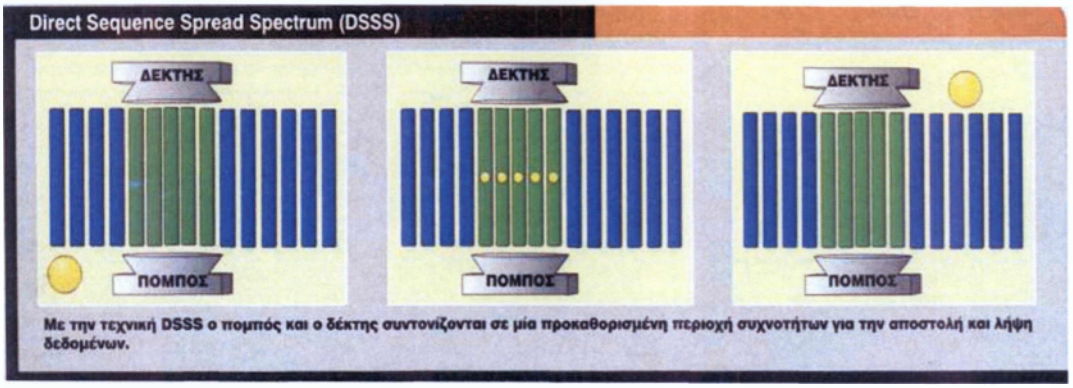
Σχήμα 2.1: Αποστολή και λήψη δεδομένων με την τεχνική FHSS

2.1.2 Η τεχνική Απλωμένου Φάσματος Ευθείας Ακολουθίας DSSS (Direct Sequence Spread Spectrum)

Η λειτουργία της τεχνικής αυτής είναι να πολλαπλασιάζει ένα φερον με ένα ψευδοθορυβώδες ψηφιακό σήμα και το σήμα που προκύπτει εμφανίζεται ως θόρυβος. Το εύρος ζώνης του μεταδιδόμενου σήματος καθορίζεται από το λόγο διεύρυνσης, ο οποίος είναι ίσος με τη διάρκεια ενός bit δεδομένων προς τη διάρκεια της δομικής μονάδας του κώδικα διεύρυνσης. Το μεγαλύτερο εύρος ζώνης της ευθείας ακολουθίας σήματος δίνει την δυνατότητα στην ισχύ του θορύβου να πέσει κάτω από το όριο του θορύβου, χωρίς να υπάρχουν καθόλου απώλειες πληροφορίας. Η τεχνική αυτή χρησιμοποιείται για να παραδώσει ρυθμούς δεδομένων στη ζώνη των 2,4GHz. Η διασπορά φάσματος είναι η μέθοδος που χρησιμοποιείται για τη μετάδοση δεδομένων σε περισσότερες από μια συχνότητες. Με αυτό τον τόπο διαμόρφωσης το σήμα είναι καλύτερα θωρακισμένο από το θόρυβο και τις παρεμβολές, επιτρέποντας να μοιράζονται τις συχνότητες λειτουργίας της περιοχής των 2,4 GHz πολλοί χρήστες με όσο γίνεται μικρότερες παρεμβολές. Η τεχνική μετάδοσης DSSS αντικαθιστά καθε bit πληροφορίας με μια σειρά από bits που ονομάζονται **κώδικας εξάπλωσης-διεύρυνση.** Τα bits του κώδικα διεύρυνσης ονομάζονται chips, τα οποία μεταδίδονται σε πολύ υψηλότερο ρυθμό από τα αρχικά bit πληροφορίας με αποτέλεσμα το φάσμα του μεταδιδόμενου σήματος να απλώνεται. Για παράδειγμα, αν αντικαθιστούσαμε κάθε bit με μια ακολουθία από 15 chips, θα είχε ως αποτέλεσμα το τελικό σήμα να καταλαμβάνει 15 φορές μεγαλύτερο φασματικό εύρος από ότι το αρχικό. Το χαρακτηριστικό αυτής της τεχνικής είναι ότι διευρύνει το φάσμα του προς μετάδοση σήματος μειώνοντας ταυτόχρονα το πλάτος του, αναγκάζοντας έτσι την ισχύ του σήματος να απλώνεται σε μεγαλύτερο φασματικό εύρος. Ο δέκτης ακολουθεί την αντίστροφη διαδικασία, εξάγει τα αρχικά bit πληροφορίας δημιουργώντας ξανά ένα σήμα στενής ζώνης. Για να το επιτύχει αυτό θα πρέπει να γνωρίζει τον κώδικα διεύρυνσης που είχε χρησιμοποιήσει ο πομπός. Το πλεονέκτημα της τεχνικής αυτης είναι η ανοχή της σε παρεμβολές στενης ζώνης καθώς και μεγαλύτερη ασφάλεια, εφόσον το απλωμένο σήμα μοιάζει σαν απλός θόρυβος σε πομπό που λαμβάνει σήμα στενής ζώνης. Τέλος, έχουν οριστεί 14 κανάλια στην μπάντα των 2,4 GHz με εύρος 5 MHz το κάθε ένα. Το κανάλι 1 έχει κεντρική συχνότητα τα 2,412 GHz και τα υπόλοιπα ακολουθούν κάθε 5 MHz. Στην πράξη κάθε κανάλι καταλαμβάνει περίπου 22 MHz εύρος γύρω από την κεντρική του συχνότητα.

Περιοχή και Υπεύθυνη Αρχή	Επιτρεπόμενα Κανάλια
ΗΠΑ, FCC – Καναδάς, IC	1 έως 11 (2,412 – 2,462 GHz)
Ευρώπη εκτος Γαλλίας και Ισπανίας, ETSI	1 έως 13 (2,412 – 2,472 GHz)
Γαλλία	10 έως 13 (2,457 – 2,472 GHz)
Ισπανία	10 έως 11 (2,457 – 2,462 GHz)
Ιαπωνία, MKK	14 (2,484 GHz)

Πίνακας 2.2 : Διαθέσιμα κανάλια DSSS στο 802.11

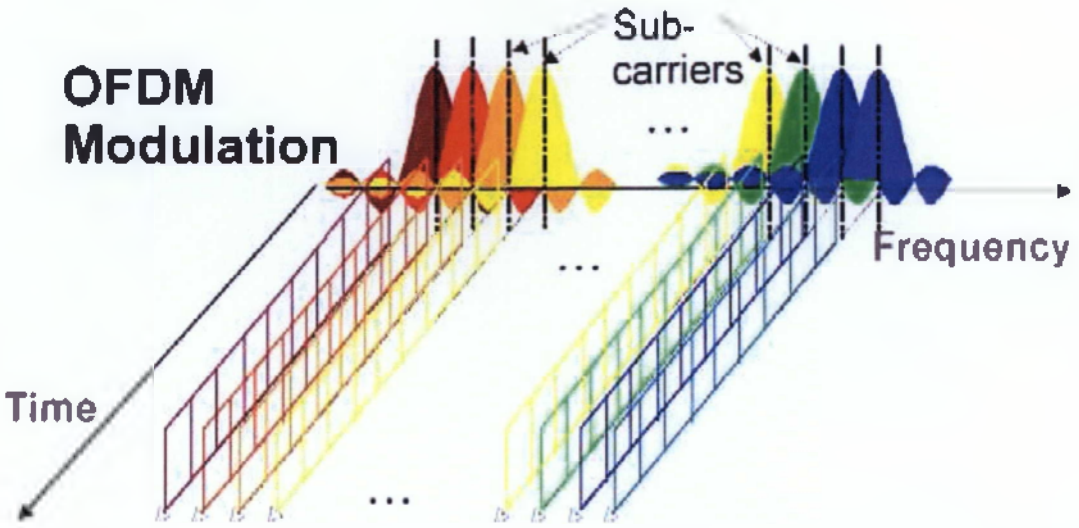


Σχήμα 2.2: Αποστολή και λήψη δεδομένων με την τεχνική DSSS

2.1.3 Η τεχνική OFDM (Orthogonal Frequency Division Multiplexing)

Η κωδικοποίηση OFDM, είναι μια μορφή διαμόρφωσης πολλών φερόντων σημάτων και έχει διαφορά από αυτήν της διασποράς φάσματος. Η τεχνική OFDM χωρίζει το σήμα σε πολύ μικρότερα υποσήματα, τα οποία εκπέμπουν σε διαφορετικές συχνότητες. Έτσι, έχουμε μείωση της διαφωνίας (crosstalk) στις μεταδόσεις σημάτων κάτι που κάνει το OFDM αρκετά χρήσιμο για την μετάδοση υψίρυθμων και ευρυζωνικών πληροφοριών. Επιπλέον με αυτό τον τρόπο η μετάδοση είναι αρκετά ανθεκτική στις παρεμβολές. Η IEEE έχει επιλέξει να χρησιμοποιήσει το OFDM στα πρότυπα 802.11a και 802.11g, με ταχύτητα μετάδοσης που φτάνει τα 54 Mbps. Αυτή η διαμόρφωση χρησιμοποιείται και στην τεχνολογία ADSL πετυχαίνοντας πολύ υψηλές ταχύτητες στα κοινά τηλεφωνικά δίκτυα, αλλά χρησιμοποιείται και στην ψηφιακή τηλεόραση. Ένα σύστημα OFDMA διαιρεί το διαθέσιμο φάσμα σε ομάδες, που ονομάζονται «sub channels» και διαμοιράζει σε πολλούς χρήστες ένα ή περισσότερα sub channels επιτρέποντας έτσι την ταυτόχρονη μετάδοση του σήματος. Τα σήματα που λαμβάνονται από διαφορετικούς χρήστες επικαλύπτονται στο πεδίο συχνοτήτων αλλά καταλαμβάνουν διαφορετικούς μεταφορείς και η ορθογωνικότητα μεταξύ των υποφερόντων αποτρέπει την ύπαρξη παρεμβολής πολλών χρηστών μεταξύ των

χρηστών. Τα συστήματα OFDM είναι αρκετά ευαίσθητα σε σφάλματα συγχρονισμού, τα οποία μπορεί να οδηγήσουν στην απώλεια της ορθογωνικοτητας αλλά και στην δημιουργία παρεμβολών μεταξύ των γειτονικών υποφερόντων.



Πρωτόκολλο	Χρονολογία	Συχνότητα Λειτουργίας	Ρυθμός Μετάδοσης Διδομένων (τυπικός)	Ρυθμός Μετάδοσης Διδομένων (μέγιστος)	Θεωρητικό Εύρος (σε κλειστό χώρο)	Θεωρητικό Εύρος (σε ανοιχτό χώρο)
802.11	1997	2.4-2.5 GHz	1Mbit/s	2Mbit / s	?	?
802.11 a	1999	5.15-5.35 5.47-5.725 5.725-5.875 GHz	25Mbit/s	54Mbit/s	30 μέτρα	?
802.11 b	1999	2.4-2.5 GHz	6.5Mbit/s	11Mbit/s	30 μέτρα	?
802.11 g	2003	2.4-2.5 GHz	25Mbit/s	54Mbit/s	30 μέτρα	?
802.11 n	2006 (πρώιμο)	Ζώνες 2.4 GHz ή 5 GHz	200Mbit/s	540Mbit/s	50 μέτρα	125 μέτρα

Πίνακας 2.3: Συνοπτική συγκριτική παρουσίαση των σημαντικότερων χαρακτηριστικών των πρωτοκόλλων 802.11

2.2 802.11a

Το πρότυπο 802.11a μπήκε στην αγορά, αφού το 802.11b είχε ήδη εισέρθει. Αντίθετα με το πρότυπο 802.11b, το οποίο λειτουργεί στην ISM μπάντα των 2,4 GHz, το πρότυπο 802.11a χρησιμοποιεί την μπάντα των 5 GHz. Το πρότυπο 802.11a παρέχει ταχύτητες μέχρι και 54 Mbps (από τα οποία τα ωφέλιμα είναι περίπου 25 Mbps), το οποίο μας δίνει αύξηση της ταχύτητας 5 φορές σε σύγκριση με το πρότυπο 802.11b. Οι υψηλότερες ραδιοσυχνότητες έχουν ως αποτέλεσμα την μείωση σε μεγάλο βαθμό της απόστασης κάλυψης καθώς και την διεισδυτική δύναμη του 802.11a, πιο πολύ σε εσωτερικούς χώρους. Για παράδειγμα, αν μια μετάδοση που χρησιμοποιούσε το πρότυπο 802.11b θα περνούσε από ένα τοίχο η ίδια μετάδοση αλλά με το πρότυπο 802.11a θα εμποδιζόταν. Στις ΗΠΑ η μπάντα των 5 GHz η οποία διατίθεται για ελεύθερη χρήση ονομάζεται **U-NII (Unlicensed National Information Infrastructure).** Εκτός από τα οφέλη που προσφέρει η χρήση των υψηλότερων συχνοτήτων, παρατηρούνται και διάφορα προβλήματα. Αυτά παρατηρούνται περισσότερο στις αυξημένες απώλειες διάδοσης που εμφανίζονται στην μπάντα των 5 GHz σε σύγκριση με αυτές των 2,4 GHz. Το πρόβλημα αυτό λύνεται είτε με πυκνότερη διάταξη των AP για την κάλυψη μιας δεδομένης περιοχής είτε με αυξημένη ακτινοβολούμενη ισχύ από τους πομπούς. Ενδεχομένως, η πρώτη λύση να μην είναι τόσο εφικτή οικονομικά, ενώ η δεύτερη αυξάνει σε μεγάλο βαθμό την κατανάλωση ενέργειας των κινητών τερματικών , με αποτέλεσμα να υπάρξει μείωση της αυτονομίας τους. Το πρότυπο 802.11a χρησιμοποιεί την τεχνική πολυπλεξίας **OFDM (Orthogonal Frequency Division Multiplexing).**

2.3 802.11b

Το πρότυπο αυτό ανακοινώθηκε από την IEEE το 1999. Χρησιμοποιεί την ελεύθερη μπάντα των 2,4 GHz και προσφέρει ρυθμούς μετάδοσης μέχρι και 11 Mbps. Είναι το πιο διαδεδομένο πρότυπο στην αγορά αυτή την στιγμή παρότι το πρότυπο 802.11a παρέχει υψηλότερους ρυθμούς μετάδοσης. Είναι συμβατό με το πρότυπο 802.11g. Χρησιμοποιεί την τεχνική Απλωμένου Φάσματος Ευθείας Ακολουθίας **DSSS (Direct Sequence Spread Spectrum).** Εξαιτίας των επιβαρύνσεων στη μεταδιδόμενη πληροφορία από τα πρωτόκολλα διασύνδεσης, το ωφέλιμο bandwidth μειώνεται στα 6 Mbps. Η απόσταση μεταξύ των συσκευών είναι περίπου στα 30 μέτρα σε εσωτερικό χώρο και πάνω από 120 μέτρα σε εξωτερικό χώρο. Οι αποστάσεις αυτές εύκολα αυξάνονται με την τοποθέτηση εξωτερικών κεραιών που ενισχύουν το σήμα.

2.4 802.11g

Το 2003 η IEEE κοινοποίησε το πρότυπο 802.11g, το οποίο υποστηρίζει ρυθμούς μετάδοσης έως και 54 Mbps .Έχει εμβέλεια εσωτερικού χώρου έως και 38m. Χρησιμοποιεί την ISM μπάντα των 2,4 GHz. Σε αντίθεση με το 802.11b, χρησιμοποιεί την OFDM τεχνική για να πετύχει τους επιθυμητούς ρυθμούς μετάδοσης. Το σημαντικότερο χαρακτηριστικό του 802.11g είναι η συμβατότητα του με το 802.11b.

2.5 802.11n

Ένα σημαντικό πρότυπο ασύρματης τοπικής δικτύωσης, το οποίο αναπτύχτηκε από τον οργανισμό IEEE είναι το 802.11n, το οποίο δημοσιεύτηκε τον Οκτώβριο του 2009. Το πρότυπο 802.11g το οποίο επικυρώθηκε το 2003, καθίσταται ανεπαρκές, γιατί οι εφαρμογές γίνονται αρκετά πολύπλοκες και απαιτούν μεγαλύτερο εύρος ζώνης. Για παράδειγμα ένα streaming video ή μια ταινία κανονικής διάρκειας στο σπίτι, δεν μπορεί να υλοποιηθεί με το πρότυπο 802.11g. Όλα τα προϊόντα που χρησιμοποιούν το πρότυπο 802.11g έχουν μέγιστη διεκπεραιωτική ικανότητα η οποία είναι ίση με 54 Mbits/sec, αλλά σε πραγματικές συνθήκες , η ταχύτατα αυτή είναι περίπου στη μέση ή ακόμα χαμηλότερα, δεν είναι εφικτή για αναπαραγωγή video. Για να ξεπεραστεί το πρόβλημα αυτό εφαρμόστηκε η αναθεώρηση του προτύπου 802.11n, το οποίο υπόσχεται ταχύτητες έως 100Mbps ανώτερες από αυτές του προτύπου 802.11g και ανώτερη εμβέλεια εκπομπής. Το νέο πρότυπο 802.11n χρησιμοποιεί μια καινούργια τεχνολογία η οποία βελτιώνει τις ήδη υπάρχουσες τεχνολογίες για να αποδώσει στο Wi-Fi μεγαλύτερη ταχύτητα και εμβέλεια. Η νέα τεχνολογία είναι **Multiple Input Multiple Output (MIMO).** Η τεχνολογία **MIMO** χρησιμοποιεί πολλαπλές κεραίες για την μεταφορά πολλαπλών ροών δεδομένων από ένα σημείο σε ένα άλλο. Αντί να στείλει και να λάβει μόνο μια ροή δεδομένων, έχει την ικανότητα να μεταδώσει ταυτόχρονα τρεις ροές δεδομένων και να παραλάβει δύο, αυτό έχει ως αποτέλεσμα να αποστέλλονται περισσότερα δεδομένα την ίδια χρονική περίοδο. Η τεχνική αυτή μπορεί επιπλέον να αυξήσει την εμβέλεια εκπομπής ή την απόσταση μεταξύ των δεδομένων που θα αποσταλούν. Μια δεύτερη τεχνολογία, η οποία ενσωματώνεται στο πρότυπο 802.11n είναι η **channel bonding**, η οποία χρησιμοποιεί δυο ξεχωριστά και μη αλληλεπικαλυπτόμενα κανάλια την ίδια χρονική στιγμή για την μετάδοση δεδομένων. Η τεχνική αυτή επίσης αυξάνει την ποσότητα των δεδομένων που μπορούν να αποσταλούν.

2.6 802.11ac

Το νέο πρότυπο 802.11ac είναι υπό κατασκευή και γίνονται οι πρώτες δοκιμές από την Ιαπωνική εταιρεία **NTT (Nippon Telegraph and Telephone Corporation)**. Το νέο πρότυπο θα προσφέρει θεωρητικές ταχύτητες Gigabit περίπου 125MB/s, όμως θα λειτουργεί κοντά στα 6 GHz (όπως και το πρότυπο 802.11a) και όχι στα 2,4 GHz όπως τα πρότυπα 802.11b/g/n. Σύμφωνα με υπολογισμούς της εταιρείας In-Stat μετά από έρευνα που έγινε, υπολογίζεται ότι το 2015 θα διανεμηθούν πάνω από 1 δισεκατομμύριο συσκευές που θα χρησιμοποιούν το πρότυπο αυτό. Ένα από τα βασικά πλεονεκτήματα του προτύπου αυτού είναι ότι θα εξασφαλίσει την απρόσκοπτη μετάδοση HD Video, κάτι που δεν γινόταν πάντοτε από το πρότυπο 802.11n. Όπως είναι λογικό θα υπάρξουν και κάποια μειονεκτήματα από την χρήση του προτύπου αυτού. Για παράδειγμα, θα πρέπει να υποστηρίζεται από θύρες USB 3.0 για να μπορεί να αποδίδει το μέγιστο. Επίσης, οι συσκευές που θα υποστηρίζουν το πρότυπο, αυτό όπως laptops και tablets, θα έχουν μεγάλο κόστος αγοράς.

2.7 802.11ad

Το νέο "WI Gig" είναι ένα καινούργιο ασύρματο πρότυπο, το οποίο έχει την πιστοποίηση της IEEE, με τους ειδικούς να υποστηρίζουν ότι πρόκειται για μια τεχνολογία που κατά πάσα πιθανότητα θα αντικαταστήσει το HDMI ίσως και νωρίτερα από το 2015. Το 802.11ad ή "WI Gig" (η κοινή ονομασία του) είναι το νέο πρότυπο ασύρματης επικοινωνίας, το οποίο θα μπορούσε να αντικαταστήσει τόσο το HDMI όσο και τα υπόλοιπα καλώδια οθονών. Το 802.11ad πρότυπο έχει σαν στόχο να παρέχει ταχύτητες μετάδοσης δεδομένων μέχρι και 7 Gbps. Για την επίτευξη αυτών των ταχυτήτων χρησιμοποιεί την ISM μπάντα με ζώνη συχνοτήτων στα 60 GHz για να επιτευχθούν τα επίπεδα του εύρους ζώνης που απαιτούνται και για να εξασφαλίσει μειωμένα επίπεδα παρεμβολών. Κάνοντας χρήση συχνοτήτων στην περιοχή των χιλιοστών, το IEEE 802.11ad microwave WI-FI έχει εμβέλεια της τάξεως των μερικών μέτρων. Στόχος είναι να χρησιμοποιείται σε πολύ μικρές αποστάσεις (για παράδειγμα σε ένα δωμάτιο) για την μεταφορά μεγάλων όγκων δεδομένων, όπως για παράδειγμα βίντεο υψηλής ευκρίνειας(High Definition, HD). Για μεγαλύτερες αποστάσεις απαιτείται η χρήση άλλων προτύπων, όπως το 802.11ac.

2.8 Πλαίσια και τύποι πλαισίων

Το μοντέλο αυτό είναι βασισμένο σε μια πρόταση που έχει αναπτυχθεί από το Διεθνή Οργανισμό Τυποποίησης (International Standards Organization ISO), ως ένα πρώτο βήμα για τη διεθνή τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων. Αναθεωρήθηκε το 1995.

Σχήμα 2.3: Layer Δικτύου / Μοντέλο Αναφοράς OSI - Μετάδοση δεδομένων στο μοντέλο αναφοράς OSI

Το μοντέλο ονομάζεται **Μοντέλο Αναφοράς ISO OSI** (ISO OSI Reference Model), όπου OSI σημαίνει **Διασύνδεση Ανοικτών Συστημάτων** (Open Systems Interconnection), επειδή ασχολείται με τη διασύνδεση ανοικτών συστημάτων. Δηλαδή, συστημάτων, τα οποία είναι ανοικτά στην επικοινωνία με αλλά συστήματα. Το μοντέλο OSI έχει επτά επίπεδα. Οι αρχές που εφαρμόστηκαν για να καταλήξουμε σε αυτά τα επτά επίπεδα συνοψίζονται ως εξής:

- Όπου χρειάζεται μια διαφορετική λογική αφαίρεση πρέπει να δημιουργείται ένα επίπεδο.
- Κάθε επίπεδο πρέπει να εκτελεί μια σαφώς καθορισμένη λειτουργία.
- Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται με στόχο τον καθορισμό διεθνώς τυποποιημένων πρωτοκόλλων.
- Τα σύνορα των επιπέδων πρέπει να επιλέγονται έτσι ώστε να ελαχιστοποιείται η ροή πληροφοριών μέσω της διασύνδεσης των επιπέδων.

- Το πλήθος των επιπέδων πρέπει να είναι αρκετά μεγάλο για να μην χρειάζεται να ανακατεύονται χωρίς λόγο διαφορετικές λειτουργίες στο ίδιο επίπεδο και ταυτόχρονα αρκετά μικρό για να μην γίνεται άβολη η αρχιτεκτονική.

2.8.1 Layer 1: Φυσικό Επίπεδο (Physical Layer)

Το **φυσικό επίπεδο** (physical layer) ασχολείται με τη μετάδοση ανεπεξέργαστων δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Τα ζητήματα σχεδίασης του σχετίζονται με την εξασφάλιση του ότι, όταν η μια πλευρά στέλνει το bit 1, αυτό θα λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Τα ερωτήματα που τίθενται στο επίπεδο αυτό είναι πόσα Volt πρέπει να χρησιμοποιούνται για την αναπαράσταση του 1 bit και πόσα για το 0, πόσα νανοδευτερόλεπτα διαρκεί ένα bit, κατά πόσον θα μπορεί να γίνεται η μετάδοση ταυτόχρονα και προς τις δυο κατευθύνσεις, πως μπορεί να εγκαθιδρυθεί η αρχική σύνδεση και πως τερματίζεται όταν τελειώσουν και οι δυο πλευρές. Τα ζητήματα σχεδίασης εδώ έχουν να κάνουν κυρίως, με μηχανικές, ηλεκτρονικές και χρονικές διασυνδέσεις καθώς και με το φυσικό μέσο μετάδοσης, το οποίο βρίσκεται κάτω από το φυσικό επίπεδο.

2.8.2 Layer 2: Επίπεδο Μετάδοσης Δεδομένων (Data Link Layer)

Η βασική λειτουργία του **επιπέδου συνδέσμου μετάδοσης δεδομένων** (data link layer) είναι να μετασχηματίζει μια υπηρεσία μετάδοσης ανεπεξέργαστων δεδομένων σε μια γραμμή η οποία να φαίνεται στο επίπεδο δικτύου ότι δεν παρουσιάζει τον κίνδυνο μη εντοπισμένων σφαλμάτων μετάδοσης. Ο στόχος αυτός μπορεί να επιτευχτεί με το να βάλουμε τον αποστολέα να τεμαχίζει τα δεδομένα εισόδου σε **πλαίσια δεδομένων**(data frames) με τυπικό μέγεθος λίγες εκατοντάδες ή λίγες χιλιάδες byte και έτσι να μεταδίδει τα πλαίσια με τη σειρά. Αν η υπηρεσία είναι αξιόπιστη ,ο παραλήπτης επιβεβαιώνει την ορθή λήψη κάθε πλαισίου επιστρέφοντας ένα **πλαίσιο επιβεβαίωσης** (acknowledgment frame). Ένα ακόμη πρόβλημα που παρουσιάζεται στο επίπεδο συνδέσμου μετάδοσης δεδομένων είναι το πώς μπορεί να αποτραπεί ένας γρήγορος αποστολέας από το να κατακλύσει με δεδομένα έναν αργό παραλήπτη. Συχνά απαιτείται κάποιος μηχανισμός ο οποίος θα ρυθμίζει την κυκλοφορία έτσι ώστε ο αποστολέας να γνωρίζει πόσο χώρο προσωρινής αποθήκευσης διαθέτει ανά πάσα στιγμή ο παραλήπτης. Τις περισσότερες φορές οι μηχανισμοί ρύθμισης της κυκλοφορίας και διαχείρισης των σφαλμάτων είναι ενοποιημένοι. Στα δίκτυα εκπομπής υπάρχει άλλο ένα ζήτημα στο επίπεδο συνδέσμου μετάδοσης δεδομένων: το πώς θα γίνεται ο έλεγχος πρόσβασης στο κοινόχρηστο κανάλι. Με το πρόβλημα αυτό ασχολείται ένα ειδικό υποεπίπεδο του επιπέδου σύνδεσης μετάδοσης δεδομένων, το υποεπίπεδο ελέγχου προσπέλασης μέσων.

2.8.3 Layer 3: Επίπεδο Δικτύου (Network Layer)

Το **επίπεδο δικτύου** (network layer) ελέγχει την λειτουργία του υποδικτύου. Ένα βασικό ζήτημα σχεδίασης είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την προσέλευση προς τον προορισμό τους. Τα δρομολόγια μπορεί να βασίζονται σε στατικούς πίνακες οι οποίοι είναι "προσηλωμένοι" στο δίκτυο και μεταβάλλονται σπάνια. Επίσης, μπορεί να προσδιορίζονται στην αρχή κάθε συνομιλίας για παράδειγμα, στην αρχή μιας περιόδου εργασίας τερματικού (δηλαδή, όταν πραγματοποιείται μια σύνδεση σε κάποια απομακρυσμένη μηχανή). Τέλος, μπορεί να είναι εντελώς δυναμικά , δηλαδή να καθορίζονται εκ νέου για κάθε πακέτο, έτσι ώστε να αντανακλούν το τρέχον φορτίο του δικτύου. Σε περίπτωση που υπάρχουν πάρα πολλά πακέτα στο υποδίκτυο την ίδια χρονική στιγμή, θα αρχίσουν να "παρεμποδίζουν" το ένα το άλλο, δημιουργώντας έτσι συμφόρηση. Όταν ένα πακέτο πρέπει να ταξιδέψει από ένα δίκτυο σε κάποιο άλλο με σκοπό να φτάσει στον προορισμό του, υπάρχει η πιθανότητα εμφάνισης πολλών προβλημάτων. Η διευθυνσιοδότηση που χρησιμοποιείται από το δεύτερο δίκτυο μπορεί να διαφέρει από εκείνη του πρώτου. Υπάρχει πιθανότητα το δεύτερο δίκτυο να μη δεχτεί καθόλου το πακέτο, αν αυτό είναι πολύ μεγάλο. Επίσης, μπορεί να διαφέρουν τα πρωτόκολλα. Στα δίκτυα εκπομπής το πρόβλημα της δρομολόγησης είναι απλό, έτσι το επίπεδο δικτύου είναι συνήθως υποτυπώδες ή ακόμα και ανύπαρκτο.

2.8.4 Layer 4: Επίπεδο Μεταφοράς (Transport Layer)

Η βασική λειτουργία του **επιπέδου μεταφοράς** (transport layer) είναι να δέχεται δεδομένα από το ανώτερο επίπεδο, να τα διασπά αν χρειάζεται σε μικρότερες μονάδες, να τα μεταβιβάζει στο επίπεδο δικτύου, και να εξασφαλίζει ότι όλα τα τμήματα φτάνουν σωστά στο άλλο άκρο. Επιπλέον, όλα αυτά πρέπει να γίνονται με αποδοτικό τρόπο έτσι ώστε να απομονώνονται τα ανώτερα επίπεδα από τις αναπόφευκτες τεχνολογικές αλλαγές που προκύπτουν στο χρησιμοποιούμενο υλικό. Επίσης, το επίπεδο μεταφοράς καθορίζει τον τύπο της υπηρεσίας που θα παρέχεται στο επίπεδο συνδιάλεξης και τελικά στους χρήστες του δικτύου. Ο πιο δημοφιλής τύπος σύνδεσης στο επίπεδο μεταφοράς είναι ένα απαλλαγμένο από σφάλματα κανάλι από σημείο σε σημείο, το οποίο παραδίδει μηνύματα ή byte με τη σειρά που στάλθηκαν. Αλλά πιθανά είδη υπηρεσίας μεταφοράς είναι η μεταφορά μεμονωμένων μηνυμάτων χωρίς εγγυήσεις για τη σειρά μετάδοσης τους και η εκπομπή μηνυμάτων σε πολλαπλούς προορισμούς. Ο τύπος της υπηρεσίας καθορίζεται όταν εγκαθιδρύεται η σύνδεση. Παρεμπιπτόντως είναι αδύνατο να επιτύχουμε ένα κανάλι χωρίς καθόλου σφάλματα. Αυτό που εννοεί ο όρος *«απαλλαγμένο από σφάλματα»* είναι ότι το ποσοστό σφαλμάτων είναι αρκετά χαμηλό ώστε πρακτικέ να παραβλέπεται. Το επίπεδο μεταφοράς είναι ένα πραγματικό επίπεδο "απ' άκρου εις άκρο (end to end), δηλαδή από

την προέλευση έως τον προορισμό. Ένα πρόγραμμα στη μηχανή προέλευσης πραγματοποιεί "συνομιλία" με ένα παρόμοιο πρόγραμμα στη μηχανή προορισμού, χρησιμοποιώντας τις κεφαλίδες των μηνυμάτων και τα μηνύματα ελέγχου. Στα κατώτερο επίπεδα τα πρωτόκολλα λειτουργούν ανάμεσα σε κάθε μηχανή και τους άμεσους γείτονες της και όχι ανάμεσα στις ακραίες μηχανές προέλευσης και προορισμού όπου ενδιαμέσως μπορεί να υπάρχουν πολλοί δρομολογητές.

2.8.5 Layer 5: Το επίπεδο συνδιάλεξης (session layer)

Το **επίπεδο συνδιάλεξης** ή **επίπεδο περιόδου σύνδεσης** (session layer) επιτρέπει σε χρήστες διαφορετικών μηχανών να εγκαθιδρύουν **συνδιαλέξεις** (sessions) μεταξύ τους. Οι συνδιαλέξεις προσφέρουν διάφορες υπηρεσίες, στις οποίες περιλαμβάνονται ο **έλεγχος διαλόγου** (dialog control, η παρακολούθηση του ποιος έχει σειρά να μεταδώσει), η **διαχείριση σκυτάλης** (token management, η αποτροπή των δυο πλευρών από το να επιχειρήσουν ταυτόχρονα την εκτέλεση της ίδιας κρίσιμης λειτουργίας) και ο **συγχρονισμός** (synchronization, η τήρηση σημείων ελέγχου σε μακρόχρονες μεταδόσεις έτσι ώστε αυτές να μπορούν να συνεχιστούν από το σημείο όπου διακόπηκαν, μετά από μια κατάρρευση του συστήματος).

2.8.6 Layer 6: Το επίπεδο παρουσίασης (presentation layer)

Σε αντίθεση με τα κατώτερα επίπεδα, που ασχολούνται κυρίως με τη μεταφορά bit, το **επίπεδο παρουσίασης** (presentation layer) ασχολείται με τη σύνταξη και τη σημασιολογία των μεταδιδομένων πληροφοριών. Για να είναι εφικτή η επικοινωνία μεταξύ υπολογιστών που χρησιμοποιούν διαφορετικές αναπαραστάσεις δεδομένων, μπορούν να οριστούν με αφαιρετικό τρόπο οι δομές δεδομένων που θα ανταλλάσσονται, μαζί με μια τυποποιημένη κωδικοποίηση που θα χρησιμοποιείται "μέσα στο καλώδιο". Το επίπεδο παρουσίασης διαχειρίζεται αυτές τις αφαιρετικές δομές δεδομένων και επιτρέπει τον ορισμό και την ανταλλαγή δομών δεδομένων υψηλού επιπέδου όπως για παράδειγμα τραπεζικών εγγραφών.

2.8.7 Layer 7: Το επίπεδο εφαρμογών (application layer)

Το **επίπεδο εφαρμογών** (application layer) περιέχει μια ποικιλία πρωτοκόλλων που απαιτούνται συχνά από τους χρήστες. Ένα ευρέως χρησιμοποιούμενο πρωτόκολλο εφαρμογής είναι το **Πρωτόκολλο Μεταφοράς Υπέρ-κειμένου** ή **HTTP** (Hyper Text Transfer Protocol), το οποίο είναι η βάση του Παγκόσμιου Ιστού. Όταν ένα πρόγραμμα φυλλομέτρησης (browser) χρειάζεται μια ιστοσελίδα, στέλνει το όνομα της επιθυμητής σελίδας στο διακομιστή, χρησιμοποιώντας το πρωτόκολλο HTTP. Ο διακομιστής επιστρέφει στη συνέχεια τη

σελίδα. Αλλά πρωτόκολλα εφαρμογών χρησιμοποιούνται για τη μεταφορά αρχείων, το ηλεκτρονικό ταχυδρομείο και τις ομάδες ειδήσεων δικτύου.

Κεφάλαιο 3

Η οικογένεια 802.11Πρότυπα / Οργανισμοί Τυποποίησης Κανονικοποίησης Προτύπων (Standards Association)

3.1 Wi-Fi Alliance

Η **Wi-Fi Alliance** είναι μια παγκόσμια μη κερδοσκοπική ένωση του κλάδου των εκατοντάδων από τις κορυφαίες εταιρείες που διατίθενται για απρόσκοπτη συνδεσιμότητα. Με την ανάπτυξη της τεχνολογίας, την οικοδόμηση της αγοράς και των ρυθμιστικών προγραμμάτων, η **Wi-Fi Alliance** επέτρεψε την ευρεία υιοθέτηση της Wi-Fi σε όλο τον κόσμο. Το **Wi-Fi CERTIFIED** πρόγραμμα ξεκίνησε το Μάρτιο του 2000. Παρέχει μια ευρέως αναγνωρισμένη ονομασία της διαλειτουργικότητας και της ποιότητας και βοηθά να εξασφαλιστεί ότι τα **Wi-Fi enabled** προϊόντα προσφέρουν καλύτερη εμπειρία στον χρήστη. Η Wi-Fi Alliance έχει πιστοποιήσει περισσότερα από 15.000 προϊόντα, ενθαρρύνοντας την εκτεταμένη χρήση των Wi-Fi προϊόντων και υπηρεσιών σε νέες και καθιερωμένες αγορές. Το 1999, αρκετοί οραματιστές ηγέτες ενώθηκαν για να σχηματίσουν μια παγκόσμια μη κερδοσκοπική οργάνωση με στόχο την προώθηση της υιοθέτησης των υψηλών ταχυτήτων ασύρματων τοπικών δικτύου περιοχής. Σήμερα, σε κάθε ήπειρο, ένας στους δέκα ανθρώπους σε όλο τον κόσμο χρησιμοποιούν το Wi-Fi στο σπίτι, στην εργασία, με αμέτρητους τρόπους. Η Wi-Fi έκδοση συνεχίζει να αυξάνεται και οι κοινοί στόχοι εξακολουθούν να συνδέουν πάνω από 500 Wi-Fi εταιρείες-μέλη της Συμμαχίας από δεκάδες χώρες. Ο αρχικός στόχος των οραματιστών ηγετών που διαμόρφωσαν την Wi-Fi Alliance το 1999 έχει πραγματοποιηθεί και όμως η Wi-Fi Alliance δεν γίνεται. Η ηγεσία της καινοτομίας και της σκέψης του Wi-Fi Alliance εξακολουθεί να οδηγεί τις νέες Wi-Fi εφαρμογές και τα προϊόντα και συνεχίζει να εμπλουτίζει την ζωή μας. Το Wi-Fi CERTIFIED οδηγεί τον χρήστη σε βελτιωμένη εμπειρία, σε υψηλότερα ποσοστά ικανοποίησης των πελατών, σε λιγότερες κλήσεις υποστήριξης και επιστροφές προϊόντων αλλά και μειωμένο κόστος. Τα προγράμματα με την πιστοποίηση της **Wi-Fi Alliance** υπήρξαν σημαντικός παράγοντος για την ταχεία εξάπλωση των προϊόντων Wi-Fi σε οικείες, χώρους εργασίας και δημόσιους χώρους κατά την υφήλιο.

3.2 IEEE

Το **Ινστιτούτο Ηλεκτρολογίας και Ηλεκτρονικής (IEEE)** είναι ένας επαγγελματικός σύλλογος με έδρα την Πόλη της Νέας Υόρκης που είναι αφιερωμένη στην προώθηση της τεχνολογικής καινοτομίας και αριστείας. Έχει περίπου 425.000 μέλη σε 160 χώρες , ελαφρώς λιγότερα από τους διαμένοντες στις Ηνωμένες Πολιτείες.

Το IEEE είναι ενσωματωμένο συμφώνα με το νόμο Μη Κερδοσκοπικών Εταιρειών της πολιτείας της Νέας Υόρκης στις Ηνωμένες Πολιτείες. Σχηματίστηκε το 1963 από τη

συγχώνευση του Ινστιτούτου Ράδιο-μηχανολογίας και του Αμερικανικού Ινστιτούτου Ηλεκτρολογίας. Τα μεγάλα συμφέροντα του **AIEE** (American Institute of Electrical Engineers) ήταν οι ενσύρματες επικοινωνίες (η τηλεγραφία και η τηλεφωνία), το φως και η δύναμη των συστημάτων. Το **IRE** (Institute of Radio Engineers) αφορούσε περισσότερο τη ράδιο-μηχανολογία και σχηματίστηκε από δυο μικρότερους οργανισμούς, την Κοινότητα Μηχανολογίας Ασύρματων και Τηλέγραφου και το Ινστιτούτο Ασυρμάτων. Με την ανάπτυξη των ηλεκτρονικών στη δεκαετία του 1930, οι ηλεκτρονικοί μηχανικοί έγιναν μέλη του IRE, αλλά οι εφαρμογές της ηλεκτρονικής τεχνολογίας σωλήνα έγινε τόσο εκτεταμένη που τα τεχνικά όρια τα οποία διαφοροποιούσαν την **IRE** και την **AIEE** ήταν δύσκολο να διαχωριστούν. Μετά τον Δεύτερο Παγκόσμιο Πόλεμο οι δυο οργανισμοί έγιναν πολύ ανταγωνιστικοί και το 1961 η ηγεσία και των δυο **IRE** και **AIEE** κατέληξε στην εδραίωση των δυο οργανισμών. Οι δυο οργανισμοί συγχωνεύτηκαν επίσημα ως **IEEE** την 1η Ιανουαρίου του 1963. Αξιοσημείωτοι Πρόεδροι του IEEE και ιδρυτικά μέλη της περιλαμβάνουν τον **Elihu Thomson** (AIEE ,1889-1890), **Alexander Graham Bell** (AIEE, 1891-1892), **Charles Proteus Steinmetz** (AIEE , 1901-1902), **Lee De Forest** (IRE, 1930), **Frederic E. Terman** (IRE, 1941), William **R. Hewlett** (IRE, 1954), Ernst **Weber** (IRE, 1959), **Ivan Getting** (IEEE, 1978). Το Σύνταγμα της IEEE, καθορίζει τους σκοπούς του οργανισμού ως επιστημονικούς και εκπαιδευτικούς, οδηγούμενους προς την ανάπτυξη της θεωρίας και της πρακτικής της Ηλεκτρολογίας, Ηλεκτρονικής, των Επικοινωνιών και Μηχανικών Ηλεκτρονικών Υπολογιστών , καθώς και την Επιστήμη των Υπολογιστών , των συμμαχικών κλάδους της μηχανικής και των σχετικών τεχνών και επιστημών. Για την επίτευξη αυτών των στόχων, το IEEE χρησιμεύει ως ο κύριος εκδότης επιστημονικών κειμένων και διοργανωτής συνεδριών, ημερίδων και συμπονιών. Είναι επίσης ένας σημαντικός οργανισμός ανάπτυξης προτύπων για την ανάπτυξη των βιομηχανικών προτύπων (έχοντας αναπτύξει πάνω από 900 ενεργές βιομηχανίες τεχνικών προτύπων) σε ένα ευρύ φάσμα επιστημονικών κλάδων, συμπεριλαμβανομένου της ηλεκτρικής ενέργειας και της ενέργειας, της βίο-ιατρικής τεχνολογίας και της υγειονομικής περίθαλψης, της τεχνολογίας των πληροφοριών, τη διασφάλιση των πληροφοριών, των τηλεπικοινωνιών, των ηλεκτρικών ειδών ευρείας κατανάλωσης, των μεταφορών, της αεροδιαστημικής και της νανοτεχνολογίας. Το IEEE αναπτύσσει και συμμετέχει σε εκπαιδευτικές δραστηριότητες όπως η διαπίστευση των ηλεκτρικών προγραμμάτων μηχανικής σε ιδρύματα ανώτερης εκπαίδευσης. Το λογότυπο της IEEE είναι ένα διαμάντι και δημιουργήθηκε το χρόνο της συγχώνευσης το 1963. Το IEEE έχει μια διπλή συμπληρωματική περιφερειακή και τεχνική δομή, με τις οργανωτικές μονάδες που βασίζονται στη γεωγραφική και τεχνολογική εστίαση. Διαχειρίζεται μια ξεχωριστή οργανωτική μονάδα, η οποία συνιστά τη διαμόρφωση πολιτικών και υλοποιεί προγράμματα που προορίζονται ειδικά προς όφελος των μελών της, του επαγγέλματος

και του κοινού στις Ηνωμένες Πολιτείες. Το IEEE περιλαμβάνει 38 τεχνικές εταιρείες, οι οποίες οργανώνονται γύρω από εξειδικευμένους τεχνικούς τομείς, με περισσότερες από 300 τοπικές οργανώσεις που πραγματοποιούν τακτικές συναντήσεις.

3.2.1 Ιδιότητα και Βαθμός του μέλους

Τα περισσότερα μέλη του **IEEE** είναι ηλεκτρονικοί και ηλεκτρολόγοι μηχανικοί, αλλά ο κύριος σκοπός του οργανισμού είναι να προσελκύσει ανθρώπους από άλλους κλάδους για παράδειγμα από την μηχανολογία, την φυσική , τη βιολογία και τα μαθηματικά. Ένα άτομο μπορεί να ενταχτεί στην **IEEE** ως φοιτητικό μέλος, ως επαγγελματικό μέλος ή ως συνέταιρος. Υπάρχουν διάφορες κατηγορίες και επίπεδα των μελών και της ένταξης τους της IEEE:

- **Φοιτητικά Μέλη:** Η συμμετοχή των φοιτητών είναι διαθέσιμη με μειωμένη συνδρομή για όσους είναι εγγεγραμμένοι σε διαπιστευμένο ίδρυμα της τριτοβάθμιας εκπαίδευσης, όπως προπτυχιακούς ή μεταπτυχιακούς φοιτητές στον τομέα της τεχνολογίας ή της μηχανικής.
- **Μέλη:** Η συνηθισμένη ή η επαγγελματική ιδιότητα του μέλους απαιτεί ότι το άτομο έχει αποφοιτήσει από ένα τεχνολογικό ή μηχανολογικό πρόγραμμα ενός διαπιστευμένου ιδρύματος της τριτοβάθμιας εκπαίδευσης ή να έχουν επιδείξει επαγγελματική επάρκεια στην τεχνολογία ή την μηχανολογία μέσα από τουλάχιστον έξι χρόνια επαγγελματικής εμπειρίας.
- **Εταιρικοί Συνεργάτες:** Κάποιοι σύλλογοι του IEEE επιτρέπουν σε ένα άτομο το οποίο δεν είναι μέλος του IEEE να γίνει μέλος του συλλόγου ενός συγκεκριμένου συλλόγου μέσα στο IEEE, που του επιτρέπει περιορισμένη συμμετοχή στη δουλειά του συγκεκριμένου συλλόγου του IEEE.
- **Ανώτερα Μέλη:** Εάν πληρούν συγκεκριμένες απαιτήσεις, ένα επαγγελματικό μέλος μπορεί να θέση υποψηφιότητα για Ανώτερο Μέλος που είναι το υψηλότερο επίπεδο αναγνώρισης για το οποίο μπορεί να αιτηθεί ένα επαγγελματικό μέλος. Οι αιτούντες για Ανώτερα Μέλη πρέπει να διαθέτουν τουλάχιστον τρεις συστατικές επιστολές από Ανώτερα Τιμώμενα Μέλη και να πληρούν αλλά πρότυπα εκπαίδευσης , επίτευξης, συνεισφοράς και εμπειρίας στον τομέα. Τα Ανώτερα Μέλη είναι μια επιλεγμένη ομάδα και ορισμένες θέσεις του IEEE είναι διαθέσιμες μόνο σε Ανώτερα Μέλη. Η ανώτερη συμμετοχή είναι επίσης μια από τις απαιτήσεις για αυτούς που είναι υποψήφιοι για τον βαθμό του εταίρου του IEEE, μιας ξεχωριστής τιμής.

- **Εταίροι:** Ο βαθμός συμμετοχής του Εταίρου είναι το υψηλότερο επίπεδο συμμετοχής και δεν μπορεί να γίνει αίτηση απευθείας από το μέλος, ο υποψήφιος θα πρέπει να προταθεί από άλλους. Ο βαθμός συμμετοχής απονέμεται από το Διοικητικό Συμβούλιο του IEEE προς αναγνώριση του υψηλού επιπέδου αποδεδειγμένων εξαιρετικών επιτευγμάτων.
- **Τιμητικά Μέλη:** Τα άτομα που δεν είναι μέλη του IEEE αλλά έχουν επιδείξει εξαιρετικές συνεισφορές, όπως να έχουν λάβει Τιμητικό Μετάλλιο από το IEEE, μπορούν να λάβουν τιμητική συμμετοχή από το Διοικητικό Συμβούλιο του IEEE.
- **Παντοτινά Μέλη και Παντοτινοί Εταίροι:** Τα μέλη που έχουν φτάσει την ηλικία των 65 χρονών και ο αριθμός της συμμετοχής τους μαζί με την ηλικία τους φτάνει τα 100, αναγνωρίζονται ως Παντοτινά Μέλη και στην περίπτωση των Εταίρων Μελών, ως Παντοτινοί Εταίροι.

3.2.2 IEEE Ίδρυμα

Το ίδρυμα **IEEE** είναι ένα φιλανθρωπικό ίδρυμα που ιδρύθηκε το 1973 για να υποστηρίξει και να προωθήσει την τεχνολογία της εκπαίδευσης , της καινοτομίας και της αριστείας. Έχει ενσωματωθεί ξεχωριστά από το IEEE αν και έχει μια στενή σχέση με αυτό. Τα μέλη του Διοικητικού Συμβουλίου του Ιδρύματος πρέπει να είναι ενεργά μέλη της IEEE και το ένα τρίτο από αυτούς πρέπει να είναι εν ενεργεία ή πρώην μέλη του Διοικητικού Συμβουλίου του IEEE. Αρχικά, ο ρόλος του IEEE Ιδρύματος ήταν να δέχεται και να διαχειρίζεται δωρεές για το πρόγραμμα IEEE Awards, αλλά οι δωρεές αυξήθηκαν πέρα από ότι ήταν απαραίτητο για αυτό τον σκοπό , καθώς και το πεδίο εφαρμογής διευρύνθηκε. Επιπλέον, στο να επιδιώκουν και να διαχειρίζονται απεριόριστα ποσά , το ίδρυμα διαχειρίστηκε τα ποσά αυτά για να στηρίξει εκπαιδευτικά, ανθρωπιστικά και ιστορικά προγράμματα του IEEE. Ως προς το τέλος του 2012, τα συνολικά περιουσιακά στοιχεία ήταν κοντά στα 3,7 εκατομμύρια$.

3.2.3 Υποτροφίες

- **Η IEEE Life Members Graduate Study Fellowship in Electrical Engineering** ιδρύθηκε από την IEEE το 2000. Η υποτροφία δίνεται ετησίως σε αποφοίτους με πλήρες πρόγραμμα παρακολούθησης για τον πρώτο χρόνο , οι οποίοι κάνουν το μάστερ τους στον τομέα της ηλεκτρολογίας – μηχανολογίας σε σχολή ή πρόγραμμα διεθνούς αναγνώρισης.
- **Η IEEE Charles LeGeyt Fortescue Graduate Scholarship** ιδρύθηκε το 1939 από την IRE για να τιμήσει την μνήμη του Charles LeGeyt Fortescue για την προσφορά του στον τομέα της ηλεκτρολογίας - μηχανολογίας. Η υποτροφία

δίνεται για ένα χρόνο σε φοιτητές που παρακολουθούν ένα πλήρες πρόγραμμα μαθημάτων και επιθυμούν να αποκτήσουν μάστερ στην ηλεκτρολογία – μηχανολογία , στη σχολή ηλεκτρολογίας της ΑΝΕ η οποία αναγνωρίζεται από τις ΗΠΑ.

3.3 Federal Communication Commission (FCC)

Η Ομοσπονδιακή Επιτροπή Επικοινωνιών (**FCC**) είναι ένας ανεξάρτητος οργανισμός της κυβέρνησης των Ηνωμένων Πολιτειών , που δημιουργήθηκε από τον κανονισμό του Κογκρέσου και με την πλειοψηφία των διοικητικών επιτροπών της να έχουν διοριστεί από τον σημερινό Πρόεδρο. Η FCC εργάζεται για έξι στόχους στους τομείς των ευρυζωνικών συνδέσεων , του ανταγωνισμού, του φάσματος, των μέσων ενημέρωσης, της δημόσιας ασφάλειας και της εσωτερικής ασφάλειας. Η επιτροπή είναι επίσης στην διαδικασία του εκσυγχρονισμού της. Η FCC σχηματίστηκε από την Communications Act(Νομοθετική πράξη των Επικοινωνιών του 1934) για να αντικαταστήσει τις λειτουργίες ρύθμισης του ραδιοφώνου της Ομοσπονδιακής Επιτροπής Ραδιοφώνου. Η ανάθεση δικαιοδοσίας της FCC καλύπτει 50 πολιτείες, την περιοχή της Κολομβίας και τα κεκτημένα των Ηνωμένων Πολιτειών. Η FCC παρέχει επίσης ποικίλους βαθμούς συνεργασίας , την εποπτεία και την ηγεσία για παρόμοιους οργανισμούς επικοινωνιών και σε άλλες χώρες της Βόρειας Αμερικής. Η FCC χρηματοδοτείται εξολοκλήρου από τις ρυθμιστικές αμοιβές. Έχει κατ εκτίμηση δημοσιονομικό προϋπολογισμό για το 2011 335.8 εκατομμύρια δολάρια και ένα προτεινόμενο δημοσιονομικό προϋπολογισμό για το 2012 όπου ανέρχεται στα 354.2 εκατομμύρια δολάρια. Έχει 1898 ομοσπονδιακούς υπαλλήλους.

3.3.1 Αποστολή και Στρατηγική

Η αποστολή της FCC που καθορίζεται στον τομέα ένα της Νομοθετικής ΙΙράξης Επικοινωνιών του 1934 και τροποποιήθηκε από τη Νομοθετική Πράξη των Τηλεπικοινωνιών του 1996 είναι να καθιστά διαθέσιμες στο βαθμό που είναι δυνατόν , σε όλους τους ανθρώπους των Ηνωμένων Πολιτειών, χωρίς διάκριση όσο αναφορά τη φυλή, το χρώμα, τη θρησκεία , την εθνική καταγωγή ή το φύλλο, γρήγορες, αποτελεσματικές , Εθνικής εμβέλειας και παγκόσμιας εμβέλειας υπηρεσίες ενσύρματης επικοινωνίας με επαρκείς εγκαταστάσεις και εύλογες χρεώσεις. Η FCC έχει εντοπίσει έξι στόχους από το 2006 έως το 2011 με βάση του Στρατηγικού Σχεδίου της. Αυτοί είναι :

- **Ευρεία Ζώνη Συχνοτήτων**

Όλοι οι Αμερικανοί θα πρέπει να έχουν προσιτή πρόσβαση σε ισχυρά και αξιόπιστα προϊόντα και υπηρεσίες ευρείας ζώνης συχνοτήτων. Οι ρυθμιστικές πολιτικές πρέπει να

προωθούν την τεχνολογική ουδετερότητα, τον ανταγωνισμό, τις επενδύσεις και την καινοτομία για να εξασφαλιστεί ότι οι πάροχοι ευρυζωνικών υπηρεσιών έχουν επαρκή κίνητρα για να αναπτύξουν και να προσφέρουν τέτοια προϊόντα και υπηρεσίες.

- **Ανταγωνισμός**

Ο ανταγωνισμός στην παροχή υπηρεσιών επικοινωνίας , τόσο στο εσωτερικό όσο και στο εξωτερικό, στηρίζει την Εθνική οικονομία. Το ανταγωνιστικό πλαίσιο για τις υπηρεσίες επικοινωνιών θα πρέπει να προωθήσει την καινοτομία και να προσφέρει στους καταναλωτές αξιόπιστη και ουσιαστική επιλογή υπηρεσιών σε προσιτές τιμές.

- **Φάσμα**

Η αποτελεσματική και αποδοτική χρήση του μη-ομοσπονδιακού φάσματος στα εγχώρια αλλά και διεθνώς , προωθεί την ανάπτυξη και την ταχεία βελτίωση των καινοτόμων και αποτελεσματικών επικοινωνιακών τεχνολογιών και υπηρεσιών.

- **Μέσα Ενημέρωσης**

Οι κανονισμοί των Εθνικών μέσων πρέπει να προωθούν τον ανταγωνισμό και την ποικιλομορφία και να διευκολύνουν τη μετάβαση στους ψηφιακούς τρόπους παράδοσης.

- **Δημόσια και Εσωτερική Ασφάλεια**

Οι επικοινωνίες κατά τη διάρκεια εκτάκτων αναγκών και κρίσεων θα πρέπει να είναι διαθέσιμες για τη δημόσια ασφάλεια , την υγεία , την άμυνα και του προσωπικού έκτακτης ανάγκης καθώς επίσης όλων των καταναλωτών που τις έχουν ανάγκη.

- **Εκσυγχρονισμός FCC**

Η επιτροπή θα πρέπει να δουλέψει σκληρά προκειμένου να είναι παραγωγική, προσαρμοστική και καινοτόμα που θα μεγιστοποιεί τα οφέλη των μετόχων, του προσωπικού και της διαχείρισης από αποτελεσματικά συστήματα , τις διαδικασίες και τους πόρους.

3.3.2 Οργάνωση

Η FCC διευθύνεται από πέντε εντεταλμένους που διορίζονται από τον πρόεδρο των Ηνωμένων Πολιτειών και επιβεβαιώνονται από την Γερουσία των Ηνωμένων Πολιτειών για διάρκεια πέντε χρόνων. Ο πρόεδρος επιλέγει έναν από τους εντεταλμένους για να διατελέσει ως πρόεδρος. Μόνο τρεις εντεταλμένοι μπορούν να είναι μέλη του ίδιου πολιτικού κόμματος. Κανείς από αυτούς δεν πρέπει να έχει οικονομικό όφελος από τις σχηματιζόμενες υπηρεσίες της FCC.

Εντεταλμένοι

Όνομα	Θέση	Κατοικία	Λήξη
Jessica Rosenworcel	Εντεταλμένη	Κονέκτικατ	2015
Ajit Pai	Εντεταλμένος	Κάνσας	2016
Mignon Clyburn	Πρόεδρος	Νότια Καρολίνα	2017

Η **FCC** οργανώνεται σε **έξι Φορείς** και σε **έντεκα Γραφεία Προσωπικού.**

3.3.3 Φορείς

Οι φορείς επεξεργάζονται αιτήσεις για άδειες, αναλύουν καταγγελίες, διεξάγουν έρευνες, αναπτύσσουν και εφαρμόζουν κανονισμούς και συμμετέχουν σε ακροάσεις.

- **Ο φορέας καταναλωτών και Κυβερνητικών Υποθέσεων(CGB)** αναπτύσσει και εφαρμόζει τις πολιτικές των καταναλωτών της FCC, συμπεριλαμβανομένης και της πρόσβασης σε άτομα με αναπηρία. Ο **CGB** εξυπηρετεί την **FCC** ως δημόσιο πρόσωπο μέσω της εκπαίδευσης, καθώς επίσης και μέσω του κέντρου καταναλωτών, το οποίο είναι υπεύθυνο για να ανταποκρίνεται στα ερωτήματα και τις καταγγελίες των καταναλωτών. Ο **CGB** διατηρεί επίσης συνεργατικές σχέσεις με την πολιτεία, με τις τοπικές και φυλετικές κυβερνήσεις σε τομείς όπως η ετοιμότητα για περιστατικά έκτακτης ανάγκης και για την εφαρμογή νέων τεχνολογιών.
- **Ο φορέας Εφαρμογής (Enforcement Bureau –EB)** είναι υπεύθυνος για την εφαρμογή των προβλέψεων της Νομοθετικής Πράξης των Επικοινωνιών του 1934 , των κανόνων **FCC**, των εντολών **FCC** των όρων και των συνθηκών των σταθμών εξουσιοδότησης. Οι σημαντικοί τομείς εφαρμογής που διαχειρίζονται από τον **Φορέα Εφαρμογής** είναι η προστασία του καταναλωτή, ο τοπικός ανταγωνισμός, η δημόσια ασφάλεια και η εσωτερική ασφάλεια.
- **Ο Διεθνής Φορέας (International Bureau – IB)** αναπτύσσει διεθνείς πολιτικές στον τομέα των τηλεπικοινωνιών , όπως ο συντονισμός της κατανομής συχνοτήτων και περιφερειακών αναθέσεων έτσι ώστε να μειωθούν οι περιπτώσεις διεθνούς ηλεκτρομαγνητικών παρεμβολών που αφορούν τους δικαιούχους των Ηνωμένων Πολιτειών. Ο **Διεθνής Φορέας** επιβάλλει επίσης τη τήρηση **FCC** των διεθνών κανονισμών ασυρμάτων και άλλων διεθνών συμφωνιών.
- **Ο Φορέας Μέσων (Media Bureau – MB)** αναπτύσσει, συστήνει και διαχειρίζεται τα προγράμματα πολιτικής και αδειών που σχετίζονται με τα

ηλεκτρονικά μέσα, συμπεριλαμβανομένης της καλωδιακής τηλεόρασης και του ραδιοφώνου στις Ηνωμένες Πολιτείες και στα εδάφη της. Ο **Φορέας Μέσων** μετά την χορήγηση άδειας χειρίζεται επίσης θέματα τα οποία αφορούν την άμεση εξυπηρέτηση της δορυφορικής εκπομπής.

- **Ο Φορέας Ασύρματων Τηλεπικοινωνιών (Wireless Telecommunications Bureau)** ρυθμίζει τα προγράμματα των εγχώριων ασύρματων τηλεπικοινωνιών και πολιτικές συμπεριλαμβανομένου των αδειών. Ο Φορέας επίσης εφαρμόζει ανταγωνιστικές προσφορές για δημοπρασίες και ρυθμίζει τις ασύρματες υπηρεσίες επικοινωνιών , συμπεριλαμβανόμενων των κινητών τηλεφώνων, της δημόσιας ασφάλειας και άλλων εμπορικών και ιδιωτικών υπηρεσιών ραδιοφώνων.
- **Ο Φορέας Ενσύρματου Ανταγωνισμού (Wireline Competition Bureau - WCB)** αναπτύσσει μια πολιτική που αφορά τις ενσύρματες επικοινωνίες. Ο κύριος στόχος του **Φορέα Ενσύρματου Ανταγωνισμού** είναι να προωθήσει την ανάπτυξη και τις οικονομικές επενδύσεις στην υποδομή των ενσύρματων τεχνολογιών, της ανάπτυξης, της αγοράς και των υπηρεσιών.

3.3.4 Γραφεία

Τα γραφέα της **FCC** παρέχουν υπηρεσίες υποστήριξης στους Φορείς.

- **Το Γραφείο Διοικητικών Νομικών Κριτών (Office of Administrative Law Judges - OALJ)**, είναι υπεύθυνο για την διεξαγωγή των ακροάσεων που διατάσσονται από την επιτροπή. Η λειτουργία της ακρόασης περιλαμβάνει ενέργειες για αιτήσεις ασφαλιστικών μέτρων που κατατέθηκαν στο πλαίσιο της δίκης, όπως αίτηση για παρέμβαση, αίτηση για μεγέθυνση θεμάτων και αμφισβητούμενων αιτήσεων. Ο **Διοικητικός Νομικός Κριτής**, διορίζεται σύμφωνα με τη **Διοικητική Διαδικαστική Νομοθετική Πράξη** και προεδρεύει στην ακρόαση κατά τη διάρκεια της οποία λαμβάνονται έγγραφα και ένορκες καταθέσεις που λαμβάνονται ως αποδεικτικά στοιχεία και οι μάρτυρες επανεξετάζονται. Μετά την ολοκλήρωση της φάσης της αποδεικτικής διαδικασίας , ο προεδρεύων **Διοικητικός Νομικός Κριτής** γράφει και εκδίδει την αρχική απόφαση , με βάση της οποίας μπορεί να ασκηθεί έφεση στην Επιτροπή.
- **Το Γραφείο Επικοινωνιακών Επιχειρηματικών Ευκαιριών (Office of Communications Business Opportunities - OCBO)** προωθεί τις επιχειρηματικές ευκαιρίες τηλεπικοινωνιών για μικρές, μειονεκτικές και γυναικείες επιχειρήσεις. Το **OCBO** συνεργάζεται με τους επιχειρηματίες , με την βιομηχανία, με τους οργανισμούς δημόσιου συμφέροντος, με ιδιώτες και άλλους

για να παρέχουν πληροφορίες σχετικά με τις πολιτικές της **FCC**, την αύξηση της ιδιοκτησίας, των ευκαιριών απασχόλησης , την προώθηση μιας ποικιλίας φωνών και απόψεων μέσω των ερτζιανών κυμάτων (ραδιοφωνικά και τηλεοπτικά κύματα) και την ενθάρρυνση της συμμετοχής στις διαδικασίες της **FCC**.

- **Το Γραφείο της Εφαρμοσμένης Μηχανικής και της Τεχνολογίας (Office of Engineering and Technology- OET)**, συμβουλεύει την Επιτροπή σχετικά με θέματα μηχανικής.
- Ο κύριος ρόλος του είναι να διαχειρίζεται το ηλεκτρομαγνητικό φάσμα και συγκεκριμένα την κατανομή των συχνοτήτων και τη χρήση του ραδιοφάσματος. Το **OET** διεξάγει τεχνικές μελέτες προχωρημένων φάσεων των επίγειων επικοινωνιών και διαχειρίζεται τους κανονισμούς της **FCC** σχετικά με τις ραδιοφωνικές συσκευές, τις πειραματικές ραδιοφωνικές υπηρεσίες καθώς και τον βιομηχανικό, τον επιστημονικό και τον ιατρικό εξοπλισμό.
- Το **OET** οργανώνει το **Τεχνικό Συμβουλευτικό Συμβούλιο**, μια επιτροπή της **FCC** και των συμβουλών της από μεγάλες τηλεπικοινωνιακές και επιχειρήσεις μέσων.
- Το **OET** λειτουργεί τον Κλάδο Πιστοποίησης Εξοπλισμού που έχει ως καθήκον να επιτηρεί την πιστοποίηση του εξοπλισμού για όλες τις συσκευές που χρησιμοποιούν ηλεκτρομαγνητική ενέργεια από 9 kHz έως 300 GHz. Το OET διατηρεί μια ηλεκτρομαγνητική βάση δεδομένων όλων των πιστοποιημένων εξοπλισμών στα οποία μπορεί το κοινό να έχει εύκολη πρόσβαση.
- **Το Γραφείο Γενικής Συμβουλής (Office of General Counsel)** εξυπηρετεί ως ο κύριος νομικός σύμβουλος της Επιτροπής. Η **Γενική Συμβουλευτική** επίσης αντιπροσωπεύει την Επιτροπή σε δικαστικούς αγώνες στα ομοσπονδιακά δικαστήρια των Ηνωμένων Πολιτειών, συνιστά αποφάσεις σε υποθέσεις ενώπιων της Επιτροπής, βοηθά την Επιτροπή στη λήψη αποφάσεων και προβαίνει σε διάφορες νομικές λειτουργίες σχετικά με εσωτερικές και διοικητικές υποθέσεις.
- **Το Γραφείο του Γενικού Επιθεωρητή (The Office of the Inspector General – OIG)** προτείνει πολιτικές για την πρόληψη της απάτης στις λειτουργίες των πρακτόρων. Ο **Γενικός Επιθεωρητής** εισηγείται διορθωτικές πράξεις όπου θεωρούνται απαραίτητες, αναφέρει ποινικές υποθέσεις στο Υπουργείο Δικαιοσύνης των Ηνωμένων Πολιτειών για πιθανή δίωξη.
- **Το Γραφείο των Νομοθετικών Υποθέσεων (The Office of Legislative Affairs – OLA)** αποτελεί τη διασύνδεση στο Κογκρέσο των Ηνωμένων Πολιτειών , παρέχοντας στους νομοθέτες πληροφορίες σχετικά με τους κανονισμούς της **FCC**. Το **OLA** επίσης προετοιμάζει τους μάρτυρες της **FCC** για

τις ακροάσεις του Κογκρέσου και βοηθά στη δημιουργία των απαντήσεων της **FCC** σε νομοθετικές προτάσεις και σε έρευνες του Κογκρέσου. Επιπλέον, το **OLA** είναι μια διασύνδεση με άλλα ομοσπονδιακά πρακτορεία καθώς επίσης και με κρατικές και τοπικές κυβερνήσεις.

- **Το Γραφείο του Γενικού Διευθυντή (The Office of the Managing Director – OMD)** είναι υπεύθυνο για τη διοίκηση και τη διαχείριση της **FCC**, συμπεριλαμβανόμενου του προϋπολογισμού, του προσωπικού, της ασφάλειας , των συμβάσεων και των εκδόσεων.
- **Το Γραφείο των Σχέσεων με τα ΜΜΕ (The Office of Media Relations – OMR)** είναι υπεύθυνο για τη διάδοση των ανακοινώσεων της **Επιτροπής**, των διαταγών , των διαδικασιών καθώς και άλλων πληροφοριών ανά αίτηση μέσων. Το **OMR** διαχειρίζεται την Καθημερινή Σύντομη Ανασκόπηση της **FCC** , την ιστοσελίδα και το Οπτικοακουστικό Κέντρο.
- **Το Γραφείο του Γενικού Γραμματέα (The Office of the Secretary – OSEC)** επιβλέπει τη λήψη και τη διανομή τω έγγραφων που αρχειοθετούνται από το κοινό μέσω των ηλεκτρονικών συστημάτων συμπλήρωσης εγγράφων και τη συλλογή της βιβλιοθήκης της **FCC**. Επιπλέον, το **OSEC** εκδίδει νομικές σημειώσεις των αποφάσεων της Επιτροπής στο Ομοσπονδιακό Αρχείο και το Αρχείο της **FCC**.
- **Το Γραφείο Στρατηγικού Σχεδιασμού και Ανάλυσης Πολιτικής (The Office of Strategic Planning and Policy Analysis – OSP)**, ουσιαστικά είναι μια δεξαμενή σκέψης εντός της **FCC**, η οποία προσδιορίζει τους στόχους της πολιτικής για τον οργανισμό. Το **OSP** συνεργάζεται στενά με τον Πρόεδρο της **FCC** και είναι υπεύθυνο για την παρακολούθηση της κατάστασης του κλάδου των επικοινωνιών για τον εντοπισμό των τάσεων, των θεμάτων και της συνολικής βιομηχανικής υγείας. Το **OSP** ενεργεί ως έμπειρος σύμβουλος προς την **Επιτροπή** στους τομείς των οικονομικών, των επιχειρήσεων και την ανάλυση της αγοράς. Το **Γραφείο** επίσης ελέγχει τις νομικές τάσεις και τις βελτιώσεις που δε σχετίζονται απαραίτητα με τις παρούσες διαδικασίες της **FCC**, όπως η νομοθεσία περί πνευματικής ιδιοκτησίας, το διαδίκτυο και το ηλεκτρονικό εμπόριο. Προηγουμένως το **OSP** ονομαζόταν **Γραφείο Σχεδιασμού και Πολιτικής (The Office of Plans and Policy – OPP)**.
- **Το Γραφείο Ποικιλομορφίας στο Χώρο Εργασίας (The Office of Workplace Diversity – OWD)** αναπτύσσει πολιτική για να παρέχει πλήρεις και δίκαιες ευκαιρίες για όλους τους εργαζομένους , ανεξάρτητα από παράγοντες που έχουν να κάνουν, με τη φυλή, τη θρησκεία, το φύλο, το χρώμα , την ηλικία , την αναπηρία , του φυλετικού προσανατολισμού ή της εθνικής προελεύσεως , την εκτέλεση των καθηκόντων τους στο χώρο εργασίας απαλλαγμένο από

παράνομη διακριτική μεταχείριση, συμπεριλαμβανομένης της σεξουαλικής παρενόχλησης και των αντιποίνων για τη συμμετοχή σε νομικά προστατευόμενες δραστηριότητες.

3.4 Ιστορία

3.4.1 Νομοθετική Πράξη των Επικοινωνιών του 1934

Το 1934, το Κογκρέσο πέρασε τη Νομοθετική Πράξη , η οποία κατάργησε την Ομοσπονδιακή Επιτροπή Ραδιοφώνου και μεταφέρθηκε δικαιοδοσία αδειοδότησης ραδιοφωνικών σταθμών σε μια νέα Ομοσπονδιακή Επιτροπή Επικοινωνιών, συμπεριλαμβάνοντας σε αυτή επίσης την τηλεπικοινωνιακή δικαιοδοσία που πριν διαχειριζόταν από την Διαπολιτειακή Εμπορική Επιτροπή.

3.4.2 Η Αναφορά στο Chain Broadcasting

Το 1940 η Ομοσπονδιακή Επιτροπή Επικοινωνιών εξέδωσε την Αναφορά για broadcasting Chain που οδηγούνταν από τον νέο πρόεδρο της FCC James Lawrence Fly. Το κύριο σημείο στην αναφορά ήταν η διάλυση της Εθνικής Εταιρείας Μετάδοσης, που τελικά οδήγησε στη δημιουργία της Αμερικανικής Εταιρείας Μετάδοσης, αλλά υπήρχαν δυο ακόμα σημαντικά σημεία. Ένα από αυτά ήταν η επιλογή χρόνου του δικτύου, με υπαίτιο την CBS. Η αναφορά περιόρισε την ποσότητα του χρόνου κατά τη διάρκεια της ημέρας και ποιες ώρες μπορούν τα δίκτυα να μεταδίδουν. Η δεύτερη αφορούσε τα γραφεία καλλιτεχνών.

3.4.3 «Πάγωμα» του 1948

Κατά τον καθορισμό των τηλεοπτικών σταθμών σε διάφορες πόλεις μετά τον Δεύτερο Παγκόσμιο Πόλεμο, η FCC διαπίστωσε ότι τοποθετούνται πολλοί σταθμοί , οι οποίοι είναι πολύ κοντά ο ένας στον άλλον, με αποτέλεσμα να υπάρχουν παρεμβολές. Την ίδια στιγμή, ήταν προφανές ότι τα καθορισμένα VHF κανάλια, από 2 έως 13, ήταν ανεπαρκή για πανεθνική υπηρεσία τηλεόρασης. Ως αποτέλεσμα, η FCC σταμάτησε να δίνει νέες κατασκευαστικές άδειες τον Οκτώβριο του 1948. Το αναμενόμενο ήταν το "πάγωμα" να διαρκέσει έξι μήνες , αλλά καθώς η κατανομή καναλιών στην αναδυόμενη τεχνολογία UHF και η ανυπόμονα αναμενόμενη δυνατότητα για έγχρωμη τηλεόραση ήταν σε συζητήσεις, ο χάρτης ανακατανομής των σταθμών από την FCC δεν ήρθε μέχρι τον Απρίλιο του 1952, με την 1η Ιουλίου του 1952 ως επίσημη έναρξη της αδειοδότησης των νέων σταθμών. Άλλες δράσεις της FCC έβλαψαν τον νεοσύστατο DuMont και τα

δίκτυα ABC. Η εταιρεία AT & T ανάγκασε τους χρήστες της ομοαξονικής καλωδιακής τηλεόρασης να νοικιάσουν επιπλέον ασύρματες γραμμές, μεροληπτώντας εναντίων του Dumont, οι οποίες δεν είχαν καμία λειτουργία στο δίκτυο. Ο Dumont και η ABC διαμαρτυρήθηκαν εναντίων των πολιτικών της AT&T στην **FCC**, αλλά η Επιτροπή δεν έλαβε καμία δράση. Το αποτέλεσμα ήταν ότι ο Dumont ξόδευε μεγάλα ποσά σε μεγάλες γραμμές όπως η CBC και η NBC ενώ χρησιμοποιούσε μόνο τα 10 με 15 τοις εκατό περίπου του χρόνου και της απόστασης από αλλά μεγαλύτερα δίκτυα. Η "Έκτη Αναφορά και Διαταγή" της FCC έληξε το πάγωμα. Θα έπαιρνε πέντε χρόνια στις Ηνωμένες Πολιτείες να αυξήσει τους σταθμούς από 108 σε 550. Νέοι σταθμοί ήρθαν με αργούς ρυθμούς, μόλις πέντε μέχρι το τέλος του Νοεμβρίου του 1952. Η Έκτη Αναφορά και Διαταγή απαιτούσε κάποιους υπάρχοντες σταθμούς TV για αλλαγή καναλιών, αλλά μόνο σε λίγους σταθμούς VHF απαιτούνταν για τη μετακίνηση σε UHF. Η αναφορά επίσης αναίρεσε μια σειρά από κανάλια για το νέο αναδυόμενο πεδίο της εκπαιδευτικής τηλεόρασης, τα οποία εμπόδιζαν την μάχη της ABC και του Dumont για την ενσωμάτωση στις περισσότερο επιθυμητές αγορές όπου τα κανάλια VHF διατηρούνταν για μη εμπορική χρήση. Η Έκτη Αναφορά και Διαταγή παρείχε επίσης το "συνονθύλευμα " των καναλιών VHF και UHF στις περισσότερες αγορές. Οι μεταδότες UHF το 1950 δεν ήταν ακόμα αρκετά ισχυροί , ούτε οι δέκτες ήταν αρκετά ευαίσθητοι. Στις αγορές όπου δεν υπήρχαν σταθμοί VHF και η UHF ήταν η μοναδική διαθέσιμη υπηρεσία TV, η UHF επέζησε. Σε άλλες αγορές, οι οποίες ήταν πολύ μικρές για να υποστηρίξουν οικονομικά ένα τηλεοπτικό σταθμό, πολύ κοντά σε VHF σε κοντινές πόλεις , ή όπου η UHF καλούνταν να ανταγωνιστεί με περισσότερους από έναν καλά εδραιωμένους σταθμούς VHF , η UHF είχε ελάχιστες πιθανότητες επιτυχίας. Το Ντένβερ υπήρξε η μεγαλύτερη πόλη των Ηνωμένων Πολιτειών χωρίς τηλεοπτικό σταθμό από το 1952. Ο Γερουσιαστής Edwin Johnson πρόεδρος της Διαπολιτειακής Γερουσίας και της Επιτροπής του Εμπορίου του Εξωτερικού , έκανε δική του αποστολή το να κάνει το Ντένβερ τον πρώτο μετά-παγώματος σταθμό. Πίεσε την **FCC** και αποδεδείχθηκε απόλυτα επιτυχής ως προς τον νέο σταθμό (**VHF** σταθμό) και η **FCC** ανακοίνωσε την πρώτη κατασκευαστική άδεια μετά το πάγωμα.

3.4.4 Το μονοπώλιο του τηλεφώνου στον ανταγωνισμό

Η σημαντική σχέση της FCC και της Αμερικανικής Εταιρείας Τηλεφώνου και Τηλεγράφου εξελίχτηκε με την πάροδο πολλών ετών. Η FCC είχε τον έλεγχο του τηλεφώνου για να περιορίσει τα κέρδη της AT&T και για να διασφαλίσει την τιμολόγηση χωρίς διακρίσεις. Το 1960 η FCC ξεκίνησε να επιτρέπει σε άλλες απομακρυσμένες εταιρείες όπως η MCI, να προσφέρουν εξειδικευμένες υπηρεσίες. Το 1970 η FCC επέτρεψε και σε άλλες εταιρείες να επεκτείνουν τις προσφορές τους στο

κοινό. Μια μήνυση το 1972 που οδηγήθηκε από το Τμήμα Δικαιοσύνης αφού η AT&T υποτίμησε άλλες εταιρείες, είχε ως αποτέλεσμα τη διάσπαση των Bells από την AT&T. Ξεκινώντας το 1984, η FCC εφάρμοσε ένα νέο στόχο με τον οποίο όλες οι διεθνείς εταιρείες είχαν ισότιμη πρόσβαση στους πελάτες των τοπικών εταιρειών τηλεφωνίας.

3.4.5 Νομοθετική Πράξη Τηλεπικοινωνιών του 1996

Το 1996, το Κογκρέσο θέσπισε τη Νομοθετική Πράξη Τηλεπικοινωνιών του 1996, στην έναρξη της διάλυσης της AT&T ως αποτέλεσμα της μήνυσης του Τμήματος Δικαιοσύνης των Ηνωμένων Πολιτειών της AT&T. Η νομοθεσία επιχείρησε να δημιουργήσει περισσότερο ανταγωνισμό στις υπηρεσίες τοπικής τηλεφωνίας ζητώντας από τους Επιβεβλημένους Φορείς Τοπικών Ανταλλαγών την παροχή πρόσβασης στις εγκαταστάσεις τους για τους Ανταγωνιστικούς Τοπικούς Φορείς Ανταλλαγών. Η πολιτική αυτή είχε μέχρι σήμερα μικρή επιτυχία και έλαβε έντονη κριτική. Η ανάπτυξη του Διαδικτύου, των καλωδιακών υπηρεσιών και των ασύρματων υπηρεσιών έφερε ερωτήματα κατά πόσο οι νέες νομοθετικές πρωτοβουλίες χρειάζονται. Το Κογκρέσο είχε καταγράψει τις εξελίξεις αλλά από το 1009 δεν πραγματοποιήθηκε κάποια σημαντική αλλαγή στον εφαρμόσιμο κανονισμό. Η Νομοθετική Πράξη της Τοπικής Κοινότητας Ραδιοφώνου στην 111η του Κογκρέσου βγήκε εκτός της επιτροπής και θα έχει την στήριξη της FCC.

3.4.6 Ανεκτικότητα σύνδεσης, Προσβολή

Η εγκατάσταση του Ronald Reagan ως Προέδρου των Ηνωμένων Πολιτειών το 1981 επιτάχυνε την ήδη υπάρχουσα μετακίνηση της **FCC** προς μια σαφώς αναμφισβήτητα πιο προσανατολισμένη στην αγορά στάση. Μια σειρά από κανονισμούς που πιστεύεται ότι ήταν ξεπερασμένη απομακρύνθηκαν, με το πιο αμφιλεγόμενο να είναι το Δόγμα Αμεροληψίας του 1987. Η **FCC** επίσης, έκανε βήματα για την αύξηση του ανταγωνισμού σε ραδιοτηλεοπτικούς φορείς, για την προώθηση εναλλακτικών λύσεων μετάδοσης, όπως η καλωδιακή τηλεόραση. Όσο αναφορά τα πρόστιμα περί προσβολής , δεν υπήρχε καμία δράση από την **FCC** μέχρι το 1987. Στις αρχές του 2000, η FCC ξεκίνησε να εντείνει τη λογοκρισία και την ενίσχυση των κανονισμών προσβολής. Ωστόσο, η ρυθμιστική επικράτεια της **FCC** όσο αναφορά την προσβολή παραμένει περιορισμένη στην τηλεόραση στα VHF και UHF κανάλια και στο ραδιόφωνο στις AM και FM συχνότητες. Στις 15 Ιουνίου 2006 , ο Πρόεδρος George W. Bush υπέγραψε τη Νομοθετική Πράξη Ενίσχυσης της Εντιμότητας της Μετάδοσης του 2005 που είχε ως σπόνσορα το Γερουσιαστή Sam Brownback, έναν υπεύθυνο τηλεοπτικής εκπομπής και επιδοκιμάστηκε από τον Fred Upton του Κογκρέσου του

Μίσιγκαν, ο οποίος πιστοποίησε ένα παρόμοιο νομοσχέδιο στη Βουλή των Ηνωμένων Πολιτειών. Ο νέος νόμος σκληραίνει τις κυρώσεις για κάθε παραβίαση του νόμου. Η Ομοσπονδιακή Επιτροπή Επικοινωνιών θα είναι σε θέση να επιβάλλει πρόστιμα, που ανέρχονται στο ποσό των $32,500 για κάθε παραβίαση από οποιονδήποτε σταθμό που θα παραβιάζει τα πρότυπα ευπρέπειας. Η νομοθεσία αύξησε το πρόστιμο κατά δέκα φορές από το προηγούμενο που ήταν $32,500 ανά παραβίαση.

3.4.7 Αρχηγείο - Επιτελείο

Η **FCC** μισθώνει χώρο στο κτίριο Portals στο νοτιοδυτικό Ουάσινγκτον. Η κατασκευή του κτιρίου Portals προγραμματίστηκε να ξεκινήσει στις 1 Μάρτιου 1996. Τον Ιανουάριο του 1996 η Γενική Διαχείριση Υπηρεσιών υπέγραψε μισθωτήριο με τους ιδιοκτήτες του κτιρίου, οι οποίοι συμφώνησαν να επιτρέψουν τη χρήση από την **FCC** 450,000τμ για 20 χρόνια, στην τιμή των $17.3 εκατομμυρίων το χρόνο. Πριν από αυτή τη συμφωνία η **FCC** είχε χώρο σε έξι κτίρια. Η **FCC** ήθελε να μετακομίσει σε μια πιο ακριβή περιοχή στη Λεωφόρο Πενσυλβανία

ΚΕΦΑΛΑΙΟ 4

Ασφάλεια

4.1 Χαρακτηριστικά Ασφαλείας

Ιδιότητες μιας ασφαλούς επικοινωνίας αποτελούν τα παρακάτω:

- **Επικύρωση**: Πριν από την μετάδοση των δεδομένων, οι κόμβοι αναγνωρίζονται και ανταλλάσσουν επικυρωμένα πιστοποιητικά.
- **Κρυπτογράφηση**: Πριν από την αποστολή ενός ασύρματου πακέτου δεδομένων, ο κάθε υπολογιστής που το στέλνει θα πρέπει να το κρυπτογραφήσει.
- **Ακεραιότητα**: Διασφαλίζει ότι το στοιχείο που μεταδίδεται δεν έχει υποστεί καμία τροποποίηση.
- **Μυστικότητα**: Ο όρος αυτός χρησιμοποιείται για να περιγράψει τα δεδομένα που προστατεύονται ενάντια στην ανάγνωση από αναρμόδια συμβαλλόμενα μέρη.

4.1.1 Επικύρωση και Μυστικότητα

Η έννοια της επικύρωσης αφορά τον έλεγχο πρόσβασης. Για να πραγματοποιήσουμε την επικύρωση πρέπει να αποκτήσουμε πρώτα πρόσβαση στο μέσο και στην περίπτωση μας στο ασύρματο δίκτυο. Αρχικά ελέγχονται τα διαθέσιμα ασύρματα δίκτυα και ακολούθως το δίκτυο επικυρώνει το σταθμό και ο σταθμός επικυρώνει το δίκτυο. Τα σημεία πρόσβασης σε ένα ασύρματο δίκτυο, εκπέμπουν περιοδικά πακέτα που ονομάζονται **beacons – πλαίσια διαχείρισης** (υπάρχει και η περίπτωση να μην στείλει beacons επειδή έχει κρυφό ssid όπου σε αυτή την περίπτωση περιμένει να λάβει αίτηση για να απαντήσει). Τα beacons είναι αυτά τα οποία ανακοινώνουν την ύπαρξη του δικτύου. Το κάθε beacon περιλαμβάνει ένα **Service Set Identifier (SSID)** ή αλλιώς όνομα δικτύου. Ένας σταθμός μπορεί να επιλέξει να συνδεθεί σε ένα δίκτυο είτε παθητικά είτε ενεργητικά. Στην παθητική σάρωση ο σταθμός ελέγχει τα κανάλια προσπαθώντας να βρει beacons από τα σημεία πρόσβασης και στην ενεργητική σάρωση στέλνει αιτήσεις διερεύνησης (είτε σε ένα συγκεκριμένο SSID είτε με το SSID ρυθμισμένο στο 0), σε όλα τα κανάλια ένα προς ένα. Όλοι οι σταθμοί που λαμβάνουν αιτήσεις διερεύνησης θα πρέπει να στείλουν απάντηση. Στο πρότυπο 802.11 έχουμε δυο τρόπους επικύρωσης , την επικύρωση ανοιχτού κλειδιού (**Open System Authentication – OSA**) και την επικύρωση μοιρασμένου κλειδιού (**Shared Key Authentication – SKA**). Ο σταθμός προτείνει την μέθοδο επικύρωσης που αυτός επιθυμεί στο μήνυμα της αίτησης επικύρωσης. Το δίκτυο μπορεί να δεχτεί ή να απορρίψει αυτή την πρόταση ανάλογα με τις ρυθμίσεις ασφαλείας. Χρησιμοποιώντας επικύρωση ανοιχτού κλειδιού οποιαδήποτε ασύρματη συσκευή μπορεί να επικυρωθεί από το σημείο πρόσβασης όμως όχι και να επικοινωνήσει. Η συσκευή μπορεί να

επικοινωνεί μόνο αν τα WEP κλειδιά της ταιριάζουν με αυτά του σημείου πρόσβασης. Η επικύρωση μοιρασμένου κλειδιού βασίζεται στο σύστημα πρόσκλησης -απάντησης. Για να χρησιμοποιήσουμε αυτή τη μέθοδο επικύρωσης , προϋποθέτει ότι το σημείο πρόσβασης και ο σταθμός είναι συμβατοί με τη λειτουργία **WEP (Wired Equivalent Privacy)** και ότι έχουν μεταξύ τους ένα προ-μοιρασμένο κλειδί. Αυτό σημαίνει ότι ένα κοινό κλειδί πρέπει να μοιραστεί σε όλους τους σταθμούς που τους έχει επιτραπεί να έχουν πρόσβαση στο δίκτυο, πριν επιχειρήσουν την διαδικασία της επικύρωσης.

4.1.2 Κρυπτογράφηση WEP (Wired Equivalent Privacy)

Κρυπτογράφηση καλείται η διαδικασία κατά την οποία τα δεδομένα αλλάζουν μορφή, μεταμφιέζονται προκειμένου να επιτευχτεί η ασφαλής μετάδοση πληροφοριών (**Encryption**, συμβολίζεται με E). Τα δεδομένα πριν από την κρυπτογράφηση ονομάζονται **plaintext** (και συμβολίζεται με P), ενώ τα δεδομένα μετά την κρυπτογράφηση αποτελούν το **cipher text** (και συμβολίζεται με C). Η αντίστροφη διαδικασία μετατροπής ονομάζεται **αποκρυπτογράφηση** (decryption). Ο αλγόριθμος κρυπτογράφησης είναι η μαθηματική ακολουθία που χρησιμοποιείται για την μεταμφίεση και την αποκάλυψη των δεδομένων. Συνήθως οι αλγόριθμοι κρυπτογράφησης εμπεριέχουν ακολουθίες κλειδιών για να τροποποιήσουν τα εξαγόμενα τους. Η πιο γνωστή επιλογή παροχής ασφάλειας για τα ασύρματα δίκτυα από το αρχικό πρότυπο 802.11 είναι το **Wired Equivalent Privacy (WEP)**. Με την επιλογή του **WEP** ένα κοινό κλειδί μοιράζεται ανάμεσα στο σημείο πρόσβασης και στους ασύρματους πελάτες του. Εάν θέλουμε εμπιστευτικότητα , μπορούμε να χρησιμοποιήσουμε την επιλογή του **WEP** και να κρυπτογραφήσουμε τα δεδομένα πριν αυτά σταλούν. Το WEP χειρίζεται ταυτόχρονα τόσο την προστασία όσο και την ακεραιότητα των δεδομένων. Με τη βοήθεια ενός συμμετρικού αλγορίθμου κρυπτογράφησης, RC4, επιτυγχάνεται η εμπιστευτικότητα των πληροφοριών που μεταφέρονται μέσω του δικτύου.

4.1.3 Επαλήθευση Ταυτότητας

Σε ένα ασύρματο δίκτυο, μια κινητή συσκευή προκειμένου να συνδεθεί στο δίκτυο μέσω ενός σημείου πρόσβασης , θα πρέπει να αποδείξει την ταυτότητα της. Αυτό θα μπορούσε να γινόταν και από το σημείο πρόσβασης. Στην επαλήθευση ταυτότητας **WEP**, η συσκευή θα πρέπει να αποδείξει στο σημείο πρόσβασης ότι γνωρίζει το μυστικό κλειδί της κρυπτογράφησης. Αρχικά υποβάλλεται αίτηση επαλήθευσης ταυτότητας από την κινητή συσκευή προς το σημείο πρόσβασης. Το σημείο πρόσβασης με τη σειρά του στέλνει ένα τυχαίο αριθμό μήκους 128 bit προς κρυπτογράφηση στην ασύρματη

συσκευή. Ο αριθμός κρυπτογραφείται από την συσκευή με το μυστικό κλειδί **WEP** και αποστέλλεται πίσω. Τέλος , το σημείο πρόσβασης ελέγχει εάν η κρυπτογράφηση έγινε με το σωστό κλειδί. Ωστόσο η μέθοδος αυτή αποτελεί ένα μεγάλο πρόβλημα για την ασφάλεια της κρυπτογράφησης γιατί δίνει πληροφορίες σε κακόβουλους χρήστες, που παρακολουθούν την επικοινωνία τόσο της κρυπτογραφημένης όσο και της μη κρυπτογραφημένης πληροφορίας.

4.1.4 Κατακερματισμός

Σε ένα ασύρματο δίκτυο, το πακέτο δεδομένων που καταφθάνει περιέχει τις κατάλληλες πληροφορίες για την αποστολή του. Το συγκεκριμένο πακέτο δεδομένων ονομάζεται **MSDU(Mac Service Data Unit)**. Τα δεδομένα καταφθάνουν στο επίπεδο MAC του προορισμού και σκοπός είναι να περάσουν στο λειτουργικό σύστημα και να μετατεθούν στην κατάλληλη εφαρμογή. Παρόλα αυτά, πριν από αυτή τη διαδικασία τα δεδομένα πρέπει να χωριστούν σε μικρότερα κομμάτια, για να υποστούν τη διαδικασία του **θραυματισμού (fragmentation).** Στη συνέχεια το κάθε κομμάτι ακολουθεί τη δική του πορεία στην κρυπτογράφηση **WEP.** Επομένως το αρχικό πακέτο δεδομένων χωρίζεται σε μικρότερα μηνύματα, MPDU (Mac Protocol Data Unit) στα οποία προστίθενται και αλλά bytes.

4.1.5 Διάνυσμα Αρχικοποίησης

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στην κρυπτογράφηση **WEP** έχουν μήκος 40 ή 104 bits, ωστόσο συχνά μιλούν για 68 ή 128 bits. Αυτό συμβαίνει επειδή κάποιοι παραλείπουν να αναφέρουν τα επιπλέον 24 bits που χρησιμοποιούνται από το **διάνυσμα αρχικοποίησης (Initialization Vector –IV).** Το **IV** ουσιαστικά αλλάζει για κάθε πακέτο και συνδυάζεται με το μυστικό κλειδί. Το αποτέλεσμα αυτών των δυο κρυπτογραφείται. Έτσι, ακόμα και αν τα αρχικά δεδομένα είναι ίδια, η κρυπτογραφημένη μορφή τους είναι πάντα διαφορετική. Το **IV** δεν είναι μυστικό, ενώ στέλνεται σε μη κρυπτογραφημένη μορφή σε κάθε μετάδοση ώστε ο παραλήπτης να είναι σε θέση να αποκρυπτογραφήσει την πληροφορία χρησιμοποιώντας την αντίστοιχη τιμή **IV.**

4.1.6 Τα κλειδιά που χρησιμοποιούνται στο WEP

Τα κλειδιά κρυπτογράφησης που χρησιμοποιούνται στο WEP έχουν τα εξής χαρακτηριστικά :

- **Σταθερό μήκος:** Συνήθως 40 ή 104 bit.
- **Στατικά:** Δεν μεταβάλλεται η τιμή του κλειδιού εφόσον δεν αλλάξουν οι ρυθμίσεις.
- **Διαμοιραζόμενα (shared):** Τόσο το σημείο πρόσβασης όσο και η κινητή συσκευή διαθέτουν αντίγραφο των ίδιων κλειδιών.
- **Συμμετρικά:** Γίνεται χρήση του ίδιου κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση των πληροφοριών.

Σύμφωνα με το **πρότυπο 802.11**, η διάθεση των κλειδιών στα σημεία πρόσβασης και στις ασύρματες συσκευές πρέπει να γίνεται με ασφαλείς μεθόδους. Η επαναχρησιμοποίηση των κλειδιών είναι μια αδυναμία των κρυπτογραφικών πρωτοκόλλων. Για αυτό το λόγο το **WEP**, έχει μια δεύτερη κατηγορία κλειδιών τα οποία χρησιμοποιούνται για τα ζευγάρια επικοινωνιών. Τα κλειδιά αυτά μοιράζονται μόνο μεταξύ των δυο σταθμών επικοινωνίας. Οι δυο σταθμοί μοιράζονται ένα κλειδί και έχουν μια σχέση χαρτογράφησης κλειδιού. Ένα 128-bit **WEP** κλειδί σχεδόν πάντα εισάγεται από τους χρήστες σαν μια ακολουθία 26 δεκαεξαδικών (με βάση το 16) χαρακτήρων (0-9 και A-F). Κάθε χαρακτήρας αντιπροσωπεύει 4 bit του κλειδιού. 26 ψηφία τεσσάρων bit δίνουν 104 bit και η προσθήκη του 24 bit **IV** παράγει το τελικό 128 – bit **WEP** κλειδί. Ένα 256 – bit σύστημα **WEP** είναι διαθέσιμο από μερικούς προμηθευτές και όπως με το 128 – bit **WEP** , τα 24 bit είναι για το **IV**, αφήνοντας 232 πραγματικά bit για την προστασία. Αυτά τα 232 bit εισάγονται χαρακτηριστικά ως 58 δεξαεξαδικοί χαρακτήρες. 58 *4 =232 bit + 24 IV bit = 256 bit **WEP** κλειδί. Ωστόσο, το μέγεθος του κλειδιού δεν είναι ο μόνος σημαντικός περιορισμός ασφάλειας στο **WEP.** Το **WEP** έχει αρκετά μειονεκτήματα και τα πρόσθετα bit στο κλειδί δεν έχουν ιδιαίτερη σημασία. Η καλύτερη δημόσια επίθεση ενάντια στο **WEP** μπορεί να ανακτήσει το κλειδί μέσα σε λίγα δευτερόλεπτα.

4.1.7 Διανομή κλειδιού

Το βασικότερο μειονέκτημα του **WEP** είναι το πρόβλημα της διανομής του κλειδιού. Τα μυστικά κομμάτια του κλειδιού **WEP** πρέπει να μοιραστούν σε όλους τους σταθμούς που συμμετέχουν στο δίκτυο. Το πρότυπο **802.11** δεν μας παρέχει ένα μηχανισμό παραγωγής κλειδιού με αποτέλεσμα ο καθένας μας πρέπει να δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή να έχει πρόσβαση σε συσκευές με το χέρι. Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι οι εξής :

- Τα κλειδιά δεν είναι ουσιαστικά μυστικά, αφού εισάγονται στους οδηγούς software της ασύρματης κάρτας. Έτσι ένας τοπικός χρήστης μπορεί να έχει πρόσβαση στο "μυστικό" κλειδί.

- Εάν τα κλειδιά είναι προσιτά στους χρήστες, αυτά θα πρέπει να αλλάζουν συχνά. Η γνώση των κλειδιών **WEP** επιτρέπει σε ένα χρήστη να φτιάξει έναν **802.11** σταθμό και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί.
- Οι επιχειρήσεις με ένα μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύουν το κλειδί στους χρήστες και πλέον δεν υφίσταται η "μυστικότητα" του κλειδιού.

4.1.8 Τιμή Ελέγχου Ακεραιότητας

Η τιμή ελέγχου ακεραιότητας (**Integrity Check Value – ICV**) συνεισφέρει στην αποφυγή από την τροποποίηση του μηνύματος κατά τη μετάδοση. Γενικότερα, σε κρυπτογραφημένα και μη κρυπτογραφημένα μηνύματα , συνηθίζεται έλεγχος για την αλλαγή των bits κατά τη μετάδοση. Το σύνολο των Bytes του μηνύματος συνενώνονται στον έλεγχο κυκλικού πλεονασμού (**Cyclic Redundancy Check –CRC**) . Η τιμή αυτή, μήκους τεσσάρων bytes, προστίθεται στο τέλος του πλαισίου πριν την επεξεργασία για μετάδοση. Αν αλλάξει έστω και ένα bit από το μήνυμα, ο παραλήπτης θα υπολογίσει διαφορετική τιμή **CRC** από αυτή που μεταφέρει ο πομπός και επομένως θα απορρίψει το μήνυμα. Παρόλο που ο έλεγχος εντοπίζει τυχαία λάθη, δεν είναι δυνατόν να αναγνωρίσει σκόπιμα λάθη, καθώς ο εισβολέας είναι σε θέση να υπολογίσει τη νέα τιμή **CRC** και να αντικαταστήσει την αρχική. Το **ICV** λειτουργεί όπως το **CRC**, αλλά υπολογίζεται και εφαρμόζεται πριν την διαδικασία της κρυπτογράφησης. Ωστόσο το **CRC** μπορεί να προστεθεί και μετά την κρυπτογράφηση. Επομένως, ο εισβολέας δεν μπορεί να υπολογίσει εκ νέου το μήνυμα. Έτσι το **ICV** υπολογίζεται ως ένας συνδυασμός όλων των δεδομένων και προκύπτει ως μια τιμή μήκους τεσσάρων bytes , η οποία προστίθεται στο τέλος.

4.1.9 Αλγόριθμος κρυπτογράφησης RC4

Ο αλγόριθμος **RC4** χρησιμοποιείται κατά τη διαδικασία της κρυπτογράφησης **WEP**. Ο **RC4** είναι απλός στην υλοποίηση του και ισχυρός. Βασική ιδέα είναι η δημιουργία μιας τυχαίας ακολουθίας bytes , που ονομάζεται ροη κλειδιού (**key stream**) και έχει ως στόχο το συνδυασμό της με τα δεδομένα μέσω της λογικής πράξης του αποκλειστικού Η (**XOR**). Η τυχαία ακολουθία κλειδιού ονομάζεται <<ψευδοτυχαία>> διότι θα πρέπει να δείχνει τυχαία σε εισβολέα αλλά τα δυο άκρα της ζεύξης που επικοινωνούν θα πρέπει να παράγουν την ίδια τυχαία τιμή για κάθε byte που επεξεργάζονται. Η πράξη XOR είναι εύκολα υλοποιήσιμη οπότε το πιο δύσκολο είναι ο υπολογισμός μιας καλής <<ψευδοτυχαίας>> ροής bytes. Δηλαδή χρειαζόμαστε ένα

«ψευδοτυχαίο» byte για κάθε byte του μηνύματος προς κρυπτογράφηση. Ο αλγόριθμος **RC4** παράγει μια ροη αυτής της μορφής.

4.1.10 Η κρυπτογράφηση

Αρχικά, το μυστικό κλειδί συνδέεται με το **διάνυσμα έναρξης IV** και το αποτέλεσμα τους εισάγεται στον **αλγόριθμο RC4**. Ο αλγόριθμος RC4 παράγει μια ακολουθία κλειδιού key stream από «ψευδοτυχαία» bits ίσα στο μήκος με τον αριθμό bits δεδομένων που πρέπει να διαβιβαστούν συν 4. Στην συνέχεια, για προστασία από αναρμόδια τροποποίηση δεδομένων , εφαρμόζεται ο αλγόριθμος ακεραιότητας στα δεδομένα και παράγεται το **ICV**. Η κρυπτογράφηση ολοκληρώνεται με τη λογική πράξη του αποκλειστικού Η (XOR) μεταξύ της ακολουθίας κλειδιού και των δεδομένων που μετατράπηκαν σε **ICV**. Το αποτέλεσμα της διαδικασίας είναι ένα μήνυμα το οποίο περιέχει το **IV** και το κρυπτογράφημα. Ο αλγόριθμος **RC4** είναι ένας από τους σημαντικότερους παράγοντες της κρυπτογράφησης **WEP**, αφού μεταμορφώνει ένα σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτή η μέθοδος κάνει απλή τη διαδικασία διανομής κλειδιού, αφού το μόνο που θα πρέπει να μεταδοθεί μεταξύ των σταθμών είναι το μυστικό κλειδί. Το διάνυσμα αρχικοποίησης επεκτείνει τη διάρκεια ζωής του μυστικού κλειδιού. Στη μέθοδο WEP λοιπόν το μόνο που αλλάζει ανά συχνά διαστήματα είναι το διάνυσμα αρχικοποίησης ενώ το μυστικό κλειδί παραμένει πάντα ίδιο. Κάθε νέο **IV** καταλήγει σε μια νέα ακολουθία κλειδιού. Το **IV** δεν είναι μυστικό αφού δεν παρέχει πληροφορίες για το μυστικό κλειδί. Για την αποκρυπτογράφηση πρέπει να το διάνυσμα αρχικοποίησης να αποσταλεί μαζί με το κρυπτογραφημένο πακέτο. Όταν ο παραλήπτης αποκρυπτογραφήσει το πακέτο υπολογίζει ξανά την τιμή ελέγχου ακεραιότητας και τη συγκρίνει με αυτή που περιείχε το πακέτο που παρέλαβε. Αν οι δυο τιμές ταυτίζονται , τότε το πακέτο θεωρείται έγκυρο. Γενικά χρησιμοποιούνται στατικά κλειδιά μήκους 40 bits και ενός **IV** μήκους 24 bits. Νεότερες εκδόσεις του **WEP** υποστηρίζουν μήκος κλειδιού 104 bits και μήκος **IV** 24 bits. Το κλειδί και το **IV** ενώνονται για να σχηματίσουν το κλειδί μήκους 64 bits ή 128 bits αντίστοιχα, το οποίο χρησιμοποιείται ως είσοδος για τον αλγόριθμο **RC4**. Ο αλγόριθμος **RC4** είναι πολύ σημαντικός παράγοντας για την αποδοτικότητα του **WEP**, όσο αναφορά την εμπιστευτικότητα των δεδομένων, αφού αυτός είναι η μηχανή κρυπτογράφησης. Το μυστικό κλειδί είναι στατικό, οπότε το **IV** είναι αυτό που καθορίζει κάθε φορά την ψευδοτυχαία ακολουθία. Οπότε, ο αλγόριθμος εξαρτάται μόνο από το **IV**.

4.1.11 Προβλήματα του WEP

Οι αδυναμίες του **WEP** είναι αρκετές. Μερικά από τα προβλήματα του **WEP** αναφέρονται παρακάτω :

- Το θέμα της **διανομής των κλειδιών** είναι ιδιαίτερα σημαντικό θέμα. Όταν κάποιος αποχωρήσει από το σύστημα , τα κλειδιά θα πρέπει να αλλάξουν. Για να επιτύχει μια επίθεση sniffing χρειάζεται μόνο τα μυστικά κλειδιά τα οποία σπάνια αλλάζουν. Συνήθως το WEP χρησιμοποιεί ένα δημόσιο μυστικό κλειδί 40 bit. Η καταλληλότητα αυτού του κλειδιού δεν έχει κριθεί ιδιαίτερα καλή , για το λόγο αυτό, πολλοί συστήνουν τη χρήση των 128 bit κλειδιών.

Η σπάνια **νέα εισαγωγή κλειδιών** επιτρέπει στους επιτιθέμενους να αποκτήσουν αποθέματα κρυπτογραφημένων δεδομένων δηλαδή, μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια κλειδιά.

- Προβληματική φαίνεται να είναι και η διαδικασία της **επαλήθευσης ταυτότητας**. Η επαλήθευση ταυτότητας στηρίζεται σε μια μέθοδο πρόκλησης – απόκρισης. Αρχικά στέλνεται μια τυχαία ακολουθία bits, η οποία κρυπτογραφείται , μετά αποστέλλεται πίσω και τέλος το σημείο πρόσβασης την αποκρυπτογραφεί και τη συγκρίνει με την αρχική ακολουθία. Το κλειδί που χρησιμοποιείται σε αυτή τη διαδικασία είναι το ίδιο με αυτό της κρυπτογράφησης , παρέχοντας έτσι την ευκαιρία σε έναν επιτιθέμενο να αποκτήσει στοιχεία. Η όλη διαδικασία δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί στα κλειδιά κρυπτογράφησης. Αυτό συμβαίνει διότι οποιοσδήποτε παρακολουθεί τη διαδικασία της επαλήθευσης έχει πρόσβαση σε ένα κρυπτογραφημένο και μη κρυπτογραφημένο μήνυμα.
- **Ο έλεγχος πρόσβασης** συνίσταται στην απαγόρευση ή όχι της επικοινωνίας μιας συσκευής με το δίκτυο. Η πρόσβαση ελέγχεται συνήθως διατηρώντας μια λίστα με τις επιτρεπόμενες συσκευές ή με ένα ηλεκτρονικό πιστοποιητικό. Στο πρότυπο **802.11** δεν έχουμε κάποιο συγκεκριμένο μηχανισμό υλοποίησης πρόσβασης. Οι συσκευές αναγνωρίζονται συνήθως από τις διευθύνσεις MAC , όμως αυτό δεν είναι και η καλύτερη προσέγγιση γιατί οι διευθύνσεις αυτές μπορούν να αντιγραφούν εύκολα. Έτσι, το μόνο που απομένει για το **WEP** είναι τα κλειδιά κρυπτογράφησης ξανά.
- Ένα άλλο μεμπτό σημείο του **WEP** είναι η αδυναμία του να διαχειριστεί **επιθέσεις μέσω αναπαραγωγής μηνυμάτων**. Όταν ένας επιτιθέμενος παρακολουθεί και καταγράφει τα πλαίσια που ανταλλάσσονται σε μια νόμιμη επικοινωνία (sniffing) , μπορεί να συνδεθεί στο δίκτυο χρησιμοποιώντας τη

MAC διεύθυνση της κινητής συσκευής. Στέλνοντας έτσι ένα αντίγραφο παλιού μηνύματος μπορεί να αποκτήσει πρόσβαση στον εξυπηρετητή. Η προστασία από τέτοιου είδους επιθέσεων στο **WEP** δεν είναι μόνο ελλιπής αλλά ανύπαρκτη.

- Ιδιαίτερη βαρύτητα έχει η **επαναχρησιμοποίηση της τιμής του διανύσματος αρχικοποίησης IV**. Εάν μαζευτούν πολλά δείγματα επαναλαμβανόμενου IV τότε μπορεί κάποιος να τα υποθέσει ως τμήματα της ροής του κλειδιού και να προχωρήσει στην αποκρυπτογράφηση. Όταν κάποιος γνωρίζει το keystream για ένα συγκεκριμένο IV , μπορεί να αποκρυπτογραφήσει κάθε πλαίσιο που χρησιμοποιεί το ίδιο. Ωστόσο ο κίνδυνος αυτός δεν είναι και τόσο μεγάλος επειδή δεν υπάρχει κάποιο αυτοματοποιημένο εργαλείο που θα μπορέσει να καταφέρει να διαχειριστεί τον προσδιορισμό ενός κρυπτογραφήματος με την μέθοδο αυτή.
- **Η τιμή του διανύσματος αρχικοποίησης** όπως αναφέραμε , **δεν είναι μυστική**, όμως αυτό δίνει την ευκαιρία σε έναν εισβολέα να επιτεθεί σε ένα αδύναμο σχετικά κλειδί. Τα πρώτα bytes ενός μη κρυπτογραφημένου μηνύματος είναι γνωστά συνήθως , επειδή αποτελούν μια επικεφαλίδα **802.11.** Με την παρακολούθηση της μετάδοσης αναζητείται ένα αδύναμο κλειδί . Υπάρχει σχέση ανάμεσα στο κρυπτογραφημένο , στο μη κρυπτογραφημένο μήνυμα και στο μυστικό κλειδί. Έχοντας καταγράψει έναν μεγάλο αριθμό από τέτοια μηνύματα, ο εισβολέας μπορεί να ανακαλύψει το πρώτο byte του κλειδιού. Η μέθοδος αυτή μπορεί να εφαρμοστεί για κάθε byte και έτσι να αποκαλυφθεί το μυστικό κλειδί.

4.2 Το πρωτόκολλο TKIP

Μετά από τη συνειδητοποίηση της κρισιμότητας της κατάστασης και του κενού ασφαλείας που άφηνε τα **WEP**, ανακαλύφθηκε η λύση του **TKIP (Temporal Key Integrity Protocol – TKIP).** Το **TKIP** προσφέρει μεγαλύτερη ασφάλεια καθώς παρέχει ανάμιξη κλειδιών ανά πακέτο, έλεγχο ακεραιότητας μηνύματος και μηχανισμό αναπαραγωγής κλειδιών , ο οποίος επιδιορθώνει τα ελαττώματα του **WEP.** Αυτό που απαιτούσε όταν ξεκίνησε ήταν η αναβάθμιση του **firmware** και πιθανώς του **λογισμικού (driver)** της συσκευής. Αρχικά το TKIP χρησιμοποιήθηκε πάνω στο **WEP** για να ενισχύσει την ασφάλεια και για να μειώσει τον αριθμό των επιθέσεων του **WEP.** Το πρώτο βήμα στη διαδικασία της κρυπτογράφησης **TKIP** είναι ο υπολογισμός του κώδικα ακεραιότητας δεδομένων **MIC**, που γίνεται με τον **αλγόριθμο Michael**. Με τον αλγόριθμο αυτό προστατεύονται το μήνυμα και οι διευθύνσεις του αποστολέα και του παραλήπτη. Αυτά και ένα κλειδί **MIC** είναι οι είσοδοι στον αλγόριθμο. Στο τέλος

προκύπτουν 8 bytes , τα οποία προστίθενται στο αρχικό μήνυμα το οποίο στη συνέχεια κρυπτογραφείται. Η TKIP κρυπτογράφηση λειτουργεί **σε δυο φάσεις. Η πρώτη φάση χρησιμοποιεί ένα μη γραμμικό πίνακα αντικατάστασης (S – Box)** και συνδυάζει το κλειδί συνόδου **TK** , τη MAC διεύθυνση του αποστολέα **(TA)**, και τα τέσσερα πιο σημαντικά bytes της τιμής του μετρητή ακολουθίας **(TKIP Sequence Counter)**, ο οποίος αυξάνεται για κάθε τμήμα δεδομένων που τεμαχίζεται. Το κλειδί συνόδου αποτελείται από μια τιμή 128 bit , παρόμοια με την τιμή του **WEP** κλειδιού. Ο **TKIP** μετρητής ακολουθίας **(TSC)** είναι φτιαγμένος από την **πηγαία διεύθυνση SA** , την **διεύθυνση προορισμού DA**, την **ιεραρχία** και τα **δεδομένα**. Στην έξοδο παράγεται μια ενδιάμεση τιμή **TTAK**. Η τιμή αυτή μπορεί να αποθηκευτεί προσωρινά και να χρησιμοποιηθεί μέχρι και για **216 πακέτα**. Εφόσον λαμβάνεται υπόψη η διεύθυνση του αποστολέα η συνάρτηση παράγει διαφορετική ενδιάμεση τιμή για κάθε συσκευή, ακόμα και αν χρησιμοποιηθεί το ίδιο κλειδί κρυπτογράφησης από όλες τις συσκευές. **Η δεύτερη φάσ**η <<ανακατεύει>> την τιμή **TTAK** με τα δυο λιγότερο σημαντικά bytes της τιμής του μετρητή ακολουθίας **TSC** και το κλειδί συνόδου **TK** για την εξαγωγή του κλειδιού κρυπτογράφησης. Τέλος κατά τα γνωστά από το **WEP**, υπολογίζεται το **IV** και γίνεται η κρυπτογράφηση από τον **αλγόριθμο RC4**.

4.3 WPA

Το 2003, όταν άρχισε να γίνεται εμφανές το κενό ασφάλειας που είχε αφήσει η κρυπτογράφηση WEP, η Wi-Fi Alliance ανέπτυξε το Wi-Fi Protected Access (WPA). Το **WPA** προέρχεται από το πρότυπο 802.11 και αποτελεί μια ενδιάμεση λύση ασφάλειας των WLAN και μπορεί να συμπεριληφθεί με κάποιες αναβαθμίσεις στις ήδη υπάρχουσες WLAN ασύρματες συσκευές. Το **WPA** κάνει χρήση της μεθόδου **TKIP** και αυξάνει σημαντικά το επίπεδο ασφάλειας και ελέγχου πρόσβασης στα ασύρματα συστήματα LAN. Το WPA παρέχει σε κάθε πακέτο το κλειδί , έναν έλεγχο ακεραιότητας μηνύματος (MIC) που ονομάζεται Michael και ένα διάνυσμα ακολουθίας (Initialization Vector – IV). Επίσης, για τους οικιακούς χρήστες , το **WPA** παρέχει ένα μηχανισμό προ-μοιρασμένου κλειδιού τον **PSK (Pre – Shared Key)**. Για να μπορέσει να εκμεταλλευτεί κάποιος την δυνατότητα του **PSK** θα πρέπει να εισάγει μια λέξη κωδικό και στο σημείο πρόσβασης και στο σταθμό. Αυτή η λέξη κωδικός χρησιμοποιείται για να μπορεί να επικυρώνει οποιονδήποτε σταθμό προσπαθεί να συνδεθεί στο συγκεκριμένο δίκτυο. Ο κωδικός θα πρέπει να αποτελείται από 8 έως 63 χαρακτήρες σε **ASCII**. Ακολούθως το σημείο πρόσβασης παρέχει στο σταθμό ένα προσωρινό κλειδί το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Το **Pre – Shared Key WPA** είναι ανθεκτικό στις επιθέσεις σπασίματος του κωδικού πρόσβασης εάν χρησιμοποιείται ένας αδύναμος κωδικός. Για να προστατευτεί από μια επίθεση ένας τυχαίος κωδικός 13 χαρακτήρων είναι πιθανώς

αρκετός. Τα προϊόντα που αναγράφουν ότι έχουν "**WPA Personal**" σημαίνει ότι υποστηρίζουν τον **PSK μηχανισμό επικύρωσης**. Το πρότυπο WPA επίσης ορίζει τη χρήση του προτύπου **AES (Advanced Encryption Standard)** ως επιπλέον αντικατάσταση για την κρυπτογράφηση **WEP**. Η υποστήριξη του προτύπου **AES** είναι προαιρετική και εξαρτάται από την υποστήριξη που παρέχει ο προμηθευτής, ανάλογα με τα προγράμματα οδήγησης.

4.3.1 AES (Advanced Encryption Standard)

Το **WPA** παρέχει τη δυνατότητα για κρυπτογράφηση με δυο αλγορίθμους, τον **RC4** και τον **AES** (**Advanced Encryption Standard**) για την εμπιστευτικότητα των δεδομένων και την ακεραιότητα. Ο **AES** αποτελεί την νεότερη μέθοδο κρυπτογράφησης που έχει επιλεγεί από την κυβέρνηση των Ηνωμένων Πολιτειών. Ο **AES** χρησιμοποιεί έναν αλγόριθμο γνωστό ως **Rijndael**. Ο αλγόριθμος Rijndael πήρε το όνομα του από τους δυο Ελβετούς εφευρέτες του , Joan Daemen και Vincent Rijmen. Πρόκειται για έναν αλγόριθμο κρυπτογράφησης ομάδας (block) , που σημαίνει ότι λειτουργεί σε μια ομάδα σταθερού μεγέθους bits , η οποία ονομάζεται **block**. Αρχικά ο Rijndael παίρνει σαν είσοδο ένα μπλοκ συγκεκριμένου μεγέθους , συνήθως 128, και παράγει ένα αντίστοιχο μπλοκ εξόδου ίδιου μεγέθους. Ο μετασχηματισμούς απαιτεί μια δεύτερη είσοδο ,η οποία είναι το μυστικό κλειδί. Είναι σημαντικό να αναφέρουμε ότι το μυστικό κλειδί δεν έχει συγκεκριμένο μέγεθος και ότι ο **AES** χρησιμοποιεί τρία βασικά μεγέθη : 128, 192 και 256 bytes. Η χρησιμοποίηση του προτύπου **AES** μας προστατεύει από τις ενεργές ασύρματες επιθέσεις.

4.3.2 CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)

Η προσθήκη στο πρότυπο 802.11 που ορίζει την ασφάλεια της επόμενης γενιάς για τα ασύρματα δίκτυα ονομάζεται **802.11i**. Το πρότυπο αυτό εκδόθηκε το 2004. Το πρότυπο αυτό ορίζει μια νέα μέθοδο, για την ασφάλεια των δεδομένων στο **επίπεδο MAC**. Η μέθοδος **CCMP** λειτουργεί σύμφωνα με τον αλγόριθμο κρυπτογράφησης **AES.**Το CCMP παρέχει εμπιστευτικότητα, επικύρωση, ακεραιότητα και προστασία από την επανάληψη των πακέτων. Το **CCMP** χρησιμοποιεί μέγεθος κλειδιού 128 bit και μέγεθος μπλοκ 128 bit. Μετά το **CCMP** το μέγεθος του πακέτου έχει επεκταθεί κατά 16 bytes, τα 8 bytes για την επικεφαλίδα του **CCMP** και τα αλλά 8 bytes για την ψηφιακή υπογραφή **MIC** (**Message Integrity Code**). Τα δεδομένα του πακέτου και το **MIC** μεταδίδονται κρυπτογραφημένα , αφού προστεθεί η αρχική επικεφαλίδα του πακέτου και η επικεφαλίδα του **CCMP.**

4.4 WPA2 (WI-FI Protected Access Version 2)

Το **WPA2** είναι ο διάδοχος του **WPA** και προορίζεται για να θέσει σε απευθείας σύνδεση το **WPA** με το πρότυπο **802.11i**. Τα ασύρματα δίκτυα που υποστηρίζουν την λειτουργία του **WPA** και του **WPA2** κάνουν πιο εύκολη τη μεταφορά των δεδομένων ανάμεσα στα πρότυπα. Μια από τις βελτίωσης του **WPA2** είναι ότι με την προσθήκη του **AES** και του **CCMP** , παρέχει τη δυνατότητα ισχυρής κρυπτογράφησης. Μια άλλη βελτίωση που περιλαμβάνει το **WPA2** είναι η δυνατότητα για γρήγορη περιαγωγή. Η ικανότητα αυτή είναι σημαντική για τις εφαρμογές ήχου, όπου η μεταφορά τους είναι υψηλής ευαισθησίας. Η γρήγορη περιαγωγή επιτυγχάνεται με την επικύρωση των σταθμών και στα γειτονικά σημεία πρόσβασης αλλά και στο τελικό σημείο πρόσβασης όπου επιτυγχάνεται η επικοινωνία. Υπάρχουν δυο εκδόσεις του **WPA2.** Το **WPA 2 – Personal** και το **WPA2 –Enterprise**. Το **WPA2 – Personal** προστατεύει την πρόσβαση στο δίκτυο από μη εξουσιοδοτημένους χρήστες με την χρήση της εγκατάστασης ενός κωδικού πρόσβασης. Το **WPA 2 – Enterprise** πιστοποιεί τους χρήστες του δικτύου μέσω ενός εξυπηρετητή.

4.5 Τεχνολογίες Κεραιών

Αν ο **client** βρίσκεται σε μεγάλη απόσταση από το **κεντρικό access point**, τοποθετούνται κεραίες για ενισχυμένο και πιο σταθερό σήμα. Η κεραία είναι ένας ηλεκτρικός αγωγός, ο οποίος μπορεί να κάνει και μετάδοση και λήψη σημάτων. Κατά τη **μετάδοση του σήματος** έχουμε **εκπομπή ηλεκτρομαγνητικής ενέργειας** και κατά τη **λήψη** έχουμε **συλλογή ηλεκτρομαγνητικής ενέργειας**. Η κεραία είναι αυτή που εκπέμπει το διαμορφωμένο σήμα , ώστε ο client να μπορέσει να το λάβει. Οι κεραίες έχουν τα εξής χαρακτηριστικά :

- **Μορφή διάδοσης**
- **Κέρδος**
- **Ισχύ εκπομπής**
- **Bandwidth**

.5.1 Μορφή διάδοσης

Η μορφή διάδοσης καθορίζει τη δυνατή κάλυψη από την κεραία. Μια πολυκατευθυντική κεραία εκπέμπει με την ίδια ισχύ προς όλες τις κατευθύνσεις , ενώ μια κατευθυντική δίνει όλη σχεδόν την ισχύ της προς μια κατεύθυνση.

.5.2 Κέρδος

Έχει να κάνει με τον βαθμό ενίσχυσης μιας κεραίας , ο οποίος εξαρτάται κυρίως από την κατευθυντικότητά της.

.5.3 Ισχύ εκπομπής

Η ισχύς εκπομπής καθώς και το κέρδος καθορίζουν μαζί την απόσταση από την κεραία στην οποία θα γίνει εκπομπή του σήματος. Όσο μεγαλύτερη είναι η απόσταση τόσο μεγαλύτερη ισχύς εκπομπής χρειάζεται. Σε ασύρματα δίκτυα η ισχύς εκπομπής είναι χαμηλή συνήθως (1 W περίπου ίσως και λιγότερο).

.5.4 Bandwidth

Αφορά το τμήμα του φάσματος εντός του οποίου διαδίδεται το σήμα. Η κεραία για το Bandwidth των ασύρματων δικτύων θα πρέπει να είναι κατάλληλη. Σε μεγαλύτερες συχνότητες έχουμε μεγαλύτερο Bandwidth αλλά και μεγαλύτερη εξασθένηση.

4.6 MIMO κεραίες (Multiple Input and Multiple Output)

Στις **MIMO κεραίες** γίνεται χρήση πολλαπλών κεραιών τόσο στον πομπό όσο και στον δέκτη για να βελτιωθεί η επίδοση της επικοινωνίας. Η **τεχνολογία MIMO** χρησιμοποιεί πολλαπλές κεραίες για την μεταφορά πολλαπλών ροών δεδομένων από ένα σημείο σε ένα άλλο. Αντί να στείλει και να λάβει μόνο μια ροη δεδομένων, έχει την ικανότητα να μεταδώσει ταυτόχρονα τρεις ροές δεδομένων και να παραλάβει δυο , αυτό έχει ως αποτέλεσμα να αποστέλλονται περισσότερα δεδομένα την ίδια χρονική περίοδο. Η τεχνική αυτή μπορεί επιπλέον να αυξήσει την εμβέλεια εκπομπής ή την απόσταση μεταξύ των δεδομένων που θα αποσταλούν. Η τεχνολογία αυτή χρησιμοποιείται στο πρότυπο **802.11n**.

4.6.1 Μορφές των MIMO κεραιών

- **SISO/SIMO/MISO** είναι ειδικές περιπτώσεις των MIMO κεραιών.
- **MISO:** Πολλαπλής εισόδου και μιας εξόδου είναι μια ειδική περίπτωση, όταν ο δέκτης έχει μια ενιαία κεραία.

- **SIMO:** Μονής εισόδου και πολλαπλής εξόδου είναι μια ειδική περίπτωση, όταν πομπός έχει μόνο κεραία.
- **SISO:** Μονής εισόδου μόνης εξόδου είναι ένα συμβατικό σύστημα ραδιοφώνου, όπου ούτε ο πομπός ούτε ο δέκτης έχουν πολλαπλές κεραίες.

4.6.2 Εξοικονόμηση Ενέργειας

Ένα από τα προβλήματα με την χρήση των **MIMO κεραιών** είναι η αύξηση της ισχύς του κυκλώματος υλικού. Πρέπει να υποστηρίξουν περισσότερους πομπούς και δέκτες με αποτέλεσμα να χρειάζεται περισσότερο ρεύμα. Αν και δεν είναι δυνατό να εξαλείψει την αύξηση ισχύος που προκύπτει και από την χρήση των **MIMO κεραιών** σε **802.11n** πρότυπα , είναι δυνατόν να γίνει πιο αποτελεσματικότερη η χρήση του. Τα κανονικά δεδομένα που διαβιβάζονται είναι σε μια "εκρηχτική " μόδα. Αυτό σημαίνει ότι υπάρχουν μεγάλες χρονικοί περίοδοι που το σύστημα παραμένει σε αδράνεια ή τρέχει σε μια πολύ αργή ταχύτητα. Κατά τις περιόδους όπου οι **MIMO κεραίες** δεν χρειάζονται, το κύκλωμα μπορεί να θεωρηθεί ανενεργό , με αποτέλεσμα να μην καταναλώνει ενέργεια.

4.6.3 Αυξανόμενο εύρος ζώνης

Ένας προαιρετικός τρόπος για το πρότυπο **802.11n** είναι να τρέξει με ένα κανάλι διπλού εύρου ζώνης. Τα προηγούμενα συστήματα χρησιμοποιούσαν 20 MHz εύρος ζώνης , οι νέοι στόχοι έχουν τη δυνατότητα να χρησιμοποιούν 40 MHz. Στα 2,4 GHz υπάρχει αρκετός χώρος για τρία 20 MHz κανάλια , αλλά μόνο ένα 40 MHz κανάλι μπορεί να φιλοξενηθεί.

ΚΕΦΑΛΑΙΟ 5

Πειραματικό Μέρος

5.1 Μέρος Α

- **802.11n:** η θεωρητική μέγιστη ταχύτητα του είναι 150 Mbits/sec με εύρος ζώνης 20 MHz (2 streams)

- **802.11g:** η θεωρητική μέγιστη ταχύτητα είναι 22 Mbits/sec (τα 54 Mbits/sec είναι το θεωρητικό μέγιστο των bursts) για μικρό χρονικό διάστημα

Τα **κριτήρια σύγκρισης - σενάρια σύγκρισης** που επιλέχθησαν αντικατοπτρίζουν ρεαλιστικά σενάρια χρήσης των πρωτοκόλλων **802.11g** και **802.11n**.

5.1.1 Κριτήρια Αξιολόγησης

- **Απόσταση**: Οι συγκεκριμένες αποστάσεις που επιλέχθησαν προσομοιάζουν τυπικά σενάρια χρήσης σε οικίες και επιχειρήσεις. Η μικρότερη απόσταση(5m) προσομοιάζει τις καλύτερες δυνατές συνθήκες για την θεωρητική μέγιστη απόδοση του κάθε πρωτόκολλου ξεχωριστά. Η μεγαλύτερη απόσταση (30 m) εξετάζει την απόδοση των πρωτοκόλλων στα όρια της τυπικής εμβέλειας που επιτυγχάνεται από την πλειονότητα των AP (ισχύς : 100-200mW), για αυτό και είναι ενδιαφέρουσα η συγκεκριμένη μέτρηση.

- **Ύπαρξη ή όχι εμποδίων:** Ένα από τα σημαντικότερα κριτήρια αξιολόγησης είναι η ύπαρξη ή όχι εμποδίων διότι η μπάντα των **2,4 GHz** είναι ευάλωτη στην ύπαρξη εμποδίων από τσιμέντο ή οικοδομικά υλικά. Δεδομένου ότι τα 2 πρωτόκολλα έχουν αναπτυχτεί για λειτουργία σε εσωτερικούς χώρους δεν θα μπορούσαμε να παραβλέψουμε αυτό το κριτήριο αξιολόγησης.

- **Μέγεθος αρχείου:** Επίσης ενδιαφέρον παρουσιάζει η μέτρηση της μεταφοράς αρχείων διαφορετικών μεγεθών για να ελεγχτεί αν επιτυγχάνεται η μέγιστη απόδοση του κάθε πρωτοκόλλου στα αρχικά στάδια της μεταφοράς (0-1 sec) , για παράδειγμα τα πειράματα έδειξαν πως η μεταφορά πολύ μικρών αρχείων δεδομένων έχει σημαντικές επιπτώσεις στην ταχύτητα σε σύγκριση με μεγαλύτερα αρχεία.
- **Ασφάλεια/Κρυπτογράφηση**: Επιλέχθησαν διαφορετικά σενάρια μετάδοσης με cleartext (καμία ασφάλεια) ή κρυπτογραφημένα δεδομένα για να εξεταστεί η ενδεχόμενη επιρροή στην απόδοση από το επιπλέον επεξεργαστικό κόστος (επεξεργαστής) που λαμβάνει χώρα κατά την κρυπτογράφηση.

5.2 Μέρος Β

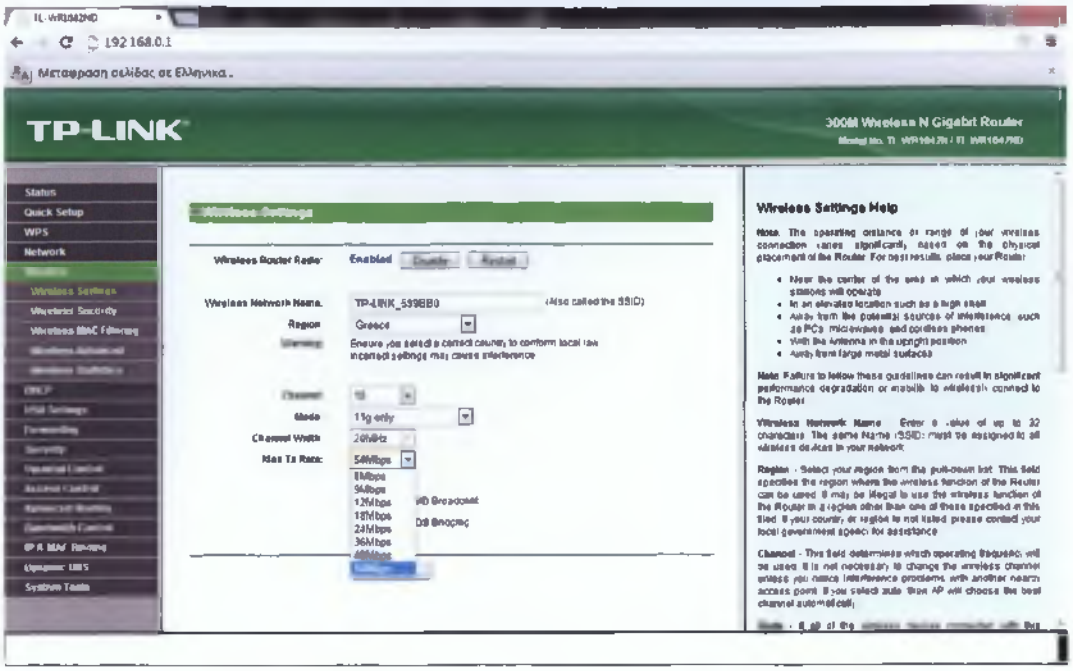
Για την υλοποίηση του πειραματικού μέρους της παρούσας πτυχιακής εργασίας, χρησιμοποιήθηκε ένα Access Point οικιακής χρήσης – μικρών επιχειρήσεων, **TP –Link TL –WR1042ND Wireless N Gigabit Router.**

Εικόνα 5.1: Access Point TP –Link TL –WR1042ND Wireless N Gigabit Router

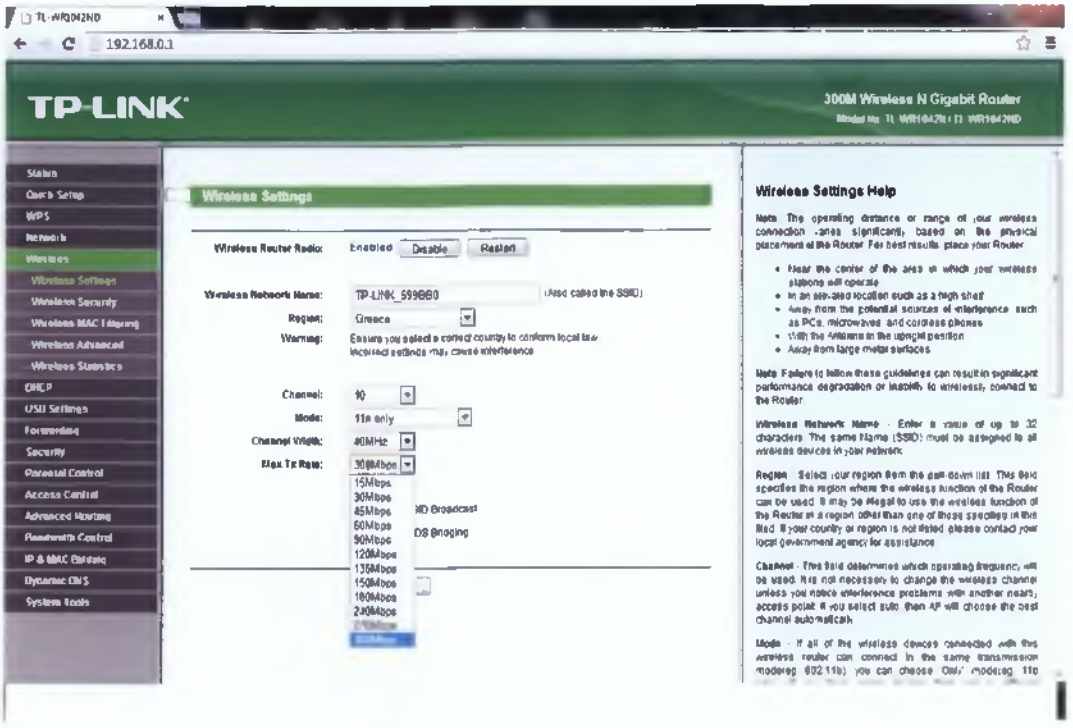
Σχετικά με τα τεχνικά χαρακτηριστικά του, το συγκεκριμένο AP διαθέτει ένα (1) Gigabit WAN Port και τέσσερα (4) Gigabit LAN Ports. Είναι συμβατό με τα εξής πρωτοκόλλα: 802.11b, 802.11g, 802.11n, με signal Rate τα 11Mbps, 54Mbps και 300Mbps αντίστοιχα. Διαθέτει σύστημα προστασίας με κρυπτογραφήσεις 64/128-bit WEP ,WPA/WPA2 και WPA-PSK/WPA2-PSK. Η ισχύς του σήματος του ασύρματου δικτύου δεν ξεπερνάει τα 20dBm (EIRP). Τέλος, όλες οι μετρήσεις έγιναν με συχνότητα 2.4-2.4835GHz (ανάλογα το κανάλι που επιλέγουμε για εκπομπή), η οποία είναι και η ελεύθερη συχνότητα για τα ασύρματα δίκτυα.

Για την δικτύωση, έχω χρησιμοποιήσει IP C κλάσης, και πιο συγκεκριμένα την IP 192.168.0.1 και Subnet Mask 255.255.255.0 στο Access Point.

Παρακάτω παραθέτονται εικόνες από το configuration του Access Point σχετικά με τα πρωτόκολλα (Modes) και την ταχύτητα εκπομπής (Rate).



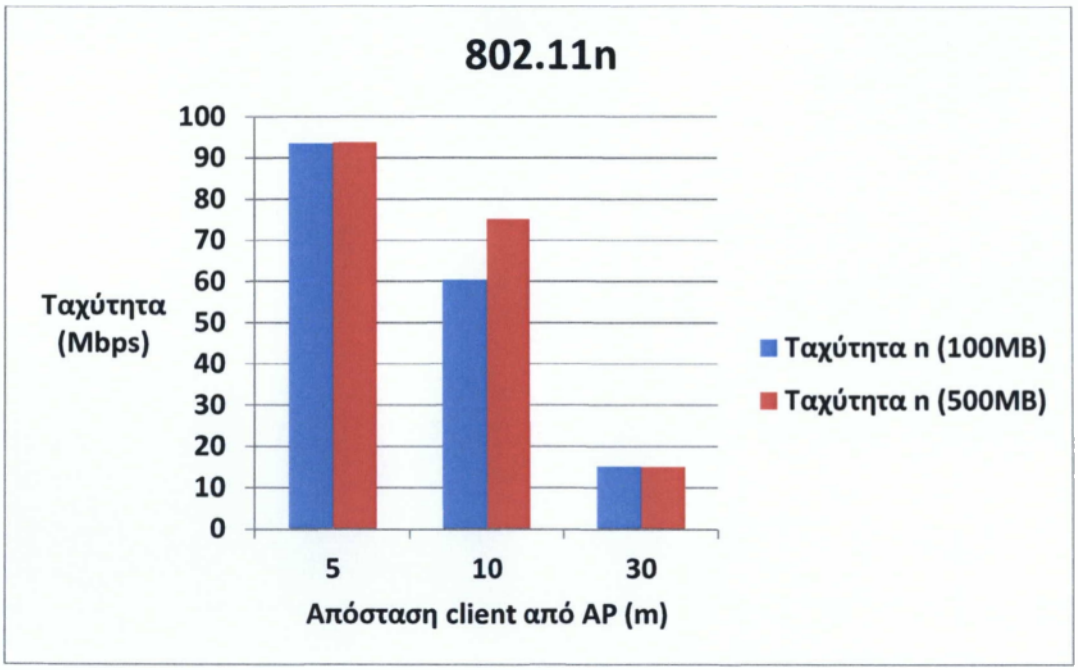
Εικόνα 5.2: Ρυθμίσεις Access Point για το 802.11g πρωτόκολλο



Εικόνα 5.3: Ρυθμίσεις Access Point για το 802.11n πρωτόκολλο

Απόσταση (m)	Ταχύτητα n (100 MB)	Ταχύτητα n (500MB)
5	93,5	93,7
10	60,32	75,10
30	15,00	15,10

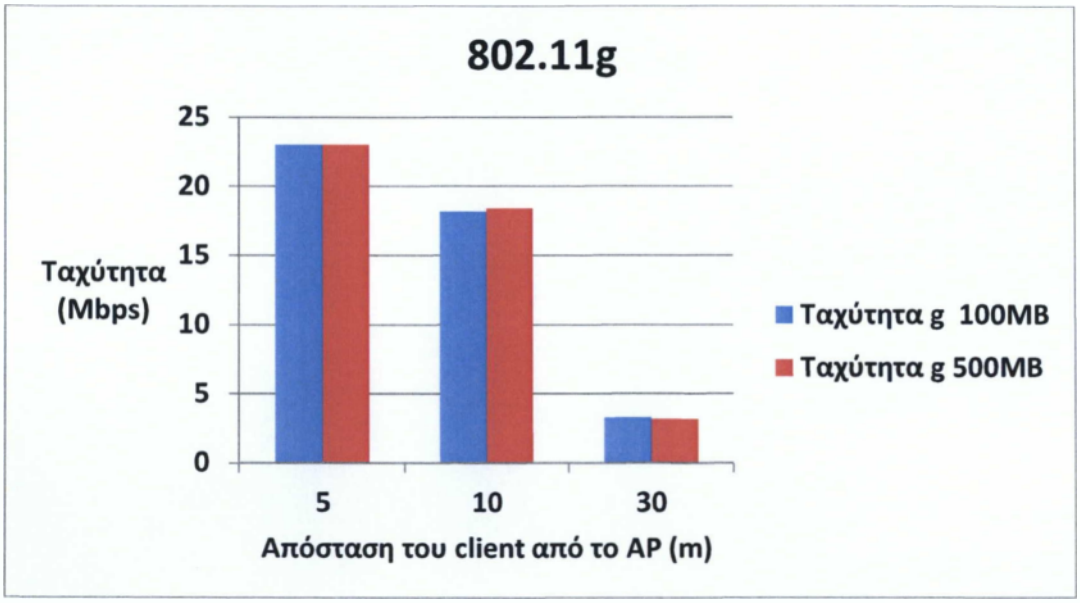
Πίνακας 5.1: Αποτελέσματα προτύπου 802.11n



Στο παραπάνω διάγραμμα συγκρίνουμε την ταχύτητα του προτύπου 802.11n σε σχέση με την απόσταση του client από το AP, αλλά και το μέγεθος του μεταφερόμενου αρχείου. Στα 5 m παρατηρούμε ότι οι ταχύτητες είναι ίδιες και στα 100 και στα 500MB. Στα 10m παρατηρούμε ότι η ταχύτητα μειώνεται σταδιακά και ότι υπάρχει μεγαλύτερη μείωση στα 100MB μεταφερόμενου αρχείου. Τέλος στα 30m παρατηρούμε ότι υπάρχει σημαντική μείωση της ταχύτητας του προτύπου 802.11n. Οι ταχύτητες σε σχέση με το μέγεθος του μεταφερόμενου αρχείου παρουσιάζουν ελάχιστες αποκλίσεις στην τιμή.

Απόσταση (m)	Ταχύτητα g (100MB)	Ταχύτητα g (500 MB)
5	23	23
10	18,16	18,4
30	3,29	3,15

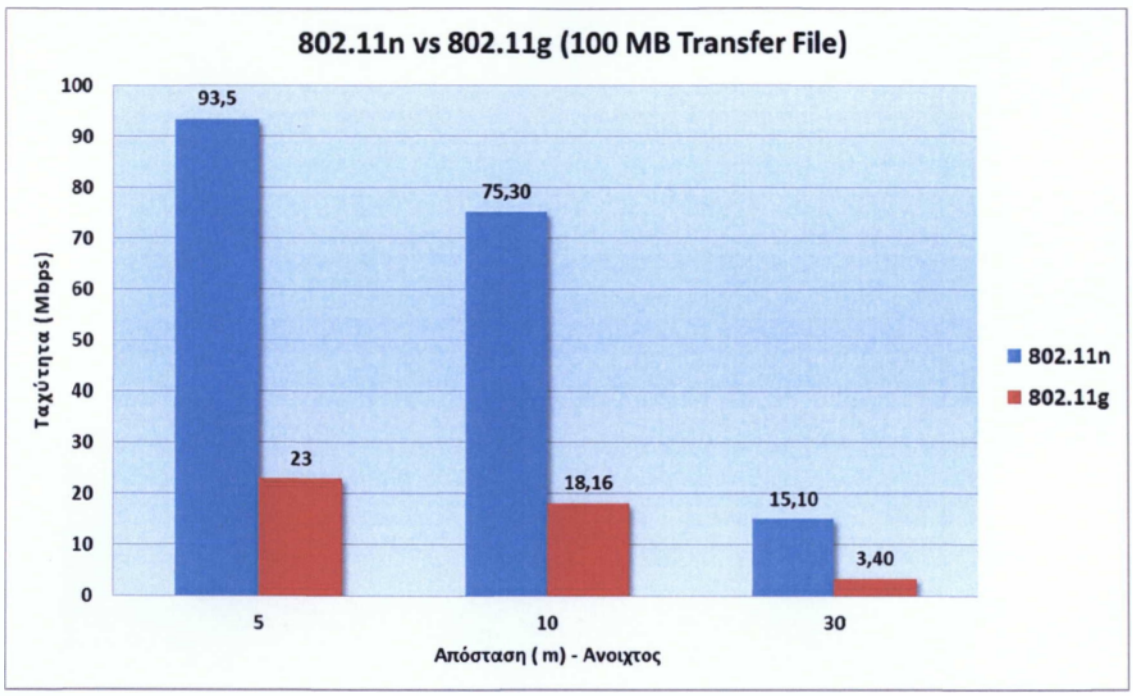
Πίνακας 5.2: Αποτελέσματα προτύπου 802.11g



Στο παραπάνω σχήμα, συγκρίνουμε την ταχύτητα του προτύπου 802.11g σε σχέση με την απόσταση του client από τον AP αλλά και το μέγεθος του μεταφερόμενου αρχείου. Όπως παρατηρήσαμε και στο προηγούμενο σχήμα, για το πρότυπο 802.11n έτσι και σε αυτό το σχήμα παρατηρούμε ότι στα 5m η ταχύτητα στα 100 και στα 500MB είναι σχεδόν ίδια με μικρές αποκλίσεις. Στα 10m παρατηρούμε ότι υπάρχει μείωση της ταχύτητας αλλά και ότι η ταχύτητα με μέγεθος αρχείου 500MB είναι μεγαλύτερη σε σχέση με το μέγεθος αρχείου 100MB. Τέλος στα 30m παρατηρούμε μια σημαντική μείωση της ταχύτητας του προτύπου αλλά και ότι οι ταχύτητες στα 100 και στα 300MB είναι ίδιες με μικρές αποκλίσεις στην τιμή.

Απόσταση (m)	Ταχύτητα n	Ταχύτητα g
5	93,5	23
10	75,30	18,16
30	15,10	3,40

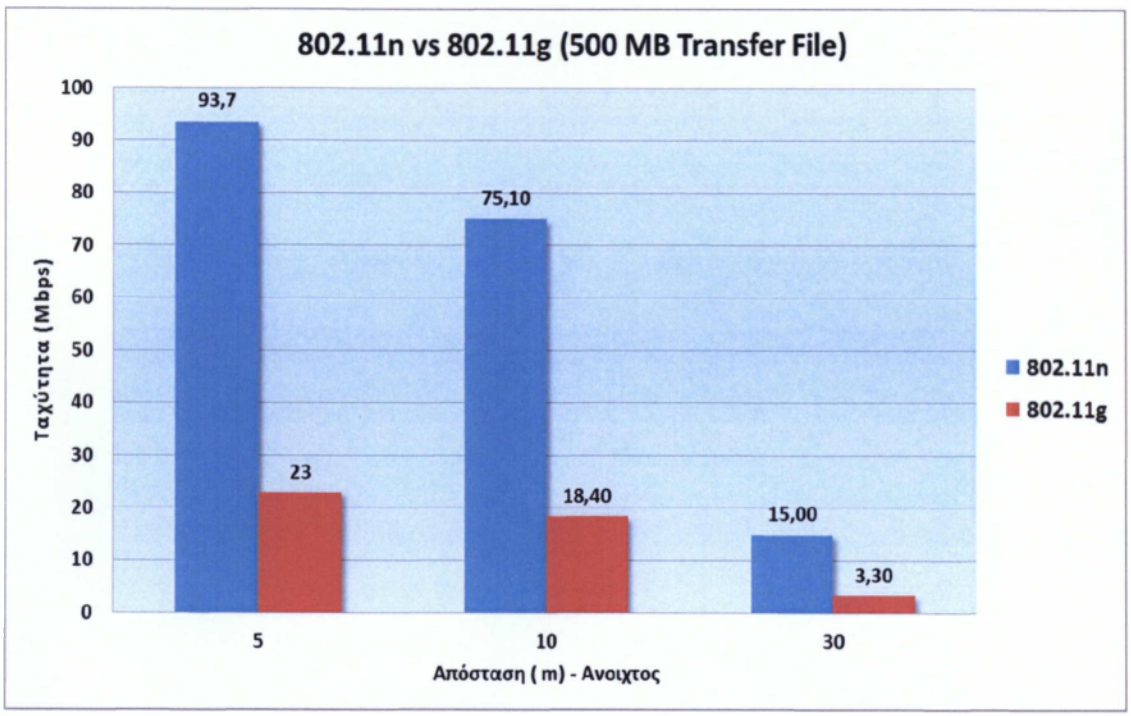
Πίνακας 5.3: Σύγκριση προτύπων στα 100MB σε σχέση με την απόσταση



Στο παραπάνω σχήμα, συγκρίνουμε τα πρότυπα 802.11g και 802.11n και εξετάζουμε την αλλαγή της ταχύτητας και στα δύο πρότυπα, ανάλογα με την απόσταση με μέγεθος μεταφερόμενου αρχείου τα 100 MB. Από τα 5 μέχρι τα 10m παρατηρούμε ότι υπάρχει μείωση της ταχύτητας και των δύο προτύπων. Από τα 10 έως τα 30m παρατηρούμε ότι υπάρχει ραγδαία μείωση της ταχύτητας και στα δύο πρωτόκολλα. Επίσης, οι μετρήσεις γίνονται σε ανοιχτό χώρο χωρίς παρεμβολή εμποδίων.

Απόσταση	Ταχύτητα n	Ταχύτητα g
5	93,7	23
10	75,10	18,40
30	15,00	3,30

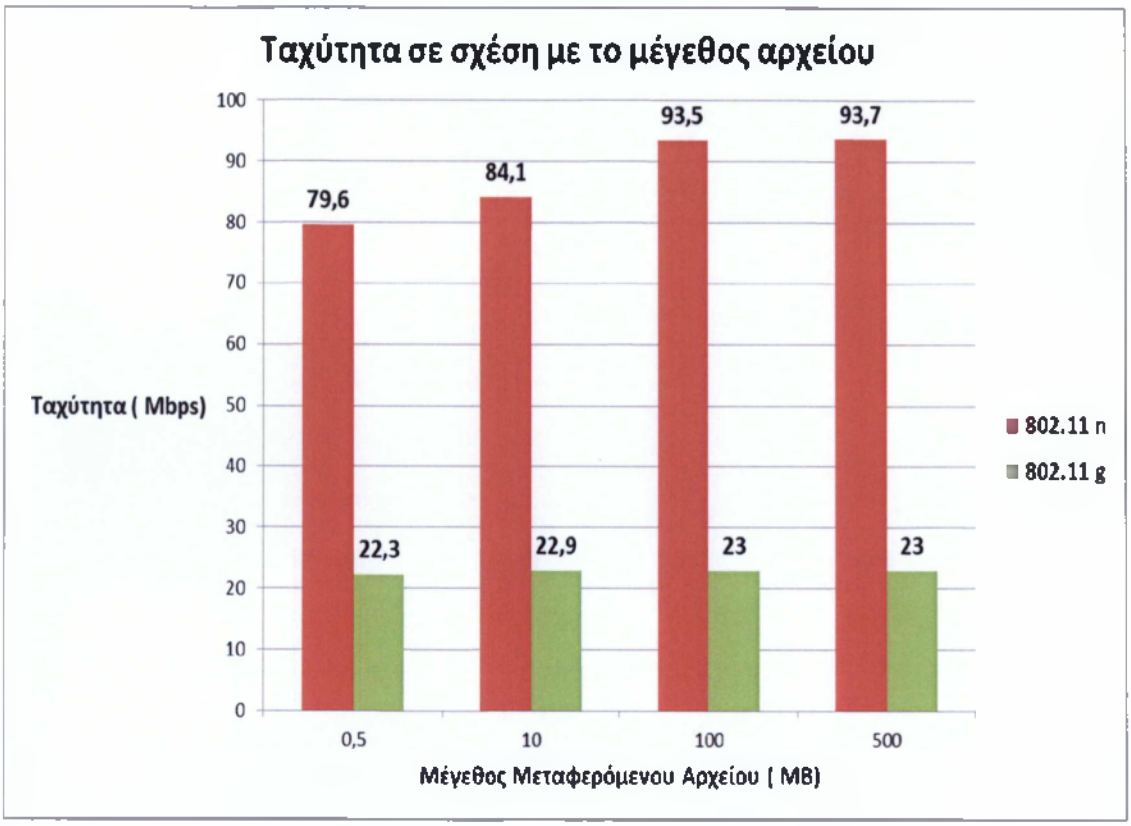
Πίνακας 5.4: Σύγκριση προτύπων στα 500MB σε σχέση με την απόσταση



Στο παραπάνω σχήμα, θα συγκρίνουμε την ταχύτητα των προτύπων 802.11g και 802.11n σε σχέση με την απόσταση με μέγεθος μεταφερόμενου αρχείου 500 MB. Οι μετρήσεις έγιναν σε ανοιχτό χώρο, χωρίς την ύπαρξη εμποδίων. Από τα 5 μέχρι τα 10 m παρατηρούμε ότι η ταχύτητα και στα δύο πρότυπα μειώνεται σταδιακά. Από τα 10 μέχρι τα 30 μέτρα παρατηρούμε ότι υπάρχει απότομη μείωση της ταχύτητας και των δύο προτύπων.

File size	802.11n	802.11g
0,5	79,6	22,3
10	84,1	22,9
100	93,5	23
500	93,7	23

Πίνακας 5.5: Σύγκριση προτύπων στα 500MB σε σχέση με το μέγεθος του μεταφερόμενου αρχείου



Στο παραπάνω σχήμα, συγκρίνουμε την ταχύτητα των δυο πρότυπων 802.11g και 802.11n σε σχέση με το μέγεθος του μεταφερόμενου αρχείου. Για το πρότυπο 802.11n παρατηρούμε ότι από τα 0,5MB μέχρι τα 100MB η ταχύτητα αυξάνεται συνεχώς. Από τα 100 έως τα 500MB η ταχύτητα παρουσιάζει μικρή αύξηση. Όσον αναφορά το πρότυπο 802.11g, παρατηρούμε ότι από τα 0,5 έως τα 100MB υπάρχει μια πολύ μικρή αύξηση της ταχύτητας του. Από τα 100 έως τα 500MB παρατηρούμε ότι η ταχύτητα παραμένει σταθερή.

Για το πρότυπο 802.11n, βλέπουμε πως η μέγιστη ταχύτητα είναι κοντά στα 100Mbps. Αυτό συμβαίνει διότι, η κάρτα δικτύου με την οποία είναι συνδεδεμένο το Access Point είναι 10/100Mbps. Αν οι μετρήσεις γίνονταν με κάρτα δικτύου, η οποία διέθετε ταχύτητες 10/100/1000Mbps, θα παρατηρούσαμε ακόμα μεγαλύτερες ταχύτητες της τάξης κοντά στα 300Mbps. Οι τιμές των μετρήσεων που πάρθηκαν στην εργασία είναι ένας μέσος όρος πολλών δοκιμών, ώστε να πάρουμε ένα πιο γενικό, αλλά πιο ξεκάθαρο αποτέλεσμα. Τέλος, όσο μεγάλωνε η απόσταση στις μετρήσεις, τόσο μεγάλωναν και τα επίπεδα εμποδίων για πιο πραγματικές τιμές.

Το γενικό συμπέρασμα είναι ότι πρότυπο 802.11n είναι αρκετά καλύτερο από το πρότυπο 802.11g. Θεωρητικά, το πρότυπο 802.11n παρέχει ταχύτητες έως 300Mbps, ενώ το πρότυπο 802.11g ταχύτητες έως 54Mbps. Πρακτικά, και με τον ανωτέρω εξοπλισμό, παρατηρούμε πως η μέγιστη ταχύτητα για το πρότυπο 802.11n φτάνει στα 100Mbps, και η μέγιστη ταχύτητα για το πρότυπο 802.11g αγγίζει την θεωρητική προσέγγιση κοντά στα 54Mbps.

Όπως παρατηρούμε και από τις γραφικές παραστάσεις, φτάνουμε στο συμπέρασμα πως το πρότυπο 802.11n παρέχει μεγαλύτερες ταχύτητες και μεγαλύτερη αξιοπιστία από το πρότυπο 802.11g.

Πηγές / Βιβλιογραφία

- Δίκτυα Υπολογιστών, Andrew S. Tanenbaum, Εκδόσεις Παπασωτηρίου, 5η Έκδοση
- Ο Πλήρης Οδηγός της Εγκατάστασης Δικτύων, David Groth Jim McBee, Εκδόσεις Μ. Γιούρδας
- Network Security, Charlie Kaufman – Radia Perlman – Mike Speciner, Second Edition
- Ασφάλεια Πληροφοριών, Τεχνικά Νομικά και Κοινωνικά Θέματα, Ελληνική Εταιρία Επιστημών Ηλεκτρονικών και Υπολογιστών και Πληροφορικής
- Σχεδιασμός και Υλοποίηση Δικτύων, Αρσένης Δ. Σπύρος, Εκδόσεις Κλειδάριθμος, 2η έκδοση