Τ.Ε.Ι. ΑΡΤΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΤΙΤΛΟ

WIRELESS FIDELITY

ΚΑΘΗΓΗΤΗΣ ΕΠΙΤΗΡΗΤΗΣ: ΜΑΡΓΑΡΙΤΗ ΣΠΥΡΙΔΟΥΛΑ
ΦΟΙΤΗΤΗΣ: ΜΑΡΗΣ ΜΗΝΑΣ

ΑΡΤΑ 2005

Τ.Ε.Ι. ΑΡΤΑΣ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΜΕ ΤΙΤΛΟ

WIRELESS FIDELITY

ΚΑΘΗΓΗΤΗΣ ΕΠΙΤΗΡΗΤΗΣ: ΜΑΡΓΑΡΙΤΗ ΣΠΥΡΙΔΟΥΛΑ
ΦΟΙΤΗΤΗΣ: ΜΑΡΗΣ ΜΗΝΑΣ

ΑΡΤΑ 2005

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την καθηγήτρια κυρία Μαργαρίτη Σπυριδούλα που μου έδωσε την ευκαιρία και την βοήθεια για να πραγματοποιήσω την παρούσα εργασία. Επίσης θα ήθελα να ευχαριστήσω την οικογένεια μου για την υποστήριξη και την υπομονή που είχαν στην διάρκεια της ολοκλήρωσης των σπουδών μου.

ΠΕΡΙΕΧΟΜΕΝΑ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ACK: Acknowledge
AES: Advanced **E**ncryption **S**tandard
AID: Association ID
AP: Access **P**oint
ATIM: Announcement **T**raffic **I**ndication **M**essages
BSA: Basic **S**ervice **A**rea
BSS: Basic **S**ervice **S**et
BSSID: Basic **S**ervice **S**et ID
CA: Collision **A**voidance
CCK: Complementary **C**ode **K**eying
CCM: Cipher-**B**lock **M**ode
CD: Collision **D**etection
CDMA: Code **D**ivision **M**ultiple **A**ccess
CRC: Cyclic **R**edundancy **C**ode
CSMA: Carrier **S**ense **M**ultiple **A**ccess
DBPSK: Differential **B**inary **P**hase **S**hift **K**eying
DCF: Distributed **C**oordination **F**unction
DCLA: DC Level **A**djustment
DHCP: Dynamic **H**ost **C**ontrol **P**rotocol
DIFS: DCF **I**nter-**F**rame **S**pace
DQPSK: Differential **Q**uadrature **P**hase **S**hift **K**eying
DS: Distribution **S**ystem
DSSS: Direct **S**equence **S**pread **S**pectrum
DTIM: Delivery **T**raffic **I**ndication **M**ap
EAP: Extensible **A**uthentication **P**rotocol
EIFS: Extended **I**nter-**F**rame **S**pace
ESS: Extended **S**ervice **S**et
ETSI: European **T**elecommunications **S**tandard **I**nstitute
FCC: Federal **C**ommunications **C**ommission
FCS: Frame **C**heck **S**equence
FDM: Frequency **D**ivision **M**ultiplexing
FDMA: Frequency **D**ivision **M**ultiple **A**ccess
FSSS: Frequency **H**opping **S**pread **S**pectrum
GFSK: Gaussian **F**requency **S**hift **K**eying
GSM: Groupe **S**peciale **M**obile
IAPP: Inter **A**ccess **P**oint **P**rotocol
IBSS: Independent **B**asic **S**ervice **S**et
ICI: Inter **C**arrier **I**nterference
IEEE: Institute of **E**lectrical and **E**lectronics **E**ngineers
IFS: Inter-**F**rame **S**pace
IR: Infrared
ISI: Inter **S**ymbol **I**nterference
ISM: Industrial, **S**cientific, **M**edical
LAN: Local **A**rea **N**etwork
LLC: Logical **L**ink **C**ontrol
MAC: Medium **A**ccess **C**ontrol
MIB: Management **I**nformation **B**ases
MIC: Message **I**ntegrity **C**heck
MLME: MAC **L**ayer **M**anagement **E**ntity
MSB: Most **S**ignificant **B**it

MSDU: Mac **S**ervice **D**ata **U**nit
NAT: Network **A**ddress **T**ranslation
NAV: Network **A**llocation **V**ector
NCI: Network **I**nterface **C**ard
NIST: National **I**nstitute of **S**tandards and **T**echnology
OFDM: Orthogonal **F**requency **D**ivision **M**ultiplexing
OSI: Open **S**ystem **I**nterconnection
PBCC: Packet **B**inary **C**onvolutional **C**oding
PCF: Point **C**oordination **F**unction
PCMCIA: Personal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation
PDU: Protocol **D**ata **U**nit
PEAP: Protected **E**xtensible **A**uthentication **P**rotocol
PIFS: PCF **I**nter-**F**rame **S**pace
PLCP: Physical **L**ayer **C**onvergence **P**rocedure
PLME: Physical **L**ayer **M**anagement **E**ntity
PMD: Physical **M**edium **D**ependent
PPM: Pulse **P**osition **M**odulation
PS mode: Power **S**aving **m**ode
PSDU: Protocol **S**ervice **D**ata **U**nit
PSK: Pre-**S**hared **K**ey
PS-Poll: Power **S**ave **P**oll
QoS: Quality **o**f **S**ervices
RADIUS: Remote **A**uthentication **D**ial-**I**n **U**ser **S**ervices
RF: Radio **F**requency
RTS: Ready **T**o **S**end
SAP: Service **A**ccess **P**oint
SFD: Start **F**rame **D**elimiter
SIFS: Short **I**nter-**F**rame **S**pace
SME: System **M**anagement **E**ntity
SOHO: Small **O**ffice **H**ome **O**ffice
SSID: Service **S**et ID
SSL: Secure **S**ocket **L**ayer
TBTT: Target **B**eacon **T**ransmission **T**ime
TIM: Traffic **I**ndication **M**ap
TKIP: Temporal **K**ey **I**ntegrity **P**rotocol
TLS: Transport **L**ayer **S**ecurity
TSF: Timing **S**ynchronization **F**unction
TTLS: Tunneled **T**ransport **L**ayer **S**ecurity
UNII: Unlicensed **N**ational **I**nformation **I**nfrastructure
USB: **U**niversal **S**erial **B**us
VLAN: Virtual **L**ocal **A**rea **N**etwork
VPN: Virtual **P**rivate **N**etwork
WECA: Wireless **E**thernet **C**ompatibility **A**lliances
WEP: Wired **E**quivalent **P**rivacy
Wi-Fi: **Wi**reless **Fi**delity
WISP: Wireless **I**nternet **S**ervice **P**rovider
WLAN: Wireless **L**ocal **A**rea **N**etwork
WNCI: Wireless **N**etwork **I**nterface **C**ard
WPA: Wi-Fi **P**rotected **A**ccess

Πρόλογος

Τα ασύρματα δίκτυα έχουν μπει πλέον στην ζωή μας. Στην παρούσα πτυχιακή εργασία θα γίνει μία παρουσίαση για μία κατηγορία των ασύρματων δικτύων, τα δίκτυα Wi-Fi (Wireless Fidelity) τα οποία έχουν κερδίσει την μεγαλύτερη ανταπόκριση από τους καταναλωτές και τους κατασκευαστές χάρης της οργάνωσης Wi-Fi Alliances και το πρότυπο 802.11. Παρακάτω θα γίνει αναφορά για την τεχνολογία που χρησιμοποιούν και τις τοπολογίες, τον εξοπλισμό που χρειάζεται για να δημιουργηθεί ένα δίκτυο Wi-Fi, τις εφαρμογές που έχουν στην ζωή μας και στις επιχειρήσεις, για την ασφάλεια που έχει καθιερωθεί για την προστασία των δεδομένων που διακινούνται μέσων των συσκευών Wi-Fi και για την εξέλιξη που θα έχουν στο μέλλον.

1. ΕΙΣΑΓΩΓΗ

1.1 Τι είναι το Wi-Fi

Wi-Fi ή Wireless Fidelity αναφέρεται στην τεχνολογία που περιβάλλει τη ράδιο-μετάδοση δεδομένων internet πρωτοκόλλου από μια ασύρματη σύνδεση internet σε έναν Host υπολογιστή. Συχνότερα η σύνδεση με το internet είναι μια σύνδεση υψηλής ταχύτητα όπως η δορυφορική ή DSL παρά τις πιο αργές συνδέσεις dial-up. Είναι ουσιαστικά μια ασύρματη σύνδεση μεταξύ του υπολογιστή στο σπίτι με το internet (π.χ. DSL router ή modem)

Το Wi-Fi όχι μόνο είναι διαθέσιμο στο καταναλωτικό σπίτι αλλά και σε αυτά που αναφέρονται ως Wi-Fi hotspots. Αυτές είναι συνήθως περιοχές όπως τα καφετέριες ή εστιατόρια όπου το Wi-Fi είναι διαθέσιμα για την πρόσβαση στο internet σε μια καθορισμένη τιμή.

Τα δίκτυα Wi-Fi βασίζονται στο πρότυπο IEEE 802.11b ή 802.11a για να μεταδώσουν τα δεδομένα από τη σύνδεση με το internet στον host υπολογιστή (π.χ. το lap-top) και το αντίστροφο. Αυτές οι τεχνολογίες παρέχουν την αξιόπιστη και γρήγορη ασύρματη συνδεσιμότητα και μέχρι ενός ορισμένου βαθμού ένα επίπεδο ασφάλειας. Ένα δίκτυο Wi-Fi μπορεί να χρησιμοποιηθεί για να συνδέσει τους υπολογιστές τον έναν με το άλλο, με το internet, και με τα ενσύρματα δίκτυα.

Τα WI-FI δίκτυα λειτουργούν στις ζώνες 2,4 και 5 GHz που χρησιμοποιούνται χωρίς άδεια, με 11 Mbps (802.11b) ή 54 Mbps (802.11a) ταχύτητες ή με τα προϊόντα που περιέχουν και τις δύο ζώνες (διπλή ζώνη) και έτσι μπορούν να παρέχουν την πραγματική απόδοση παρόμοια με τα βασικά 10BaseT ενσύρματα δίκτυα Ethernet που χρησιμοποιούνται σε πολλά γραφεία.

1.2 Εξέλιξη του Wi-Fi

Το Ινστιτούτο ηλεκτρολόγων και ηλεκτρονικών μηχανικών (IEEE, Institute of Electrical and Electronics Engineers) επικύρωσε την αρχική έκδοση των προτύπων για τα ασύρματα δίκτυα τοπικής περιοχής γνωστά ως IEEE 802.11 το 1997. Ανήκοντας στην ίδια οικογένεια προτύπων με τα Ethernet, παρονομάστηκε "ασύρματο Ethernet" και θεωρήθηκε κατάλληλη τεχνολογία δικτύωσης για τα γραφεία επειδή δεν στηρίζονταν στα καλώδια. Αν και φορτώνεται από την έμφυτη αβεβαιότητα (Fluhrer, 2001) και τις χαμηλές ταχύτητες (Mbps) έναντι του ενσύρματου αντιπάλου του, το IEEE 802.11 ήταν μια επιτυχία. Το κόστος παραγωγής των chipsets 802.11 έπεσε γρήγορα και οι 802.11 adapters πελατών βρήκαν τον δρόμο τους στον υπολογιστή γραφείου, στα lap-top και τους προσωπικούς ψηφιακούς βοηθούς (PDA). Wi-Fi (συντομία του wireless fidelity), ένα φιλικό προς τον καταναλωτή παρατσούκλι για 802.11 που υιοθετήθηκε και η Wireless Ethernet Compatibility Alliance

(WECA), μια μη κερδοσκοπική διεθνής ένωση διαμορφώθηκε το 1999 για να πιστοποιήσει τη διαλειτουργικότητα των προϊόντων Wi-Fi. Η WECA άλλαξε το όνομα της σε Wi-Fi Alliance το 2002 (Wi-Fi Alliance, 2004).

Οι νεώτερες IEEE προδιαγραφές περιλαμβάνουν τα πρότυπα 802.11g, που επιτρέπουν στους σταθμούς και τα σημεία πρόσβασης (Access Point) να συνδέσουν το ένα με το άλλο με τις ταχύτητες μέχρι και 54 Mbps, και 802.11i, που υιοθετεί τους προηγμένους αλγορίθμους επικύρωσης και κρυπτογράφησης που προστατεύουν από τους αναρμόδιους χρήστες που προσπαθούν να αποκτήσουν πρόσβαση στα ιδιωτικά δίκτυα (IEEE πρότυπα, το 2004). 802.11i επίσης προστατεύει την εμπιστευτικότητα και την ακεραιότητα των ασύρματων εργασιών που είναι συνήθως ευαίσθητες να υποκλαπούν από τις επιθέσεις Hacking.

1.3 Επικύρωση Wi-Fi (Wi-Fi CERTIFIED)

Η Wi-Fi Alliances δημιούργησε τον Μάρτιο του 2000 το πρόγραμμα Wi-Fi CERTIFIED για να πιστοποιήσει την διαλειτουργικότητα των συσκευών Wi-Fi. Η πιστοποίηση Wi-Fi βεβαιώνει τη δοκιμασμένη και αποδεδειγμένη διαλειτουργικότητα μεταξύ του ασύρματου εξοπλισμού των υπολογιστών. Αυτή η πιστοποίηση δίνει την εμπιστοσύνη καταναλωτών και επιχειρησιακών αγοραστών ότι τα ασύρματα προϊόντα του τοπικού LAN (Local Area Network) που έχουν το λογότυπο Wi-Fi έχουν περάσει τις αυστηρές απαιτήσεις πιστοποίησης διαλειτουργικότητας. Τέτοια προϊόντα Wi-Fi περιλαμβάνουν κάρτες PCMCIA για τα laptop, κάρτες PCI για τους υπολογιστές γραφείου, USB modules (που μπορούν να χρησιμοποιηθούν με τα laptop ή τους υπολογιστές γραφείου), και ασύρματοι σταθμοί βάσεων όπως τα Access Point και gateway. Τα προϊόντα πιστοποίησης Wi-Fi υποστηρίζουν μέγιστη ταχύτητα είτε 11 Mbps (802.11b) είτε 54 Mbps (802.11a και 802.11g).

Τα προϊόντα με την πιστοποίηση Wi-Fi πρέπει να:

- Προσαρμόζονται στα πρότυπα IEEE 802.11
- Να περάσουν δοκιμές διαλειτουργικότητας
- Να εφαρμόζουν ορισμένα προαιρετικά μέρη των προτύπων

Η πιστοποίηση Wi-Fi υποδεικνύεται από μια ετικέτα στο προϊόν και τη συσκευασία της που δείχνει τη ζώνη συχνότητας και την ταχύτητα που υποστηρίζει..

1.4 Wi-Fi connects you anywhere

Φανταστείτε να δουλεύεται στο lap-top σας ή στο ηλεκτρονικό ταχυδρομείο σας από οπουδήποτε στο σπίτι σας. Με τα δίκτυα Wi-Fi μπορείτε να συνδέεστε με το δίκτυο των γραφείων σας μέσω ενός Wi-Fi Hotspot. Ο όρος "Wi-Fi Hotspot" χρησιμοποιείται για να περιγράφει μια περιοχή όπου η συνδεσιμότητα Wi-Fi είναι διαθέσιμη μέσω ενός κοντινού σημείου πρόσβασης (Access Point). Τα δημόσια Hotspot μπορούν να βρεθούν στα σαλόνια

αερολιμένων, στα καταστήματα και τα εστιατόρια, στα ξενοδοχεία, στις καφετέριες και τα κέντρα έκθεσης. Οι χρήστες Wi-Fi που περιλαμβάνουν τους επιχειρησιακούς ταξιδιώτες και άλλοι επισκέπτες μπορούν να χρησιμοποιήσουν τις φορητές συσκευές τους σε αυτά τα Hotspot για να μπορούν να ανακτήσούν τα αρχεία ή τις παρουσιάσεις τους από το εταιρικό δίκτυο, να σερφάρουν στο Διαδίκτυο ή να στέλνουν στιγμιαία μηνύματα στους συναδέλφους τους και να τα κάνούν όλα αυτά από ένα δωμάτιο διασκέψεων ή την καφετέρια της επιχείρησης.

Με τα δίκτυα Wi-Fi μπορεί κάποιος να είναι σε θέση να κινήσει ολόκληρο το γραφείο του χωρίς απώλεια της επένδυσής του στην εγκατάσταση δικτύωσης, ή να προστεθεί νέο προσωπικό, όλα χωρίς την κίνηση των καλωδίων ή εγκατάσταση των περίπλοκων hub και των δρομολογητών.

2. ΤΕΧΝΟΛΟΓΙΑ Wi-Fi

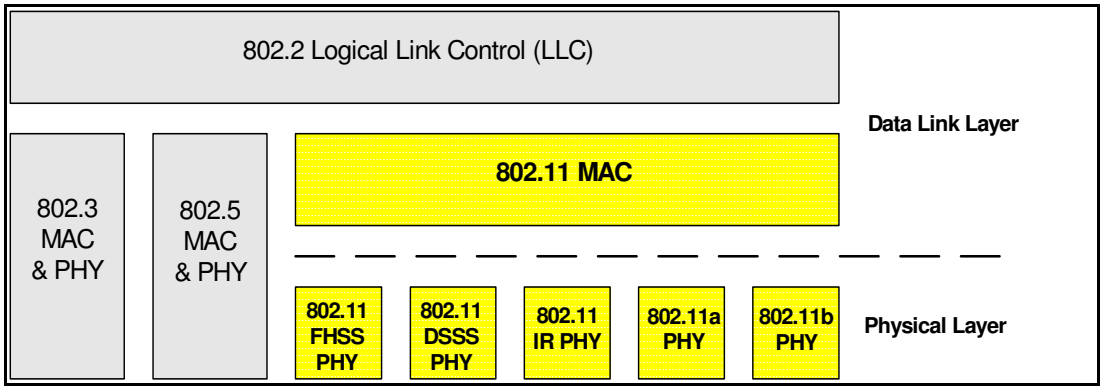
Τα δίκτυα Wi-Fi χρησιμοποιούν ράδιο-τεχνολογίες αποκαλούμενες IEEE 802.11b ή 802.11a για να παρέχει ασφαλής, αξιόπιστη και γρήγορη ασύρματη σύνδεση. Τα δίκτυα Wi-Fi λειτουργούν στις ζώνες 2,4 και 5 GHz , που χρησιμοποιούνται χωρίς ειδική άδεια, με 11 Mbps (802.11b) ή 54 Mbps (802.11a) ταχύτητες ή με τα προϊόντα που περιέχουν και τις δύο ζώνες (διπλή ζώνη), έτσι μπορούν να παρέχουν την πραγματική απόδοση παρόμοια με τα βασικά 10BaseT ενσύρματα δίκτυα Ethernet που χρησιμοποιούνται σε πολλά γραφεία. Στο παρακάτω κεφάλαιο γίνεται μια ανάλυση του πρότυπου 802.11 και των 802.11a και 802.11b που αποτελούν εξέλιξη του και ο βασικός λόγος της εξάπλωσης των δικτύων Wi-Fi**.**

2.1 Πρότυπο 802.11

Το πρότυπο 802.11 ανακοινώθηκε από την IEEE επίσημα το 1997. Στη συνέχεια ανακοινώθηκαν συμπληρωματικά πρότυπα, όπως τα 802.11a και 802.11b το 1999. Σήμερα τα ασύρματα δίκτυα που βασίζονται σε αυτήν την οικογένεια προτύπων είναι τα πλέον διαδεδομένα, ενώ κυκλοφορεί μεγάλη ποικιλία σχετικών προϊόντων στην αγορά.

2.1.1 Διαστρωμάτωση

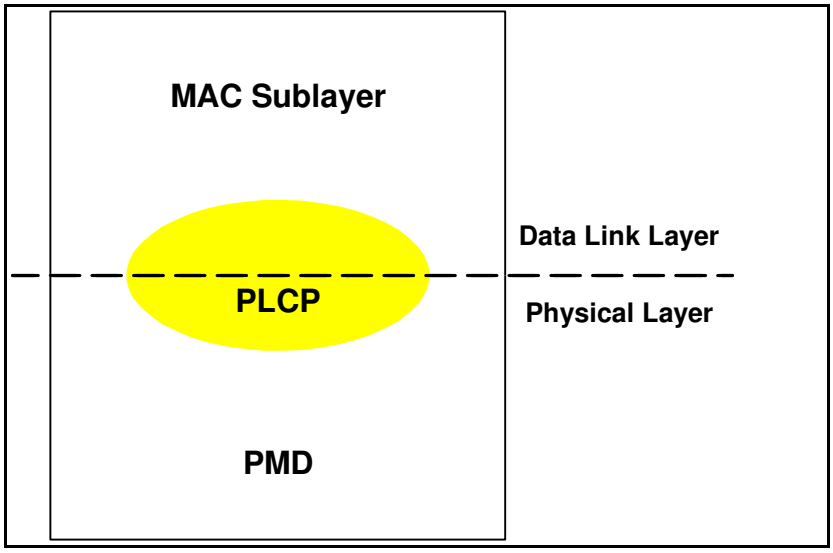
Το 802.11 αναφέρεται στα δύο χαμηλότερα στρώματα του μοντέλου διαστρωμάτωσης OSI (Open System Interconnection), δηλαδή στο φυσικό στρώμα (Physical Layer – PHY) και στο υπόστρωμα MAC (Medium Access Control) του στρώματος ζεύξης δεδομένων (Data Link Layer). Το άλλο υπόστρωμα του στρώματος ζεύξης δεδομένων, δηλαδή το υπόστρωμα ελέγχου λογικής ζεύξης (Logical Link Control – LLC), είναι αυτό που έχει προτυποποιηθεί ως IEEE 802.2 και χρησιμοποιείται σε συνδυασμό με όλα τα διαφορετικά MAC της σειράς IEEE 802, όπως φαίνεται στο Σχήμα 2.1.



Σχήμα 2.1: Διαστρωμάτωση του προτύπου 802.11

Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC (Medium Access Control) που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Κάθε φυσικό στρώμα χωρίζεται σε δύο υποστρώματα, όπως φαίνεται στο Σχήμα 2.2.

Το υπόστρωμα PLCP (Physical Layer Convergence Procedure) χρησιμεύει στην προσαρμογή των διαφόρων φυσικών στρωμάτων στο κοινό MAC. Το υπόστρωμα PMD (Physical Medium Dependent) περιέχει όλες τις λειτουργίες που απαιτούνται για τη μετάδοση της πληροφορίας από το εκάστοτε φυσικό στρώμα.



Σχήμα 2.2: Φυσικό στρώμα του προτύπου 802.11

2.1.2 Βασικές μονάδες – Τοπολογίες

Τα ασύρματα δίκτυα 802.11 αποτελούνται από τέσσερις βασικές μονάδες. Αυτές είναι:

- *Σημείο πρόσβασης (Access Point – AP):* Το AP είναι η μονάδα που παίζει το ρόλο γέφυρας μεταξύ του ενσύρματου και του ασύρματου δικτύου, μετατρέποντας κατάλληλα τα πλαίσια που ανταλλάσσονται μεταξύ αυτών. Επιτελεί και πολλές άλλες λειτουργίες στο ασύρματο δίκτυο που θα αναφερθούν στη συνέχεια.

- *Σύστημα διανομής (Distribution System):* Το σύστημα διανομής ενώνει τα διάφορα AP του ίδιου δικτύου, επιτρέποντάς τους να ανταλλάσσουν πλαίσια. Το 802.11 δεν προσδιορίζει τον τρόπο που θα γίνεται αυτό.

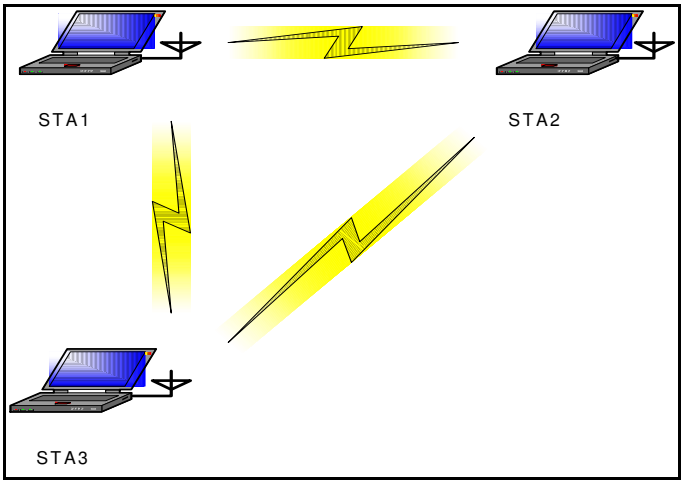
- *Ασύρματο μέσο μετάδοσης (Wireless Medium):* Έχουν οριστεί διάφορα φυσικά στρώματα που χρησιμοποιούν είτε ραδιοσυχνότητες είτε υπέρυθρες ακτίνες για τη μετάδοση των πλαισίων μεταξύ των σταθμών του ασύρματου δικτύου.

- *Σταθμοί (Stations):* Οι σταθμοί που ανταλλάσσουν πληροφορία μέσω του ασυρμάτου δικτύου συνήθως είναι φορητές συσκευές (για παράδειγμα laptops), χωρίς όμως αυτό να είναι απαραίτητο.

Η βασική δομική μονάδα κάθε 802.11 δικτύου αποκαλείται Basic Service Set (BSS) και αποτελείται από μία ομάδα σταθμών που επικοινωνούν μεταξύ τους. Τα όρια του BSS ορίζονται από την περιοχή ράδιο-κάλυψης, που ονομάζεται Basic Service Area (BSA). Ένας σταθμός σε ένα BSS μπορεί να επικοινωνεί με οποιονδήποτε άλλο σταθμό στο ίδιο BSS.

Επιπλέον υπάρχουν δύο βασικές τοπολογίες, βάσει των οποίων ορίζονται δύο είδη ασυρμάτων δικτύων. Τα είδη αυτά είναι τα **ανεξάρτητα δίκτυα** (independent networks) και τα **δίκτυα υποδομής** (infrastructure networks).

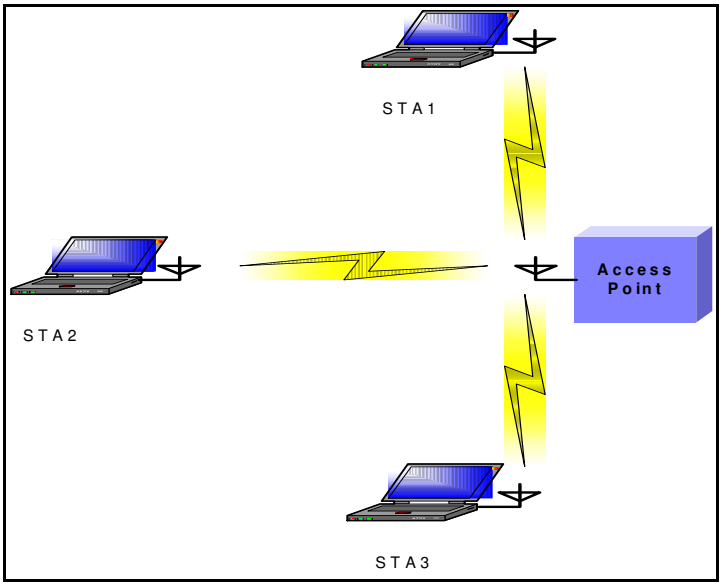
Σε ένα independent δίκτυο κάθε σταθμός επικοινωνεί απευθείας με όλους τους υπόλοιπους. Το BSS σε αυτήν την περίπτωση ονομάζεται και IBSS (Independent BSS) ή ad hoc BSS ή πιο απλά ad hoc δίκτυο. Το IBSS αποτελείται το λιγότερο από δύο σταθμούς και συνήθως είναι προσωρινό, δηλαδή δημιουργείται για κάποιο σκοπό και μετά διαλύεται. Είναι ο απλούστερος τύπος ασύρματου δικτύου. Ένα IBSS φαίνεται στο Σχήμα 2.3.



Σχήμα 2.3: *Τοπολογία IBSS*

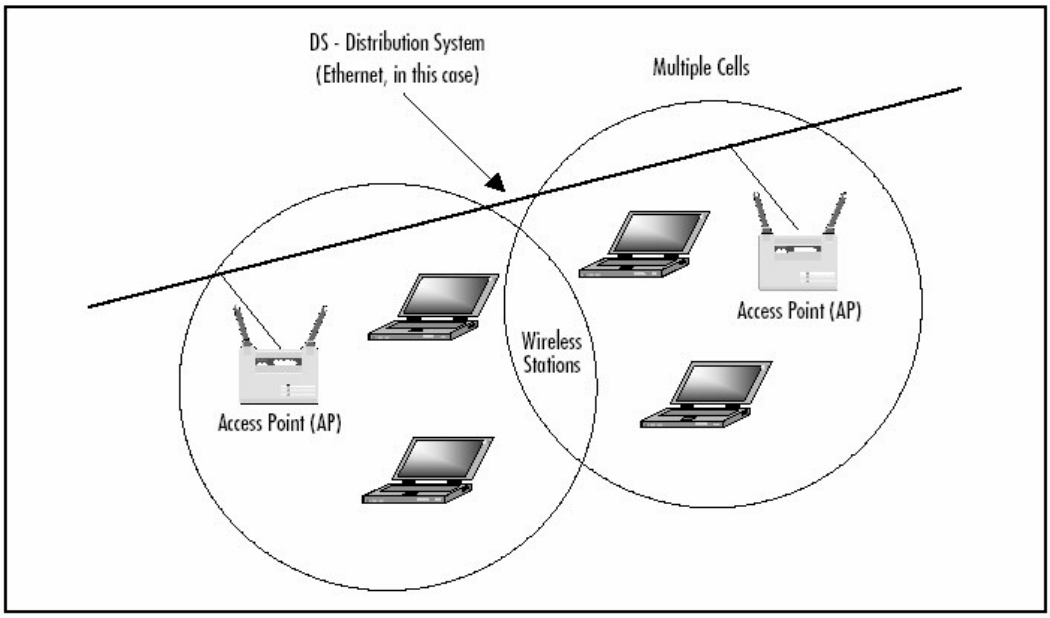
Ο άλλος τύπος δικτύου είναι το infrastructure δίκτυο. Σε αυτήν την περίπτωση το BSS διακρίνεται από την παρουσία σε αυτό ενός AP. Το AP, εκτός από το ότι συνδέει το BSS με το ενσύρματο δίκτυο, είναι υπεύθυνο για την ανταλλαγή πλαισίων μεταξύ των σταθμών και γενικότερα για τον κεντρικό έλεγχο της λειτουργίας του BSS. Όταν ένας σταθμός θέλει να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, το πλαίσιο αρχικά αποστέλλεται στο AP και αυτό το στέλνει στον τελικό προορισμό του. Η BSA σε αυτήν την περίπτωση είναι η περιοχή όπου υπάρχει ράδιο-κάλυψη από το AP. Έτσι σε αντίθεση με το IBSS, όπου όλοι οι σταθμοί πρέπει να βρίσκονται στην περιοχή ράδιο-κάλυψης των υπολοίπων, για να επικοινωνήσουν με αυτούς, εδώ αρκεί να βρίσκονται στην περιοχή ράδιο-κάλυψης του AP, άσχετα με την μεταξύ τους απόσταση. Για να συμμετέχει ένας σταθμός στο BSS πρέπει να ακολουθήσει τη διαδικασία του association με το AP. Η διαδικασία αυτή ξεκινάει πάντα με πρωτοβουλία του σταθμού και είναι απόφαση του AP αν ο σταθμός θα γίνει τελικά δεκτός στο BSS. Το 802.11 δεν ορίζει μέγιστο αριθμό σταθμών που μπορούν να συμμετάσχουν σε ένα BSS, αλλά

τίθενται περιορισμοί στις διάφορες υλοποιήσεις AP. Τα παραπάνω φαίνονται καλύτερα στο Σχήμα 2.4.



Σχήμα 2.4: Τοπολογία infrastructure BSS

Στην περίπτωση infrastructure δικτύων ένας αριθμός από BSS's μπορούν να συνδεθούν και να αποτελέσουν ένα Extended Service Set (ESS). Αυτό δημιουργείται ενώνοντας τα AP's των BSS's μέσω ενός ενσύρματου δικτύου κορμού. Με αυτόν τον τρόπο είναι εφικτή η επικοινωνία μεταξύ σταθμών που ανήκουν σε διαφορετικά BSS's αλλά στο ίδιο ESS. Σε αυτήν την περίπτωση πρέπει τα AP's να επικοινωνούν στο στρώμα ζεύξης δεδομένων μέσω του δικτύου κορμού, επιτελώντας τη λειτουργία της γέφυρας για τους σταθμούς διαφορετικών BSS's. Το ESS τελειώνει όταν παρεμβληθεί μεταξύ των AP's οντότητα δικτύου που λειτουργεί σε υψηλότερο στρώμα, όπως είναι ο δρομολογητής (router) Σχήμα 2.5.



Σχήμα 2.5: Τοπολογία ESS

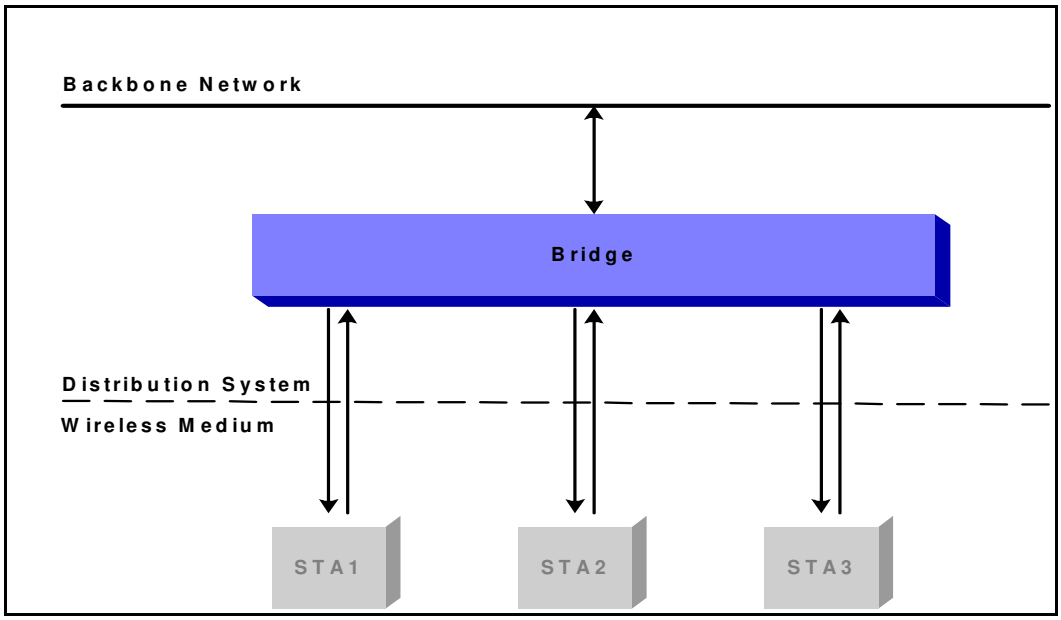
Το 802.11 προσφέρει κινητικότητα σε ένα ESS, αρκεί το δίκτυο κορμού να είναι ένα απλό LAN ή και VLAN (Virtual LAN). Σε κάθε άλλη περίπτωση η σύνδεση στα ανώτερα επίπεδα θα χαθεί, εκτός κι αν χρησιμοποιείται κάποια άλλη τεχνολογία όπως το Mobile IP.

2.1.3 Σύστημα διανομής

Το σύστημα διανομής παίζει πολύ σημαντικό ρόλο στη λειτουργία του 802.11, αν και δεν περιγράφεται στο πρότυπο η υλοποίησή του, αλλά μόνο οι υπηρεσίες που πρέπει να προσφέρει στους ασύρματους σταθμούς. Όπως αναφέρθηκε και παραπάνω, το σύστημα διανομής είναι υπεύθυνο για τη διασύνδεση AP's, δηλαδή BSS's, και τη δημιουργία ESS's. Με αυτόν τον τρόπο καθιστά δυνατή την ανταλλαγή πλαισίων ανάμεσα σε σταθμούς που ανήκουν σε διαφορετικά BSS's εντός του ιδίου ESS.

Για τη σωστή παράδοση των πλαισίων τα AP's πρέπει να επικοινωνούν μεταξύ τους μέσω του συστήματος διανομής. Αυτή η επικοινωνία γίνεται με χρήση ενός πρωτοκόλλου που ονομάζεται Inter Access Point Protocol (IAPP), το οποίο δεν έχει προδιαγραφεί στο 802.11 και αποτελεί αυτή τη στιγμή έναν τομέα εργασίας της ομάδας προτυποποίησης. Εφόσον ανά πάσα στιγμή κάθε σταθμός μπορεί να ανήκει σε ένα μόνο BSS, έχοντας προχωρήσει στο association με το αντίστοιχο AP, πρέπει όλα τα AP's να ενημερώνονται μέσω του συστήματος διανομής, ώστε να προωθούν τα πλαίσια προς το συγκεκριμένο σταθμό στο κατάλληλο AP.

Στο Σχήμα 2.6 φαίνεται καλύτερα η λειτουργία του συστήματος διανομής.



Σχήμα 2.6: Σύστημα διανομής

Τα AP's παίζουν το ρόλο γέφυρας μεταξύ του συστήματος διανομής και του ασυρμάτου δικτύου. Μπορούν να θεωρηθούν και αυτά ως μέρη του συστήματος διανομής, τουλάχιστον όσο αναφορά το interface τους προς το ενσύρματο LAN που αποτελεί το μέσο

μετάδοσης του συστήματος διανομής. Στο Σχήμα 2.6 τα βέλη αντιπροσωπεύουν ροή πλαισίων από και προς το σύστημα διανομής μέσω ενός AP. Αν ο σταθμός STA1 θέλει να στείλει ένα πλαίσιο στον STA2 αυτό πρέπει να πάει στο αντίστοιχο AP, να μετατραπεί σε πλαίσιο του μέσου μετάδοσης του συστήματος διανομής (συνήθως Ethernet), να μεταδοθεί στο AP που εξυπηρετεί το STA2, να μετατραπεί ξανά σε πλαίσιο 802.11 και να μεταδοθεί από το AP στον STA2.

Το σύστημα διανομής είναι δυνατόν να είναι κι αυτό ασύρματο δίκτυο. Τέτοια περίπτωση είναι η διασύνδεση δύο LANs σε διαφορετικές φυσικές τοποθεσίες μέσω μιας ασύρματης ζεύξης σημείο – προς – σημείο. Τότε το ασύρματο δίκτυο χρησιμεύει ως γέφυρα που ενώνει τα δύο LANs στο στρώμα ζεύξης δεδομένων. Ο μηχανισμός αυτός ονομάζεται wireless bridging.

Σημειώνεται τέλος ότι οι σταθμοί χρησιμοποιούν κανονικές 48-μπιτες διευθύνσεις MAC, κάτι που κάνει τη θεώρηση του ασύρματου δικτύου ως επέκταση του ενσύρματου ευκολότερη.

2.1.4 Υπηρεσίες ασύρματου δικτύου 802.11

Το 802.11 προσφέρει εννέα βασικές υπηρεσίες. Από αυτές τρεις σχετίζονται με τη μεταφορά δεδομένων και οι υπόλοιπες έξι σχετίζονται με τη διαχείριση. Οι υπηρεσίες αυτές είναι οι εξής:

- Distribution: Η υπηρεσία αυτή είναι απαραίτητη για την παράδοση ενός πλαισίου από το AP στον τελικό προορισμό του. Συνίσταται στον εντοπισμό του παραλήπτη για να είναι δυνατή η τελική παράδοση του πλαισίου.

- Integration: Η υπηρεσία αυτή παρέχεται από το σύστημα διανομής. Είναι υπεύθυνη για τη διασύνδεση του συστήματος διανομής σε ένα δίκτυο διαφορετικό του 802.11.

- MSDU (Mac Service Data Unit) Delivery: Η παράδοση των πλαισίων MAC στον τελικό προορισμό τους.

- Association: Απαραίτητη διαδικασία συσχετισμού ενός σταθμού με το AP, προκειμένου να είναι σε θέση να στείλει και να δεχτεί πλαίσια μέσω του ασυρμάτου δικτύου.

- Reassociation: Χρησιμοποιείται από τους κινητούς σταθμούς σε περίπτωση μετακίνησης από μία BSS σε μία άλλη. Είναι μέρος του μηχανισμού της διαπομπής.

- Disassociation: Η διαδικασία αυτή αφαιρεί έναν σταθμό από το δίκτυο. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να κάνουν πρώτα disassociation.
- Authentication: Αν απαιτείται από το διαχειριστή του δικτύου, πρέπει κάθε χρήστης να πιστοποιεί την ταυτότητά του πριν να προχωρήσει στη διαδικασία του association.

- Deauthentication: Τερματισμός μιας ισχύουσας κατάστασης authentication. Τερματίζει επίσης και το association, εφόσον το authentication είναι προαπαιτούμενο αυτού.

- Privacy: Λόγω του ασύρματου περιβάλλοντος μετάδοσης έχει οριστεί από το 802.11 μία προαιρετική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (Wired Equivalent Privacy). Το WEP δεν προσφέρει σε καμία περίπτωση ασφαλής μεταφορά δεδομένων και ήδη μελετάται η αντικατάστασή του.

Οι έξι τελευταίες υπηρεσίες σχετίζονται με τη διαχείριση και παρουσιάζονται με περισσότερες λεπτομέρειες στην παράγραφο 2.6**.**

2.2 Φυσικό στρώμα 802.11

Το αρχικό πρότυπο 802.11 ορίστηκε από την IEEE το 1997 και περιελάμβανε προδιαγραφές για το υπόστρωμα MAC καθώς και για τρία διαφορετικά φυσικά στρώματα. Το 1999 η IEEE συμπλήρωσε τα διαθέσιμα φυσικά στρώματα προδιαγράφοντας άλλα δύο, τα 802.11b και 802.11a. Σε αυτό το κεφάλαιο θα παρουσιαστούν όλα τα παραπάνω φυσικά στρώματα. Όπως αναφέρθηκε και παραπάνω, τρία φυσικά στρώματα είχαν οριστεί αρχικά για το πρότυπο 802.11. Αυτά είναι τα εξής:

- Direct Sequence Spread Spectrum (Απλωμένο Φάσμα Ευθείας Ακολουθίας) στην ISM (Industrial, Scientific, Medical)μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps

- Frequency Hopping Spread Spectrum (Απλωμένο Φάσμα και Πήδημα Συχνότητας) στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps

- Infrared (Υπέρυθρες Ακτίνες) σε μήκη κύματος μεταξύ 850 και 950 nm με ρυθμούς μετάδοσης 1 και 2 Mbps.

2.2.1 Φυσικό στρώμα Direct Sequence Spread Spectrum

Η τεχνική Direct Sequence είναι η πιο επιτυχημένη τεχνική που έχει χρησιμοποιηθεί σε συνδυασμό με τα ασύρματα δίκτυα. Σε σχέση με τη Frequency Hopping τεχνική μετάδοσης απαιτεί περισσότερη ενέργεια για να επιτύχει παρόμοια διέλευση, όμως το μεγάλο πλεονέκτημά της είναι ότι μπορεί εύκολα να αναβαθμιστεί για την επίτευξη υψηλότερων ρυθμών μετάδοσης.

2.2.1.1 Direct Sequence Μετάδοση

Η τεχνική μετάδοσης Direct Sequence Spread Spectrum (DSSS) αντικαθιστά κάθε bit πληροφορίας με μία σειρά από bits που ονομάζεται spreading code (κώδικας εξάπλωσης). Τα bits του spreading code κατά σύμβαση ονομάζονται chips. Τα chips μεταδίδονται σε πολύ υψηλότερο ρυθμό από τα αρχικά bits πληροφορίας και έτσι το φάσμα του μεταδιδόμενου

σήματος «απλώνεται». Για παράδειγμα αν αντικαθίσταται κάθε bit με μια ακολουθία από 10 chips το τελικό σήμα θα καταλαμβάνει 10 φορές μεγαλύτερο φασματικό εύρος από το αρχικό. Υποθέτουμε πάντα ότι ο ρυθμός μετάδοσης bits είναι ο ίδιος και στις δύο περιπτώσεις, δηλαδή ότι τα 10 chips πρέπει να μεταδοθούν στον ίδιο χρόνο με το αρχικό bit. Ο αριθμός των chips που κωδικοποιούν κάθε bit ονομάζεται και processing gain (κέρδος επεξεργασίας) ή και spreading ratio (παράγοντας εξάπλωσης).

Αυτή η τεχνική έχει λοιπόν το χαρακτηριστικό ότι διευρύνει το φάσμα του προς μετάδοση σήματος, μειώνοντας ταυτόχρονα το πλάτος του, δηλαδή απλώνει την ισχύ του σήματος σε πολύ μεγαλύτερο φασματικό εύρος. Ο δέκτης εκτελεί την αντίστροφη διαδικασία, δηλαδή εξάγει τα αρχικά bits πληροφορίας, δημιουργώντας ξανά ένα σήμα στενής ζώνης. Για να το κάνει αυτό πρέπει να γνωρίζει το spreading code που χρησιμοποίησε ο πομπός. Ένα πλεονέκτημα της τεχνικής αυτής είναι η ανοχή σε παρεμβολές στενής ζώνης, καθώς και μεγαλύτερη ασφάλεια, εφόσον το «απλωμένο» σήμα μοιάζει σαν απλός θόρυβος σε πομπό που λαμβάνει μόνο σήμα στενής ζώνης.

2.2.1.2 Εφαρμογή στο 802.11 DS φυσικό στρώμα

Στην προδιαγραφή του φυσικού στρώματος αυτού ορίστηκε σαν spreading code μία λέξη Barker των 11 bits και συγκεκριμένα η λέξη «10110111000». Κάθε bit προστίθεται κατά modulo-2 στην παραπάνω ακολουθία για να προκύψει η ακολουθία των chips που θα μεταδοθούν. Αυτό σημαίνει ότι για bit «1» η ακολουθία που μεταδίδεται είναι η λέξη Barker με όλα τα bit ανεστραμμένα, ενώ για bit «0» μεταδίδεται αυτούσια η λέξη Barker. Η χρήση μιας ακολουθίας Barker σαν spreading code αποφασίστηκε επειδή προσφέρει αρκετά μεγάλη ανοχή στη διασπορά της χρονικής καθυστέρησης λόγω διάδοσης μέσω πολλαπλών διαδρομών (multipath delay spread) και σε παρεμβολές στενής ζώνης.

Για το φυσικό στρώμα αυτό ορίστηκαν 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 τα υπόλοιπα ακολουθούν κάθε 5 MHz. Στην πράξη κάθε κανάλι καταλαμβάνει περίπου 22 MHz εύρος, γύρω από την κεντρική του συχνότητα. Γίνεται χρήση RF φίλτρων για να καταπιέζονται οι πλευρικοί λοβοί έξω από τα 22 MHz κατά 30 και 50 dB κάτω από την ισχύ της κεντρικής συχνότητας. Ακόμα και έτσι, κανάλια που χρησιμοποιούνται σε διπλανές «κυψέλες» πρέπει να απέχουν μεταξύ τους 25 MHz (πέντε κανάλια των 5 MHz) για να αποφεύγονται οι παρεμβολές. Αυτό περιορίζει τον μέγιστο αριθμό καναλιών που μπορούν να χρησιμοποιηθούν. Σε κάθε χώρα επιτρέπεται η χρήση συγκεκριμένων καναλιών. Στον Πίνακα 2.1 φαίνονται τα κανάλια που χρησιμοποιούνται σε διάφορες γεωγραφικές περιοχές.

Περιοχή / Υπεύθυνη Αρχή	Επιτρεπόμενα Κανάλια
ΗΠΑ / FCC – Καναδάς / IC	1 έως 11 (2,412 – 2,462 GHz)
Ευρώπη (εκτός Γαλλίας & 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 2.1: Διαθέσιμα κανάλια φυσικού στρώματος 802.11 DSSS σε διάφορες περιοχές

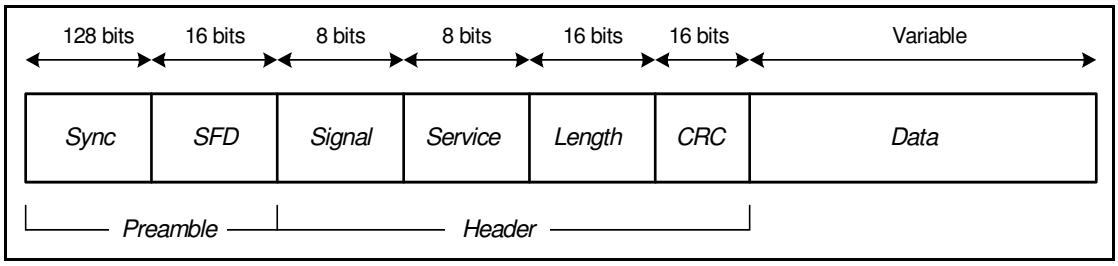
Στην Ευρώπη υπάρχουν διαθέσιμα 13 κανάλια. Με βάση όμως τον περιορισμό για τον διαχωρισμό των καναλιών που χρησιμοποιούνται σε διπλανές «κυψέλες» μένουν τελικά μόνο 3 διαθέσιμα κανάλια, για παράδειγμα τα 1, 6 και 11.

Τέλος, σε σύγκριση με το εναλλακτικό Frequency Hopping Spread Spectrum φυσικό επίπεδο, μπορούν να γίνουν οι εξής παρατηρήσεις:

- Το Direct Sequence είναι πιο ανθεκτικό στις παρεμβολές, λόγω της φασματικής εξάπλωσης του σήματος.
- Ο θόρυβος αντιμετωπίζεται πολύ καλά μέχρι ενός συγκεκριμένου επιπέδου, από εκεί και πέρα η μετάδοση καταστρέφεται.
- Σε σχέση με το Frequency Hopping είναι πιο εύκολη η συνύπαρξη ενός Direct Sequence συστήματος με έναν πρωταρχικό χρήστη που εκπέμπει σήματα στενής ζώνης. Αντίθετα η συνύπαρξη δύο ή περισσοτέρων Direct Sequence συστημάτων είναι πρόβλημα που αντιμετωπίζεται με τον σωστό διαχωρισμό των χρησιμοποιούμενων καναλιών.

2.2.1.3 DSSS – Υπόστρωμα PLCP

Το πλαίσιο του PLCP υποστρώματος φαίνεται στο Σχήμα 2.7.



Σχήμα 2.7: Πλαίσιο PLCP υποστρώματος του φυσικού στρώματος 802.11 DSSS

Πριν τη μετάδοση ολόκληρο το πλαίσιο υπόκειται στη διαδικασία του ανακατώματος (scrambling), η οποία αλλάζει τη διάταξη των bits του, ώστε να τους δώσει μια πιο τυχαία κατανομή. Στη συνέχεια περιγράφονται τα διάφορα τμήματα του PLCP πλαισίου.

Preamble

Το τμήμα αυτό χρησιμεύει για το συγχρονισμό πομπού και δέκτη και για τη δήλωση της αρχής του πλαισίου. Περιέχει τα πεδία Sync και SFD (Start Frame Delimiter).

Sync

Πεδίο του preamble, αποτελείται εξολοκλήρου από bits «1» και χρησιμεύει στον συγχρονισμό του δέκτη.

SFD (Start Frame Delimiter)

Πεδίο του preamble, χρησιμεύει στον δέκτη για τον εντοπισμό της αρχής του πλαισίου. Η τιμή του είναι «0000010111001111».

Header

Η επικεφαλίδα του PLCP πλαισίου, αποτελείται από τα επιμέρους πεδία που φαίνονται στο Σχήμα 2.7.

Signal

Σε αυτό το πεδίο κωδικοποιείται κατάλληλα ο ρυθμός μετάδοσης (1 ή 2 Mbps).

Service

Το πεδίο αυτό είναι διαθέσιμο για μελλοντική χρήση, έχει όλα τα bits ίσα με «0».

Length

Περιέχει τον αριθμό των microseconds που χρειάζονται για την εκπομπή του πλαισίου ως 16-μπιτου ακεραίου χωρίς πρόσημο.

CRC

Κυκλικός κώδικας πλεονασμού (Cyclic Redundancy Code) που προστατεύει τα υπόλοιπα πεδία του header.

Data

Το MAC πλαίσιο, δεν υπάρχει κανένας περιορισμός σχετικά με το τμήμα αυτό.

2.2.1.4 DSSS – Υπόστρωμα PMD

Στο PMD υπόστρωμα προβλέπεται η υποστήριξη των δύο διαθέσιμων ρυθμών μετάδοσης. Μετά την κωδικοποίηση τα chips εκπέμπονται με ρυθμό 11 Mbps. Για την επίτευξη των διαφορετικών ρυθμών μετάδοσης, 1 και 2 Mbps, χρησιμοποιούνται δύο διαφορετικές τεχνικές διαμόρφωσης. Για τον ρυθμό του 1 Mbps χρησιμοποιείται η DBPSK (Differential Binary Phase Shift Keying). Κάθε bit πληροφορίας κωδικοποιείται από μια ακολουθία 11 chips. Αυτή μεταδίδεται με ρυθμό 11 Mbps όπου κάθε μεταδιδόμενο σύμβολο (symbol) μεταφέρει 1 chip, άρα ο πραγματικός ρυθμός μετάδοσης bit είναι 1 Mbps. Για το ρυθμό των 2 Mbps χρησιμοποιείται διαμόρφωση DQPSK (Differential Quadrature Phase Shift Keying), όπου κάθε σύμβολο μεταφέρει 2 chips. Σημειώνεται ότι σε αυτήν την περίπτωση τα τμήματα Preamble και Header του PLCP πλαισίου μεταδίδονται σε ρυθμό 1 Mbps χρησιμοποιώντας διαμόρφωση DBPSK. Αυτό γίνεται διότι η DBPSK είναι πιο ανθεκτική από την DQPSK στον θόρυβο και γι' αυτό είναι μικρότερη η πιθανότητα λανθασμένης λήψης των δύο τμημάτων αυτών.

Στη συνέχεια παρουσιάζονται κάποιοι επιπλέον παράμετροι του φυσικού στρώματος στον Πίνακα 2.2.

Παράμετρος	Τιμή
Μέγιστο μήκος πλαισίου MAC	4000 – 8191 bytes
Slot time	20 μsec
SIFS time	10 μsec
Contention window size	31 έως 1023 slots
Preamble duration	144 μsec
PLCP header duration	48 μsec

Πίνακας 2.2: Παράμετροι του φυσικού στρώματος 802.11 DSSS

2.2.2 Φυσικό Στρώμα Frequency Hopping Spread Spectrum

Το φυσικό στρώμα αυτό ήταν το πρώτο που χρησιμοποιήθηκε ευρέως σε εμπορικά προϊόντα. Πλεονεκτήματά του έναντι του εναλλακτικού Direct Sequence 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.

2.2.2.1 Frequency Hopping Μετάδοση

Η τεχνική Frequency Hopping Spread Spectrum (FHSS) βασίζεται στην ιδέα της αλλαγής της φέρουσας ενός σήματος μέσα σε ένα μεγάλο εύρος συχνοτήτων και σύμφωνα με μια συγκεκριμένη ψευδοτυχαία ακολουθία (hopping pattern). Μοιάζει με την κλασσική FDMA (Frequency Division Multiple Access), με τη διαφορά ότι κάθε χρήστης χρησιμοποιεί κάθε διάφορες φέρουσες ανάλογα με το hopping pattern του. Για να επιτευχθεί επικοινωνία μεταξύ πομπού και δέκτη πρέπει ο δέκτης να γνωρίζει το hopping pattern του πομπού και να υπάρχει καλός συγχρονισμός μεταξύ τους.

Πλεονέκτημα της τεχνικής αυτής είναι η δυνατότητα συνύπαρξης διαφορετικών ασυρμάτων δικτύων, αρκεί τα hopping patterns τους να είναι διαφορετικά, δηλαδή σε κάθε χρονική στιγμή κάθε σύστημα να μεταδίδει σε διαφορετική φέρουσα. Τότε τα hopping patterns ονομάζονται ορθογώνια και η συνολική διέλευση μεγιστοποιείται.

Ένα ακόμη πλεονέκτημα είναι η δυνατότητα συνύπαρξης με χρήστες που εκπέμπουν σήματα στενής ζώνης. Αν η εκπομπή γίνεται με αρκετά μεγάλη ισχύ τότε η παρεμβολή από το Frequency Hopping σύστημα σε αυτούς είναι αμελητέα. Αλλά και η δική τους παρεμβολή στο Frequency Hopping σύστημα είναι αμελητέα, εφόσον μπλοκάρουν μία μόνο φέρουσα από όσες αυτό χρησιμοποιεί.

2.2.2.2 Εφαρμογή στο 802.11 Frequency Hopping φυσικό στρώμα

Το φυσικό στρώμα αυτό διαιρεί την ISM μπάντα των 2,4 GHz σε κανάλια εύρους 1 MHz., με το πρώτο κανάλι (κανάλι 0) να έχει τη κεντρική του συχνότητα στα 2,4 GHz. Επιπλέον ορίζεται ότι περίπου το 99% της ενέργειας του εκπεμπόμενου σήματος πρέπει να

βρίσκεται μέσα στο κανάλι. Διαφορετικά κανάλια είναι διαθέσιμα για χρήση σε διάφορες χώρες, όπως φαίνεται στον Πίνακα 2.4.

Επιπλέον έχει προδιαγραφεί αυστηρά τόσο ο χρόνος εκπομπής σε ένα κανάλι (dwell time), που ισούται με 0,4 seconds περίπου, όσο και οι λεπτομέρειες της μεταπήδησης από κανάλι σε κανάλι ανάλογα με το hopping pattern. Έχουν οριστεί συγκεκριμένες αριθμητικές ακολουθίες των διαθέσιμων καναλιών ως hopping patterns και έχουν διαιρεθεί σε μη επικαλυπτόμενες ομάδες. Οποιαδήποτε δύο μέλη της ίδιας ομάδας είναι ορθογώνια μεταξύ τους. Όπως και στα διαθέσιμα κανάλια, έτσι και στα hopping patterns κάθε χώρα έχει διαφορετικούς περιορισμούς. Τα παραπάνω φαίνονται συγκεντρωμένα στον Πίνακα 2.3.

Στις ΗΠΑ και στην Ευρώπη οι αρμόδιοι οργανισμοί έχουν θεσπίσει διαφορετικούς περιορισμούς για τα συστήματα Frequency Hopping. Για παράδειγμα, στις ΗΠΑ η FCC (Federal Communication Commision) απαιτεί τουλάχιστον 75 διαφορετικά κανάλια (hopping channels) ενώ η Ευρωπαϊκή ETSI (European Telecommunication Standard Institute) μόλις 20, περιορίζοντας όμως περισσότερο την ακτινοβολούμενη ισχύ. Τελικά, για να ικανοποιεί ένα προϊόν τις προδιαγραφές και της FCC και της ETSI πρέπει να ικανοποιεί τις αυστηρότερες από αυτές σε κάθε τομέα (στο παραπάνω παράδειγμα δηλαδή ένα σύστημα πρέπει να έχει τουλάχιστον 75 hopping channels και να ικανοποιεί και τους αυστηρούς περιορισμούς ισχύος της ETSI).

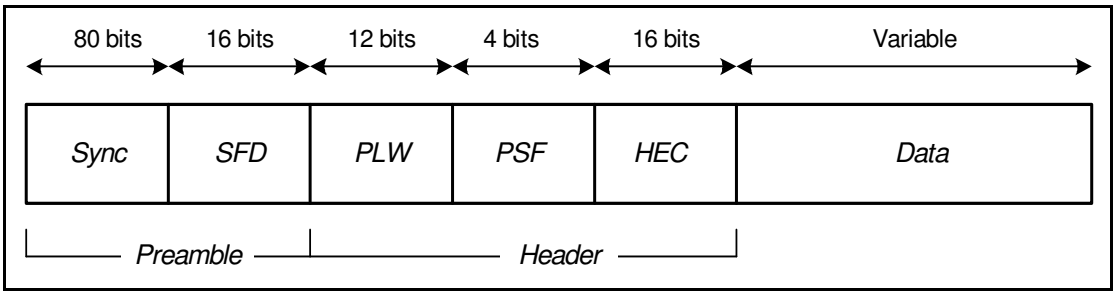
Περιοχή / Υπεύθυνη Αρχή	**Επιτρεπόμενα Κανάλια**	**Αριθμός hopping patterns / ομάδα**
ΗΠΑ / FCC – Καναδάς / IC	2 έως 79 (2,402 – 2,479 GHz)	26
Ευρώπη (εκτός Γαλλίας & Ισπανίας) / ETSI	2 έως 79 (2,402 – 2,479 GHz)	26
Γαλλία	48 έως 82 (2,448 – 2,482 GHz)	27
Ισπανία	47 έως 73 (2,447 – 2,473 GHz)	35
Ιαπωνία / MKK	73 έως 95 (2,473 – 2,495 GHz)	13

Πίνακας 2.3: Διαθέσιμα κανάλια φυσικού στρώματος 802.11 FHSS σε διάφορες περιοχές

Όσο αναφορά την επίδοση του Frequency Hopping φυσικού στρώματος παρουσία θορύβου και παρεμβολών στενής ζώνης, αυτή είναι αρκετά καλή και μειώνεται γραμμικά όσο αυξάνονται οι παρεμβολές. Μεγάλες παρεμβολές σε ένα από τα χρησιμοποιούμενα κανάλια δεν προκαλεί σπουδαία χειροτέρευση της επίδοσης. Όσο όμως ο αριθμός των καναλιών που επηρεάζονται από τις παρεμβολές αυξάνει, η χειροτέρευση της επίδοσης αρχίζει να γίνεται πιο έντονη.

2.2.2.3 FHSS – Υπόστρωμα PLCP

Η μορφή του PLCP πλαισίου του FHSS φυσικού στρώματος φαίνεται στο Σχήμα 2.8.



Σχήμα 2.8: Πλαίσιο PLCP υποστρώματος του φυσικού στρώματος 802.11 FHSS

Στη συνέχεια περιγράφονται συνοπτικά τα διάφορα τμήματα του πλαισίου.

Preamble

Χρησιμεύει για τον συγχρονισμό πομπού και δέκτη και για τον ορισμό της αρχής του πλαισίου. Περιέχει τα πεδία Sync και SFD.

Sync

Το πεδίο αυτό περιέχει μία ακολουθία από εναλλασσόμενα «0» και «1» και χρησιμεύει για την επίτευξη συγχρονισμού μεταξύ πομπού και δέκτη. Επιπλέον χρησιμοποιείται και για άλλους σκοπούς, όπως για παράδειγμα μέτρηση συχνότητας του λαμβανόμενου σήματος ή ανίχνευση δυνατότερου σήματος σε συστήματα που χρησιμοποιούν περισσότερες της μίας κεραίες.

Start Frame Delimiter (SFD)

Το πεδίο αυτό σηματοδοτεί το τέλος του preamble και την αρχή του υπόλοιπου πλαισίου. Περιέχει την ακολουθία «0000 1100 1011 1101».

Header

Η επικεφαλίδα του πλαισίου, περιέχει τα πεδία PLW, PSF και HEC που περιγράφονται στη συνέχεια.

PSDU (Protocol Service Data Unit) Length Word (PLW)

Το μήκος του MAC πλαισίου που κουβαλάει το PLCP πλαίσιο. Μπορεί να είναι μέχρι 4095 bytes.

PLCL Signaling (PSF)

Το πρώτο bit είναι δεσμευμένο για μελλοντική χρήση και τίθεται πάντα «0». Στα υπόλοιπα τρία κωδικοποιείται ο χρησιμοποιούμενος ρυθμός μετάδοσης. Παρόλο που το πρότυπο ορίζει ρυθμούς μετάδοσης από 1 Mbps μέχρι και 4,5 Mbps, με διαφορά διαδοχικών ρυθμών 500 kbps, έχει οριστεί σχήμα διαμόρφωσης μόνο για τους ρυθμούς 1 και 2 Mbps.

Header Error Check (HEC)

Το πεδίο αυτό περιέχει έναν 16-μπιτο CRC που προστατεύει την επικεφαλίδα (header) του πλαισίου.

Data

Το τμήμα αυτό περιέχει το MAC πλαίσιο. Πριν την τοποθέτησή του περνάει από μια διαδικασία ανακατώματος προκειμένου να μοιάζει με λευκό θόρυβο (whitening). Σε αντίθεση με το Direct Sequence φυσικό στρώμα, μόνο το τμήμα Data υπόκειται σε αυτήν την διαδικασία και όχι ολόκληρο το PLCP πλαίσιο.

2.2.2.4 FHSS – Υπόστρωμα PMD

Όπως αναφέρθηκε και παραπάνω το πρότυπο υποστηρίζει κανονικά δύο ρυθμούς μετάδοσης, 1 και 2 Mbps. Για το ρυθμό μετάδοσης 1 Mbps χρησιμοποιείται διαμόρφωση 2-GFSK (Gaussian Frequency Shift Keying), όπου κάθε σύμβολο (symbol) μεταφέρει 1 bit πληροφορίας. Η ισχύς εκπομπής που έχει οριστεί από το πρότυπο είναι μεταξύ 10 και 100 mWatt. Για μετάδοση με ρυθμό 2 Mbps χρησιμοποιείται διαμόρφωση 4-GFSK, δηλαδή κάθε σύμβολο μεταφέρει 2 bits πληροφορίας. Η επικεφαλίδα του PLCP πλαισίου μεταδίδεται με χρήση 2-GFSK σε ρυθμό 1 Mbps. Τέλος, υπάρχει πρόβλεψη για υποβάθμιση του ρυθμού μετάδοσης στο 1 Mbps αν η ποιότητα σήματος είναι πολύ χαμηλή.

Στον Πίνακα 2.4 φαίνονται κάποιες επιπλέον παράμετροι του φυσικού στρώματος αυτού.

Παράμετρος	Τιμή
Μέγιστο μήκος πλαισίου MAC	4095 bytes
Slot time	50 μsec
SIFS time	28 μsec
Contention window size	15 έως 1023 slots
Preamble duration	96 μsec
PLCP header duration	32 μsec

Πίνακας 2.4: Παράμετροι του φυσικού στρώματος802.11 FHSS

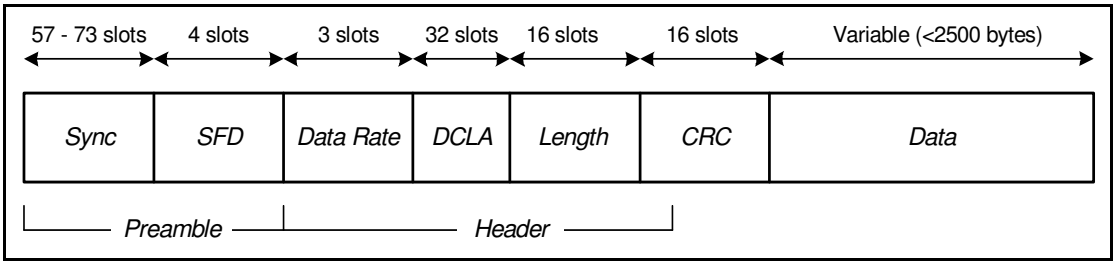
2.2.3 Φυσικό στρώμα Υπέρυθρων Ακτινών

Το φυσικό στρώμα υπέρυθρων ακτινών (Infrared – IR) δεν χρησιμοποιείται ιδιαίτερα και γι' αυτό το λόγο θα παρουσιαστεί συνοπτικά. Η λειτουργία του βασίζεται στην εκπομπή παλμών διάρκειας 250 nsec, που παράγονται από τα LEDs (Light Emitting Diode) του πομπού. Η ακτίνα λειτουργίας του μπορεί να φτάσει περίπου τα 20 μέτρα, σε ελεύθερο φυσικά οπτικό πεδίο. Άλλη περίπτωση είναι η ανάκλαση των υπέρυθρων ακτινών από κατάλληλη επιφάνεια, για παράδειγμα τοίχος λευκού χρώματος, ώστε να επιτευχθεί κάλυψη μιας συγκεκριμένης περιοχής.

Το PMD υπόστρωμα χρησιμοποιεί δύο σχήματα διαμόρφωσης για να πετύχει τους διαθέσιμους ρυθμούς μετάδοσης των 1 και 2 Mbps. Η διαμόρφωση 16-PPM (Pulse Position Modulation) χρησιμοποιείται για το ρυθμό 1 Mbps. Κάθε 4 bits πληροφορίας αντιστοιχίζονται σε μία ακολουθία 16 bits (ή slots). Κάθε bit διαρκεί 250 nsec και κάθε ακολουθία 16 bits έχει μόνο από αυτά ίσο με «1» και όλα τα υπόλοιπα μηδενικά. Έτσι κάθε

τετράδα από bits πληροφορίας κωδικοποιείται από τη θέση του «1» στην 16-μπιτη ακολουθία. Για το ρυθμό των 2 Mbps χρησιμοποιείται η 4-PPM, όπου με την ίδια λογική κάθε ζευγάρι από bits πληροφορίας κωδικοποιούνται σε μία ακολουθία 4 bits. Κατά τη μετάδοση τα bits «1» από την παρουσία ισχύος (οπτικού παλμού) ενώ τα bits «0» από την απουσία. Η ισχύς μετάδοσης έχει όριο τα 2 Watt με μία μέση τιμή ίση με 125 ή 250 mWatt, ενώ το μήκος κύματος του φωτός που χρησιμοποιείται έχει οριστεί στα 850 με 950 nm.

Το PLCP πλαίσιο φαίνεται στο Σχήμα 2.9.



Σχήμα 2.9: Πλαίσιο PLCP υποστρώματος του φυσικού στρώματος 802.11 Infrared

Στο παραπάνω πλαίσιο το μήκος μετριέται σε σχισμές (slots) των 250 ns, όσο δηλαδή διαρκεί ο βασικός παλμός. Τα διάφορα τμήματά του περιγράφονται στη συνέχεια.

Preamble

Όπως και στα προηγούμενα φυσικά στρώματα, το τμήμα αυτό χρησιμεύει για συγχρονισμό και οριοθέτηση της αρχής του πλαισίου. Περιέχει τα πεδία Sync και SFD, μόνο που το μήκος του είναι μικρότερο από αυτό των άλλων φυσικών στρωμάτων επειδή η μέθοδος αποδιαμόρφωσης είναι ασύμφωνη (non-coherent) και δεν απαιτεί ανάκτηση φέροντος σήματος και ακριβή συγχρονισμό.

Header

Η επικεφαλίδα. Στο πεδίο Data Rate κωδικοποιείται ο ρυθμός μετάδοσης. Τα πεδία Length και CRC είναι τα ίδια με αυτά του φυσικού στρώματος Direct Sequence. Το πεδίο DCLA (DC Level Adjustment) περιέχει μία ακολουθία 16 σχισμών, επιτρέποντας στον δέκτη να θέσει το κατώφλι ισχύος για την λήψη απόφασης της τιμής του κάθε bit.

Data

Περιέχει το MAC πλαίσιο προς μετάδοση. Το μήκος του περιορίζεται στα 2500 bytes.

2.3 802.11 – Υπόστρωμα MAC

Το υπόστρωμα MAC του 802.11 είναι ίσως το πιο σημαντικό κομμάτι της προτυποποίησης. Υποστηρίζει όλα τα φυσικά στρώματα και προσφέρει υπηρεσίες αξιόπιστης μεταφοράς δεδομένων και πρόσβασης στο μέσο στα ανώτερα στρώματα. Οι όποιες διαφοροποιήσεις του από το αντίστοιχο MAC ενσύρματων δικτύων οφείλονται στις ιδιαιτερότητες του ασύρματου μέσου μετάδοσης που χρησιμοποιείται στο φυσικό επίπεδο.

Σαν μηχανισμός πρόσβασης στο μέσο έχει επιλεχτεί ο CSMA (Carrier Sense Multiple Access). Για να αποφευχθούν όσο το δυνατόν περισσότερο οι συγκρούσεις αντί για το μηχανισμό ανίχνευσης συγκρούσεων CD (Collision Detection) που χρησιμοποιείται στο 802.3 επιλέχτηκε ο μηχανισμός αποφυγής συγκρούσεων CA (Collision Avoidance). Αιτία για την επιλογή αυτή είναι η αδυναμία του δέκτη να αντιλαμβάνεται την κατάσταση του ασύρματου μέσου την χρονική στιγμή που μεταδίδει κάποια πληροφορία. Επομένως, το φαινόμενο της σύγκρουσης (δυο ή περισσότεροι σταθμοί μεταδίδουν την ίδια ακριβώς χρονική στιγμή) γίνεται αντιληπτό από τους σταθμούς εργασίας μόνο εκ του αποτελέσματος που είναι φυσικά η μη παράδοση των πακέτων της πληροφορίας.

Η αξιόπιστη μεταφορά δεδομένων μεταξύ των διαφόρων κόμβων δυσχεραίνεται ακόμα περισσότερο εξαιτίας του ασύρματου φυσικού μέσου. Προβλήματα όπως η κακή ποιότητα της ασύρματης ζεύξης λόγω θορύβου ή παρεμβολών, η πιθανότητα κάποιος κόμβος να βγει προσωρινά εκτός της περιοχής κάλυψης του δικτύου και η ύπαρξη κρυμμένων κόμβων (hidden nodes) δεν υπάρχουν σε ενσύρματα δίκτυα. Για να αντιμετωπιστούν τα παραπάνω το 802.11 MAC προσφέρει τους κατάλληλους μηχανισμούς, όπως η θετική επιβεβαίωση (positive acknowledgment) κάθε πλαισίου και την ανταλλαγή πλαισίων RTS (Ready To Send) και CTS (Clear To Send) πριν την μετάδοση κάποιου πλαισίου. Περισσότερες λεπτομέρειες για τους παραπάνω μηχανισμούς θα αναφερθούν στη συνέχεια του κεφαλαίου.

2.3.1 Πρόσβαση στο μέσο

Όπως αναφέρθηκε ήδη ο μηχανισμός πρόσβασης στο μέσο που χρησιμοποιείται από το 802.11 MAC είναι ο CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance). Έχουν προβλεφθεί δύο τρόποι λειτουργίας, ένας αποκεντρωμένος μέσω του αλγορίθμου DCF (Distributed Coordination Function) και ένας με κεντρικό έλεγχο μέσω του αλγορίθμου PCF (Point Coordination Function) που αποτελεί προέκταση του DCF. Ο αλγόριθμος PCF εκτελείται μόνο σε AP, οπότε μπορεί να χρησιμοποιηθεί μόνο σε infrastructure δίκτυα.

2.3.1.1 Χρόνοι Αναμονής (Interframe Spacing)

Οι παραπάνω αλγόριθμοι χρησιμοποιούν διάφορες χρονικές περιόδους για τον έλεγχο της πρόσβασης στο μέσο. Γενικά, κάθε σταθμός που θέλει να μεταδώσει κάποιο πλαίσιο πρέπει πρώτα να περιμένει ένα ορισμένο χρονικό διάστημα (interframe space) και αν δεν ανιχνεύσει άλλη μετάδοση σε αυτό τότε να προχωρήσει στο επόμενο βήμα της διαδικασίας απόκτησης πρόσβασης στο μέσο, που διαφέρει ανάλογα με τον αλγόριθμο που χρησιμοποιείται (DCF ή PCF). Το χρονικό διάστημα αυτό ποικίλει ανάλογα με τον τύπο του πλαισίου που πρόκειται να μεταδοθεί. Οι ορισμένοι από το πρότυπο χρόνοι αναμονής είναι οι εξής:

- Short Interframe Space (SIFS): Ο μικρότερος χρόνος αναμονής Χρησιμοποιείται για μεταδόσεις μέγιστης προτεραιότητας, όπως είναι τα πλαίσια RTS/CTS και οι επιβεβαιώσεις.

- PCF Interframe Space (PIFS): Μεγαλύτερο χρονικό διάστημα από το SIFS, χρησιμοποιείται σε συνδυασμό με τον αλγόριθμο PCF. Οι σταθμοί περιμένουν PIFS χρόνο πριν μεταδώσουν κατά την περίοδο που την πρόσβαση στο μέσο ελέγχει ο κεντρικός αυτός αλγόριθμος (περίοδος χωρίς ανταγωνισμό - contention – free period), αποκτώντας προτεραιότητα έναντι αυτών που προσπαθούν να μεταδώσουν με χρήση του DCF.

- DCF Interframe Space (DIFS): Ο μικρότερος χρόνος αναμονής για λειτουργία με βάση τον αλγόριθμο DCF (περίοδος με ανταγωνισμό - contention period). Μεγαλύτερος σε διάρκεια από τους δύο προηγούμενους χρόνους.

- Extended Inter-Frame Space (EIFS): Ο μέγιστος χρόνος αναμονής, δεν έχει κάποια συγκεκριμένη τιμή και χρησιμοποιείται όταν συμβεί κάποιο σφάλμα κατά την μετάδοση του πλαισίου.

Από τα παραπάνω είναι προφανές ότι κάθε σταθμός πρέπει να έχει τη δυνατότητα να ανιχνεύει αν υπάρχει κάποια άλλη μετάδοση σε εξέλιξη πριν αρχίσει να μεταδίδει αυτός. Ο μηχανισμός ανίχνευσης φέροντος που χρησιμοποιείται παρουσιάζει ιδιαίτερο ενδιαφέρον και παρουσιάζεται αναλυτικά στην επόμενη παράγραφο.

2.3.1.2 Μηχανισμός Ανίχνευσης Φέροντος

Στα ενσύρματα δίκτυα ο τρόπος λειτουργίας του μηχανισμού ανίχνευσης φέροντος είναι σχετικά απλός. Κάθε σταθμός παρακολουθεί το μέσο μετάδοσης και αν εντοπίσει σήμα συγκεκριμένη ισχύος καταλαβαίνει ότι κάποια μετάδοση πλαισίου βρίσκεται σε εξέλιξη. Όταν όμως το μέσο μετάδοσης γίνει ασύρματο τότε αυτός ο μηχανισμός δεν είναι επαρκής. Εξαιτίας του μεγάλου αριθμού στα σχήματα διαμόρφωσης που χρησιμοποιούνται, των διαφόρων περιπτώσεων όσο αφορά τις αποστάσεις μεταξύ των σταθμών αλλά και με το πρόβλημα των hidden nodes είναι πολύ δύσκολο να δημιουργηθεί αξιόπιστος μηχανισμός ανίχνευσης φέροντος που να λειτουργεί αποκλειστικά στο φυσικό επίπεδο.

Γι' αυτό το λόγο το πρότυπο 802.11 προβλέπει και έναν δεύτερο μηχανισμό ανίχνευσης φέροντος που λειτουργεί όμως στο υπόστρωμα MAC. Ο εικονικός μηχανισμός ανίχνευσης φέροντος (virtual carrier sensing) χρησιμοποιεί έναν μετρητή χρόνου που ονομάζεται NAV (Network Allocation Vector). Αυτός ο μετρητής συμπεριλαμβάνεται στα περισσότερα πλαίσια που ανταλλάσσονται. Κάθε σταθμός θέτει το πεδίο αυτό ίσο με το χρόνο που θέλει να κρατήσει δεσμευμένο το μέσο μετάδοσης, όταν αποκτήσει βέβαια δικαίωμα να το κάνει. Οι υπόλοιποι σταθμοί βλέποντας ότι το πεδίο NAV είναι μη μηδενικό καταλαβαίνουν ότι το μέσο είναι δεσμευμένο και ξεκινάνε έναν αντίστροφο τοπικό μετρητή με αρχική τιμή ίση με NAV, αν η τιμή του NAV είναι μεγαλύτερη από την υπάρχουσα τιμή του τοπικού μετρητή αυτού. Με χρήση του NAV οι σταθμοί μπορούν να επιτελέσουν συγκεκριμένες ενέργειες χωρίς να χάσουν τον έλεγχο του μέσου μετάδοσης. Ένα τέτοιο παράδειγμα είναι η αποστολή ενός πλαισίου με χρήση του μηχανισμού RTS/CTS. Για να ολοκληρωθεί αυτή η ενέργεια οι δύο σταθμοί πρέπει να ανταλλάξουν συνολικά 4 πλαίσια. Παίρνοντας τον έλεγχο με χρήση του NAV μπορούν να το κάνουν χωρίς να διακοπούν από άλλη μετάδοση.

2.3.1.3 Πρόσβαση στο μέσο με χρήση του αλγορίθμου DCF

Ο αλγόριθμος DCF, όπως έχει ήδη αναφερθεί, είναι αποκεντρωμένος και έτσι μπορεί να χρησιμοποιηθεί σε κάθε είδους ασύρματο δίκτυο. Ο αλγόριθμος αυτός περιλαμβάνει κάποια βασικά βήματα που ακολουθεί κάθε σταθμός πριν εκπέμψει κάποιο πλαίσιο. Τα βήματα αυτά είναι τα εξής:

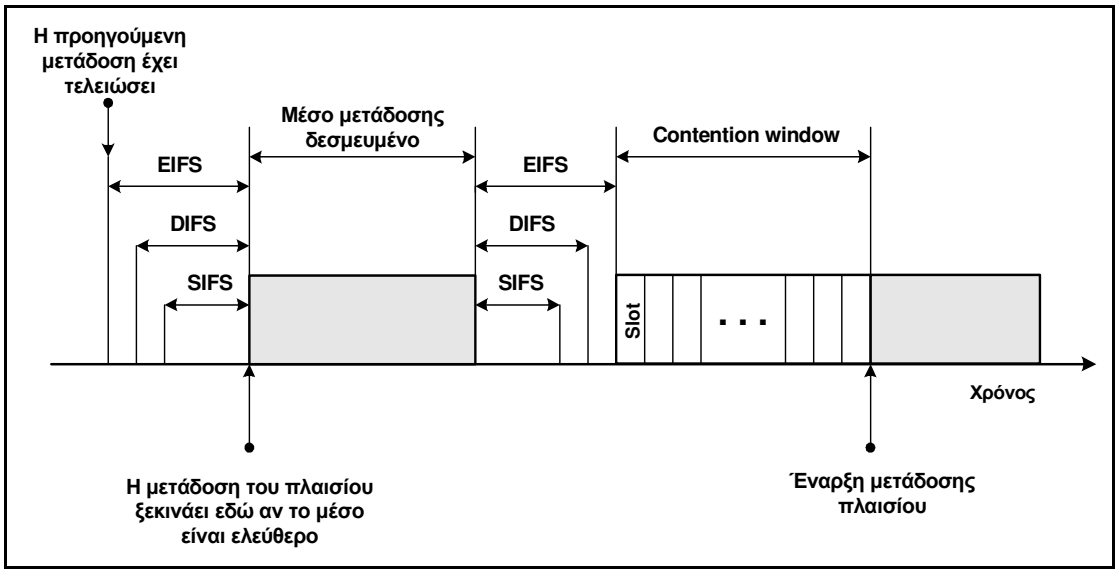
- Κάθε σταθμός, πριν επιχειρήσει να εκπέμψει, ελέγχει το μέσο μετάδοσης για να δει αν είναι διαθέσιμο. Ο έλεγχος γίνεται και σε φυσικό επίπεδο και μέσω εικονικής ανίχνευσης φέροντος.
- Αν το μέσο μετάδοσης είναι δεσμευμένο τότε ο σταθμός συνεχίζει να ελέγχει το ασύρματο μέσο περιοδικά περιμένοντας να ελευθερωθεί. Αν το μέσο είναι διαθέσιμο ο σταθμός περιμένει ένα χρονικό διάστημα που εξαρτάται από το είδος του πλαισίου που θέλει να μεταδώσει (IFS, Inter-Frame Space) και ελέγχει ξανά το μέσο. Ο χρόνος αναμονής που χρησιμοποιείται συνήθως είναι ο DIFS. Στην περίπτωση που ο σταθμός θέλει να στείλει πλαίσιο CTS, πλαίσιο θετικής επιβεβαίωσης (ACK, Acknowledge), ή τμήμα (fragment) μεγαλύτερου πλαισίου τότε ο χρόνος αναμονής είναι ο SIFS. Τέλος, στην περίπτωση που η μετάδοση του προηγούμενου πλαισίου περιείχε λάθη τότε ο χρόνος αναμονής είναι ο EIFS.

- Αν πάλι το μέσο είναι ελεύθερο τότε ο σταθμός μεταδίδει το πλαίσιο που θέλει. Αν το μέσο είναι δεσμευμένο ο σταθμός περιμένει μέχρι το μέσο να μείνει ελεύθερο για IFS. Τότε ξεκινάει τη διαδικασία της δυαδικής εκθετικής υποχώρησης (binary exponential backoff) για να καθορίσει πόσο θα είναι το επιπλέον χρονικό διάστημα αναμονής. Αυτό γίνεται επιλέγοντας τυχαία μια σχισμή του παραθύρου ανταγωνισμού (contention window). Αφού περάσει και

αυτό το τελευταίο χρονικό διάστημα, ο σταθμός μεταδίδει το πλαίσιο που θέλει.

- Αν η μετάδοση είναι αποτυχημένη θεωρείται ότι έχει συμβεί σύγκρουση (collision). Τότε ο σταθμός επιλέγει πάλι τυχαία μια σχισμή του contention window, το οποίο όμως είναι μεγαλύτερο αυτή τη φορά, και επιχειρεί ξανά να μεταδώσει. Αυτή η διαδικασία επαναλαμβάνεται μέχρι να υπάρξει επιτυχής μετάδοση του πλαισίου ή να απορριφθεί το πλαίσιο. Περισσότερες λεπτομέρειες για τη διαδικασία αυτή αναφέρονται στις Παραγράφους 2.3.1.3.1 και 2.3.1.3.2.

Τα παραπάνω βήματα φαίνονται καλύτερα στο Σχήμα 2.10.



Σχήμα 2.10: Διαδικασία πρόσβασης στο μέσο με χρήση του αλγορίθμου DCF

Αυτός είναι ο βασικός μηχανισμός για να μπορέσει ένας σταθμός να αποκτήσει τον έλεγχο του μέσου. Υπάρχουν και άλλοι κανόνες που συμπληρώνουν τα παραπάνω και εξαρτώνται από την συγκεκριμένη κατάσταση ή από την κατάληξη της προηγούμενης μετάδοσης. Μερικοί τέτοιοι κανόνες παρουσιάζονται στη συνέχεια.

- Κάθε μετάδοση πλαισίου θεωρείται επιτυχημένη μόνο αν ληφθεί σωστά και το αντίστοιχο πλαίσιο ACK. Όλα τα πλαίσια μονοεκπομπής (unicast) πρέπει να επιβεβαιώνονται από τον παραλήπτη. Αντίθετα, πλαίσια τύπου πολυεκπομπής (multicast) και ευρυεκπομπής (broadcast) δεν απαιτούν επιβεβαίωση. Είναι ευθύνη του αποστολέα να ξαναστείλει το πλαίσιο αν δεν ληφθεί η ανάλογη επιβεβαίωση. Κάθε αποτυχία αποστολής που οφείλεται είτε σε αδυναμία ελέγχου του μέσου είτε σε μη λήψη ACK αυξάνει έναν μετρητή (retry counter) που χρησιμεύει για τον προσδιορισμό του χρόνου μέχρι την επόμενη προσπάθεια αποστολής του πλαισίου.

- Κάθε σταθμός που συμμετέχει στην ανταλλαγή πολλαπλών πλαισίων μπορεί να ανανεώνει το NAV μετά από κάθε λήψη πλαισίου. Έτσι ο έλεγχος του μέσου διατηρείται μέχρι να ολοκληρωθεί η ανταλλαγή. Η διατήρηση του ελέγχου μπορεί να εξασφαλιστεί επιπλέον με τη χρήση του SIFS στις περιπτώσεις που έχουν ήδη αναφερθεί.

- Υπάρχουν συγκεκριμένα κατώφλια μεγέθους για τα πλαίσια. Κάθε πλαίσιο μεγαλύτερο από το κατώφλι RTS πρέπει να σταλεί χρησιμοποιώντας το μηχανισμό RTS/CTS (θα παρουσιαστεί στη συνέχεια). Κάθε πλαίσιο μεγαλύτερο από το κατώφλι κατακερματισμού (fragmentation threshold) διασπάται σε μικρότερα πλαίσια πριν σταλεί.

2.3.1.3.1 Αντιμετώπιση αποτυχημένης προσπάθειας μετάδοσης

Όπως έχει ήδη αναφερθεί, ο εντοπισμός και η διόρθωση κάποιου λάθους κατά τη μετάδοση είναι ευθύνη του αποστολέα. Σε περίπτωση που η αποστολή ενός πλαισίου δεν ολοκληρωθεί κανονικά ο αποστολέας πρέπει να το ξαναστείλει. Για τον έλεγχο της διαδικασίας αυτής κάθε πλαίσιο έχει έναν μετρητή (retry counter) συσχετισμένο με αυτό. Κάθε φορά που το πλαίσιο αυτό επανεκπέμπεται ο retry counter που του αντιστοιχεί αυξάνεται κατά 1. Αν ο μετρητής ξεπεράσει κάποιο προκαθορισμένο όριο, το πλαίσιο απορρίπτεται και η απώλειά του αναφέρεται στα υψηλότερα στρώματα.

Κάθε σταθμός διακρίνει τα πλαίσια σε short και long. Ως short χαρακτηρίζονται τα πλαίσια που έχουν μήκος μικρότερο από το RTS threshold και ως long τα υπόλοιπα. Ο σταθμός διατηρεί και δύο αντίστοιχους μετρητές, τους short retry count και long retry count. Κάθε φορά που η μετάδοση ενός πλαισίου αποτυγχάνει ο αντίστοιχος μετρητής αυξάνεται. Οι μετρητές αυτοί μηδενίζονται σε συγκεκριμένες περιπτώσεις. Για τον short retry count αυτές είναι:

- Λήψη CTS πλαισίου σε απάντηση ενός RTS.
- Λήψη πλαισίου ACK μετά από μη κατακερματισμένη μετάδοση πλαισίου.
- Λήψη broadcast ή multicast πλαισίου.

Αντίστοιχα, ο long retry count μηδενίζεται στις ακόλουθες περιπτώσεις:

- Λήψη πλαισίου ACK για πλαίσιο μεγαλύτερο του RTS threshold.
- Λήψη broadcast ή multicast πλαισίου.

Σε περίπτωση κατακερματισμού ενός πλαισίου όλα τα fragments έχουν έναν μετρητή διάρκειας ζωής (lifetime counter). Αυτός ξεκινάει όταν μεταδοθεί το πρώτο fragment. Αν μέχρι να μηδενιστεί δεν έχει μεταδοθεί ολόκληρο το πλαίσιο, αυτό απορρίπτεται και δεν γίνεται προσπάθεια μετάδοσης των υπόλοιπων fragments του.

2.3.1.3.2 Παράθυρο Ανταγωνισμού (Contention window)

Ήδη έχει αναφερθεί η έννοια του παραθύρου ανταγωνισμού (contention window) και που χρησιμεύει. Το contention window χωρίζεται σε σχισμές (slots) που η διάρκειά τους είναι εξαρτώμενη από το φυσικό στρώμα. Κάθε σταθμός διαλέγει μια σχισμή και περιμένει τη σειρά του πριν επιχειρήσει να αποκτήσει πρόσβαση στο μέσο μετάδοσης. Η επιλογή γίνεται

τυχαία, με χρήση μιας διαδικασίας που ονομάζεται δυαδική εκθετική υποχώρηση. Αν περισσότεροι του ενός σταθμοί διεκδικούν τον έλεγχο του μέσου, νικητής θα αναδειχθεί αυτός που θα επιλέξει την πρώτη σχισμή.

Κάθε σταθμός επιλέγει τη σχισμή του contention window μέσα από ένα εύρος τιμών που αυξάνεται όσο αποτυγχάνει η επιθυμητή μετάδοση πλαισίου. Υπενθυμίζεται ότι η μετάδοση θεωρείται αποτυχημένη αν δεν ληφθεί έγκαιρα επιβεβαίωση ή αν ο σταθμός δεν καταφέρει καν να πάρει τον έλεγχο του μέσου για να μεταδώσει το πλαίσιο. Το εύρος τιμών από το οποίο καλείται να επιλέξει τυχαία ο κάθε σταθμός είναι πάντα αριθμός κατά ένα μικρότερος από κάποια δύναμη του 2. Κάθε φορά που η μετάδοση αποτυγχάνει το εύρος υπολογίζεται ξανά με βάση την αμέσως επόμενη δύναμη του 2. Αυτό γίνεται μέχρι να φτάσει το εύρος μία μέγιστη τιμή, οπότε δεν μεγαλώνει άλλο. Το εύρος αυτό επανέρχεται στην ελάχιστη τιμή του μετά από επιτυχημένη μετάδοση ή από απόρριψη του προς μετάδοση πλαισίου. Κάθε φυσικό στρώμα χρησιμοποιεί δικές του παραμέτρους για την παραπάνω διαδικασία. Με αυτόν τον τρόπο εξασφαλίζεται η σταθερότητα της λειτουργίας του δικτύου, ακόμη και κάτω από καταστάσεις έντονης κίνησης.

2.3.1.4 Πρόσβαση στο μέσο με χρήση του αλγορίθμου PCF

Ο αλγόριθμος PCF είναι η εναλλακτική λύση στο πρόβλημα του ελέγχου της πρόσβασης στο μέσο. Η λειτουργία του μοιάζει αρκετά με σχήματα ελέγχου πρόσβασης με σκυτάλη (token based). Ο συγκεκριμένος αλγόριθμος δεν χρησιμοποιείται ιδιαίτερα στα προϊόντα που κυκλοφορούν στην αγορά, ενώ οι κατασκευαστές δεν είναι υποχρεωμένοι να τον υποστηρίξουν, αφού αποτελεί προαιρετικό μέρος του προτύπου 802.11. Επιπλέον, εφόσον απαιτεί κεντρικό έλεγχο από κάποιο AP, μπορεί να χρησιμοποιηθεί μόνο σε infrastructure δίκτυα.

Σκοπός του PCF είναι να προσφέρει πρόσβαση στο μέσο χωρίς ανταγωνισμό μεταξύ των σταθμών (contention - free medium access). Υλοποιείται χρησιμοποιώντας την υποδομή του αλγορίθμου DCF και προσθέτοντας την επιπλέον λειτουργικότητα. Η χρήση του συνεπάγεται τη δημιουργία χρονικών περιόδων χωρίς ανταγωνισμό (contention - free periods), ενώ κατά τον υπόλοιπο χρόνο η πρόσβαση ελέγχεται κανονικά από τον DCF (contention periods). Υπάρχει δυνατότητα καθορισμού της σχέσης των δύο παραπάνω χρονικών περιόδων ανάλογα με τη χρήση του δικτύου. Αυτές οι περίοδοι επαναλαμβάνονται διαδοχικά, ενώ η διάρκειά τους κάθε φορά ονομάζεται contention - free repetition interval.

Κατά τη διάρκεια του contention - free period η διαδικασία πρόσβασης στο μέσο για τους σταθμούς ελέγχεται από το AP. Στην αρχή της περιόδου αυτής το AP στέλνει ένα πλαίσιο Beacon το οποίο περιέχει τη μέγιστη διάρκεια της contention - free period. Οι

σταθμοί θέτουν το NAV σε αυτήν την τιμή αποτρέποντας την πρόσβαση μέσω του DCF γι' αυτήν την περίοδο.

Όταν το AP πάρει τον έλεγχο του μέσου δίνει την άδεια σε κάθε σταθμό διαδοχικά να μεταδώσει στέλνοντάς του ένα polling πλαίσιο (CF – Poll). Τα polling πλαίσια πρέπει να επιβεβαιωθούν από τους σταθμούς. Αν κάποιος σταθμός δεν στείλει ACK αφού λάβει το polling πλαίσιο το AP προχωράει στον επόμενο σταθμό. Όλοι οι σταθμοί κατά τη διαδικασία του association με το AP μπαίνουν σε μία λίστα (polling list) ώστε το AP να τους δίνει το δικαίωμα μετάδοσης κατά την contention - free period. Σημειώνεται ότι κάθε πλαίσιο polling δίνει στο σταθμό που το έλαβε δικαίωμα μετάδοσης ενός μόνο πλαισίου.

Για να διασφαλιστεί περισσότερο ότι ο έλεγχος του μέσου θα μείνει στο AP κατά την contention - free period όλοι οι χρόνοι αναμονής που χρησιμοποιούνται είναι SIFS ή PIFS. Ο χρόνος αναμονής από το AP για να επιβεβαιωθεί το polling πλαίσιο που έστειλε είναι ίσος με τον PIFS ενώ όλοι οι υπόλοιποι χρόνοι αναμονής είναι ίσοι με SIFS.

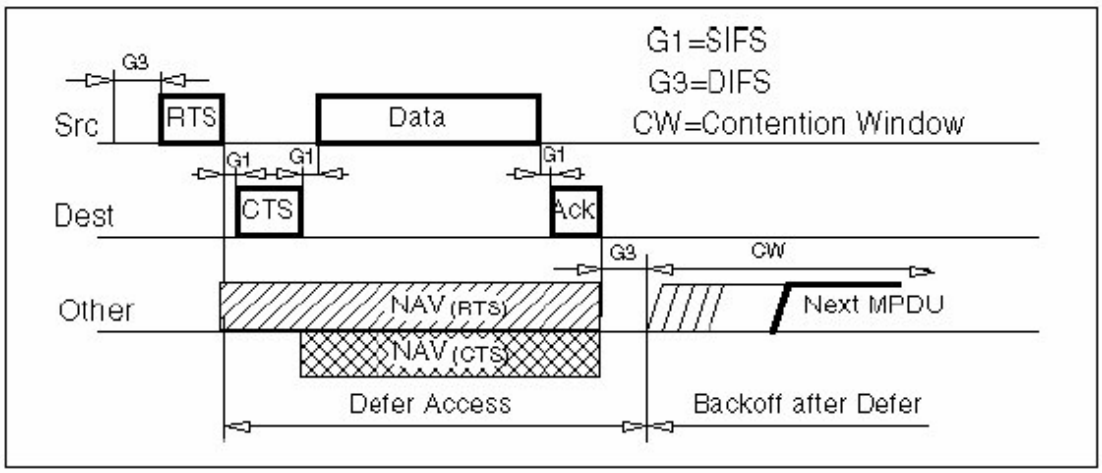
Η διάρκεια της contention - free period πρέπει να είναι τουλάχιστον ίση με το χρόνο που απαιτείται να μεταδοθεί και να επιβεβαιωθεί ένα πλαίσιο μεγίστου μεγέθους. Σε περίπτωση που η contention period δεν τελειώσει όταν πρέπει να αρχίσει η contention - free period, η δεύτερη έχει μειωμένη διάρκεια. Το AP που τρέχει τον PCF μπορεί να διακόψει νωρίτερα την contention - free period για οποιοδήποτε λόγο. Τέλος, για να εκμεταλλεύονται οι σταθμοί όσο το δυνατόν περισσότερο την contention - free period είναι σύνηθες να συνδυάζουν σε ένα πλαίσιο επιβεβαιώσεις, polling και μεταφορά δεδομένων, οπότε προκύπτουν σύνθετα πλαίσια με πολλές λειτουργίες. Για παράδειγμα ένας σταθμός μπορεί να συνδυάσει τη μεταφορά δεδομένων με την επιβεβαίωση του πλαισίου polling σε ένα κοινό πλαίσιο και να το στείλει. Το AP που θα το λάβει μπορεί να στείλει σε κοινό πλαίσιο στην επιβεβαίωση λήψης των δεδομένων στον αποστολέα και τα δεδομένα στον παραλήπτη.

2.3.1.5 Λειτουργία RTS/CTS

Για να διασφαλιστεί ότι μία συγκεκριμένη ανταλλαγή πλαισίων θα γίνει χωρίς διακοπή από μετάδοση τρίτου σταθμού το 802.11 υποστηρίζει το μηχανισμό RTS/CTS. Αυτός ο μηχανισμός διαφοροποιεί την διαδικασία αποστολής πλαισίου που είχε αναφερθεί σε προηγούμενη παράγραφο, εισάγοντας δύο επιπλέον πλαίσια, τα RTS (Ready To Send) και CTS (Clear To Send). Προστατεύοντας την ανταλλαγή πλαισίων, ο μηχανισμός RTS/CTS βελτιώνει την απόδοση της χρήσης του ασύρματου δικτύου σε περιπτώσεις μεγάλου φόρτου εξαιτίας της ύπαρξης πολλών τερματικών και αντιμετωπίζει το πρόβλημα του κρυμμένου κόμβου. Αν όμως χρησιμοποιείται χωρίς λόγο, έχει το ακριβώς αντίθετο αποτέλεσμα, εφόσον προσθέτει επιπλέον φορτίο στο ασύρματο δίκτυο.

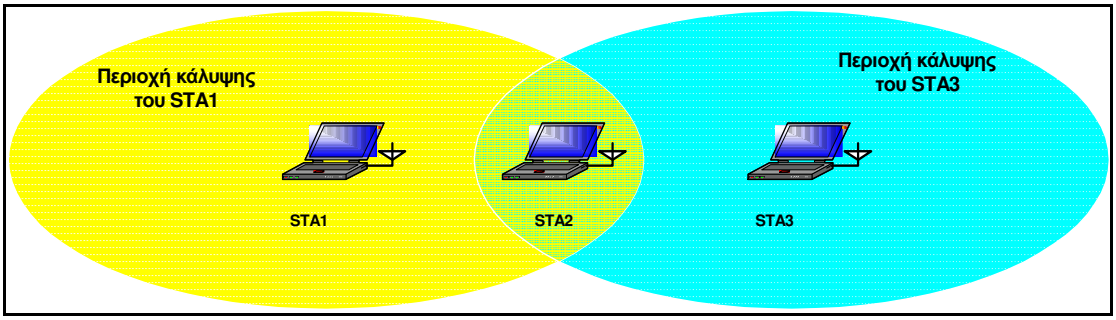
Η βασική ιδέα είναι ότι ο αποστολέας στέλνει αρχικά ένα πλαίσιο RTS στον παραλήπτη που δεν περιέχει δεδομένα. Αυτό το πλαίσιο έχει ως σκοπό να δεσμεύσει ο αποστολέας το μέσο μετάδοσης για όσο χρόνο υπολογίζει ότι θα διαρκέσει η αποστολή του πλαισίου δεδομένων και να το ανακοινώσει στους υπόλοιπους σταθμούς μέσω του μετρητή NAV στο πλαίσιο RTS. Ο παραλήπτης λαμβάνοντας το RTS απαντάει με ένα πλαίσιο CTS. Υπενθυμίζεται ότι η αποστολή πλαισίου CTS γίνεται με το συντομότερο χρόνο αναμονής SIFS. Τότε ο αποστολέας στέλνει το πλαίσιο δεδομένων και περιμένει την επιβεβαίωση ορθής λήψης του από τον παραλήπτη. Έτσι η διαδικασία αποστολής πλαισίου απαιτεί την ανταλλαγή τεσσάρων πλαισίων για να ολοκληρωθεί σωστά.

Ο μηχανισμός αυτός ενεργοποιείται αυτόματα όταν το μέγεθος ενός πλαισίου είναι μεγαλύτερο από το RTS threshold για να διασφαλίσει την ομαλή αποστολή μεγάλων πλαισίων. Επίσης μπορεί να χρησιμοποιηθεί σε συνδυασμό με τον κατακερματισμό. Συνήθως τα κατώφλια RTS threshold και Fragmentation threshold τίθενται στην ίδια τιμή. Αυτό έχει σαν αποτέλεσμα όλα τα fragments ενός πλαισίου να μεταδίδονται με τη σειρά προστατευμένα από το μηχανισμό RTS/CTS. Σε αυτήν την περίπτωση το πλαίσιο RTS που στέλνει ο αποστολέας στην αρχή της διαδικασίας δεσμεύει το μέσο για όσο χρόνο απαιτεί η αποστολή και η επιβεβαίωση του πρώτου τμήματος του πλαισίου. Όταν ο αποστολέας πάρει το CTS αρχίζει να στέλνει διαδοχικά τα τμήματα περιμένοντας φυσικά κάθε φορά για το αντίστοιχο πλαίσιο ACK, του οποίου η αποστολή γίνεται με χρήση του χρόνου SIFS. Ο αποστολέας και ο παραλήπτης ανανεώνουν το NAV κατά τη διάρκεια της ανταλλαγής πλαισίων, εξασφαλίζοντας ότι θα διατηρήσουν τον έλεγχο του μέσου. Το μέσο αποδεσμεύεται με την λήψη από τον αποστολέα του τελευταίου πλαισίου ACK από τον παραλήπτη. Σημειώνεται εδώ ότι ένας άλλος τρόπος μετάδοσης των τμημάτων ενός πλαισίου είναι να δεσμεύσει ο αποστολέας το μέσο με χρήση του μετρητή NAV στο πρώτο τμήμα που θα στείλει. Τα παραπάνω φαίνονται στο Σχήμα 2.11.



Σχέδιο 2.11: Τρόπος λειτουργίας του μηχανισμού RTS\CTS

Αυτός ο μηχανισμός αντιμετωπίζει αποτελεσματικά το πρόβλημα ύπαρξης κρυμμένου κόμβου (hidden node). Το πρόβλημα αυτό φαίνεται στο Σχήμα 2.12.



Σχήμα 2.12: Πρόβλημα κρυμμένου κόμβου

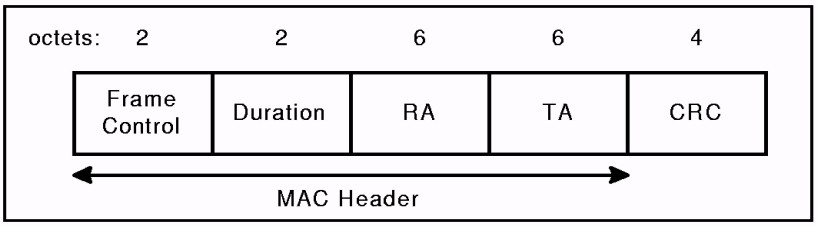
Όπως φαίνεται στο Σχήμα 2.12, ο σταθμός STA1 δεν γνωρίζει την ύπαρξη του STA3, εφόσον αυτός είναι έξω από την περιοχή κάλυψής του. Το ίδιο συμβαίνει και με τον STA3. Ο STA2 βρίσκεται στην κοινή περιοχή κάλυψης των STA1 και STA3 και μπορεί να ανταλλάσσει πλαίσια και με τους δύο. Το πρόβλημα προκύπτει όταν οι STA1 και STA3 επιχειρούν να επικοινωνήσουν με τον STA2 ταυτόχρονα. Τότε προκύπτουν συγκρούσεις και τα πλαίσια που έχουν εκπεμφθεί χάνονται.

Αν όμως χρησιμοποιηθεί ο μηχανισμός RTS/CTS ο κόμβος STA2 θα εκπέμψει ένα πλαίσιο CTS σε απάντηση του RTS που θα του έχει στείλει νωρίτερα ο STA1. Αυτό το πλαίσιο CTS θα το λάβει και ο STA3 και έτσι θα αποφύγει να μεταδώσει κι αυτός κάποιο πλαίσιο που θα προκαλούσε σύγκρουση. Τον ίδιο ρόλο παίζει και το πλαίσιο RTS που μεταδίδει ο STA1, δηλαδή ενημερώνει άλλους κρυφούς κόμβους που μπορεί να βρίσκονται γύρω του και δεν βλέπουν τον STA2.

2.3.1.6 Ποίο κοινό σχήμα πλαισίων

Σχήμα πλαισίων RTS (Σχήμα 2.13)

Το πλαίσιο RTS κοιτάζει ως εξής:



Σχήμα 2.13: Τύπος πλαισίων RTS

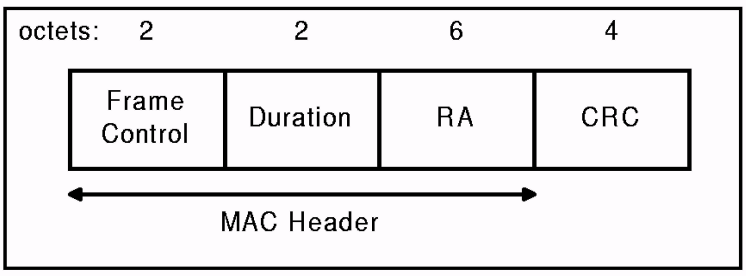
Το RA του πλαισίου RTS είναι η διεύθυνση STA, στο ασύρματο μέσο, το οποίο είναι ο προοριζόμενος άμεσος παραλήπτης του επόμενου πλαισίου δεδομένων ή διαχείρισης.

Το TA θα είναι η διεύθυνση STA που διαβιβάζει το πλαίσιο RTS.

Η Duration είναι ο χρόνος, στα μικρό-δευτερόλεπτα, που απαιτούνται για να διαβιβαστούν τα πλαίσια δεδομένων ή διαχειρίσεις, συν ένα πλαίσιο CTS, συν ένα πλαίσιο ACK, συν τρία Διαστήματα SIFS.

Σχήμα πλαισίων CTS (Σχήμα 2.14)

Το πλαίσιο CTS κοιτάζει ως εξής:



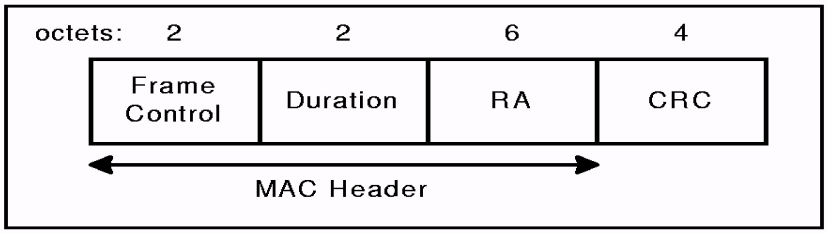
Σχήμα 2.14: Σχήμα πλαισίων CTS

Η διεύθυνση δεκτών (RA) του πλαισίου CTS αντιγράφεται από τον πεδίο μεταδιδόμενης διεύθυνσης (TA) του αμέσως προηγούμενου πλαισίου RTS στο οποίο στο CTS είναι μια απάντηση.

Η τιμή Duration είναι η τιμή που λαμβάνεται από το πεδίο Duration του αμέσως προηγούμενου πλαισίου RTS, μείον το χρόνο, στα μικρό-δευτερόλεπτα, που απαιτούνται για να διαβιβάσουν το πλαίσιο CTS και το διάστημα SIFS της.

Σχήμα πλαισίων ACK (Σχήμα 2.15)

Το πλαίσιο ACK κοιτάζει ως εξής:.



Σχήμα 2.15: Τύπος πλαισίων ACK

Η διεύθυνση δεκτών (RA) του πλαισίου ACK αντιγράφεται από τη πεδίο Address-2 του αμέσως προηγούμενου πλαισίου.

Εάν τα bit των περισσότερων τεμαχίων είναι ρυθμισμένα 0 στο πεδίο ελέγχου πλαισίων του προηγούμενου πλαισίου, η τιμή διάρκειας τίθεται 0, διαφορετικά η τιμή διάρκειας λαμβάνεται από το πεδίο Duration του προηγούμενου πλαισίου, μείον το χρόνο, στα μικρό-δευτερόλεπτα, που απαιτούνται για να διαβιβάσουν το πλαίσιο ACK και το διάστημα SIFS της.

2.3.2 Εξοικονόμηση Ενέργειας

Εφόσον οι σταθμοί που κατεξοχήν χρησιμοποιούν ένα ασύρματο δίκτυο είναι κινητοί, πρέπει να ληφθεί ιδιαίτερη μέριμνα για την όσο το δυνατόν μικρότερη κατανάλωση ισχύος από αυτούς, κάτι που επιμηκύνει τη διάρκεια ζωής της μπαταρίας τους και αυξάνει την αυτονομία τους. Η μεγαλύτερη κατανάλωση ισχύος σε ασύρματα συστήματα προέρχεται από τους ενισχυτές που ενισχύουν το σήμα αμέσως πριν την εκπομπή ή μετά τη λήψη του.

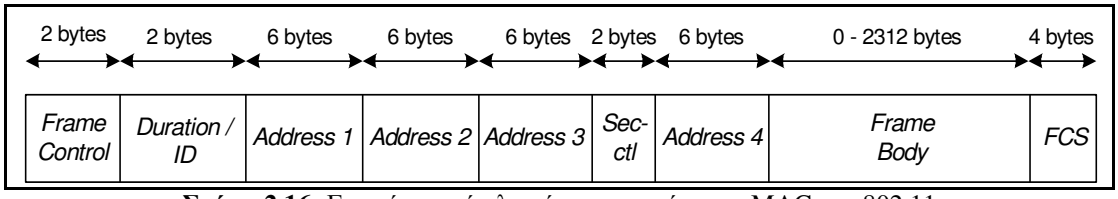
Γι' αυτό το λόγο στο πρότυπο 802.11 υπάρχει η δυνατότητα ένας σταθμός να σταματήσει τη λειτουργία του πομποδέκτη του για κάποια περίοδο, που ονομάζεται sleeping period. Παράλληλα οι σταθμοί, συμπεριλαμβανομένων και των AP's, έχουν τη δυνατότητα της προσωρινής αποθήκευσης (buffering) των πλαισίων που προορίζονται για σταθμούς που έχουν εισέλθει σε sleeping period. Με αυτόν τον τρόπο οι σταθμοί μπορούν να «ξυπνούν» περιοδικά και να δέχονται τα πλαίσια που έχει αποθηκεύσει το AP ή να στέλνουν οι ίδιοι πλαίσια στο AP.

Ένας σταθμός που μόλις έχει ξυπνήσει μπορεί να ζητήσει από το AP να του στείλει όσα πλαίσια έχει αποθηκευμένα για αυτόν με την αποστολή ενός PS-Poll πλαισίου. Το AP όταν λάβει ένα τέτοιο πλαίσιο μπορεί είτε να αρχίσει να στέλνει αμέσως πλαίσια στον σταθμό, αν φυσικά υπάρχουν, ή να του στείλει άμεσα ένα πλαίσιο ACK και να στείλει αργότερα τα αποθηκευμένα πλαίσια. Ο σταθμός στη δεύτερη περίπτωση πρέπει να περιμένει μέχρι να του αποσταλούν τα πλαίσια χωρίς φυσικά να ξαναμπεί σε sleeping period.

Οι σταθμοί έχουν επίσης την υποχρέωση να ξυπνούν κατά περιόδους και να λαμβάνουν Beacon πλαίσια από το AP. Αυτά, πέραν των άλλων λειτουργιών που επιτελούν, έχουν ένα πεδίο που ονομάζεται TIM (Traffic Indication Map). Εκεί σημειώνεται κάθε σταθμός για τον οποίο το AP έχει αποθηκευμένα πλαίσια, τα οποία ο σταθμός μπορεί στη συνέχεια να τα ζητήσει με ένα PS-Poll πλαίσιο. Περισσότερα για την ελαχιστοποίηση της κατανάλωσης ενέργειας θα αναφερθούν σε επόμενη παράγραφος.

2.3.3 Πλαισίωση MAC υποστρώματος

Στο Σχήμα 2.16 φαίνεται η γενική μορφή του πλαισίου του υποστρώματος MAC του 802.11.

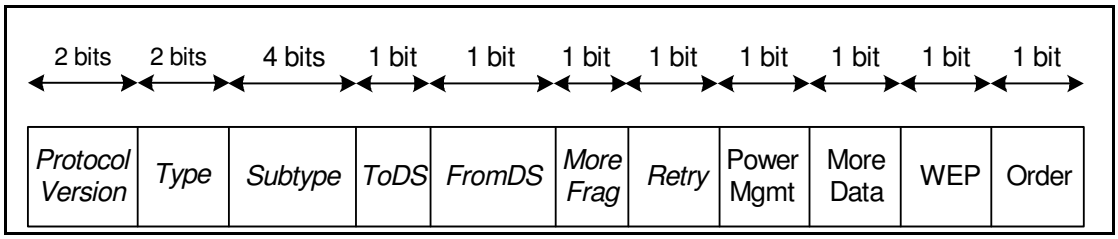


Σχήμα 2.16: Γενική μορφή πλαισίου υποστρώματος MAC του 802.11

Η παραπάνω μορφή χρησιμοποιείται σε όλους τους τύπους πλαισίων (Data, Control, Management), αλλά δεν χρησιμοποιούνται όλα τα πεδία από κάθε τύπο με τον ίδιο τρόπο. Στη συνέχεια αναλύονται τα διάφορα πεδία και η λειτουργία που εξυπηρετούν.

Frame Control

Το πεδίο αυτό διαιρείται εκ νέου σε υποπεδία. Αυτά φαίνονται στο Σχήμα 2.17.



Σχήμα 2.17: Πεδίο Frame Control του πλαισίου MAC του 802.11

Protocol Version

Πεδίο που κωδικοποιεί την έκδοση του πρωτοκόλλου MAC που χρησιμοποιείται. Προς το παρών μόνο μία τέτοια έκδοση υπάρχει που αντιστοιχεί στην τιμή «00».

Type & Subtype

Τα δύο αυτά πεδία χρησιμοποιούνται για την δήλωση του τύπου του πλαισίου. Υπάρχουν 3 βασικοί τύποι πλαισίων, τα πλαίσια Data, τα πλαίσια Control και τα πλαίσια Management. Κάθε βασικός τύπος περιλαμβάνει με η σειρά του έναν ορισμένο αριθμό διαφορετικών πλαισίων. Η κωδικοποίηση των παραπάνω στα πεδία Type και Subtype φαίνεται στον Πίνακα 2.5.

Πεδίο Subtype	Είδος Πλαισίου
Πλαίσια Management – Type = 00	
0000	Association Request
0001	Association Response
0010	Reassociation Request
0011	Reassociation Response
0100	Probe Request
0101	Probe Response
1000	Beacon
1001	Announcement Traffic Indication Message
1010	Disassociation
1011	Authentication
1100	Deauthentication
Πλαίσια Control – Type = 01	
1010	Power Save Poll (PS-Poll)
1011	RTS
1100	CTS
1101	ACK
1110	Contention Free End (CF-End)
1111	CF-End + CF-Ack
Πλαίσια Data – Type = 10	
0000	Data
0001	Data + CF-Ack
0010	Data + CF-Poll
0011	Data + CF-Ack + CF-Poll
0100	Null
0101	CF-Ack
0110	CF-Poll
0111	CF-Ack + CF-Poll

Πίνακας 2.5: Σημασία πεδίων Type και Subtype του πλαισίου MAC του 802.11

Όλες οι τιμές των δύο πεδίων που δεν αναφέρονται στον πίνακα είναι δεσμευμένες και δεν χρησιμοποιούνται προς το παρών. Στη συνέχεια του κεφαλαίου αυτού θα παρουσιαστούν οι διάφοροι τύποι πλαισίων πιο αναλυτικά.

ToDS & FromDS

Τα δύο αυτά bits δείχνουν αν το πλαίσιο προορίζεται για το σύστημα διανομής (distribution system). Όλα τα πλαίσια σε infrastructure δίκτυα έχουν το ένα από τα δύο bits ίσο με «1».

More Fragments

Το πεδίο αυτό είναι ίσο με «1» για να υποδηλώσει ότι το πλαίσιο αυτό είναι τμήμα (fragment) ενός μεγαλύτερου πλαισίου.

Retry

Το πεδίο αυτό είναι ίσο με «1» αν το πλαίσιο αυτό έχει μεταδοθεί ξανά.

Power Management

Το πεδίο αυτό είναι ίσο με «1» για να δηλώσει ο σταθμός που το στέλνει ότι μόλις τελειώσει η αποστολή, δηλαδή αφού ληφθεί και η επιβεβαίωση αν χρειάζεται, θα περάσει σε λειτουργία εξοικονόμησης ενέργειας (power-save mode).

More Data

Όταν το πεδίο αυτό είναι ίσο με «1» σε ένα πλαίσιο σημαίνει ότι ο παραλήπτης του έχει κι άλλα πλαίσια αποθηκευμένα στο AP και πρέπει να τα παραλάβει. Αυτό το πεδίο το αλλάζει μόνο το AP.

WEP

Το πεδίο αυτό είναι ίσο με «1» για να υποδηλώσει ότι το πλαίσιο προστατεύεται από τον αλγόριθμο ασφαλείας WEP (Wired Equivalent Privacy).

Order

Το πεδίο αυτό τίθεται ίσο με «1» όταν τα πλαίσια ή τα τμήματα πλαισίων μεταδίδονται με τη σειρά.

Duration/ID

Το πεδίο αυτό έχει τρεις διαφορετικές χρήσεις.

- Όταν το τελευταίο bit του είναι ίσο με «0» το πεδίο χρησιμοποιείται για να ενημερώσει την τιμή του NAV. Το περιεχόμενό του είναι ο χρόνος σε microseconds που το μέσο θα είναι δεσμευμένο.

- Κατά τη διάρκεια των contention free περιόδων το bit 14 είναι ίσο με «0», το bit 15 ίσο με 1 και όλα τα υπόλοιπα bits μηδενικά. Τότε η τιμή του πεδίου (32768) χρησιμεύει ως NAV για να μπλοκάρει την πρόσβαση στο μέσο σε αυτούς τους σταθμούς που δεν έλαβαν το Beacon πλαίσιο που ανακοίνωνε την αρχή της περιόδου αυτής.

- Τέλος, τα bits 14 και 15 τίθενται ίσα με «0» στα PS-Poll πλαίσια. Το πεδίο αυτό περιέχει το Association ID (AID) του σταθμού που στέλνει το PS-Poll πλαίσιο προκειμένου να λάβει αποθηκευμένα στο AP πλαίσια που προορίζονται για αυτόν. Οι έγκυρες τιμές για το AID είναι από 1 έως 2007, οι υπόλοιπες είναι δεσμευμένες και δεν χρησιμοποιούνται.

Σημειώνεται τέλος ότι το Most Significant Bit (MSB) του πεδίου είναι το τελευταίο (bit 15).

Πεδία Address

Το πλαίσιο μπορεί να περιέχει μέχρι 4 πεδία διευθύνσεων. Το ποιες διευθύνσεις περιέχονται σε κάθε πεδίο εξαρτάται από το είδος του πλαισίου. Ένας γενικός κανόνας είναι ότι η πρώτη διεύθυνση είναι του παραλήπτη, η δεύτερη του αποστολέα ενώ η τρίτη χρησιμοποιείται για φιλτράρισμα. Όλες οι διευθύνσεις είναι 48-μπιτες στα πρότυπα του Ethernet. Κάποιο από τα πεδία αυτά μπορεί να περιέχει και το Basic Service Set ID (BSSID) του δικτύου. Τα περισσότερα πλαίσια πάντως χρησιμοποιούν μόνο τα τρία πεδία διευθύνσεων.

Sequence Control

Το πεδίο αυτό χρησιμεύει για την επανένωση κατατμημένων πλαισίων και για την απόρριψη αντιγράφων. Χωρίζεται σε δύο υποπεδία, το Fragment Number μήκους 4 bits και το Sequence Number μήκους 12 bits. Κάθε πακέτο που περνάει στο MAC από ανώτερα στρώματα αποκτάει ένα Sequence Number. Το πεδίο αυτό λοιπόν χρησιμεύει ως modulo-4096 μετρητής. Αν κάποιο πακέτο χρειαστεί να χωριστεί σε περισσότερα του ενός πλαίσια για να μεταδοθεί όλα θα έχουν τον ίδιο Sequence Number. Το ίδιο συμβαίνει και αν ένα πλαίσιο επαναμεταδοθεί. Αυτό που διαχωρίζει τα τμήματα μεταξύ τους είναι το πεδίο Fragment Number. Αυτό αυξάνεται κατά 1 για κάθε νέο τμήμα ενός μεγαλύτερου πλαισίου που μεταδίδεται.

FCS (Frame Check Sequence)

Το πεδίο αυτό περιέχει ένα CRC κώδικα που προστατεύει ολόκληρο το πλαίσιο MAC.

Frame Body

Το πεδίο αυτό περιέχει το ωφέλιμο φορτίο του πλαισίου (payload), δηλαδή το πακέτο ανωτέρου στρώματος που πρέπει να μεταφερθεί. Το μέγιστο μέγεθος του πεδίου είναι 2304 bytes.

2.3.4 Τύποι πλαισίων του υποστρώματος MAC

2.3.4.1 Πλαίσια Data

Τα πλαίσια αυτά χρησιμεύουν για τη μεταφορά δεδομένων από ανώτερα επίπεδα του πρωτοκόλλου, αλλά επιτελούν κι άλλες λειτουργίες. Στη συνέχεια φαίνονται τα διάφορα πλαίσια αυτού του τύπου.

- Data: Το απλούστερο πλαίσιο του τύπου αυτού, μπορεί να χρησιμοποιηθεί και σε contention - free period και σε contention period. Το μόνο που κάνει είναι να μεταφέρει δεδομένα.

- Data + CF-Ack: Το πλαίσιο αυτό χρησιμοποιείται μόνο κατά την contention - free period. Μεταφέρει δεδομένα και ταυτόχρονα επιβεβαιώνει κάποιο πλαίσιο που έχει ήδη ληφθεί.

- Data + CF-Poll: Το πλαίσιο αυτό αποστέλλεται από το AP που τρέχει τον PCF αλγόριθμο κατά την contention - free period. Μεταφέρει δεδομένα προς έναν σταθμό και ζητάει από αυτόν να στείλει ότι πλαίσια έχει αποθηκεύσει προσωρινά.

- Data + CF-Ack + CF-Poll: Συνδυάζει τις λειτουργίες των δύο προηγούμενων πλαισίων, αποστέλλεται μόνο από το AP (Access Point).

- Null: Το πλαίσιο αυτό δεν μεταφέρει δεδομένα. Αποστέλλεται από έναν σταθμό στο AP έχοντας το bit Power Management του πεδίου Frame Control ίσο με «1» για να δηλώσει στο AP ότι μπαίνει σε λειτουργία εξοικονόμησης ενέργειας. Το AP όταν λάβει τέτοιο πλαίσιο πρέπει να αποθηκεύει μελλοντικά πλαίσια προς το σταθμό αυτόν.

- CF-Ack: Ίδια λειτουργία με το Data + CF-Ack χωρίς να μεταφέρει δεδομένα.

- CF-Poll: Ίδια λειτουργία με το Data + CF-Poll χωρίς να μεταφέρει δεδομένα.

- CF-Ack + CF-Poll: Ίδια λειτουργία με το Data + CF-Ack +CF-Poll χωρίς να μεταφέρει δεδομένα.

2.3.4.2 Πλαίσια Control

Τα πλαίσια του τύπου Control λειτουργούν βοηθητικά για την αξιόπιστη μεταφορά των Data πλαισίων και την πρόσβαση στο μέσο των σταθμών. Υπάρχουν έξι διαφορετικά πλαίσια αυτού του τύπου που παρουσιάζονται στη συνέχεια.

- Power Save Poll (PS-Poll): Το πλαίσιο αυτό αποστέλλεται από οποιοδήποτε σταθμό στο AP, όταν αυτός επανέλθει στην κανονική του λειτουργία μετά από περίοδο λειτουργίας εξοικονόμησης ενέργειας, για να ζητήσει να του αποσταλούν όσα πλαίσια προορίζονται για αυτόν και είναι προσωρινά αποθηκευμένα στο AP.

- RTS: Το πλαίσιο αυτό, όπως έχει ήδη αναφερθεί, είναι μέρος του μηχανισμού RTS/CTS για την απρόσκοπτη μεταφορά ενός ή περισσοτέρων πλαισίων. Ειδοποιεί τον σταθμό προορισμού αλλά και όσους άλλους το λάβουν ότι ζητάει άδεια να στείλει δεδομένα.

- CTS: Το έτερο πλαίσιο του μηχανισμού RTS/CTS. Δίνει την άδεια σε κάποιον σταθμό να στείλει δεδομένα, ενώ ειδοποιεί τους υπόλοιπους ότι επίκειται ανταλλαγή πλαισίων.

- ACK: Το πλαίσιο αυτό επιβεβαιώνει τη λήψη του αμέσως προηγούμενου πλαισίου. Η σωστή λήψη του είναι απαραίτητη για να θεωρήσει ο αποστολέας ότι το πλαίσιο που έστειλε παραδόθηκε κανονικά.

- Contention Free End (CF-End): Το πλαίσιο αυτό αποστέλλεται από το AP που ελέγχει την πρόσβαση κατά μία contention - free period για να δηλώσει τη λήξη της.

- CF-End + CF-Ack: Σύνθετο πλαίσιο που δηλώνει τη λήξη της contention free period και επιβεβαιώνει τη λήψη του τελευταίου πλαισίου που είχε σταλεί.

2.3.4.3 Πλαίσια Management

Τα ασύρματα δίκτυα έχουν αυξημένες ανάγκες διαχείρισης σε σχέση με τα ενσύρματα. Το θέμα αυτό καλύπτεται εξολοκλήρου στην παράγραφο 2.6. Εδώ θα παρουσιαστούν οι διάφοροι τύποι πλαισίων που επιτελούν τις απαραίτητες λειτουργίες. Η δομή των πλαισίων Management διαφέρει αρκετά από αυτή των πλαισίων Data, αφού χρησιμοποιούν διάφορα πεδία για διαφορετικό λόγο. Τέτοιο παράδειγμα είναι το πεδίο Frame Body που χρησιμοποιείται από κάποια Management πλαίσια για να μεταφέρει επιπλέον πληροφορίες. Στη συνέχεια δεν θα γίνει ιδιαίτερη αναφορά στην πλαισίωση αλλά στην λειτουργία που επιτελεί κάθε πλαίσιο Management.

- Association Request: Το πλαίσιο αυτό στέλνεται από έναν σταθμό στο AP για να δηλώσει την πρόθεσή του να ξεκινήσει τη διαδικασία του association με το BSS αυτό. Το πλαίσιο περιέχει πληροφορίες όπως το SSID (Service Set ID), το είδος του δικτύου, τη χρήση ή όχι του αλγορίθμου WEP, τους υποστηριζόμενους από το σταθμό ρυθμούς μετάδοσης και άλλα.

- Association Response: Στέλνεται από το AP σε σταθμό ως απάντηση σε πλαίσιο Association Request. Δηλώνει αν ο σταθμός έγινε αποδεκτή η αίτηση του σταθμού και σε περίπτωση θετικής απάντησης περιέχει το AID.

- Reassociation Request: Το ίδιο με το Association Request, αποστέλλεται όταν ένας σταθμός κινείται μεταξύ διαφορετικών BSS εντός του ιδίου ESS ή αν χάσει προσωρινά τη σύνδεση στο BSS που βρίσκεται.

- Reassociation Response: Απάντηση στο πλαίσιο Reassociation Request.

- Disassociation: Το πλαίσιο αυτό αποστέλλεται από έναν σταθμό στο AP του BSS για να τερματίσει τη σχέση association με αυτό. Περιέχει έναν κωδικό που δηλώνει την αιτία του τερματισμού (Reason Code).

- Probe Request: Πλαίσιο που αποστέλλεται από έναν σταθμό που ψάχνει ασύρματα δίκτυα στην περιοχή του. Περιέχει το SSID του δικτύου που ψάχνει ο σταθμός και τους υποστηριζόμενους από αυτόν ρυθμούς μετάδοσης.

- Probe Response: Απάντηση σε πλαίσιο Probe Request. Περιέχει διάφορες παραμέτρους του δικτύου ώστε να μπορέσει ο σταθμός που το λαμβάνει να συνεχίσει τη διαδικασία ένταξης στο δίκτυο.

- Authentication: Πλαίσια που ανταλλάσσονται μεταξύ AP και ενδιαφερόμενου σταθμού για τη διαδικασία του authentication που προηγείται του association.

- Deauthentication: Αντίστοιχο του Disassociation, περιέχει και αυτό πεδίο Reason Code.

- Beacon: Το πλαίσιο αυτό εκπέμπεται περιοδικά από το AP και έχουν ήδη αναφερθεί κάποιες λειτουργίες που σχετίζονται με αυτό (δήλωση έναρξης contention free period). Κύριος ρόλος τους είναι η γνωστοποίηση της ύπαρξης του δικτύου στην περιοχή κάλυψής του. Περιέχει διάφορες παραμέτρους λειτουργίας του δικτύου.

- IBSS Announcement Traffic Indication Message: Αυτό το πλαίσιο συναντάται αποκλειστικά σε IBSS δίκτυα. Αποστέλλεται από οποιονδήποτε σταθμό έχει αποθηκευμένα πλαίσια που προορίζονται για άλλον σταθμό, ο οποίος λειτουργούσε σε κατάσταση εξοικονόμησης ενέργειας για να τον ειδοποιήσει. Ο παραλήπτης πρέπει να εκκινήσει τη διαδικασία παραλαβής των αποθηκευμένων πλαισίων.

2.4 Πρότυπο 802.11b

Το 802.11b είναι ένα εναλλακτικό φυσικό στρώμα πέραν των τριών που ορίστηκαν με το αρχικό πρότυπο 802.11. Το πρότυπο αυτό ανακοινώθηκε από την IEEE το 1999. Φυσικά, χρησιμοποιεί το ίδιο υπόστρωμα MAC όπως και τα υπόλοιπα φυσικά στρώματα του προτύπου. Χρησιμοποιεί την ελεύθερη μπάντα συχνοτήτων των 2,4 GHz και προσφέρει ρυθμούς μετάδοσης μέχρι και 11 Mbps με την έλευση του 802.11b η επιτροπή αποφάσισε να αφήσει στο πρότυπο μόνο την κωδικοποίηση DSSS, παρόλο που το FHSS αρχικά φαίνονταν σαν ευκολότερο αλλά και φθηνότερο στην υλοποίηση του. Με αυτό τον τρόπο το 802.11b απέκτησε ένα από τα μεγαλύτερα του πλεονεκτήματα, την υψηλή διαμεταγωγής δεδομένων. Αυτή τη στιγμή είναι το πιο διαδεδομένο πρότυπο στην αγορά, παρότι το 802.11a προσφέρει υψηλότερους ρυθμούς μετάδοσης. Είναι συμβατό με το νέο πρότυπο 802.11g, που ακόμα δεν έχει ανακοινωθεί στην τελική του μορφή, κάτι που καθιστά την επιλογή του ακόμα πιο δελεαστική. Χρησιμοποιεί την τεχνική HR/DSSS (High Rate/ Direct Sequence Spread Spectrum) και την διαμόρφωση CCK (Complementary Code Keying). Το πρότυπο 802.11b

δεν χρησιμοποιεί στις περισσότερες υλοποιήσεις την μέθοδο PCF καθώς περιορίζει εμμέσως αλλά αυστηρώς την εμβέλεια ενός ασύρματου δικτύου. Μπορεί να θεωρηθεί σαν επέκταση του αρχικού DSSS φυσικού στρώματος που ορίστηκε στο 802.11 και μάλιστα χρησιμοποιεί τα ίδια κανάλια με αυτό, πετυχαίνοντας αρκετά μεγαλύτερους ρυθμούς μετάδοσης.

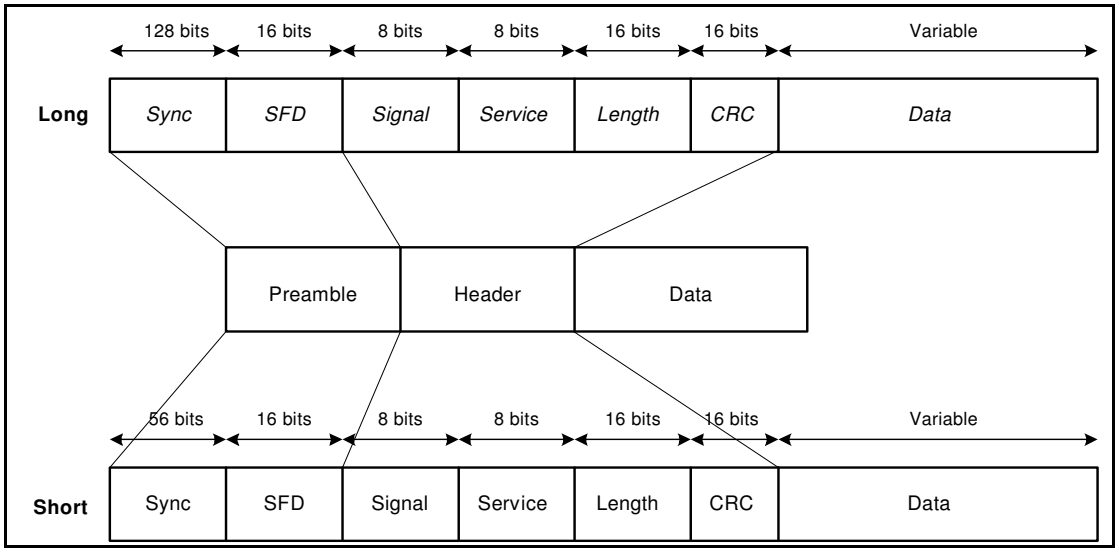
2.4.1 802.11b – Υπόστρωμα PLCP

Το PLCP του 802.11b, σε αντίθεση με τα αντίστοιχα υποστρώματα των άλλων φυσικών στρωμάτων του προτύπου 802.11, χρησιμοποιεί δύο διαφορετικές μορφές πλαισίου, το σύντομο (Short) και το κανονικό (Long). Η μορφή Long είναι ίδια με τη μορφή του κλασσικού πλαισίου του φυσικού στρώματος DSSS του 802.11. Η υποστήριξη της Short μορφής είναι προαιρετική και γίνεται για επίτευξη αυξημένης διέλευσης. Η μορφή πλαισίου Short μπορεί να χρησιμοποιηθεί μόνο αν όλοι οι σταθμοί εργασίας σε ένα BSS την υποστηρίζουν. Επιπλέον, το AP είναι υποχρεωμένο να απαντά στους σταθμούς που κάνουν active scanning με την ίδια μορφή πλαισίου που στέλνουν, ακόμα κι αν το δίκτυο λειτουργεί με την εναλλακτική μορφή.

Στο Σχήμα 2.18 φαίνονται και οι δύο μορφές PLCP πλαισίου. Επειδή η δομή τους είναι ίδια με αυτήν του PLCP πλαισίου του 802.11 DSSS φυσικού στρώματος θα τονιστούν μόνο τα σημεία στα οποία παρατηρούνται διαφορές.

Preamble

Το τμήμα Preamble αποτελείται από τα πεδία Sync και SFD. Το Long Sync πεδίο είναι μεγαλύτερου μήκους από το Short Sync, 128 bits αντί 56. Το Long SFD πεδίο περιέχει την ακολουθία «1111 0011 1010 0000» ενώ το Short SFD περιέχει την αντίστροφη ακολουθία «0000 0101 1100 1111». Το τμήμα Preamble μεταδίδεται πάντα σε ρυθμό 1 Mbps με χρήση DBPSK διαμόρφωσης.



Σχήμα 2.18: Πλαίσιο PLCP υποστρώματος του φυσικού στρώματος 802.11b

Header

Το τμήμα αυτό περιέχει τα πεδία Signal, Service, Length και CRC. Το μήκος τους είναι ίδιο και στην Long και στην Shot μορφή πλαισίου. Το πεδίο Signal κωδικοποιεί το ρυθμό μετάδοσης. Στη μορφή Long είναι διαθέσιμοι 4 ρυθμοί 1, 2, 5,5 και 11 Mbps ενώ στη μορφή Short δεν είναι διαθέσιμος ο ρυθμός του 1 Mbps. Το πεδίο Length έχει την κλασσική του χρήση, περιέχει δηλαδή το χρόνο σε msec που απαιτείται για τη μετάδοση του ενσωματωμένου MAC πλαισίου. Από το πεδίο Service χρησιμοποιούνται τρία bits, ενώ τα υπόλοιπα παραμένουν δεσμευμένα και έχουν τιμή «0». Το bit 8 χρησιμεύει ως συμπληρωματικό bit του πεδίου Length. Το bit 3 δηλώνει το αν η συχνότητα μετάδοσης και το ρολόι συμβόλων χρησιμοποιούν τον ίδιο ταλαντωτή. Το bit 4 δηλώνει το είδος της κωδικοποίησης και είναι «1» για PBCC (Packet Binary Convolutional Coding) και «0» για CCK. Τέλος, το πεδίο CRC περιέχει τον κυκλικό κώδικα που προστατεύει την επικεφαλίδα. Η επικεφαλίδα της Long μορφής πλαισίου μεταδίδεται με ρυθμό 1 Mbps και χρήση DBPSK ενώ η επικεφαλίδα της Short μορφής με ρυθμό 2 Mbps και χρήση DQPSK.

Πριν τη μετάδοση όλα τα bits του πλαισίου υφίστανται τη διαδικασία του scrambling, όπως και στην περίπτωση του 802.11 DSSS.

2.4.2 802.11b – Υπόστρωμα PMD

Στο υπόστρωμα PMD χρησιμοποιείται η τεχνική διαμόρφωσης CCK για την επίτευξη των υψηλότερων ρυθμών μετάδοσης των 5,5 και 11 Mbps, πάντα σε συνδυασμό με το Direct Sequence. Μάλιστα για την διατήρηση της συμβατότητας με τους ρυθμούς των 1 και 2 Mbps προβλέπεται η μετάδοση με τον ίδιο τρόπο, όπως στο αντίστοιχο φυσικό στρώμα του 802.11. Σημειώνεται εδώ ότι εφόσον γίνεται χρήση των ίδιων καναλιών αυτό που επιτρέπει τους υψηλότερους ρυθμούς μετάδοση είναι η χρήση της διαμόρφωσης CCK.

Για τον ρυθμό μετάδοσης των 5,5 Mbps με χρήση CCK η ακολουθία των προς μετάδοση chips διαιρείται σε τετράδες. Τα δύο πρώτα chips κάθε τετράδας διαμορφώνονται με βάση την κλασσική DQPSK. Τα δύο άλλα χρησιμεύουν για την επιλογή μίας εκ των τεσσάρων κωδικών λέξεων (code words) που υποστηρίζονται. Τελικά παράγεται το προς μετάδοση σύμβολο, στο οποίο έχουν κωδικοποιηθεί 4 chips, ως η ολική διαφορά φάσης από το προηγούμενο σύμβολο.

Για το ρυθμό μετάδοσης των 11 Mbps κωδικοποιούνται 8 chips σε κάθε μεταδιδόμενο σύμβολο. Τα δύο πρώτα bits της οκτάδας διαμορφώνονται με DQPSK, ενώ τα υπόλοιπα έξι χωρίζονται εκ νέου σε ζευγάρια, από όπου παράγονται οι επιπλέον στροφές φάσης. Ο συνδυασμός των παραπάνω δίνει τελικά την τελική διαφορά φάσης από το προηγούμενο

σύμβολο. Σημειώνεται ότι η μαθηματική επεξεργασία της CCK είναι αρκετά πολύπλοκη και δεν θεωρείται σκόπιμο να παρουσιαστεί εδώ.

Το πρότυπο 802.11b προσφέρει και μία επιπλέον τεχνική διαμόρφωσης την PBCC (Packet Binary Convolutional Coding), η οποία δεν έχει βρει ευρεία αποδοχή. Επιπλέον υπάρχει και η δυνατότητα να αλλάζει το δίκτυο δυναμικά κανάλι λειτουργίας μέσω της παραμέτρου Channel Agility. Αυτό γίνεται για να μειωθεί η παρεμβολή με δίκτυο Frequency Hopping στην ίδια περιοχή.

Στον Πίνακα 2.6 παρουσιάζονται μερικά επιπλέον χαρακτηριστικά του φυσικού στρώματος 802.11b.

Παράμετρος	Τιμή
Μέγιστο μήκος πλαισίου MAC	4095 bytes
Slot time	20 μsec
SIFS time	10 μsec
Contention window size	31 έως 1023 slots
Preamble duration	144 μsec
PLCP header duration	48 bits

Πίνακας 2.6: Παράμετροι του φυσικού στρώματος 802.11b

2.5 Πρότυπο 802.11a

Σε αντίθεση με το 802.11b που λειτουργεί στην ISM μπάντα των 2,4 GHz, το πρότυπο 802.11a χρησιμοποιεί την μπάντα των 5 GHz. Σχεδιάστηκε έτσι για δύο κυρίως λόγους:

- Η μπάντα των 5 GHz χρησιμοποιείται πολύ λιγότερο από αυτήν των 2,4 GHz.
- Η μπάντα των 5 GHz προσφέρει πιο μεγάλο διαθέσιμο εύρος ζώνης.

Στις ΗΠΑ η μπάντα στα 5 GHz που έχει διατεθεί για ελεύθερη χρήση ονομάζεται UNII (Unlicensed National Information Infrastructure).

Παρά τα οφέλη που προσφέρει η χρήση υψηλότερων συχνοτήτων, που αναφέρονται παραπάνω, υπάρχουν και τα αντίστοιχα προβλήματα. Αυτά εντοπίζονται κυρίως στις αυξημένες απώλειες διάδοσης που εμφανίζονται στην μπάντα των 5 GHz σε σχέση με αυτές της μπάντας των 2,4 GHz. Αυτό το πρόβλημα αντιμετωπίζεται είτε με πυκνότερη διάταξη των AP για να καλυφθεί μία δεδομένη περιοχή είτε με αυξημένη ακτινοβολούμενη ισχύ από τους πομπούς. Η πρώτη λύση μπορεί να είναι οικονομικά ασύμφορη, ενώ η δεύτερη αυξάνει αρκετά την κατανάλωση ενέργειας των κινητών τερματικών, μειώνοντας έτσι την αυτονομία τους.

Το 802.11a βασίζεται στην τεχνική πολυπλεξίας OFDM (Orthogonal Frequency Division Multiplexing / Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας). Στη συνέχεια παρουσιάζεται συνοπτικά η OFDM.

2.5.1 Παρουσίαση OFDM

Η βασική ιδέα πίσω από την OFDM είναι η διαίρεση ενός κύριου υψηλού ρυθμού σε πολλούς μικρότερους ρυθμούς και η χρήση αυτών για την αποστολή των δεδομένων ταυτόχρονα. Όλα τα «αργά» κανάλια πολυπλέκονται τελικά σε ένα «γρήγορο» κανάλι και μεταδίδονται. Η OFDM διαφέρει από άλλες τεχνικές πολυπλεξίας όπως η CDMA (Code Division Multiple Access) στο ότι είναι πιο απλή από άποψη μαθηματικής επεξεργασίας.

Η απλή τεχνική FDM (Frequency Division Multiplexing) έδινε σε κάθε κανάλι ένα συγκεκριμένο εύρος ζώνης, γύρω από κάποια φέρουσα συχνότητα, δίνοντας έτσι τη δυνατότητα να χωρίζεται το εύρος ζώνης σε πολλά διακριτά κανάλια. Το πρόβλημα ήταν η σπατάλη εύρος ζώνης για το σωστό διαχωρισμό αυτών των καναλιών. Εφόσον στην πράξη κάθε κανάλι καταλαμβάνει μεγαλύτερο εύρος ζώνης από το θεωρητικό είναι απαραίτητη η ύπαρξη αχρησιμοποίητου εύρους ζώνης ανάμεσα σε διαδοχικά κανάλια. Η OFDM λύνει αυτό το πρόβλημα εξαφανίζοντας τα κενά και χρησιμοποιώντας μάλιστα υπερκαλυπτόμενα κανάλια, βασιζόμενη στην ιδιότητα της ορθογωνιότητας για να τα ξεχωρίζει.

Η ορθογωνιότητα μεταξύ των καναλιών σημαίνει ότι φασματικά κάθε φέρουσα συχνότητα έχει μηδενική παρεμβολή από τις υπόλοιπες φέρουσες. Τα φάσματα των καναλιών μπορεί να υπερκαλύπτονται, αλλά στην κεντρική συχνότητα κάθε καναλιού δεν παρεμβάλουν καθόλου τα υπόλοιπα κανάλια. Αντίστοιχη προϋπόθεση στο πεδίο του χρόνου είναι κατά τη διάρκεια συμβόλου (symbol duration) κάθε φέρον σήμα να έχει έναν ακέραιο αριθμό περιόδων και η διαφορά περιόδων μεταξύ γειτονικών φερόντων είναι ίση με ένα.

Στην περίπτωση χρήσης του OFDM δεν είναι τόσο έντονο το πρόβλημα της διασυμβολικής παρεμβολής (ISI – Inter Symbol Interference), αλλά υπάρχει πρόβλημα παρεμβολής γειτονικού φέροντος (ICI – Inter Carrier Interference). Τέτοιες παρεμβολές μπορούν να προκληθούν από μικρές μετατοπίσεις των κεντρικών συχνοτήτων, όπως αυτές που προκαλεί το φαινόμενο Doppler, ή και από μικρές διαφορές στις κεντρικές συχνότητες πομπού και δέκτη.

Για να αντιμετωπιστούν και οι δύο τύποι παρεμβολών (ISI και ICI) στην OFDM εισάγεται η παράμετρος του guard time. Αυτή η παράμετρος ορίζεται ένα αρχικό μέρος της διάρκειας συμβόλου που οι πομποδέκτες αγνοούν κατά την επεξεργασία του σήματος. Η επιλογή του guard time είναι εξαιρετικά σημαντική στην OFDM. Συγκεκριμένα πρέπει να είναι μεγαλύτερο από τη μέγιστη χρονική καθυστέρηση λόγω διάδοσης πολλαπλών διαδρομών, αλλά και αρκετά μικρό ώστε να μην χάνεται μεγάλο μέρος από τη διάρκεια συμβόλου. Κατά τη διάρκεια του guard time τα φέροντα σήματα υφίστανται κυκλικής επέκταση (cyclic extension), ώστε να εξασφαλιστεί ότι και οι καθυστερημένες χρονικά εκδοχές τους θα έχουν ακέραιο αριθμό περιόδων κατά το μέρος της διάρκειας συμβόλου που

θα υποστεί επεξεργασία. Στο τελικό σήμα αυτό που φαίνεται είναι μία διαφορά φάσης, αλλά διατηρείται η ορθογωνιότητα.

Η OFDM χρησιμοποιείται κυρίως σε εφαρμογές όπου το σήμα υφίσταται βαθιές διαλείψεις (deep fadings). Για να αντιμετωπιστούν οι δυσκολίες που προκύπτουν χρησιμοποιούνται κώδικες διόρθωσης λαθών και πιο συγκεκριμένα συνελικτικοί κώδικες (convolutional codes), οι οποίοι φυσικά μειώνουν τη συνολική διέλευση του συστήματος, εφόσον προσθέτουν bits για διόρθωση λαθών. Τέλος, χρησιμοποιούνται διάφορες τεχνικές για την καταπίεση των φασματικών συνιστωσών που προκύπτουν από τις απότομες αλλαγές φάσης στα όρια των συμβόλων (windowing, filtering).

2.5.2 Εφαρμογή OFDM στο 802.11a – Επιλογή παραμέτρων

Η επιλογή των παραμέτρων εξαρτάται κυρίως από τρεις παράγοντες:

- *Εύρος ζώνης:* Συνήθως είναι δεδομένο.
- *Διασπορά καθυστέρησης:* Εξαρτάται από το περιβάλλον.
- *Ρυθμός μετάδοσης:* Ζητούμενη είναι η μεγιστοποίησή του με δεδομένους τους άλλους δύο παράγοντες.

Η παράμετρος του guard time ορίστηκε ίση με 800 ns, εφόσον πρέπει να είναι δύο με τέσσερις φορές μεγαλύτερη από τη μέγιστη χρονική καθυστέρηση. Η διάρκεια συμβόλου ορίστηκε στα 4 μs. Το κάθε κανάλι (operating channel) έχει εύρος 20 MHz και περιλαμβάνει 52 φέρουσες συχνότητες, δηλαδή 52 υποκανάλια. Διαδοχικά υποκανάλια απέχουν μεταξύ τους 0,3125 MHz. Τέσσερα από αυτές χρησιμοποιούνται ως πιλοτικές συχνότητες για παρακολούθηση και τα υπόλοιπα για μετάδοση δεδομένων.

Στις ΗΠΑ έχει κρατηθεί συγκεκριμένο τμήμα της μπάντας των 5 GHz (U-NII) για χρήση από ασύρματα δίκτυα 802.11a. Συνολικά είναι διαθέσιμα 12 κανάλια των 20 MHz. Στον Πίνακα 2.7 φαίνονται αυτά τα κανάλια.

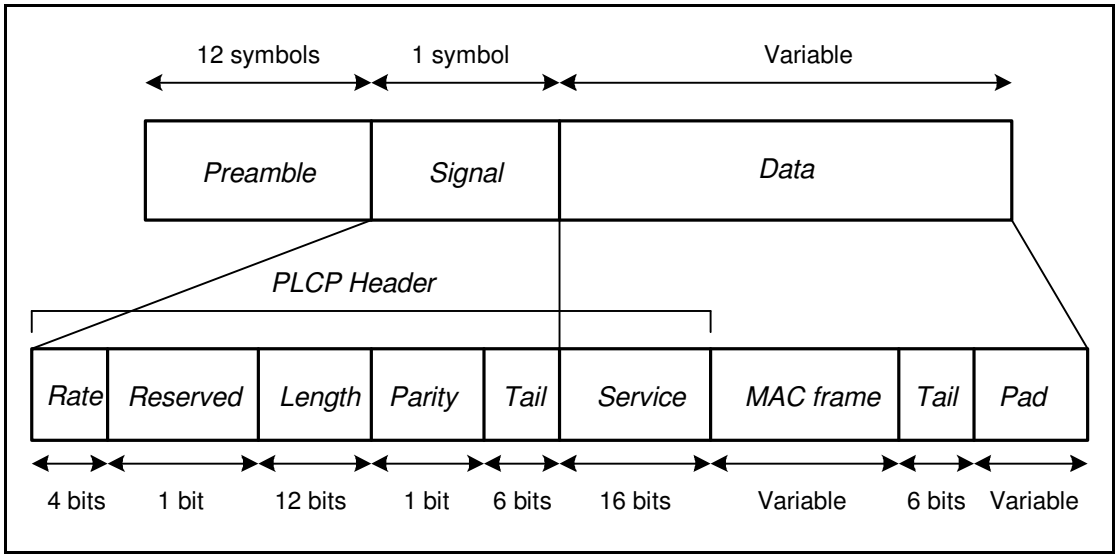
Μπάντα	Εκπεμπόμενη ισχύς	Κεντρική συχνότητα (GHz)
U-NII lower band (5,15 – 5,25 GHz)	40 mW	5,180
		5,200
		5,220
		5,240
U-NII mid – band (5,25 – 5,35 GHz)	200 mW	5,260
		5,280
		5,300
		5,320
U-NII upper band (5,725 – 5,825 GHz)	800 mW	5,745
		5,765
		5,785
		5,805

Πίνακας 2.7: Διαθέσιμα κανάλια του φυσικού στρώματος 802.11α στις ΗΠΑ. Η εκπεμπόμενη ισχύς είναι η μέγιστη επιτρεπτή τιμή με κέρδος κεραίας 6 dBi

Τέλος, σημειώνεται ότι τα κανάλια πρέπει να ικανοποιούν μία συγκεκριμένη μάσκα ισχύος, ώστε να περιορίζονται οι παρεμβολές εκτός του εύρους τους.

2.5.3 OFDM – Υπόστρωμα PLCP

Η μορφή του πλαισίου του υποστρώματος PLCP του 802.11a φαίνεται στο Σχήμα 2.19. Ακολουθεί περιγραφή των διαφόρων τμημάτων του πλαισίου.



Σχήμα 2.19: Πλαίσιο PLCP υποστρώματος του φυσικού στρώματος 802.11α

Preamble

Το πρώτο τμήμα του πλαισίου είναι το Preamble, που αποτελείται από 12 σύμβολα και χρησιμεύει κυρίως για την επίτευξη συγχρονισμού μεταξύ πομπού και δέκτη. Επίσης χρησιμεύει στον δέκτη και για άλλους λόγους, όπως το «κλείδωμα» στο σήμα ή την επιλογή καλύτερης λήψης αν χρησιμοποιούνται περισσότερες της μίας κεραίες.

Signal

Το τμήμα Signal περιέχει τμήμα της επικεφαλίδας του πλαισίου. Πιο συγκεκριμένα περιέχει τα πεδία Rate, Reserved, Length, Parity και Tail. Το μήκος του είναι 1 σύμβολο ή 24 bits

Rate

Στο πεδίο Rate κωδικοποιείται ο ρυθμός μετάδοσης. Υπάρχουν 8 διαθέσιμοι ρυθμοί μετάδοσης που κωδικοποιούνται κατάλληλα στα 4 bits του πεδίου αυτού.

Reserved

Το πεδίο Reserved είναι διαθέσιμο για μελλοντική χρήση και τίθεται πάντα «0».

Length

Το πεδίο Length περιέχει τον αριθμό των bytes του ενσωματωμένου MAC πλαισίου.

Parity

Το πεδίο Parity είναι bit άρτιας ισοτιμίας για τα πρώτα 16 bit του τμήματος Signal.

Tail

Το πεδίο Tail περιέχει έξι bits «0» που χρησιμεύουν στον συνελικτικό κώδικα που χρησιμοποιείται.

Data

Το τμήμα Data του πλαισίου PLCP περιέχει το πλαίσιο MAC και είναι μεταβλητού μήκος. Επίσης περιέχει το πεδίο Service της επικεφαλίδας του PLCP πλαισίου, το πεδίο Tail και το πεδίο Pad.

Service

Το πεδίο Service, που ανήκει στην επικεφαλίδα του πλαισίου PLCP, έχει όλα τα bits μηδενικά. Κάποια χρησιμοποιούνται για το ανακάτωμα (scrambling) των bits του πλαισίου MAC, ενώ τα υπόλοιπα είναι διαθέσιμα για μελλοντική χρήση.

Tail

Το πεδίο Tail χρησιμοποιείται από τον συνελικτικό κώδικα διόρθωσης λαθών.

Pad

Το πεδίο Pad είναι μεταβλητού μήκους και χρησιμεύει στο να κάνει το μήκος του τμήματος Data κατάλληλο για μεταφορά, όπως απαιτεί η εφαρμογή της OFDM στο 802.11a.

2.5.4 OFDM – Υπόστρωμα PMD

Στο PMD υπόστρωμα χρησιμοποιούνται διάφορα σχήματα διαμόρφωσης και προβλέπεται υποστήριξη για ρυθμούς μετάδοσης 6 μέχρι και 54 Mbps. Σε κάθε περίπτωση το φυσικό στρώμα μεταδίδει 250000 bit/sec στα 48 υποκανάλια που διατίθενται για μετάδοση δεδομένων. Αυτό που μεταβάλλεται είναι ο αριθμός των bits ανά σύμβολο, που σε συνδυασμό με τα επιπλέον bits λόγω της συνελικτικής κωδικοποίησης που προστίθενται καθορίζει τελικά τον πραγματικό ρυθμό μετάδοσης δεδομένων. Στον Πίνακα 2.8 φαίνονται οι διάφοροι ρυθμοί μετάδοσης και τα αντίστοιχα σχήματα κωδικοποίησης και διαμόρφωσης.

Ρυθμός Μετάδοσης (Mbps)	Διαμόρφωση, Ρυθμός Κώδικα	Bits ανά Σύμβολο	Bits Δεδομένων ανά Σύμβολο
6	BPSK, 1/2	48	24
9	BPSK, 3/4	48	36
12	QPSK, 1/2	96	48
18	QPSK, 3/4	96	72
24	16-QAM, 1/2	192	96
36	16-QAM, 3/4	192	144
48	64-QAM, 2/3	288	192
54	64-QAM, 3/4	288	216

Πίνακας 2.8: Ρυθμοί μετάδοσης και σχήματα διαμόρφωσης / κωδικοποίησης του φυσικού στρώματος 80211a

Κάθε σχήμα διαμόρφωσης που αναφέρεται στον Πίνακα 2.8 χρησιμοποιείται σε κάθε υποκανάλι, ενώ κάθε σύμβολο συμπεριλαμβάνει τα 48 υποκανάλια κάθε καναλιού που

μεταφέρουν δεδομένα. Αυτό, σε συνδυασμό με τα bits που χρησιμοποιούνται για διόρθωση λαθών, δίνει τελικά των πλήθος των bits δεδομένων που μεταφέρει κάθε σύμβολο.

Τέλος, στον Πίνακα 2.9 φαίνονται μερικές ακόμα παράμετροι του 802.11a. Όπως και στα υπόλοιπα φυσικά στρώματα, υπάρχουν κι εδώ αρκετές παράμετροι που μπορούν να μεταβληθούν προκειμένου να επιτευχθεί η επιθυμητή συμπεριφορά στα διάφορα μέρη του συστήματος.

Παράμετρος	Τιμή
Μέγιστο μήκος πλαισίου MAC	4095 bytes
Slot time	9 μsec
SIFS time	16 μsec
Contention window size	15 έως 1023 σχισμές
Preamble duration	20 μsec
PLCP header duration	4 μsec

Πίνακας 2.9: Παράμετροι του φυσικού στρώματος 802.11α

2.6 Διαχείριση στα Πρότυπα 802.11

Η αποτελεσματική διαχείριση ενός δικτύου είναι απαραίτητη για να εξασφαλιστεί η απρόσκοπτη λειτουργία του και η γρήγορη διόρθωση των προβλημάτων που μπορεί να παρουσιαστούν. Αυτό ισχύει και στην περίπτωση των ασύρματων δικτύων. Στα πρότυπα 802.11 ορίζεται ξεχωριστό μοντέλο διαχείρισης του δικτύου, το οποίο πρέπει να προσφέρει συγκεκριμένες υπηρεσίες και επιτελεί διάφορες λειτουργίες. Αυτό είναι το θέμα του πρώτου μέρους του κεφαλαίου αυτού.

Τέλος, παρουσιάζονται διάφορες παράμετροι του δικτύου που επηρεάζουν τη λειτουργία του. Ο διαχειριστής είναι σε θέση αλλάζοντας κάποιες από αυτές να βελτιστοποιήσει την απόδοση του δικτύου, ανάλογα πάντα με το τι είναι επιθυμητό. Αυτή η πλευρά της διαχείρισης αποκτά ιδιαίτερο ενδιαφέρον όσο περνάει ο καιρός και οι απαιτήσεις από τα ασύρματα δίκτυα αυξάνουν . Γίνεται έτσι απαραίτητη η επίτευξη της μέγιστης απόδοσης του εκάστοτε δικτύου, κάτι που μπορεί να επιτευχθεί με κατάλληλη ρύθμιση των παραμέτρων αυτών.

2.6.1 Μοντέλο διαχείρισης στρωμάτων του προτύπου 802.11

2.6.1.1 Αρχιτεκτονική

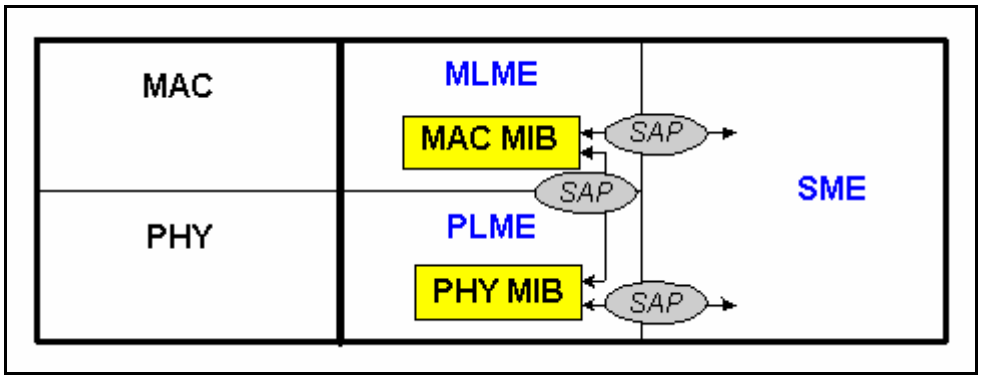
Το πρότυπο 802.11 ορίζει για το σκοπό της διαχείρισης τρεις οντότητες:

- Οντότητα διαχείρισης φυσικού στρώματος, PLME (Physical Layer Management Entity).
- Οντότητα διαχείρισης στρώματος MAC, MLME (MAC Layer Management Entity).
- Οντότητα διαχείρισης συστήματος, SME (System Management Entity).

Οι τρεις αυτές οντότητες συνεργάζονται ανταλλάσσοντας μηνύματα μέσω συγκεκριμένων σημείων πρόσβασης υπηρεσίας (Service Access Point – SAP) που υπάρχουν

μεταξύ τους. Οι παραπάνω τρεις οντότητες επικοινωνούν ανά δύο μέσω των αντίστοιχων SAPs.

Τόσο η PLME όσο και η MLME είναι υπεύθυνες για τη διατήρηση των δεδομένων που σχετίζονται με τη διαχείριση των αντίστοιχων στρωμάτων. Σε αυτά τα δεδομένα προσφέρεται πρόσβαση μέσω δύο Management Information Bases (MIBs). Όλα τα παραπάνω φαίνονται καλύτερα στο Σχήμα 2.20.



Σχήμα 2.20: Μοντέλο διαχείρισης στρωμάτων του προτύπου 802.11

Η οντότητα SME μπορεί να θεωρηθεί ότι βρίσκεται σε ένα ξεχωριστό επίπεδο διαχείρισης (management plane), ενώ δεν υπάρχει ακριβής ορισμός της στο 802.11. Πρέπει να είναι παρούσα σε κάθε σταθμό και ρόλος της είναι η συλλογή πληροφοριών διαχείρισης από τις δύο άλλες διαχειριστικές οντότητες και η αλλαγή αυτών. Για να το κάνει αυτό πρέπει φυσικά να υλοποιεί κάποιο κατάλληλο πρωτόκολλο διαχείρισης.

Τα βασικά (primitives) μηνύματα που ανταλλάσσονται μέσω των SAPs είναι της μορφής GET και SET και σκοπό έχουν την συλλογή ή την αλλαγή κάποιων δεδομένων από τις MIBs των διαχειριζόμενων στρωμάτων. Σημειώνεται τέλος ότι το MLME, όπως φαίνεται και στο Σχήμα 5.1, έχει τη δυνατότητα να επικοινωνεί κατευθείαν με το PLME και να αντλεί στοιχεία από τη MIB (Management Information Bases) του. Έτσι η επικοινωνία του SME με το PLME μπορεί να γίνεται μέσω του MLME χωρίς να υπάρχει ξεχωριστό SAP ανάμεσα στα SME και PLME.

2.6.1.2 Υπηρεσίες που υποστηρίζονται από το MLME

Το MLME υποστηρίζει μία σειρά υπηρεσιών που είναι απαραίτητες για τη σωστή λειτουργία του ασυρμάτου δικτύου. Αυτές οι υπηρεσίες είναι οι εξής:

- Διαχείριση πρόσβασης στο δίκτυο.
- Διαχείριση ενέργειας (Power Management).
- Συγχρονισμός μετρητών στο δίκτυο (Timer Synchronization).

Στη συνέχεια παρουσιάζονται αναλυτικά οι παραπάνω υπηρεσίες.

2.6.1.2.1 Διαχείριση πρόσβασης στο δίκτυο.

Η διαδικασία του association ενός κινητού σταθμού με ένα AP είναι απαραίτητη πριν αποκτήσει ο σταθμός πλήρη πρόσβαση στο ασύρματο δίκτυο. Η πρόσβαση όμως ενός σταθμού στο ασύρματο δίκτυο περιλαμβάνει κι άλλα βήματα που προηγούνται του association. Παράλληλα η διαχείριση της πρόσβασης στο δίκτυο είναι απαραίτητη για την υποστήριξη της κινητικότητας (mobility) του σταθμού και παίζει σημαντικό ρόλο στον μηχανισμό της διαπομπής (handoff). Τα βασικά βήματα για να αποκτήσει ένας σταθμός πρόσβαση σε ένα ασύρματο δίκτυο 802.11 είναι τα εξής:

- Scanning: Ο σταθμός πρέπει πρώτα να εντοπίσει το δίκτυο στο οποίο θέλει να αποκτήσει πρόσβαση.
- Joining: Αφού εντοπιστεί το δίκτυο ακολουθεί η διαδικασία του joining. Ο κινητός σταθμός δεν αποκτά ακόμα πρόσβαση στο δίκτυο.
- Authentication: Ο σταθμός πρέπει να πιστοποιήσει την αυθεντικότητά του πριν αποκτήσει πρόσβαση στο δίκτυο.
- Association: Αν όλα τα προηγούμενα βήματα ολοκληρωθούν με επιτυχία ο σταθμός μπορεί να αποκτήσει πρόσβαση στο δίκτυο, ολοκληρώνοντας με επιτυχία το association.

2.6.1.2.1.1 Scanning

Πριν από οτιδήποτε άλλο ο σταθμός πρέπει να εντοπίσει τα υπάρχοντα δίκτυα στην περιοχή που βρίσκεται. Αυτή η διαδικασία ονομάζεται scanning. Υπάρχουν δύο παραλλαγές του scanning, το ενεργό (active scanning) και το παθητικό (passive scanning).

Κατά το passive scanning ο σταθμός δεν εκπέμπει τίποτα, εξοικονομώντας έτσι ενέργεια. Παρακολουθεί τα διαθέσιμα κανάλια ψάχνοντας για πλαίσια Beacon που δηλώνουν την ύπαρξη κάποιου δικτύου. Τα πλαίσια Beacon περιέχουν όλες τις απαραίτητες πληροφορίες για το BSS απ' όπου εκπέμπονται ώστε ο σταθμός να μπορεί να προχωρήσει στο επόμενο βήμα, δηλαδή στη διαδικασία του joining.

Κατά το active scanning ο σταθμός εκπέμπει περιοδικά σε όλα τα διαθέσιμα κανάλια πλαίσια Probe Request που περιέχουν και το SSID (ή network name) του δικτύου που ψάχνει. Για να εκπέμψει αυτό το πλαίσιο ο σταθμός πρέπει να αποκτήσει κανονικά πρόσβαση στο μέσο χρησιμοποιώντας τον αλγόριθμο DCF. Επίσης έχει προβλεφθεί κάποια διαδικασία ώστε να καταλαβαίνει ο σταθμός πότε ένα κανάλι είναι ανενεργό.

Σε κάθε BSS ένας σταθμός είναι υπεύθυνος για να απαντάει σε πλαίσια Probe Request. Σε infrastructure δίκτυα υπεύθυνο είναι το AP, ενώ σε IBSS υπεύθυνος είναι ο σταθμός που εξέπεμψε το τελευταίο πλαίσιο Beacon. Σε κάθε περίπτωση ο σταθμός που

έστειλε το Probe Request θα λάβει ένα ή περισσότερα πλαίσια Probe Response αν υπάρχουν ασύρματα δίκτυα στην περιοχή του.

Όποιο τρόπο scanning κι αν ακολουθεί ο σταθμός, στο τέλος της διαδικασίας θα έχει αποκτήσει κάποιες βασικές πληροφορίες για τα διαθέσιμα δίκτυα. Αυτές φαίνονται στη συνέχεια:

- Beacon Interval: Το χρονικό διάστημα μεταξύ εκπομπής δύο διαδοχικών πλαισίων Beacon.
- DTIM (Delivery Traffic Indication Map) Period: Χρονικό διάστημα που χρησιμοποιείται για το power management.
- Παράμετροι χρονισμού: Δύο πεδία που χρησιμεύουν στο συγχρονισμό του σταθμού με το συγκεκριμένου BSS.
- Παράμετροι φυσικού στρώματος, παράμετροι contention free λειτουργίας και παράμετροι IBSS.
- Βασικοί ρυθμοί που πρέπει να υποστηρίζονται από οποιονδήποτε σταθμό για να αποκτήσει πρόσβαση στο δίκτυο.

2.6.1.2.1.2 Joining

Η διαδικασία του joining δεν δίνει σε έναν σταθμό πρόσβαση στο δίκτυο, απλώς είναι ένα απαραίτητο βήμα στη διαδικασία του association. Ο σταθμός, έχοντας τις απαραίτητες πληροφορίες από το scanning, εξετάζει τις παραμέτρους κάθε BSS και αποφασίζει με ποιο από αυτά θα προχωρήσει τη διαδικασία του association.

Για να επιλέξει ο σταθμός ένα BSS πρέπει φυσικά να μπορεί να λειτουργήσει με τις συγκεκριμένες παραμέτρους του BSS. Επιπλέον, κριτήρια όπως η το επίπεδο ισχύος ή η ένταση του σήματος από κάθε BSS παίζουν ρόλο. Παρόλα αυτά δεν υπάρχει συγκεκριμένη διαδικασία επιλογής ενός δικτύου έναντι κάποιου άλλου. Η επιλογή γίνεται εσωτερικά στο σταθμό και εξαρτάται από τον εκάστοτε κατασκευαστή.

2.6.1.2.1.3 Authentication

Αφού ο σταθμός επιλέξει σε ποιο BSS θέλει να προσχωρήσει (joining) πρέπει να ακολουθήσει τη διαδικασία του authentication. Η διαδικασία αυτή είναι εξαιρετικά σημαντική στη διατήρηση στης ασφάλειας στα ασύρματα δίκτυα, εφόσον δεν υπάρχουν ουσιαστικά φυσικοί περιορισμοί για κάποιον που θέλει να αποκτήσει πρόσβαση σε ένα δίκτυο.

Η διαδικασία αυτή έχει μεγαλύτερη σημασία σε infrastructure δίκτυα εφόσον το authentication είναι μονόδρομο και όχι αμφίδρομο. Αυτό σημαίνει ότι κάθε σταθμός που θέλει να αποκτήσει πρόσβαση στο δίκτυο πρέπει να πιστοποιήσει τον εαυτό του σε κάποιο

AP, αλλά το AP δεν έχει καμιά υποχρέωση πιστοποίησης. Αυτό εξυπηρετεί τους διαχειριστές του δικτύου που θέλουν να πιστοποιούνται όλοι οι χρήστες που αποκτούν πρόσβαση στο δίκτυο αλλά δημιουργεί πιθανά προβλήματα ασφάλειας. Για παράδειγμα ένα AP μπορεί να στέλνει πλαίσια Beacon ενός δικτύου του οποίου δεν είναι μέρος για να υποκλέψει στοιχεία του authentication από το δίκτυο αυτό.

Υπάρχουν δύο είδη authentication, το Open – System authentication και το Shared – Key authentication.

Open – System authentication

Αυτό το είδος authentication είναι το μόνο που απαιτείται από το πρότυπο 802.11. Στην ουσία δεν πρόκειται για πραγματικό authentication, εφόσον το AP δέχεται την ταυτότητα του σταθμού χωρίς οποιαδήποτε διαδικασία πιστοποίησής της. Το open – system authentication απαιτεί την ανταλλαγή δύο πλαισίων μεταξύ του σταθμού και του AP.

Το πρώτο είναι πλαίσιο management υποτύπου authentication και το στέλνει ο σταθμός στο AP. Το AP, αφού λάβει το πλαίσιο αυτό, χρησιμοποιεί τη MAC διεύθυνση του αποστολέα ως την ταυτότητα του σταθμού. Το πλαίσιο δεν περιέχει καμία επιπλέον πληροφορία για την ταυτότητα του αποστολέα. Περιέχει δύο πεδία. Το ένα είναι ένας αριθμός που ονομάζεται Authentication Transaction Sequence Number και είναι ίσος με 1, εφόσον είναι το πρώτο πλαίσιο που ανταλλάσσεται και το άλλο, που ονομάζεται Authentication Algorithm Identification, είναι ίσο με 0 για να δείξει τη χρήση open system authentication. Το AP απαντάει με ένα παρόμοιο πλαίσιο το οποίο περιέχει επιπλέον έναν κωδικό κατάστασης (Status Code) που συμβολίζει το αποτέλεσμα της πιστοποίησης. Φυσικά στο δεύτερο αυτό πλαίσιο το Authentication Transaction Sequence Number είναι ίσο με 2.

Shared – Key authentication

Αυτός ο τύπος πιστοποίησης ταυτότητας χρησιμοποιεί τον αλγόριθμο WEP. Υπενθυμίζεται ότι το πρότυπο 802.11 δεν θεωρεί υποχρεωτική την υποστήριξη του WEP, άρα αυτός ο τύπος πιστοποίησης μπορεί να μην είναι πάντα διαθέσιμος. Για να λειτουργήσει απαιτεί την ύπαρξη ενός μοιραζόμενου κλειδιού (shared key) από τους σταθμούς. Κατά τη διάρκεια του authentication ανταλλάσσονται τέσσερα πλαίσια μεταξύ του σταθμού και του AP.

Το πρώτο πλαίσιο που στέλνει ο σταθμός στο AP είναι όμοιο με το αντίστοιχο πρώτο πλαίσιο του open – system authentication, μόνο που το Authentication Algorithm Identification είναι ίσο με 1 υποδηλώνοντας τη χρήση του WEP. Το AP απαντά με ένα πλαίσιο ίδιου τύπου. Είναι επιλογή του AP αν θα συνεχίσει τη διαδικασία του authentication ή αν θα τη διακόψει απορρίπτοντας την αίτηση του σταθμού. Σε κάθε περίπτωση το δηλώνει με την κατάλληλη τιμή του Status Code. Αν συνεχίζει η διαδικασία το πλαίσιο περιλαμβάνει

και ένα πεδίο 128 bytes που αποτελεί την πρόκληση προς το σταθμό. Αυτό το κείμενο παράγεται τυχαία από τον αλγόριθμο WEP.

Ο σταθμός απαντά στην πρόκληση στέλνοντας πλαίσιο που περιέχει το τυχαίο κείμενο που έλαβε από το AP. Το πλαίσιο το κρυπτογραφεί με τον αλγόριθμο WEP πριν το στείλει, χρησιμοποιώντας φυσικά το κλειδί που έχει. Τέλος, το AP αφού αποκρυπτογραφήσει το περιεχόμενο του τρίτου πλαισίου και διαπιστώσει ότι το τυχαίο κείμενο που περιέχει είναι το ίδιο με αυτό που είχε στείλει με το δεύτερο πλαίσιο στέλνει το τελικό πλαίσιο στο σταθμό με κατάλληλο Status Code που δηλώνει επιτυχία. Αν για οποιοδήποτε λόγο η απάντηση του σταθμού στην πρόκληση δεν είναι έγκυρη το τελευταίο πλαίσιο περιέχει τον ανάλογο Status Code και η αίτηση authentication του σταθμού απορρίπτεται.

Η διαδικασία του authentication πρέπει οπωσδήποτε να ολοκληρωθεί με επιτυχία για να ακολουθήσει το association, αλλά δεν είναι υποχρεωτικό να ακολουθήσει το association αμέσως μετά. Οι σταθμοί μπορούν να ολοκληρώσουν το authentication με διάφορα AP έτσι ώστε όταν απαιτηθεί association με οποιοδήποτε από αυτά να γίνει χωρίς άλλη καθυστέρηση. Αυτό μπορεί να χρησιμεύσει στην περίπτωση διαπομπής, αν το AP έχει ήδη ολοκληρώσει το authentication με το καινούργιο AP πριν την διαπομπή. Αυτού του είδους το authentication ονομάζεται και pre-authentication.

Το shared – key authentication είναι προφανώς πιο ασφαλές από το open – system authentication αλλά έχει κληρονομήσει τις αδυναμίες που παρουσιάζει ο αλγόριθμος WEP. Στη συνέχεια περιγράφεται ο WEP, τα προβλήματα που έχουν διαπιστωθεί και οι διάφορες λύσεις που έχουν προταθεί.

WEP

Αναφέρθηκε παραπάνω πως ο αλγόριθμος κρυπτογράφησης WEP χρησιμοποιείται για το shared – key authentication. Τα αρχικά WEP σημαίνουν Wired Equivalent Privacy και αυτός ακριβώς είναι ο στόχος του WEP, να προσφέρει δηλαδή ασφάλεια στην ασύρματη μεταφορά των δεδομένων μέχρι το AP. Δεν προβλέπεται καμία ασφάλεια από το AP προς το ενσύρματο δίκτυο.

2.6.1.2.1.4 Association

Το association του σταθμού με το AP είναι το τελικό βήμα για να αποκτήσει ο σταθμός πρόσβαση στο δίκτυο. Το association απαιτεί την ανταλλαγή δύο πλαισίων μεταξύ σταθμού και AP.

Το πρώτο πλαίσιο το στέλνει ο σταθμός και είναι τύπου Association Request. Σε περίπτωση που δεν έχει προηγηθεί authentication το AP απαντά με ένα πλαίσιο De authentication. Σε περίπτωση που το authentication έχει γίνει κανονικά το AP αποφασίζει αν

θα ολοκληρώσει ή όχι τη διαδικασία. Δεν υπάρχει ούτε εδώ κάποιος προβλεπόμενος από το 802.11 τρόπος απόφασης αλλά είναι θέμα της συγκεκριμένης υλοποίησης. Αν τελικά η αίτηση γίνει δεκτή, το AP απαντά με ένα πλαίσιο Association Response με το Status Code ίσο με «0» και ένα SSID, που χρησιμεύει για να αναγνωρίζεται ο σταθμός. Επίσης, γνωστοποιεί την ύπαρξη του σταθμού στο δικό του BSS στο σύστημα διανομής (Distribution System – DS) ώστε να δρομολογούνται σωστά πλαίσια που προορίζονται για τον σταθμό αυτόν. Σε περίπτωση που η αίτηση απορριφθεί, το πλαίσιο Association Request περιέχει μόνο τον ανάλογο Status Code.

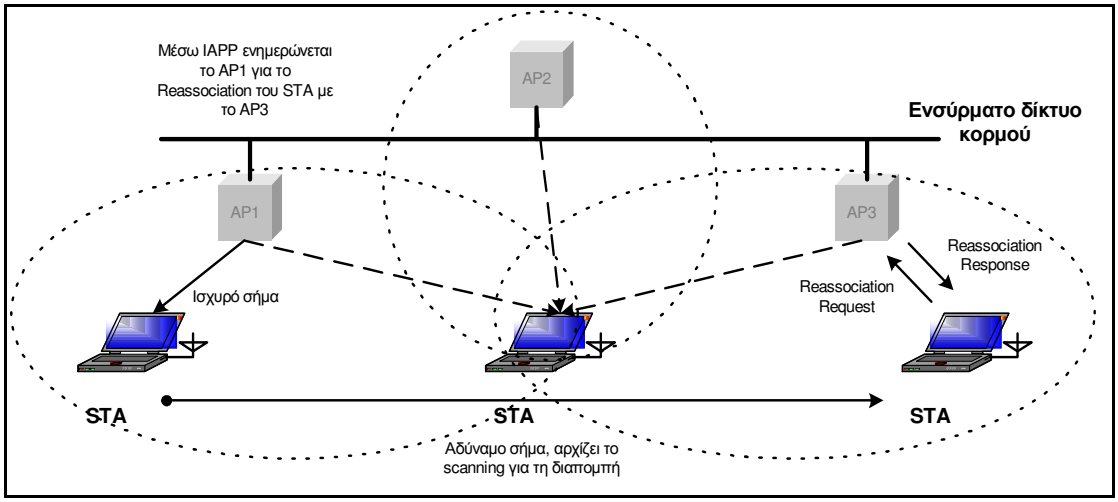
2.6.1.2.1.5 Μηχανισμός Διαπομπής (Handoff)

Υπάρχουν 3 διαφορετικά είδη κινητικότητας στο πρότυπο 802.11

- No transition: Ο κινητός σταθμός δεν κινείται ή κινείται στα όρια του ίδιου BSS.
- BSS transition: Ο κινητός σταθμός μετακινείται μεταξύ διαφορετικών BSS, εντός των ορίων όμως του ίδιου ESS.
- ESS transition: Ο κινητός σταθμός μετακινείται μεταξύ BSS που ανήκουν σε διαφορετικά ESS.

Το 802.11 δεν υποστηρίζει διατήρηση της σύνδεσης ανωτέρων στρωμάτων (για παράδειγμα IP) στην περίπτωση του ESS transition. Για να γίνει αυτό θα πρέπει να χρησιμοποιηθεί κάποιος άλλος μηχανισμός, όπως το Mobile IP.

Αντίθετα, υποστηρίζεται η διατήρηση της σύνδεσης στην περίπτωση του BSS transition μέσω ενός μηχανισμού Re-association, οπότε ο κινητός σταθμός επαναλαμβάνει τη διαδικασία του association με το νέο AP. Η διαδικασία της διαπομπής μπορεί να περιγραφεί καλύτερα με τη βοήθεια του Σχήματος 2.21.



Σχήμα 2.21: Μηχανισμός διαπομπής στο 802.11

Καθώς ο σταθμός (STA) κινείται προς τα όρια της περιοχής κάλυψης του AP1 παρατηρεί την πτώση της ισχύος του σήματος μέσω των πλαισίων Beacon που στέλνει περιοδικά το AP1 και αρχίζει να ψάχνει (με passive ή active scanning) για AP με δυνατότερο σήμα. Στο παράδειγμα του Σχήματος 2.21 ο STA θα λάβει πλαίσια (Beacon ή Probe Response, ανάλογα με το είδος του scanning) από το AP2 και το AP3. Υποθέτοντας ότι το σήμα από το AP3 είναι δυνατότερο, ο STA θα ξεκινήσει τη διαδικασία του Re-association με το AP3.

Ο STA στέλνει στο AP3 πλαίσιο Re-association Request. Η μόνη διαφορά του πλαισίου αυτού από το πλαίσιο Association Request είναι ότι περιέχει τη διεύθυνση του προηγούμενου AP (AP1). Το AP3 απαντάει με πλαίσιο Re-association Response. Αν η διαδικασία ολοκληρωθεί χωρίς πρόβλημα το AP3 πρέπει να επικοινωνήσει με το AP1 και να του γνωστοποιήσει ότι ο STA ανήκει πλέον στο δικό του BSS. Η επικοινωνία μεταξύ AP's γίνεται μέσω ενός πρωτοκόλλου IAPP (Inter Access Point Protocol) το οποίο όμως δεν έχει ακόμα προτυποποιηθεί και είναι θέμα υλοποίησης του συγκεκριμένου κατασκευαστή. Προφανώς η επικοινωνία αυτή γίνεται μέσω του ενσύρματου δικτύου (Ethernet) στο οποίο είναι συνδεδεμένα τα AP's. Σημειώνεται πάντως πως δεν είναι ευθύνη του STA να ειδοποιήσει το παλιό AP για την διαπομπή.

Μετά το Re-association το AP1 στέλνει όσα αποθηκευμένα πλαίσια έχει και προορίζονται για το STA στο AP3 και τερματίζει το association με το STA. Πλέον όλα τα πλαίσια από και προς το STA θα επεξεργάζονται από το AP3. Επαναλαμβάνεται ότι τα AP's του παραδείγματος ανήκουν στο ίδιο ESS.

2.6.1.2.2 Διαχείριση Ενέργειας

Έχει ήδη τονιστεί η σημασία που δίνεται στα ασύρματα δίκτυα για την εξοικονόμηση ενέργειας, που συνεπάγεται μεγαλύτερο χρόνο αυτονομίας των κινητών σταθμών που λειτουργούν με μπαταρία. Για να επιτευχθεί αυτό πρέπει ο πομποδέκτης κάθε σταθμού να λειτουργεί σε συγκεκριμένα χρονικά διαστήματα και για όσο το δυνατόν λιγότερο χρόνο. Όταν ένας σταθμός έχει τον πομποδέκτη του απενεργοποιημένο λέμε ότι βρίσκεται σε λειτουργία εξοικονόμησης ενέργειας (Power Saving mode – PS mode), ενώ όταν ο πομποδέκτης είναι ενεργοποιημένος ο σταθμός χαρακτηρίζεται ως ενεργός (active). Ο μηχανισμός διαχείρισης ενέργειας διαφέρει μεταξύ infrastructure και IBSS δικτύων και γι' αυτό εξετάζεται κάθε περίπτωση ξεχωριστά.

2.6.1.2.2.1 Διαχείριση Ενέργειας σε Infrastructure δίκτυα

Στα infrastructure δίκτυα είναι πολύ πιο αποτελεσματική η διαχείριση ενέργειας από ότι στα IBSS. Το AP είναι σε θέση να γνωρίζει κάθε στιγμή ποιος σταθμός είναι ενεργός και ποιος όχι και να αποθηκεύει όσα πλαίσια προορίζονται σε σταθμούς που βρίσκονται σε PS mode για να τα παραδώσει σε επόμενη χρονική στιγμή. Επιπλέον, το AP είναι πάντα ενεργό, εφόσον θεωρείται ότι έχει μόνιμη παροχή ενέργειας. Έτσι το AP διατηρεί αποθηκευμένα πλαίσια και ενημερώνει περιοδικά τους παραλήπτες σταθμούς για το γεγονός αυτό.

Μία σημαντική παράμετρος στην διαδικασία αυτή είναι το χρονικό διάστημα μετά την παρέλευση του οποίου πρέπει ο σταθμός να εγκαταλείψει το PS mode για να ελέγξει αν υπάρχουν πλαίσια αποθηκευμένα στο AP που προορίζονται για αυτόν. Αυτό το διάστημα ονομάζεται Listen Interval και είναι ακέραιο πολλαπλάσιο της περιόδου εκπομπής πλαισίων Beacon από το AP. Αυτή η παράμετρος είναι μέρος του Association του σταθμού με το AP. Μεγάλη τιμή του Listen Interval εξοικονομεί ενέργεια στους σταθμούς αλλά απαιτεί μεγαλύτερους καταχωρητές στο AP. Αν ο σταθμός δεν ελέγχει αν υπάρχουν αποθηκευμένα πλαίσια για αυτόν στο AP τουλάχιστον κάθε Listen Interval, τότε αυτά μπορεί να απορριφθούν από το AP χωρίς περαιτέρω προειδοποίηση.

Στην περίπτωση unicast πλαισίων η παράμετρος AID (Association ID) αποτελεί το αναγνωριστικό κάθε σταθμού. Το AP περιοδικά εκπέμπει με τα πλαίσια Beacon μία ακολουθία 2008 bits που ονομάζεται TIM (Traffic Indication Map). Κάθε bit του TIM αντιστοιχεί σε ένα AID. Με αυτόν τον τρόπο οι σταθμοί ειδοποιούνται ότι υπάρχουν πλαίσια που πρέπει να τους παραδοθούν. Σημειώνεται ότι συνήθως εκπέμπεται μόνο το τμήμα του TIM που χρειάζεται για εξοικονόμηση χωρητικότητας του δικτύου.

Για την λήψη των πλαισίων αυτών οι σταθμοί στέλνουν πλαίσια PS-Poll στο AP. Κάθε πλαίσιο PS-Poll είναι αίτηση για αποστολή ενός αποθηκευμένου πλαισίου από το AP στον αποστολέα του PS-Poll πλαισίου. Αν υπάρχουν περισσότερα αποθηκευμένα πλαίσια, ο ενδιαφερόμενος σταθμός πρέπει να τα παραλάβει εκπέμποντας ισάριθμα PS-Poll πλαίσια. Κάθε πλαίσιο που παραδίδεται στο σταθμό πρέπει να επιβεβαιώνεται με αντίστοιχο πλαίσιο ACK από αυτόν. Αφού ένας σταθμός εκπέμψει το πρώτο PS-Poll πλαίσιο πρέπει να παραμείνει ενεργός μέχρι να πάρει όσα πλαίσια υπάρχουν για αυτόν ή μέχρι να δει το bit που αντιστοιχεί σε αυτόν στο TIM να είναι ίσο με «0». Μετά μπορεί να περάσει πάλι σε PS mode.

Το AP χρησιμοποιεί μια συγκεκριμένη συνάρτηση (Aging Function) για να αποφασίσει πότε ένα πλαίσιο είναι αρκετά παλιό ώστε να απορριφθεί. Ο μόνος περιορισμός είναι ότι τα αποθηκευμένα πλαίσια πρέπει να διατηρούνται στο AP τουλάχιστον για χρόνο Listen Interval. Πέρα από αυτόν τον περιορισμό κάθε κατασκευαστής μπορεί να χρησιμοποιήσει όποια Aging Function επιθυμεί.

Στην περίπτωση των multicast και broadcast πλαισίων ακολουθείται παρόμοια διαδικασία. Το AID που αντιστοιχεί σε τέτοια πλαίσια όταν αποθηκεύονται είναι το μηδενικό και το AP αποθηκεύει τα πλαίσια αυτά αν οποιοσδήποτε από τους παραλήπτες είναι σε PS mode. Για την παράδοση των πλαισίων αυτών χρησιμοποιείται ένα ειδικό TIM που ονομάζεται DTIM (Delivery Traffic Indication Map). Αυτό εκπέμπεται ως μέρος ενός πλαισίου Beacon μετά την εκπομπή ενός συγκεκριμένου αριθμού τέτοιων πλαισίων. Το διάστημα αυτό ονομάζεται DTIM Period. Αμέσως μετά την εκπομπή του DTIM το AP αρχίζει να εκπέμπει τα αποθηκευμένα multicast και broadcast πλαίσια. Το AP έχει τη δυνατότητα να καθυστερήσει την αποστολή unicast πλαισίων προκειμένου να ολοκληρώσει τη διαδικασία αυτή. Σε περίπτωση που η εξοικονόμηση ενέργειας είναι πολύ σημαντική, οι σταθμοί μπορούν να αγνοήσουν το DTIM Period και να μην λαμβάνουν καθόλου τα αποθηκευμένα multicast και broadcast πλαίσια, τα οποία φυσικά θα απορρίπτονται τελικά από το AP.

Σημειώνεται ότι σε όλες τις διαδικασίες παράδοσης αποθηκευμένων πλαισίων που αναφέρθηκαν παραπάνω οι σταθμοί και το AP πρέπει να παίρνουν τον έλεγχο του μέσου μετάδοσης με χρήση των καθιερωμένων μεθόδων πριν εκπέμψουν οποιοδήποτε πλαίσιο.

2.6.1.2.2.2 Διαχείριση Ενέργειας σε IBSS δίκτυα

Η διαχείριση ενέργειας δεν είναι τόσο αποτελεσματική σε IBSS δίκτυα. Οι σταθμοί δεν μπορούν να μένουν σε PS mode τόσο πολύ όσο σε infrastructure δίκτυα. Λόγω της αποκεντρωμένης φύσης των IBSS δικτύων, είναι καθήκον του αποστολέα να βεβαιωθεί ότι ο παραλήπτης είναι ενεργός, πριν του στείλει κάποιο πλαίσιο. Επίσης οι σταθμοί πρέπει να αποθηκεύουν οι ίδιοι πλαίσια τα οποία προορίζονται για μη ενεργούς παραλήπτες.

Για να ειδοποιηθούν οι σταθμοί να παραλάβουν πλαίσια που προορίζονται για αυτούς χρησιμοποιούνται ATIMs (Announcement Traffic Indication Messages). Αυτά μεταδίδονται λίγο μετά από μετάδοση πλαισίων Beacon και όλοι οι σταθμοί πρέπει να είναι ενεργοί για να τα λάβουν. Κάθε σταθμός που έχει αποθηκευμένα πλαίσια και θέλει να τα στείλει σε άλλον σταθμό χρησιμοποιεί ένα ATIM για να ειδοποιήσει τον παραλήπτη να μείνει ενεργός μέχρι να ολοκληρωθεί η διαδικασία.

Μετά από κάθε εκπομπή πλαισίου Beacon ακολουθεί μια περίοδος που ονομάζεται ATIM window. Κατά τη διάρκεια του ATIM window όλοι οι σταθμοί πρέπει να παραμείνουν ενεργοί. Αν η εκπομπή του πλαισίου Beacon καθυστερήσει, η διάρκεια του ATIM window μειώνεται ανάλογα.

Κατά τη διάρκεια του ATIM window μόνο συγκεκριμένα είδη πλαισίων επιτρέπεται να στέλνονται. Αυτά είναι τα Beacon, RTS, CTS, ACK και φυσικά τα ATIM, τα οποία

εκπέμπονται μόνο τότε, για να είναι βέβαιο ότι ο παραλήπτης θα είναι ενεργός. Μετά την παρέλευση του ATIM window μόνο οι σταθμοί που δεν χρειάζεται να μεταδώσουν ούτε να λάβουν κάποιο πλαίσιο επιτρέπεται να περάσουν σε PS mode. Όλοι οι υπόλοιποι πρέπει να μείνουν ενεργοί μέχρι την παρέλευση και του επομένου ATIM window.

Αφού τελειώσει το ATIM window μεταδίδονται πρώτα τα broadcast και multicast πλαίσια, τα οποία μάλιστα, για εξοικονόμηση χρόνου, δεν απαιτούν επιβεβαιώσεις. Στη συνέχεια κάθε σταθμός μεταδίδει unicast πλαίσια για τα οποία είχε στείλει ATIM's κατά τη διάρκεια του ATIM window. Αν κάποιος σταθμός δεν προλάβει να στείλει πλαίσιο που είχε ανακοινώσει με ATIM πρέπει να επαναλάβει τη διαδικασία από την αρχή στο επόμενο ATIM window.

Όπως αναφέρθηκε οι σταθμοί είναι υπεύθυνοι για την αποθήκευση πλαισίων. Ο μόνος περιορισμός που υπάρχει σχετικά με την απόρριψή τους είναι ότι πρέπει να διατηρηθούν στη μνήμη του σταθμού τουλάχιστον για μια περίοδο εκπομπής πλαισίου Beacon.

2.6.1.2.3 Συγχρονισμός μετρητών

Στα ασύρματα δίκτυα είναι πολύ σημαντικό όλοι οι κόμβοι να είναι συγχρονισμένοι. Αυτό είναι απαραίτητο για τη διαδικασία πρόσβασης στο μέσο μετάδοσης, για την διαχείριση ενέργειας αλλά και για σχεδόν όλες τις λειτουργίες που απαιτούνται. Αποκτά ακόμα μεγαλύτερη σημασία σε Frequency Hopping δίκτυα, οπότε πρέπει οι σταθμοί να περνάνε από φέρουσα σε φέρουσα σε συγκεκριμένα χρονικά διαστήματα.

Κάθε σταθμός σε ένα BSS διατηρεί ένα αντίγραφο της TSF (Timing Synchronization Function). Αυτή η συνάρτηση είναι ουσιαστικά ένα τοπικό ρολόι συγχρονισμένο τους υπόλοιπους σταθμούς στο BSS. Βασίζεται σε ρολόι του 1 MHz και μετράει milliseconds. Η TSF μεταδίδεται μέσω των πλαισίων Beacon σε τακτά χρονικά διαστήματα. Όπως και στη διαχείριση ενέργειας, υπάρχουν διαφορές μεταξύ Infrastructure και IBSS δικτύων.

2.6.1.2.3.1 Συγχρονισμός Μετρητών σε Infrastructure δίκτυα

Το AP είναι υπεύθυνο για τη διατήρηση της σωστής τιμής της TSF και τη μετάδοσή της στους υπόλοιπους σταθμούς. Οι σταθμοί δέχονται ως έγκυρη την τιμή της TSF που μεταδίδει το AP και ανανεώνουν κατάλληλα τα τοπικά αντίγραφά της. Η μετάδοση της τιμής της TSF γίνεται από το AP σαν πεδίο του πλαισίου Beacon. Το μόνο που έχουν να κάνουν οι σταθμοί είναι να διορθώνουν τα τοπικά αντίγραφα της TSF με βάση το περιεχόμενο του πλαισίου Beacon, προσθέτοντας και κάποια αντιστάθμιση (offset) για το χρόνο λήψης και επεξεργασίας του πλαισίου. Ακόμα λοιπόν και αν χάσουν κάποια πλαίσια Beacon, έχουν το αντίγραφο της TSF για να διατηρούν το συγχρονισμό. Η TSF μεταδίδεται επίσης και με τα

Probe Response πλαίσια, για να συγχρονίζει τα ρολόγια των σταθμών που επιθυμούν να αποκτήσουν πρόσβαση στο δίκτυο.

2.6.1.2.3.2 Συγχρονισμός Μετρητών σε IBSS δίκτυα

Σε αυτά τα δίκτυα η διαδικασία συγχρονισμού είναι δυσκολότερη. Δεν υπάρχει κάποιος συγκεκριμένος σταθμός που να μεταδίδει συνέχεια πλαίσια Beacon και να συγχρονίζει τους υπόλοιπους στη δική του TSF. Τα πλαίσια Beacon μπορούν να μεταδίδονται από οποιονδήποτε σταθμό, αλλά πρέπει να μεταδίδονται σε ακριβή χρονικά διαστήματα, που ονομάζονται TBTT (Target Beacon Transmission Time).

Καθώς πλησιάζει η ώρα εκπομπής των πλαισίων Beacon, όλοι οι σταθμοί αναβάλλουν όλες τις υπόλοιπες εκπομπές τους για να είναι πιο εύκολη η πρόσβαση στο μέσο. Στη συνέχεια παράγεται σε κάθε σταθμό ένα τυχαίο χρονικό διάστημα, που ονομάζεται backoff timer, και είναι η καθυστέρηση από την παρούσα χρονική στιγμή μέχρι την εκπομπή του πλαισίου Beacon. Αυτό το διάστημα είναι το πολύ όσο το διπλάσιο μέγεθος του χρονικού παραθύρου διεκδίκησης για πρόσβαση στο μέσο. Όταν ο σταθμός με το μικρότερο backoff timer εκπέμψει πρώτος το πλαίσιο Beacon ενσωματώνει ένα αντίγραφο της δικής του TSF. Οι υπόλοιποι σταθμοί ακυρώνουν τη δική τους εκπομπή πλαισίου Beacon και ανανεώνουν τις TSFs τους, λαμβάνοντας υπόψη και το χρόνο λήψης και επεξεργασίας του πλαισίου.

Σε IBSS δίκτυα υπάρχουν πιο πολύπλοκοι κανόνες όσο αναφορά την αποδοχή της TSF που λαμβάνεται κάθε φορά. Σκοπός είναι ο συγχρονισμός όλων των σταθμών με αυτόν που έχει το πιο γρήγορο ρολόι και αυτό λαμβάνεται υπόψη κατά την ανανέωση της TSF.

2.6.2 Βελτιστοποίηση απόδοσης δικτύων 802.11

Όσο εξαπλώνεται η χρήση των ασυρμάτων δικτύων, τόσο αυξάνονται και οι απαιτήσεις από αυτά. Ενώ πριν από λίγα χρόνια ήταν αρκετό το να λειτουργεί το δίκτυο, σήμερα υπάρχουν πολύ πιο αυστηρά κριτήρια απόδοσης. Για να εξασφαλιστεί ότι ένα ασύρματο δίκτυο καλύπτει τις ανάγκες για τις οποίες στήθηκε πρέπει ο διαχειριστής του να επέμβει στη λειτουργία του.

Η επέμβαση σε φυσικό επίπεδο, με την τοποθέτηση για παράδειγμα εξωτερικών κεραιών ή ενισχυτών σήματος, είναι πιο δύσκολη και μπορεί εύκολα να παραβιάσει τους διάφορους περιορισμούς που έχουν τεθεί από τις κατά τόπους ελεγκτικές αρχές. Αντίθετα, η παρέμβαση σε επίπεδο παραμέτρων του δικτύου μπορεί να βελτιώσει αρκετά την απόδοση του δικτύου, αρκεί φυσικά να είναι ξεκάθαρο σε ποιους τομείς είναι επιθυμητή η βελτιστοποίηση. Στη συνέχεια παρουσιάζονται κάποιες παράμετροι που μπορεί ο διαχειριστής του δικτύου να μεταβάλλει, επηρεάζοντας την λειτουργία του.

2.6.2.1 Περίοδος εκπομπής πλαισίων Beacon

Τα πλαίσια Beacon παίζουν πολύ σημαντικό ρόλο στην λειτουργία ενός ασυρμάτου δικτύου εξυπηρετώντας πολλούς σκοπούς, όπως η ανακοίνωση της ύπαρξης του δικτύου για τη διαδικασία του passive scanning και η μεταφορά παραμέτρων όπως οι TIM και DTIM. Μειώνοντας την περίοδο εκπομπής των πλαισίων Beacon διευκολύνεται ο εντοπισμός του δικτύου από τους κινητούς σταθμούς αλλά και η διαδικασία της διαπομπής, εφόσον χρησιμοποιείται σαν κριτήριο απόφασης η ισχύς του σήματος κατά τη λήψη των Beacons. Παρόλα αυτά συχνότερη εκπομπή πλαισίων Beacon σημαίνει μικρότερη διέλευση δεδομένων από το δίκτυο και μεγαλύτερη δυσκολία πρόσβασης στο μέσο για μετάδοση. Επιπλέον, οι σταθμοί πρέπει να ενεργοποιούν τους πομποδέκτες τους πιο συχνά για τη λήψη των TIM και DTIM, θέμα που θα αναλυθεί εκτενέστερα στη συνέχεια.

2.6.2.2 Κατώφλι RTS

Το κατώφλι αυτό είναι το ελάχιστο μέγεθος του προς μετάδοση πλαισίου που χρησιμοποιεί το μηχανισμό RTS/CTS. Ο μηχανισμός αυτός αναλαμβάνει να κάνει πιο ασφαλής τη μετάδοση, όσο αναφορά την παρεμβολή ενός κρυφού κόμβου (hidden node) κατά τη διάρκειά της. Το κατώφλι που προβλέπεται από το πρότυπο 802.11 είναι τα 2347 bytes, αυτό όμως μπορεί να αλλάξει ανάλογα με τις συνθήκες. Σε περίπτωση που παρατηρούνται πολλές απώλειες πλαισίων λόγω συγκρούσεων, που προκαλούν πολλές αναμεταδόσεις του χαμένου πλαισίου, μείωση του κατωφλίου αυτού μπορεί να βελτιώσει τη διέλευση του δικτύου. Βέβαια ο μηχανισμός RTS/CTS απαιτεί την ανταλλαγή δύο επιπλέον πλαισίων κατά τη μετάδοση κάθε πλαισίου, άρα αυξάνει χωρίς λόγο το φόρτο του δικτύου, αν χρησιμοποιείται συχνότερα χωρίς λόγο.

2.6.2.3 Κατώφλι κατακερματισμού

Το κατώφλι αυτό ορίζει το μέγιστο μέγεθος ενός πλαισίου. Κάθε πλαίσιο μεγαλύτερο κατακερματίζεται σε περισσότερα μικρότερου μεγέθους. Σε περιβάλλον με πολλές παρεμβολές μείωση του κατωφλίου αυτού μπορεί να έχει σαν αποτέλεσμα μεγαλύτερη διέλευση, εφόσον θα αναμεταδίδονται μόνο τα τμήματα που χάθηκαν και όχι ολόκληρο το πλαίσιο. Από την άλλη κατακερματισμός ενός πλαισίου σημαίνει ότι πρέπει να μεταδίδεται ένα πλαίσιο ACK για κάθε τμήμα του αρχικού πλαισίου, κάτι που μειώνει τελικά την πραγματική διέλευση δεδομένων.

2.6.2.4 Όρια επαναμετάδοσης

Όπως έχει αναφερθεί, κάθε σταθμός έχει δύο μετρητές που σχετίζονται με αυτόν. Αυτοί είναι οι Short Retry Limit και Long Retry Limit και αφορούν το πλήθος των προσπαθειών επαναμετάδοσης ενός πλαισίου. Μείωση των ορίων αυτών εξοικονομεί χώρο στη μνήμη κάθε σταθμού, αφού τα προς μετάδοση πλαίσια θα απορρίπτονται γρηγορότερα. Το αν η γρηγορότερη απόρριψη ενός πλαισίου είναι ανεκτή ή όχι εξαρτάται σε μεγάλο βαθμό από την εφαρμογή, αλλά και από τα πρωτόκολλα των ανώτερων στρωμάτων.

2.6.2.5 Listen Interval / DTIM Period

Η παράμετρος αυτή καθορίζει το χρονικό διάστημα που μπορεί να μείνει ένας σταθμός σε power saving mode λειτουργίας και είναι ακέραιο πολλαπλάσιο της περιόδου εκπομπής πλαισίων Beacon. Μετά την παρέλευσή του ο σταθμός πρέπει να ενεργοποιηθεί και να λάβει από το AP τα πλαίσια που προορίζονται γι' αυτόν. Προφανώς, αύξηση της παραμέτρου αυτής αυξάνει πολύ τη διάρκεια ζωής της μπαταρίας των φορητών σταθμών, επιτρέποντάς τους να διατηρηθούν σε λειτουργία για περισσότερο χρόνο. Υπάρχουν όμως και δύο μειονεκτήματα. Το πρώτο είναι ότι το AP μπορεί να εξαντλήσει τη μνήμη που διαθέτει για αποθήκευση πλαισίων αν πολλοί σταθμοί στο BSS έχουν μεγάλο Listen Interval, κάτι που οδηγεί στην απώλεια πλαισίων. Το δεύτερο μειονέκτημα αφορά την καθυστερημένη παράδοση των πλαισίων. Το αν η καθυστέρηση είναι ανεκτή ή όχι εξαρτάται από την εκάστοτε εφαρμογή.

Το DTIM είναι κάτι ανάλογο του Listen Interval, αφορά όμως μόνο τα multicast και broadcast πλαίσια. Σε αντίθεση με το Listen Interval, που μπορεί να είναι διαφορετικό για κάθε σταθμό, το DTIM αφορά όλους τους σταθμούς σε ένα BSS. Κατά τα άλλα ισχύουν και γι' αυτό όσα αναφέρθηκαν για το Listen Interval.

2.6.2.6 Χρονικό παράθυρο ATIM

Αυτή η παράμετρος χρησιμεύει στην εξοικονόμηση ενέργειας στα ad hoc δίκτυα. Είναι το χρονικό διάστημα αμέσως μετά από μία εκπομπή πλαισίου Beacon που οι σταθμοί πρέπει να παραμείνουν ενεργοί. Μικρότερη διάρκεια του παραθύρου αυτού εξοικονομεί ενέργεια, εφόσον κάθε σταθμός θα μπορεί να περνάει γρηγορότερα σε power saving mode λειτουργίας, αλλά ταυτόχρονα απαιτεί αυξημένη μνήμη για αποθήκευση πλαισίων από όλους τους σταθμούς και προκαλεί μεγαλύτερη καθυστέρηση στην παράδοση των πλαισίων.

2.6.2.7 Χρονικά διαστήματα που σχετίζονται με την πρόσβαση στο δίκτυο

Η διαδικασία της πρόσβασης ενός σταθμού στο ασύρματο δίκτυο περιλαμβάνει τέσσερα βήματα (Scanning, Joining, Authentication, Association) και κάθε βήμα έχει κάποια ρολόγια συσχετισμένα με αυτό. Πολλοί κατασκευαστές δίνουν τη δυνατότητα αλλαγής στο χρόνο αναμονής κατά τη διαδικασία του scanning. Στο active scanning αυτός ο χρόνος είναι το διάστημα που αναμένει ο σταθμός απάντηση σε ένα Probe Request πλαίσιο, ενώ στο passive scanning ο χρόνος αναμονής σε κάθε κανάλι για πλαίσια Beacon. Κατά το authentication και το association υπάρχουν επίσης χρόνοι αναμονής ανάμεσα σε κάθε βήμα της διαδικασίας. Σε δίκτυα με πολλούς σταθμούς όλοι οι παραπάνω χρόνοι πρέπει να αυξηθούν, καθώς οι καθυστερήσεις θα είναι μεγαλύτερες.

3. ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ Wi-Fi (ΕΞΟΠΛΙΣΜΟΣ)

Σε αυτό το κεφάλαιο θα γίνει αναφορά στον εξοπλισμό που χρειάζεται να εγκατασταθεί ώστε να λειτουργήσει σωστά ένα οποιοδήποτε δίκτυο Wi-Fi. Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο τρεις είναι οι κύριες τοπολογίες των δικτύων Wi-Fi η **IBSS** (Independent Basic Services Set), **IBSS** (Infrastructure BSS) και η **ESS** (Extended Service Set) όπου η καθεμία από αυτές τις τοπολογίες χρειάζεται τον δικό της εξοπλισμό για να λειτουργεί

3.1 Εξοπλισμός Wi-Fi για την τοπολογία Independent BBS

Όπως αναφέρθηκε και στο κεφάλαιο 2 η τοπολογία IBBS είναι ποιο απλή από όλες τις άλλες και μπορεί να την συναντήσουμε και με το όνομα ad-hoc δίκτυα(Σχήμα 3.1). Χρησιμοποιείται κυρίως σε προσωρινά δίκτυα όπως ένα απλό δίκτυο μέσα στο σπίτι ή και στην περίπτωση που δύο άτομα ή και παραπάνω συναντιούνται σε δημόσια περιοχή και θέλουν να ανταλλάξουν δεδομένα. Ο εξοπλισμός που απαιτείται για την δημιουργία μία τέτοιας τοπολογίας είναι δύο ή και περισσότεροι υπολογιστές Desktop, η lap-top ή και PDAs που χρησιμοποιούνται ως σταθμοί και οπωσδήποτε σε κάθε σταθμό θα πρέπει να είναι συνδεμένος ένας Adapter Wi-Fi.Αυτοί χωρίζονται στις παρακάτω κατηγορίες.

Σχήμα 3.1 Τοπολογία Independent BBS

- **PC Card radio**: που χρησιμοποιούνται κυρίως σε υπολογιστές lap-top. Ονομάζονται και PCMCIA (Personal Computer Memory Card International Association) και διαθέτουν μια ενσωματωμένη κεραία που μπορεί να καλύψει μια μικρή περιοχή. Ορισμένες τέτοιες κάρτες έχουν την δυνατότητα να συνδέσούν μία μεγαλύτερη κεραία πάνω τους για να έχουν μεγαλύτερη εμβέλεια. Η κάρτα PC card radio συνδέεται στην θύρα PCMCIA που διαθέτουν συνήθως οι υπολογιστές lap-top (Σχήμα 3.2). Μπορεί επίσης να χρησιμοποιηθούν στις διάφορες φωτογραφικές μηχανές, σε ακουστικά συστήματα, σε PDAs και σε άλλες κινητές συσκευές υπολογιστών που έχουν ένα Slot για PCMCIA κάρτες.

Σχήμα 3.2: Κάρτες PCMCIA και η χρήση τους.

- **PCI adapter**: Χρησιμοποιούνται στους Desktop υπολογιστές που διαθέτουν PCI slot. Οι κάρτες οι οποίες έχουν ενσωματωμένη κεραία πάνω τους συνδέονται απευθείας στις θύρες PCI που διαθέτει η μητρική του Desktop υπολογιστή. (Σχήμα 3.3)

Σχήμα 3.3: Wi-Fi PCI adapter

- **USB Adapters**: Οι περισσότεροι υπολογιστές δεν διαθέτουν θύρα για κάρτες Wi-Fi PC radios η ελεύθερη θύρα PCI. Το πρόβλημα λύνεται με τις κάρτες USB (Σχήμα 3.4) που συνδέονται κατευθείαν στην θύρα USB του υπολογιστή. Ορισμένες από αυτές τις κάρτες δεν χρειάζονται καλώδιο τροφοδοσίας ρεύματος αφού η τροφοδοσία γίνεται από την θύρα USB του υπολογιστή.

Σχήμα 3.4: Κάρτες USB

- **Compact Flash and Other Small-Client Formats**: Είναι σχεδιασμένες για μικρά PDAs και άλλες κινητές συσκευές υπολογιστών, το 802.11b/Wi-Fi radios μπορεί να κατασκευαστεί σε Compact Flash διαμόρφωση. Αν και κατά πολύ μικρότερες κάρτες από όλες τις υπόλοιπες έχουν την ίδια εμβέλεια και επίδοση. (Σχήμα 3.5)

Σχήμα 3.5: Κάρτα Compact Flash and Other Small-Client Formats

- **Mini-PCI modules και ενσωματωμένη κεραία**: υπάρχει βέβαια και η περίπτωση του ότι δεν θα είναι απαραίτητος κανένας από τους παραπάνω Adapter αφού σε πολλούς υπολογιστές Desktop ή laptop υπάρχει εγκατεστημένος Adapter από τον κατασκευαστή του.

Έπειτα το μόνο που χρειάζονται για να συνδεθούν μεταξύ τους οι υπολογιστές και να δημιουργηθεί ένα ad-hoc δίκτυο είναι να βρίσκονται σε μικρή απόσταση μεταξύ τους και να γίνουν οι κατάλληλες ρυθμίσεις στο λογισμικό που διαθέτουν. Όπως παρατηρούμαι στην τοπολογία Independent BBS δεν υπάρχει Access Point με αποτέλεσμα ορισμένες λειτουργίες του, όπως ο συγχρονισμός και η παραγωγή αναγνωριστικών σημάτων, να εκτελούνται από τους υπολογιστές των χρηστών και κάποιες άλλες λειτουργίες να μην υποστηρίζονται, όπως η αποταμίευση ενέργειας και η αναμετάδοση πλαισίων μεταξύ δυο σταθμών που δεν είναι σε εμβέλεια. Φυσικά όπως αναφέραμε και στην εισαγωγή κάθε συσκευή που χρησιμοποιείται για την δημιουργία ενός δικτύου Wi-Fi θα πρέπει να έχουν την πιστοποίηση Wi-Fi που ορίζεται από την Wi-Fi Alliances.

3.2 Εξοπλισμός τοπολογία Infrastructure BSS

Η παρούσα τοπολογία χρησιμοποιείται για την δημιουργία σταθερών δικτύων Wi-Fi όπως σε μικρές επιχειρήσεις η σε σπίτια που οι χρήστες τους απαιτούν σταθερότητα (Σχήμα 3.6).

Σχήμα 3.6: Τοπολογία Infrastructure BSS

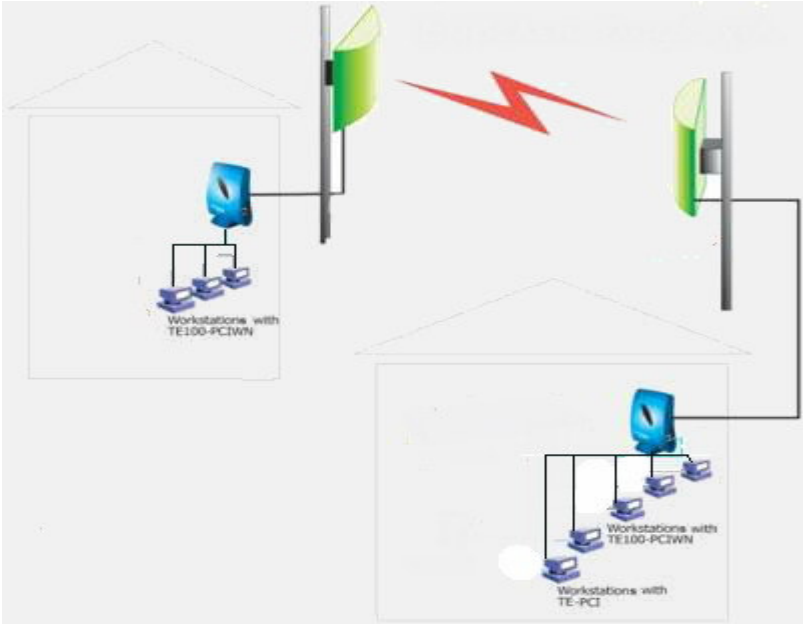
Ο εξοπλισμός που απαιτείται είναι ο ίδιος με την τοπολογία Independent BBS με την μόνη διαφορά που εδώ κρίνεται απαραίτητη η παρουσία ενός Access Point ή Gateway (Σχήμα 3.7).

Σχήμα 3.8: Access Point και Gateway

Η διαφορά του Access Point και της Gateway είναι ότι εκτός από τις λειτουργίες του πρωτοκόλλου 802.11b/a η Gateway ενσωματώνουν ικανότητες πρόσθετου λογισμικού όπως η παροχή NAT (Network Address Translation) και DHCP (Dynamic Host Control Protocol). Οι Gateway μπορούν επίσης να παρέχουν την υποστήριξη VPN, roaming, Firewall και διάφορα επίπεδα ασφάλειας. Τα δίκτυα σε σπίτια ή σε μικρές επιχειρήσεις θα πρέπει να χρησιμοποιούν Gateway. Η χρήση Gateway ή Access Point εξαρτάται από το πως είναι ήδη οργανωμένο το υπάρχον δίκτυο. Δηλαδή αν υπάρχει ήδη ένα ενσύρματο δίκτυο ή ένας συνδυασμός Broadband modem/router, μπορεί να χρησιμοποιηθεί ένα βασικό Access Point γιατί ο ήδη υπάρχον router του ενσύρματου δικτύου ή το hub χειρίζονται τις διευθύνσεις δικτύου NAT ή του DHCP. Αν υπάρχει ένα broadband modem χωρίς router συνδεμένο σε έναν μόνο υπολογιστή, η δεν υπάρχει ενσύρματο δίκτυο ήδη θα πρέπει να χρησιμοποιηθεί μία Wi-Fi Gateway που παρέχει δρομολόγηση NAT και server DHCP. Αν το ήδη συνδεμένο modem ή σύνδεση DSL παρέχει NAT και DHCP υπάρχει η δυνατότητα απενεργοποίησης των δυνατοτήτων αυτών από την Gateway αφού οι διευθύνσεις δικτύων παρέχονται από το modem η την DSL σύνδεση και μόνο μία συσκευή στο δίκτυο μπορεί να παρέχει αυτές τις υπηρεσίες. Για να εγκατασταθεί ένα τέτοιο δίκτυο θα πρέπει καταρχάς ο χειριστή του να επιλέξει το κατάλληλο Access Point ή Gateway με το πρωτόκολλο που επιθυμεί (δηλ. το 802.11b/a) ώστε οι χρήστες του να έχουν το απαραίτητο εύρος ζώνης για της εφαρμογές που χρησιμοποιούν και να κάνει τις κατάλληλες ρυθμίσεις, έπειτα θα πρέπει να δηλώσει όσους υπολογιστές και περιφερειακές συσκευές θα συνδεθούν στο Access Point.

3.3 Εξοπλισμός τοπολογίας Extended Service Set (ESS)

Σε αυτήν τη τοπολογία ο εξοπλισμός είναι ο ίδιος με την τοπολογία Infrastructure BSS αφού στην πραγματικότητα η τοπολογία ESS είναι δύο δίκτυα ή και παραπάνω με τοπολογίες Infrastructure BSS που επικοινωνούν μεταξύ τους. Μια συσκευή που μπορεί να φανεί χρήσιμη είναι οι κεραίες εξωτερικού και εσωτερικού χώρου (Σχήμα 3.9) που συνδέονται με τα Access Point και τα Gateway με την χρήση του κατάλληλου καλωδίου και συμβάλλουν στην αύξηση την εμβέλεια στα δίκτυα Wi-Fi (Σχήμα 3.10).



Σχήμα 3.9: Τοπολογία ESS

Η απόσταση που καλύπτουν εξαρτάται από τον τύπο της κεραίας και κυμαίνεται από 300 μέτρα έως 12 χιλιόμετρα..

Σχήμα 3.10: Κεραίες για δίκτυα Wi-Fi και καλώδιο.

Η χρήση της κατάλληλης κεραίας εξαρτάται από την θέση που βρίσκονται οι τοπολογίες Infrastructure BSS, δηλαδή αν θελήσουμε να επικοινωνήσουν δύο τοπολογίες Infrastructure BSS που βρίσκονται στο ίδιο κτίριο δεν είναι απαραίτητη η χρήση μία κεραίας που έχει μέγιστη εμβέλεια 12 χιλιόμετρα. Όπως στην τοπολογία Infrastructure BSS και εδώ ο χειρίστης του δικτύου θα πρέπει να επιλέξει τα κατάλληλα Access Point και Gateway και να συνδέσει επάνω τους την κατάλληλη κεραία με ειδικό καλώδιο στην υποδοχή που διαθέτουν ώστε να μην υπάρχει απώλεια σήματος και να κάνει τις κατάλληλες ρυθμίσεις πάνω σε αυτά. Έπειτα θα πρέπει να δηλώσει τους υπολογιστές και τις περιφερειακές συσκευές.

Μία κεραία βέβαια μπορεί να χρησιμοποιηθεί και σε μία τοπολογία Infrastructure BSS που οι σταθμοί που επικοινωνούν είναι σε μεγάλη απόσταση και κρίνεται απαραίτητη η χρήση κεραίας για να αυξηθεί η εμβέλεια του Access Point ή της Gateway που συνδέονται οι σταθμοί.

3.4 Άλλες χρήσιμες συσκευές

Όπως είναι φυσικό ένα δίκτυο δεν αποτελείται μόνο από τους υπολογιστές και τα Access Point αλλά και συσκευές όπως οι εκτυπωτές και τα modem. Στα δίκτυα Wi-Fi τέτοιες συσκευές δεν είναι απαραίτητο να συνδέονται με καλώδιο σε έναν υπολογιστή αφού υπάρχουν εκτυπωτές και modem που υποστηρίζουν κάρτες δικτύου Wi-Fi ή και ακόμα να έχουν την δυνατότητα ασύρματης επικοινωνίας από την κατασκευή τους.

4. ΑΣΦΑΛΕΙΑ Wi-Fi

Με την επέκταση των δικτύων Wi-Fi η ανάγκη για μεγαλύτερη ασφάλεια των δεδομένων και στην επικύρωση και του έλεγχου πρόσβασης των χρηστών αυξήθηκαν. Η IEEE σε συνεργασία την Wi-Fi alliances δημιούργησε διάφορες λύσεις όπως τους αλγόριθμους WEP, WPA και WPA2 ώστε να ικανοποιηθούν οι ανάγκες αυτές. Το παρακάτω κεφάλαιο θα γίνει αναφορά για τις λύσεις ασφάλειας στα δίκτυα Wi-Fi και στα τυχόν προβλήματα που έχουν.

4.1. Ο Αλγόριθμος WEP

4.1.1 Περιγραφή του αλγόριθμου WEP

Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP(wired equivalent privacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο.

Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί από όλους τους κατασκευαστές. Μια γρήγορη λύση για την υποκατάστασή του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων.

Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το Access Point κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο Access Point. Αυτή είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών πελατών. Κάποιος εκτός λίστας, με αρκετά δικαιώματα σε ένα UNIX-like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται MAC spoofing attacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (network sniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή Wi-Fi κάρτα και ένα lap-top να φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο Access Point-στόχο. Έτσι, αλλάζοντας την MAC διεύθυνσή του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά.

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Ο αλγόριθμος WEP χρησιμοποιεί τον κώδικα RC4 (RC4 cipher). Η βασική αρχή λειτουργία του είναι η παραγωγή μιας ακολουθίας bit κλειδιού (keystream) που συνδυάζονται με χρήση του XOR με τα δεδομένα για να παραχθεί το κρυπτογράφημα (ciphertext). Για να

πάρει κάποιος τα αρχικά δεδομένα αρκεί να εκτελέσει ακόμα ένα XOR του κρυπτογραφήματος με το keystream. Το keystream παράγεται από ένα σχετικά μικρό μυστικό κλειδί (secret key) το οποίο επεκτείνεται με συγκεκριμένο τρόπο μέχρι το μήκος που χρειάζεται. Το πιο σημαντικό στοιχείο της κρυπτογράφησης είναι η παραγωγή του keystream από το secret key. Η διαδικασία πρέπει να παράγει όσο το δυνατόν πιο τυχαίες ακολουθίες keystream.

Ο WEP χρησιμοποιεί μυστικά κλειδιά 40-bit ή 104-bit στα Access Point και τους σταθμούς για αμοιβαία επικύρωση. Η shared key επικύρωση χρησιμοποιεί αυτά τα κοινά μυστικά για να εφαρμόσει μια πρόκληση και μια ανταλλαγή απάντησης μεταξύ των πιθανών επικυρωμένων σταθμών και ενός σημείου πρόσβασης. Η WEP επικύρωση δουλεύει ως εξής: Όταν ένας σταθμός ζητά επικύρωση, το Access Point του στέλνει ένα τυχαίο μήνυμα 128-byte. Ο σταθμός κρυπτογραφεί το μήνυμα με το κλειδί WEP και στέλνει το αποτέλεσμα κρυπτογραφημάτων στο Access Point. Το Access Point αποκρυπτογραφεί το κρυπτογράφημα με το αντίγραφό του κλειδιού WEP που διαθέτει, εάν το επακόλουθο plaintext είναι το ίδιο με αυτό που στέλνεται αρχικά από το σταθμό τότε κατόπιν το Access Point επικυρώνει το σταθμό, κατά συνέπεια ο σταθμός συνδέεται με το σημείο πρόσβασης. Αλλά η shared key επικύρωση δεν μπορεί να είναι καθόλου ισχυρότερη από τους αλγορίθμους κρυπτογράφησης που κρύβονται κάτω αυτήν. Επιπλέον, θεωρείται φτωχή πρακτική ασφάλειας να υιοθετούνται τα ίδια κλειδιά για τα στοιχεία κρυπτογράφησης και έγκρισης. Ένας λόγος για αυτήν την αρχή είναι ότι η επικύρωση μπορεί να εκθέσει τις ανεπάρκειες ενός αλγορίθμου σε μια διαφορετική μόδα από την συνηθισμένη κρυπτογράφηση στοιχείων. Παραδείγματος χάριν, αν και η κοινή επικύρωση δεν περνά ποτέ τα κλειδιά στον αέρα, τα διοικητικά πλαίσια δεν κρυπτογραφούνται, έτσι οι πληροφορίες που μπορούν να συλληφθούν από τη διαδικασία επικύρωσης μπορούν να είναι χρήσιμες να νικήσουν την κρυπτογράφηση. Στην πραγματικότητα, υπάρχουν συγκεκριμένες επιθέσεις στην WEP-based shared επικύρωση. Ένας επιτιθέμενος που κατορθώνει να συλλάβει τα διοικητικά πλαίσια μιας επιτυχούς προσπάθειας επικύρωσης θα έχει την πρώτη ύλη για να επικυρωθεί επανειλημμένα, ακόμα κι αν δεν συλλαμβάνει πραγματικά το κλειδί WEP. Η λύση στο πρόβλημα αυτό δόθηκε με την υιοθέτηση των VPN (Virtual Private Network) (Σχήμα 4.2) και των RADIUS server (Remote Authentication Dial-In User Services), που αρχικά δημιουργήθηκαν με σκοπό να επικυρώνουν συνδέσεις dial-up μεταξύ modems.

Άλλο ένα σημαντικό μέρος του WEP είναι η κρυπτογράφηση των δεδομένων που μετακινούνται σε ένα δίκτυο Wi-Fi. Ο WEP αλγόριθμος παράγει μυστικά δια-μοιραζόμενα κλειδιά τα οποία μπορούν να χρησιμοποιηθούν και από την πηγή και από τον προορισμό για την κρυπτογράφηση και αποκρυπτογράφηση των μεταδιδόμενων δεδομένων. Ωστόσο, το

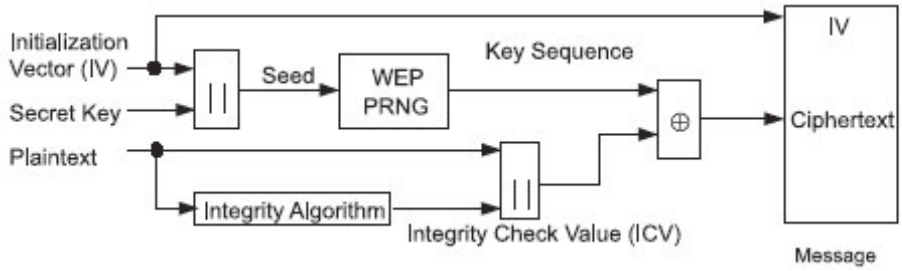
πρότυπο δεν καθορίζει τη διαδικασία εγκατάστασης των κλειδιών στους σταθμούς η οποία πρέπει να γίνει χειροκίνητα σε κάθε συσκευή . Τα βήματα που γίνονται για την κρυπτογράφηση ενός frame είναι τα ακόλουθα (Σχήμα 4.1):

• Στον σταθμό που στέλνει δεδομένα, ο WEP αλγόριθμος παράγει μια 32-bit τιμή ακεραιότητας για το payload του MAC frame. Αυτή η τιμή χρησιμοποιείται για να ειδοποιήσει το σταθμό λήψης για πιθανή αλλαγή των δεδομένων.

• Ένα δια-μοιραζόμενο κλειδί κρυπτογράφησης χρησιμοποιείται σαν είσοδος στη γεννήτρια ψευδοτυχαίων αριθμών ώστε να παραχθεί μια τυχαία ακολουθία από bit, το μήκος της οποίας ισούται με το άθροισμα των μηκών του MAC payload και της τιμής ακεραιότητας. Αυτά τα πεδία στη συνέχεια κρυπτογραφούνται με XOR με την παραγόμενη ακολουθία των bit.

• Ο σταθμός αποστολής τοποθετεί το κρυπτογραφημένο MAC payload μέσα στο MAC frame και το παραδίδει στο φυσικό επίπεδο για μετάδοση.

• Στον σταθμό λήψης ο WEP αλγόριθμος χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το MAC payload και υπολογίζει την τιμή ακεραιότητας για το MAC payload. Αν η υπολογιζόμενη τιμή είναι ίδια με αυτή που στάλθηκε με το frame τότε ο σταθμός μεταφέρει το MAC payload στο LLC.



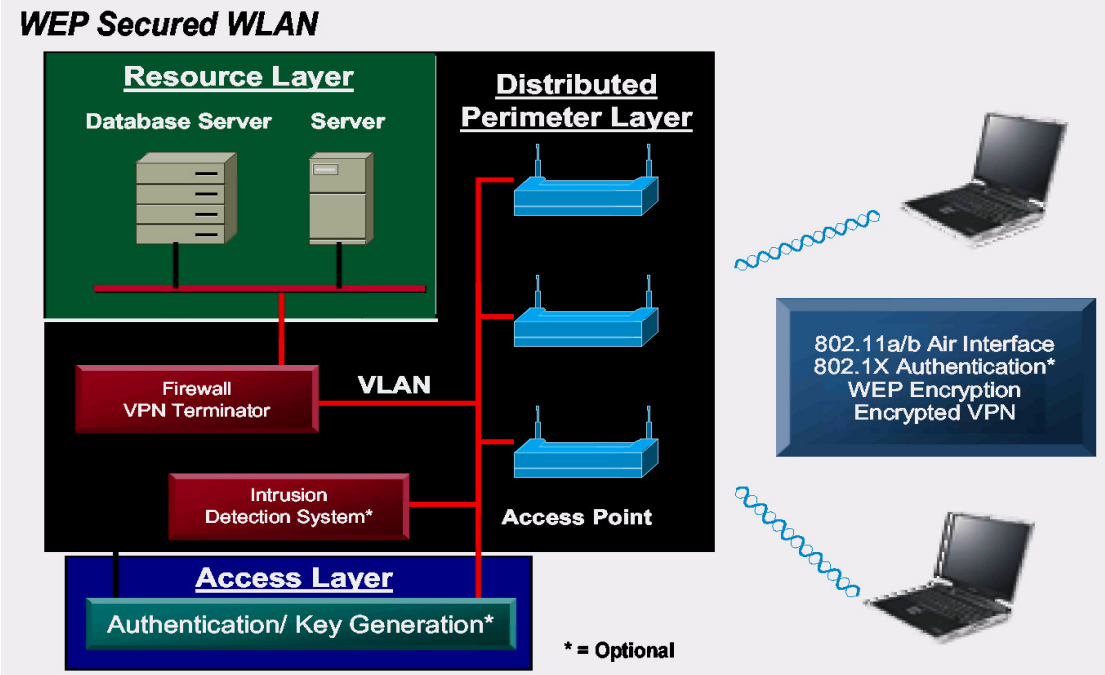
Σχήμα 4.1: Κρυπτογράφηση του αλγόριθμου WEP

4.1.2 Τα προβλήματα του αλγόριθμου WEP

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα της κυβέρνησης των Η.Π.Α. κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει ποσό τρωτό είναι ένα

ανοιχτό δίκτυο, βιάστηκαν να υιοθετήσουν το πρότυπο αυτό. Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης κλειδιών, ενώ η εργασία του Maryland θίγει της αδυναμίες στους μηχανισμούς πρόσβασης, ακόμη και αυτούς που λειτουργούν με βάση το WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου, με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για το WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP:unsafe at any key length»). Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης (RC4 της RCA), παρόλα αυτά, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι Scott Fluhrer, Itsik Mantin, και Adi Shamir, ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως το AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου – στόχος.

Επίσης στον αλγόριθμος WEP η επικύρωση των χρηστών είναι αδύναμη. Η shared key επικύρωση δεν μπορεί να είναι καθόλου ισχυρότερη από τους αλγορίθμους κρυπτογράφησης που κρύβονται κάτω αυτήν. Επιπλέον, θεωρείται φτωχή πρακτική ασφάλειας να υιοθετούνται τα ίδια κλειδιά για τα στοιχεία κρυπτογράφησης και έγκρισης. Ένας λόγος για αυτήν την αρχή είναι ότι η επικύρωση μπορεί να εκθέσει τις ανεπάρκειες ενός αλγορίθμου σε μια διαφορετική μόδα από την συνηθισμένη κρυπτογράφηση στοιχείων. Παραδείγματος χάριν, αν και η κοινή επικύρωση δεν περνά ποτέ τα κλειδιά στον αέρα, τα διοικητικά πλαίσια δεν κρυπτογραφούνται, έτσι οι πληροφορίες που μπορούν να συλληφθούν από τη διαδικασία επικύρωσης μπορούν να είναι χρήσιμες να νικήσουν την κρυπτογράφηση. Στην πραγματικότητα, υπάρχουν συγκεκριμένες επιθέσεις στην WEP-based shared επικύρωση. Ένας επιτιθέμενος που κατορθώνει να συλλάβει τα διοικητικά πλαίσια μιας επιτυχούς προσπάθειας επικύρωσης θα έχει την πρώτη ύλη για να επικυρωθεί επανειλημμένα, ακόμα κι αν δεν συλλαμβάνει πραγματικά το κλειδί WEP. Η λύση στο πρόβλημα αυτό δόθηκε με την υιοθέτηση των VPN (Virtual Private Network) (Σχήμα 4.2) και των RADIUS server (Remote Authentication Dial-In User Services), που αρχικά δημιουργήθηκαν με σκοπό να επικυρώνουν συνδέσεις dial-up μεταξύ modems.



Σχήμα 4.2: Πιστοποίηση δικτύων Wi-Fi μέσω VPN

Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα Wi-Fi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό Access Points που ανιχνεύτηκαν, έχουν πράγματι το WEP ενεργοποιημένο. Το μεγαλύτερο ποσοστό των εταιρικών δικτύων, είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν web sites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών δικτύων. Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως το netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού τους υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως το SSID του Access Point, αν έχει ενεργοποιημένο το WEP, αλλά και την ποιότητα της εκπομπής της κεραίας – στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή Wi-Fi κάρτα και μια ακόμα φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», ενονόματι war driving, επωφελούμενοι κυρίως από την δωρεάν broadband σύνδεση στο internet που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο. Η επίθεση parking lot, συνεπάγεται την χρήση της εμβελείας ενός Wi-FI δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας, για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος parking. Με μια δόση χιούμορ, πολλά άρθρα στο internet, για να ωθήσουν τους network administrators να αυξήσουν την ασφάλεια των ασύρματων δικτύων τους, ρωτούν: «μοιράζεστε την εταιρική σας σύνδεση στο internet με εκείνο τον κύριο στο

parking;». Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη» (disassociation/de-authentication packets) προς το Access Point. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης, μπορεί να απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC-πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα, και θα αποσυνδέσει όσους σταθμούς του ζητηθούν, προκαλώντας έτσι την κατάρρευση του δικτύου.

Όλα τα παραπάνω συνηγορούν ότι η προτυποποίηση της ασύρματης ασφάλειας, είναι μια εργασία σε εξέλιξη. Νέα πρότυπα μελετούνται, όπως το WPA, που υπόσχονται μια καλύτερη λύση από τον WEP. Βέβαια ένας τέτοιος στόχος φαίνεται εύκολος, δεδομένης της πλήρους και πέρα για πέρα αποτυχίας του WEP πρωτοκόλλου. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως το IPsec, το ssl κτλ.

4.2 Ο αλγόριθμος WPA

Κατά τη διάρκεια του προηγούμενου έτους, η συμμαχία Wi-Fi έχει κατευθύνει μια προσπάθεια να φέρει για να πωληθεί το πρότυπο-βασισμένη στην διαλειτουργική προδιαγραφή ασφάλειας που θα αύξανε πολύ το επίπεδο προστασία των δεδομένων και τον έλεγχο πρόσβασης για τα ασύρματα τοπικά δίκτυα Wi-Fi. Αυτή η προδιαγραφή είναι ο Wi-Fi Protected Access (WPA).

Ο WPA εξετάζει τις ρωγμές στον Wired Equivalent Privacy (WEP), ο αρχικός εγγενής μηχανισμός ασφάλεια για τα WLANs που ήταν σε ισχύ από την υιοθέτηση του ιδρύματος Electrical and Electronics Engineers (IEEE) 802.11 πρότυπα το 1997. Μέχρι το 2001, οι κρυπτογραφικές αδυναμίες του WEP είχαν γίνει γνωστές. Μια σειρά ανεξάρτητων μελετών από τα διάφορα ακαδημαϊκά και εμπορικά ιδρύματα είχε δείξει ότι ένας εισβολέας που εξοπλίζεται με τα κατάλληλα εργαλεία και με μέτριες τεχνικές γνώσεις θα μπορούσε να κερδίσει αναρμόδια πρόσβαση σε ένα WLAN ακόμη και με ενεργοποιημένο τον WEP. Παρά τις ρωγμές του, WEP παρείχε ένα περιθώριο της ασφάλειας έναντι καμίας ασφάλειας καθόλου. Παρέμεινε χρήσιμο για να απομακρύνει τους εισβολείς δικτύων σπιτιών και μικρόν γραφείων, περιβάλλοντα όπου η κυκλοφορία δικτύων είναι ελαφριά. Εντούτοις, δεν ήταν ικανοποιητικό για την επιχειρηματική χρήση. Πολλές μεγάλες επιχειρήσεις ενίσχυσαν τον WEP με την ανάπτυξη λύσεων ασφάλειας τρίτων, συμπεριλαμβανομένων των VPNs, κεντρικούς υπολογιστές επικύρωσης 802.1X, και άλλες ιδιόκτητες τεχνολογίες.

Με την ανησυχία για το ότι η έλλειψη ισχυρής εγγενούς ασύρματης ασφάλειας θα εμπόδιζε την υιοθέτηση των συσκευών Wi-Fi στην αγορά, η Wi-Fi alliances, από κοινού με

την IEEE, άρχισε μια προσπάθεια να παρουσιαστεί μια έντονα βελτιωμένη, πρότυπο βασισμένη, διαλειτουργική λύση ασφάλειας Wi-Fi στην αγορά. Ο WPA είναι η λύση. Ο WPA είναι σχεδιασμένος για να εξασφαλίσει όλες τις εκδόσεις 802.11 συσκευών, συμπεριλαμβανομένου των 802.11b, 802.11a, και 802.11g, multi-band και multi-mode. WPA είναι ένα υποσύνολο του IEEE 802.11i προσεχούς πρότυπου (επίσης γνωστός ως WPA2) που επικυρώθηκε το πρώτο τρίμηνο του 2004. Υπό αυτήν τη μορφή, είναι μπροστά και πίσω συμβατός με τον WPA2. Ο WPA θα είναι βιώσιμο στην αγορά για πολλά έτη και θα πρέπεί να είναι συμβατός άνετα με τις WPA2 συσκευές όταν αυτές γίνουν διαθέσιμες. Ο WPA απευθύνεται στην ασφάλεια Wi-FI με έναν ισχυρό νέο αλγόριθμο κρυπτογράφησης καθώς επίσης και στην επικύρωση του χρήστη, ένα χαρακτηριστικό γνώρισμα που έλειπε κατά ένα μεγάλο μέρος από τον WEP. Όταν εγκαθίσταται κατάλληλα, παρέχει ένα υψηλό επίπεδο διαβεβαίωσης ότι τα δεδομένα των χρηστών θα παραμείνουν προστατευμένα και ότι μόνο οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στο δίκτυο. Με τον WPA ενεργοποιημένο, οι επιχειρήσεις μπορούν να προσφέρουν στους υπαλλήλους την ευκολία και την ευελιξία να εργάζονται ασύρματα και ασφαλείς χωρίς ανάπτυξη των πρόσθετων λύσεων ασφάλειας, όπως VPNs. Οι επιχειρηματικοί χρήστες καθώς επίσης και εκείνοι στο σπίτι και στα περιβάλλοντα SOHO (small office/home office), έχουν μια ισχυρή ασφάλεια στο δίκτυο τους. Οι ασύρματοι φορείς παροχής υπηρεσιών internet (WISPs , Wireless Internet service providers) μπορούν επίσης να διαπιστώσουν ότι τα ενισχυμένα σχέδια κρυπτογράφησης και επικύρωσης WPA είναι ελκυστικά στα δημόσια "hot spots" δεδομένου ότι παρέχουν ένα υψηλό επίπεδο ασφάλειας για τους φορείς παροχής υπηρεσιών και τους κινητούς χρήστες που δεν χρησιμοποιούν τις συνδέσεις VPN.

4.2.1. Ο WPA σε μια ματιά

Ο WPA εξετάζει όλες τις γνωστές αδυναμίες του WEP για να εξασφαλίσει την αυθεντικότητα των δεδομένων στα ασύρματα LANs και προστατεύει ακόμη και τις πιο επικίνδυνες επιθέσεις hacker. Είναι σχεδιασμένος να ελαχιστοποιήσει τον αντίκτυπο στην απόδοση δικτύων και να τρέξει ως βελτίωση λογισμικού στα περισσότερα από 650 CERTIFIED Wi-Fi προϊόντα στη σημερινή αγορά.

Οι κρυπτογράφοι έχουν αναθεωρήσει τον WPA και έχουν επιβεβαιώσει τις αξιώσεις ότι κλείνει όλες τις γνωστές αδυναμίες του WEP και παρέχει έναν αποτελεσματικό αποτρεπτικό παράγοντα ενάντια τις γνωστές επιθέσεις.

Ο WPA χρησιμοποιεί το πρωτόκολλο ακεραιότητας προσωρινού κλειδιού (TKIP, Temporal Key Integrity Protocol) για την κρυπτογράφηση και υιοθετεί την επικύρωση

802.1X με έναν από τους τυποποιημένους τύπους έκτατου πρωτοκόλλου επικύρωσης (EAP, Extensible Authentication Protocol) που είναι διαθέσιμοι σήμερα.

Ο WPA μπορεί να εγκατασταθεί ως βελτίωση λογισμικού στις περισσότερες τρέχουσες συσκευές Wi-Fi. Τα Access Point απαιτούν βελτίωση λογισμικού. Οι τερματικοί σταθμοί πελατών απαιτούν βελτίωση λογισμικού στην κάρτα διεπαφών δικτύων (NIC, Network Interface card) και μια πιθανή βελτίωση λογισμικού στο λειτουργικό σύστημα. Η επιχείρηση θα απαιτήσει έναν κεντρικό υπολογιστή επικύρωσης (χαρακτηριστικά έναν Remote Authentication Dial-In User Service, ή αλλίως κεντρικός υπολογιστής RADIUS. Ο WPA συμβιβάζει τους χρήστες του σπιτιού και του SOHO που δεν έχουν τέτοιους κεντρικούς υπολογιστές διαθέσιμους με έναν ειδικό τρόπο που χρησιμοποιεί έναν κοινό κωδικό πρόσβασης για να ενεργοποιήσει την προστασία WPA.

Η συμμαχία Wi-Fi έχει αρχίσει να πιστοποιεί πλέον όλα τα προϊόντα WPA.. Ο WPA θα είναι προαιρετικά Certified στα προϊόντα Wi-Fi κατά τη διάρκεια της αρχικής φάσης, της περιόδου. Η ασφάλεια WPA θα υποδειχθεί στο λογότυπο πιστοποίησης Wi-Fi στα προϊόντα που τον κατέχουν. Ο WPA θα αντικαταστήσει πλήρως WEP ως λύση ασφάλειας στις νέες συσκευές Wi-Fi. Και είναι πλέον υποχρεωτικό για τα επιλεγμένα προϊόντα PC να κερδίσουν την πιστοποίηση Wi-Fi.

4.2.2 Μεταφορά του WPA στην επιχείρηση

Ο WPA παρουσιάζει μια φυσική πορεία μετανάστευσης για αυτήν την περίοδο τις εγκατεστημένες συσκευές. Οι επιχειρήσεις που χρησιμοποιούν προς το παρόν την επικύρωση 802.1X/EAP μπορούν να αναβαθμίσουν σε WPA χωρίς απώλεια της επένδυσής τους. Οι διευθυντές του IT ενθαρρύνουν για να εξασφαλίσουν ότι ο WPA είναι το παρόν στις νέες συσκευές Wi-Fi που αγοράζονται και για να ανανεώσουν τις βασισμένες εγκαταστάσεις WEP και τα AP και τους τερματικούς σταθμούς πελατών σε WPA. Για τα επιχειρηματικά δίκτυα, που εφαρμόζουν τον WPA θα περιλάβουν την ανάπτυξη μιας υποδομής 802.1X. Αυτό υπονοεί:

- Επιλογή των τύπων EAP που θα υποστηρίζουν τους πελάτες NICs και τους κεντρικούς υπολογιστές επικύρωσης.
- Επιλογή και επέκταση ενός κεντρικού υπολογιστή επικύρωσης, χαρακτηριστικά τους Remote Authentication Dial-In User Service (RADIUS) κεντρικούς υπολογιστές.
- Αναβάθμιση των APs με τον WPA ή της αγοράς νέων APs με WPA εγκατεστημένο.
- Αναβάθμιση των WLAN πελατών NICs με WPA ή της αγοράς νέου ασύρματου NICs με WPA εγκατεστημένο.

Στις μεγάλες επιχειρηματικές τοποθετήσεις, είναι πιθανό ότι τα Access Point θα αναβαθμιστούν πριν οι αναβαθμίσεις στους τερματικούς σταθμούς πελατών να μπορούν να ολοκληρωθούν. Για αυτόν τον λόγο, μερικοί προμηθευτές προγραμματίζουν να προσφέρουν έναν "μικτό τρόπο" ώστε τα Access Point να υποστηρίζουν τον WPA, καθώς επίσης οι πελάτες θα τρέχουν την αρχική ασφάλεια WEP. Ενώ αυτός ο μικτός τρόπος μπορεί να είναι χρήσιμος κατά τη διάρκεια μιας μετάβασης, είναι πλήρως επισφαλής. Οι πελάτες WEP θα συνεχίσουν να παρουσιάζουν ανοικτά σημεία μέσω των οποίων οι εισβολείς μπορούν να έχουν πρόσβαση στο ασύρματο δίκτυο. Η καθαρή επίδραση του τρόπου μικτής λειτουργίας είναι ότι ένα δίκτυο WPA δεν θα είναι πλέον ασφαλές από εάν έτρεχε την ασφάλεια WEP.

Ο μικτός τρόπος δεν είναι ένα χαρακτηριστικό γνώρισμα του WPA. Η συμμαχία Wi-FI δεν την εξετάζει για διαλειτουργικότητα και δεν συστήνει τη χρήση της. Οι μεγάλες οργανώσεις που την χρησιμοποιούν πρέπει να επιταχύνουν τη μετάβαση σε WPA, χρησιμοποιώντας τον μικτό τρόπο για τη μικρότερη πιθανόν χρονική περίοδο. Οι επιχειρήσεις που χρησιμοποιούν αυτήν την περίοδο VPN ή άλλες συγκεκριμένες λύσεις 802.1X /EAP πρέπει να συνεχίσουν τη χρήση τους μέσω της περιόδου βελτίωσης. Μετά την μετάβαση σε WPA οι περισσότερες επιχειρήσεις δεν θα βρουν ανάγκη χρήσης για αυτές τις πρόσθετες τεχνολογίες, τουλάχιστον όχι για το συγκεκριμένο σκοπό της ασφάλειας του δικτύου Wi-Fi.

Τα VPN παραμένουν μια φιλοφρονητική τεχνολογία που θα συνυπάρξουν καλά με τον WPA για να εξασφαλίσουν μακρινές συνδέσεις, όπως εκείνες των χρηστών που έχουν πρόσβαση σε ένα εταιρικό δίκτυο μέσω των Hotspot.

4.2.3 Μηχανισμοί ασφάλειας στον WPA

Μια από τις κύριες αδυναμίες του WEP ήταν ότι χρησιμοποίησε ένα μικρό στατικό κλειδί για να αρχίζει την κρυπτογράφηση. Αυτό το κλειδί 40-bit εισάγεται με το χέρι στο AP και σε όλους τους πελάτες που επικοινωνούν με το AP. Δεν αλλάζει εκτός αν επανεισάγεται με το χέρι σε όλες τις συσκευές, ένας αποθαρρυντικός εντατικός στόχος εργασία σε μια μεγάλη οργάνωση.

Οι κρυπτογραφικές μελέτες έχουν καταδείξει ότι ένας εισβολέας που συλλέγει αρκετά στοιχεία μπορεί απειλήσει ένα δίκτυο με ασφάλεια WEP με τρεις τρόπους:

- με την παρεμπόδιση και την αποκρυπτογράφηση των δεδομένων που διαβιβάζονται στον αέρα,
- με την αλλαγή των δεδομένων που επικοινωνούν,
- και με το εξαγωγή συμπεράσματος και τη σφυρηλάτηση του κλειδιού WEP για να κερδίσει την αναρμόδια πρόσβαση στις υπηρεσίες δικτύων και του internet.

Αυτό θα μπορούσε να ολοκληρωθεί σε θέμα ωρών σε ένα πολυάσχολο, εταιρικό WLAN. Επίσης, ο WEP στερείται το νόημα της επικύρωσης, που επικυρώνει τα πιστοποιητικά χρηστών για να εξασφαλίσει ότι μόνο εκείνοι που πρέπει να είναι στο δίκτυο έχουν την άδεια για να έχουν πρόσβαση σε τα. WPA εξετάζει αυτές τις ρωγμές και φέρνει τα πρόσθετα μέτρα προστασίας στην ασφάλεια Wi-Fi (Πίνακας 4.1).

Ο WPA χρησιμοποιεί ένα πολύ ενισχυμένο σχέδιο κρυπτογράφησης, το πρωτόκολλο προσωρινού κλειδιού ακεραιότητας (TKIP, Temporal Key Integrity Protocol). Μαζί με την επικύρωση 802.1X/EAP, ο TKIP υιοθετεί μια βασική ιεραρχία που ενισχύει πολύ την προστασία. Προσθέτει επίσης έναν έλεγχο ακεραιότητας μηνυμάτων (MIC, Message Integrity Check μερικές φορές αποκαλούμενος "Michael") που προστατεύει από τις παραποιήσεις πακέτων.

	WEP	**WPA**
Κρυπτογράφηση	Ελαττωματικός, ραγισμένος από τους επιστήμονες και τους χάκερ	Φτιάχνει όλα ελαττώματα του WEP
	40-bit κλειδιά	128-bit κλειδιά
	Στατικό – ίδιο κλειδί που χρησιμοποιείται από το καθένα στο δίκτυο	Δυναμικά κλειδιά συνόδου. Ανά χρήστη, ανά σύνοδο, ανά κλειδιά πακέτων
	Χειρωνακτική διανομή του κλειδιού –δακτυλογραφείται σε κάθε συσκευή	Αυτόματη διανομή των κλειδιών
Επικύρωση	Ραγισμένο, το ίδιο χρησιμοποιημένο WEP κλειδί για την επικύρωση	Ισχυρή επικύρωση χρηστών, που χρησιμοποιεί 802.1X και EAP

Πίνακας 4.1 : Διαφορές WEP από το WPA

4.2.4 Κρυπτογράφηση

Ο TKIP αυξάνει το μέγεθος του κλειδιού από 40 σε 128 bit και αντικαθιστά το ενιαίο στατικό κλειδί WEP με κλειδιά που παράγονται δυναμικά και διανέμονται από τον κεντρικός υπολογιστής επικύρωσης. TKIP χρησιμοποιεί μια μεθοδολογία ιεραρχίας κλειδιού και διαχείρισης κλειδιών που αφαιρεί την προβλεψιμότητα επάνω στην οποία οι εισβολείς στηρίχθηκαν για να εκμεταλλευτούν το κλειδί WEP.

Για να κάνει αυτό, ο TKIP δυναμώνει το πλαίσιο 802.1X/EAP. Ο κεντρικός υπολογιστής επικύρωσης, μετά που θα δεχτεί τα πιστοποιητικά ενός χρήστη, χρησιμοποιεί το 802.1X για να παραγάγει έναν μοναδικό master, ή ένα "pair-wise" κλειδί για εκείνη την σύνοδο υπολογισμού. Ο TKIP διανέμει αυτό το κλειδί στον πελάτη και στο AP και οργανώνει ένα σύστημα ιεραρχίας και διαχείρισης κλειδιού, χρησιμοποιώντας το pair-wise

κλειδί για να παραγάγει δυναμικά τα μοναδικά κλειδιά κρυπτογράφησης δεδομένων για να κρυπτογραφήσει κάθε πακέτο δεδομένων που επικοινωνούν ασύρματα κατά τη διάρκεια της συνόδου του χρήστη. Η ιεραρχία κλειδιού TKIP ανταλλάσσει το ενιαίο στατικό κλειδί WEP για περίπου 500 τρισεκατομμύρια πιθανά κλειδιά που μπορούν να χρησιμοποιηθούν σε ένα δεδομένο πακέτο δεδομένων.

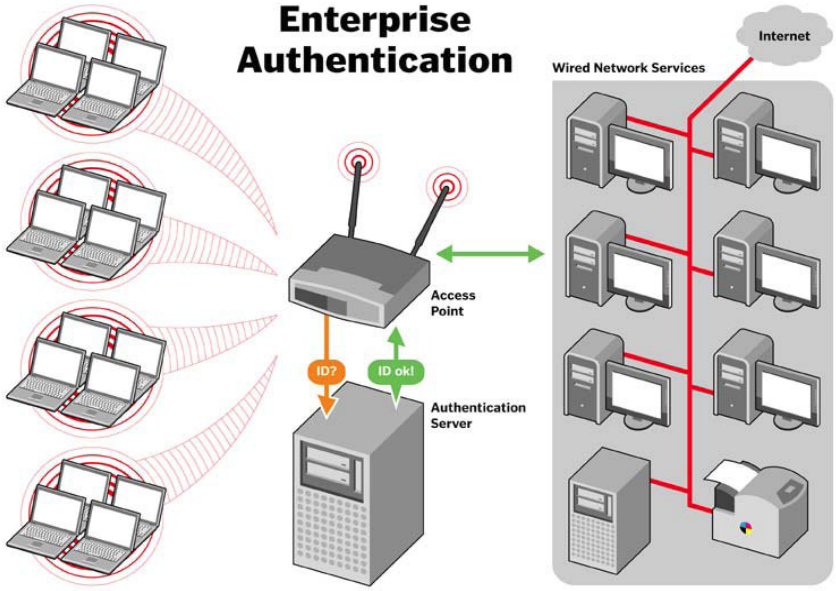
Ο έλεγχος ακεραιότητας μηνυμάτων (MIC, Message Integrity Check) έχει ως σκοπό να αποτρέψει έναν επιτιθέμενο από σύλληψη των πακέτων δεδομένων, αλλαγή τους και εκ νέου αποστολή τους. Ο MIC παρέχει μια ισχυρή μαθηματική λειτουργία στην οποία ο δέκτης και αποστολέας καθένας υπολογίζουν και συγκρίνουν έπειτα τα MIC. Εάν δεν ταιριάζουν, τα δεδομένα υποτίθεται ότι έχουν πειραχτεί και το πακέτο διαγράφεται.

Με μία μεγάλη επέκταση στο μέγεθος των κλειδιών, ο αριθμός κλειδιών σε χρήση, και με τη δημιουργία του μηχανισμού ελέγχου ακεραιότητα, ο TKIP ενισχύει την πολυπλοκότητα και τη δυσκολία στην αποκωδικοποίηση των δεδομένων όσον αφορά ένα δίκτυο Wi-Fi. TKIP αυξάνει πολύ τη δύναμη και την πολυπλοκότητα της ασύρματης κρυπτογράφησης, που την καθιστά πολύ δυσκολότερη, εάν όχι αδύνατη, για έναν εισβολέα να εισβάλει σε ένα δίκτυο Wi-Fi.

Σχεδιασμένες για να επεκταθούν με τις υπάρχον Wi-Fi CERTIFIED συσκευές, ο TKIP είναι επίσης συμπεριλαμβανόμενος στα προτεινόμενα WPA2 πρότυπα.

4.2.5 Επικύρωση

Ο WPA χρησιμοποιεί την 802.1X επικύρωση μαζί με το Extensible Authentication Protocol (EAP) τύπο που είναι διαθέσιμο σήμερα. Η 802.1X είναι μια port-based μέθοδος ελέγχου πρόσβασης για ενσύρματα δίκτυα , καθώς επίσης και ασύρματα δίκτυα (Σχήμα 4.3). Αυτό υιοθετήθηκε ως πρότυπα από IEEE τον Αύγουστο του 2001.



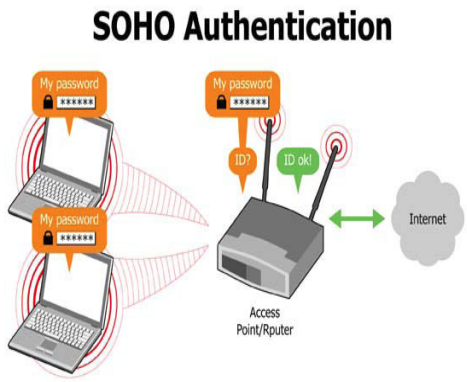
Σχήμα 4.3: Πιστοποίηση του αλγόριθμου WPA στην επιχείρηση

Ο EAP χειρίζεται την παρουσίαση των πιστοποιητικών των χρηστών, υπό μορφή ψηφιακών πιστοποιητικών (ήδη ευρέως χρησιμοποιημένος στην ασφάλεια internet), μοναδικά ονόματα χρηστών και κωδικοί πρόσβασης, έξυπνες κάρτες, ασφαλές IDs, ή οποιοδήποτε άλλο πιστοποιητικό ταυτότητας που ο administrator IT άνετα αναπτύσσει. Ο WPA επιτρέπει την ευελιξία και στα δύο, στον τύπο πιστοποιητικών που χρησιμοποιούνται και στην επιλογή ενός τύπου EAP. Ένας ευρύς αριθμός προτύπων βασισμένων εφαρμογών EAP είναι διαθέσιμες για χρήση, συμπεριλαμβανομένου του EAP – Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), και Protected Extensible Authentication Protocol (PEAP).

Μαζί με τον EAP, το 802.1X δημιουργεί ένα πλαίσιο στο οποίο οι τερματικοί σταθμοί πελατών επικυρώνουν αμοιβαία με τον κεντρικό υπολογιστή επικύρωσης. Αυτή η αμοιβαία επικύρωση αποτρέπει τους χρήστες από τυχαία σύνδεση με "απατεώνα" ή αναρμόδιο APs στο δίκτυο Wi-Fi και επίσης εξασφαλίζει ότι οι χρήστες που έχουν πρόσβαση στο δίκτυο είναι αυτοί που υποτίθεται για να είναι εκεί. Όταν ένας χρήστης ζητά πρόσβαση στο δίκτυο, ο πελάτης στέλνει τα πιστοποιητικά του χρήστη στον κεντρικό υπολογιστή επικύρωσης μέσω του AP. Εάν ο κεντρικός υπολογιστής δέχεται τα πιστοποιητικά του χρήστη, το κύριο κλειδί TKIP στέλνεται και στον πελάτη και στο AP. Μια χειραψία four-way, μια διαδικασία στην οποία ο πελάτης και το AP αναγνωρίζουν το ένα το άλλο και εγκαθιστούν τα κλειδιά, ολοκληρώνει τη διαδικασία

4.2.6 Ασφάλεια για σπίτια και μικρά γραφεία

Χρήστες των μικρών γραφείων και περιβάλλοντα γραφείων σπιτιού (SOHO) στερούνται τον προϋπολογισμό και προσωπικό IT για να εγκαταστήσει και να διατηρήσει κεντρικούς υπολογιστές επικύρωσης RADIUS. Ο WPA το αναγνωρίζει προσφέροντας σε αυτούς τους χρήστες τα οφέλη της ασφάλειας WPA μέσω της χρήσης "pre-shared key" (PSK) ή κωδικού πρόσβασης (Σχήμα 4.4).



Σχήμα 4.4: Πιστοποίηση σε περιβάλλοντα SOHO

Το PSK παρέχει στο σπίτι και τους χρήστες SOHO την ίδια ισχυρή κρυπτογράφηση TKIP, για κάθε πακέτο κατασκευή κλειδιού, και διαχείριση κλειδιού που ο WPA παρέχει στην επιχείρηση.

Η διαφορά είναι ότι εδώ, ο προσωπικός κωδικός πληκτρολογείται με το χέρι στις συσκευές πελατών και στο AP ή η ασύρματη πύλη χρησιμοποιείται για την επικύρωση. Ενώ όχι τόσο γερός όσο μια πραγματική RADIUS, η επικύρωση EAP και 802.1X πλησιάζει, το PSK παρέχει χρήσιμές εναλλαγές στα μικρότερα δίκτυα.

Η αναβάθμιση σε WPA στο σπίτι και τα μικρά περιβάλλοντα γραφείων είναι απλή. Οι χρήστες μπορούν να αγοράσουν το νέο WPA εξοπλισμό ή να ενημερώσουν τον εγκατεστημένο εξοπλισμό. Για τους περισσότερους χρήστες, η αναπροσαρμογή είναι τόσο εύκολη όπως εγκαθιστώντας έναν νέο οδηγό υλικού.

Τα βήματα είναι:

- Αναβάθμιση του APs με το λογισμικό WPA.
- Αναβάθμιση των καρτών WLAN δικτύων με WPA λογισμικό.
- Διαμόρφωση του PSK, ή τον κύριο κωδικό πρόσβασης, στο AP.
- Διαμόρφωση του PSK στους τερματικούς σταθμούς πελατών.

4.3 Ο αλγόριθμος WPA2

Σε μία προσπάθεια ενίσχυσης της ασφάλειας των δικτύων Wi-Fi η Wi-Fi alliances υλοποίησε την εξέλιξη του WPA τον WPA2 ο οποίος ενισχύει δυναμικά την ασφάλεια των προτύπων 802.11b, 802.11a και 802.11g.

4.3.1 Περιγραφή του αλγόριθμου WPA2.

Η κρυπτογράφηση TKIP, η επικύρωση 802.1X/EAP και η τεχνολογία PSK σε WPA είναι χαρακτηριστικά γνωρίσματα που έχουν τεθεί από τον WPA2. Επιπλέον, ο WPA2 θα παράσχει ένα νέο σχέδιο κρυπτογράφησης, το Advanced Encryption Standard (AES, Advanced Encryption Standard).

Το AES έχει υιοθετηθεί ήδη ως επίσημο κυβερνητικό πρότυπο από το Αμερικάνικο Τμήμα εμπορίου και το εθνικό ίδρυμα προτύπων και τεχνολογίας (NIST, National Institute of Standards and Technology). Το AES θα καθοριστεί στον τρόπο μέτρησης ακολουθίας cipher-block (CCM, cipher-block mode) και θα υποστηρίξει το IBSS για να επιτρέψει την ασφάλεια μεταξύ των τερματικών σταθμών πελατών που λειτουργούν σε ad-hoc . Το AES χρησιμοποιεί έναν μαθηματικό αλγόριθμο κρυπτογράφησης που υιοθετεί μεταβλητά μεγέθη κλειδιών 128-bit, 192-bit ή των 256-bit.

Όπως ο WPA, ο WPA2 θα χρησιμοποιήσει το πλαίσιο 802.1X/EAP ως τμήμα της υποδομής αυτή που εξασφαλίζει τη συγκεντρωμένη αμοιβαία επικύρωση και τη διαχείριση δυναμικών κλειδιών. Επίσης, προσφέρει ένα pre-shared κλειδί για τη χρήση στα περιβάλλοντα σπιτιών και μικρά γραφείων. Όπως στον WPA, ο WPA2 έχει ως σκοπό να εξασφαλίσει όλες τις εκδόσεις των 802.11 συσκευών, συμπεριλαμβανομένου του 802.11b, 802.11a, και 802.11g, multi-band και multi-mode.

Οι επιχειρήσεις που χτίζουν ένα νέο WLANs θα βρουν τον AES ελκυστικό. Εντούτοις, σε πολλές περιπτώσεις θα απαιτήσουν νέες επενδύσεις στο υλικό. Κατά συνέπεια, οι επιχείρησης πρέπει να σταθμίσει τα οφέλη της ενισχυμένης ασφάλειας που ο WPA2 προσφέρει ενάντια στο κόστος του νέου εξοπλισμού.

Δεν υπάρχει κανένας λόγος να μην αναβαθμίσει κάποιος τώρα σε WPA. Ενώ μια βελτίωση υλικού μπορεί να απαιτηθεί για να επεκτείνει τη μερίδα AES του WPA2 στις WPA συσκευές, η επικύρωση 802.1X, η κρυπτογράφηση TKIP, και τα συστατικά PSK του WPA καθιστούν τις δύο προδιαγραφές αρκετά συμβατές.

WPA2 προσφέρει μια χαριτωμένη πορεία μετάβασης από WPA που παρουσιάζει μια ακαταμάχητη περίπτωση για αναβάθμιση σε WPA τώρα. Ο WPA2 θα προσφέρει έναν ιδιαίτερα ασφαλή "μικτό τρόπο" που υποστηρίζουν και ο WPA και ο WPA2 τους τερματικούς σταθμούς πελατών. Αυτό θα επιτρέψει μια τακτική μετάβαση στις μεγάλες επιχειρήσεις που δεν μπορούν εύκολα να αναβαθμιστούν σε μικρή χρονική περίοδο.

Αντίθετα από το WEP/WPA μικτό τρόπο στις συσκευές WPA, ο μικτός τρόπος WPA2 θα υποστηρίξει και τα δύο το WPA και το WPA2. Παραδίδει ένα υψηλό επίπεδο ασφάλειας στις επιχειρήσεις δεδομένου ότι κάνουν την κίνηση στο ακόμα πιο υψηλό επίπεδο ασφάλειας που προσφέρεται ο WPA2. Δεδομένου ότι ο WPA παρέχει ήδη ισχυρή κρυπτογράφηση, η μετάβαση σε WPA2 στους πελάτες και στα APs μπορεί να γίνει βαθμιαία και με ένα υψηλό επίπεδο εμπιστοσύνης ότι η ασφάλεια δεν θα συμβιβαστεί.

4.4 Συμπεράσματα

Η ασφάλεια των δικτύων Wi-Fi είναι πρωταρχικός στόχος της IEEE και της Wi-Fi alliances με αποτέλεσμα την έκδοση των αλγόριθμών WEP, WPA και WPA2. Όπως αναφέρθηκε και στις παραπάνω παραγράφους ο WEP παρουσίασε σοβαρά προβλήματα ασφάλειας με αποτέλεσμα οι εταιρίες να στραφούν σε λύσεις τρίτων για να εξασφαλίσουν υψηλότερο επίπεδο ασφάλειας. Επειδή τα προβλήματα του WPE μπορεί να είχαν ως αποτέλεσμα την μη ευρεία διάδοση των δικτύων Wi-Fi η IEEE έκδωσε τον αλγόριθμο WPA ο οποίος έλυνε όλα τα προβλήματα του WPE και οι επιχειρήσεις δεν χρειάζονταν να καταφύγουν σε λύσεις τρίτων (VPN, RADIUS) για την ασφάλεια των δεδομένων τους. Στην προσπάθεια της αύξησης του επιπέδου ασφάλειας η Wi-Fi alliances έκδωσε την εξέλιξη του WPA τον WPA2 ο οποίος άλλαξε τον τρόπο κρυπτογράφησης των δεδομένων και είναι απόλυτα συμβατός με τον WPA (Πίνακας 4.2).

	WEP	WPA	WPA2
Κρυπτογράφηση	RC4	RC4	AES
Μέγεθος κλειδιών	40 bits	128 bits κρυπτογράφησης 64 bits επικύρωσης	128 bits
Key life	24-bit IV	48 bit-IV	48-bit IV
Packet Key	Συνδεδεμένο	Μιχτή λειτουργία	Δεν χρειάζεται
Ακεραιότητα δεδομένων	CRC-32	Michael	CCM
Ακεραιότητα Κεφαλίδας	Καμία	Michael	CCM
Replay Attack	Καμία	Συχνότητα IV	Συχνότητα IV
Διαχείριση κλειδιών	Καμία	Βασισμένο στο EAP	Βασισμένο στο EAP

Πίνακας 4.2: Διαφορές των αλγόριθμών WPE, WPA και WPA2.

Πλέον το επίπεδο ασφάλειας των δικτύων Wi-Fi είναι σε πολύ υψηλό και σε ένα βαθμό αντάξιο των ενσύρματων δικτύων οπότε είναι μία πολύ καλή λύση για τις επιχειρήσεις και τα μικρότερα δίκτυα .

5. ΧΡΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΕΣ Wi-Fi

Με την δημιουργία των δικτύων Wi-Fi και τα πλεονεκτήματα που είχαν βρέθηκαν πολλές χρήσεις για αυτά τα δίκτυα. Τα πλεονεκτήματα των δικτύων Wi-Fi είναι τα παρακάτω:

- Το χαμηλό κόστος του εξοπλισμού και της εγκατάστασης
- Χαμηλή κατανάλωσης ενέργειας
- Ασύρματη επικοινωνία που σημαίνει ευελιξία για τους χρήστες.

Τα δύο πρώτα πλεονεκτήματα ήταν σχεδιαστικοί στόχοι της ομάδας IEEE 802.11. Σε αυτό το κεφάλαιο θα γίνει αναφορά στις διάφορες εφαρμογές των δικτύων Wi-Fi και στην ποιότητα υπηρεσιών που προσφέρουν.

5.1 Εφαρμογές του Wi-Fi στο σπίτι.

Ένα δίκτυο Wi-Fi, μπορεί να δώσει την δυνατότητα για περιήγηση στο internet, παρακολούθηση video, εσωτερική βίντεο-διάσκεψη, σε οποιοδήποτε σημείο του σπιτιού. Φυσικά το στήσιμο ενός τοπικού δικτύου Wi-Fi μπορεί να γίνει χωρίς τον βραχνά των καλωδίων, hubs και λοιπών δικτυακών συσκευών, που δύσκολα χωρούν σε ένα σπίτι. Όλη η υποδομή αντικαθιστάται από μόνο ένα ή περισσότερα κεντρικά Access Points ή όταν πρόκειται για δίκτυο δύο υπολογιστών το μόνο που χρειάζεται είναι μία κάρτα δικτύου Wi-Fi σε κάθε υπολογιστή. Επίσης το κόστος του εξοπλισμού είναι πολύ μικρότερο από ότι είναι στα ενσύρματα δίκτυα. Όλα τα παραπάνω καθιστούν τα δίκτυα Wi-Fi κατάλληλα για χρήση στο σπίτι.

5.2 Τα δίκτυα Wi-Fi στις επιχειρήσεις

Τα πλεονεκτήματα των δικτύων Wi-Fi τα καθιστούν κατάλληλα για διάφορες εφαρμογές στις επιχειρήσεις. Σε αυτή την παράγραφο θα αναλύσουμε ορισμένες από αυτές.

5.2.1 Το Wi-Fi στα γραφεία

Στο γραφείο, το Wi-Fi γίνεται συνώνυμο της ευελιξίας. Οι εργαζόμενοι μπορούν ελεύθερα να κινούνται με φορητούς υπολογιστές στους εργασιακούς τους χώρους, χωρίς να χάνουν ούτε λεπτό την σύνδεσή τους στο εταιρικό δίκτυο και στο internet. Με αυτό τον τρόπο αυξάνεται η παραγωγικότητά τους καθώς μπορούν να συνεργάζονται ευκολότερα και να έχουν συνεχή πρόσβαση σε κρίσιμες πληροφορίες. Πολλά τοπικά δίκτυα σε κάθε κτίριο μπορούν εύκολα να συνενωθούν με Links μεγάλων αποστάσεων, αποδοτικά και κυρίως οικονομικά.

5.2.2 Τα δίκτυα Wi-Fi σε βιομηχανίες

Το χαμηλό κόστος των συσκευών και η χαμηλή τους κατανάλωση σε ενέργεια, δύο σχεδιαστικοί στόχοι της ομάδας 802.11, κάνουν ιδανική την χρήση του στην βιομηχανία. Συχνά μια βιομηχανία χρειάζεται την συνεχή παρακολούθηση ενός συνόλου από συσκευές που ελέγχουν την εύρυθμη λειτουργία της εγκατάστασης και επικοινωνούν με έναν κεντρικό υπολογιστή που συλλέγει τις πληροφορίες. Ένα δίκτυο Wi-Fi μπορεί να εγκατασταθεί για την παρακολούθηση συγκεκριμένων εργασιών. Ένα τέτοιο δίκτυο, μπορεί εύκολα να γίνει «έξυπνο». Οι συσκευές Wi-Fi μπορούν να βρίσκουν εναλλακτικές διαδρομές για να επικοινωνούν με τον κεντρικό υπολογιστή, δίνοντας 100% uptime στο σύστημα. Μπορούν λόγω της υψηλής δια-μεταγωγής του πρωτοκόλλου να διακινούν μεγάλους όγκους δεδομένων, και σε πραγματικό χρόνο, πράγμα που εγγυάται την παρακολούθηση του συστήματος σε πραγματικό χρόνο. Βέβαια η ασύρματη επικοινωνία είναι από μόνη της το μεγαλύτερο πλεονέκτημα της τεχνολογίας, καθώς δεν χρειάζονται άλλες καλωδιώσεις στον ήδη επιβαρημένο χώρο της εγκατάστασης.

5.2.3 Έλεγχος καταλόγων των επιχειρήσεων

Σε πολλές περιπτώσεις, μπορεί κάποιος να βρεθεί σε ένα Super Market ή άλλο κατάστημα αργά τη νύχτα και να αντιμετωπίσει έναν υπάλληλο που πηγαίνει από ράφι στο ράφι να ανιχνεύει αντικείμενα με μια ειδική συσκευή συλλογής δεδομένων. Ο υπάλληλος εκτελεί έναν κατάλογο των εμπορευμάτων, και δεδομένου ότι ανιχνεύει τις πληροφορίες στο τερματικό συλλογής δεδομένων, το τερματικό που χρησιμοποιεί διαβιβάζει τις ανιχνεύσιμες πληροφορίες σε ένα Access Point στο Wi-Fi δίκτυο του καταστήματος. Αυτό επιτρέπει στις πληροφορίες καταλόγων να διαβιβαστούν μέσω του δικτύου Wi-Fi του καταστήματος στον κεντρικό υπολογιστή της επιχείρησης.

5.2.4 Τα δίκτυα Wi-Fi σε σεμινάρια και εκθέσεις

Τα δίκτυα Wi-Fi είναι η ιδανική λύση για τα προσωρινά δίκτυα όπως σε σεμινάρια και εκθέσεις. Με αυτόν τον τρόπο οι παρευρισκόμενοι σε αυτά τα σεμινάρια μπορούν να έχουν άμεση πρόσβαση στο internet και στα εταιρικά τους δίκτυα μέσων των φορητών τους υπολογιστών. Επίσης μπορούν να έχουν άμεση ενημέρωση για διαφορές αλλαγές στο πρόγραμμα των σεμιναρίων ή να πληροφορηθούν για τις παρουσιάσεις που γίνονται στον χώρο των εκθέσεων και να μάθουν για τις εταιρίες που βρίσκονται στον χώρο αυτόν.

5.2.5 Επέκταση του ήδη ενσύρματου δικτύου με το Wi-Fi

Με τη χρησιμοποίηση των Wi-Fi σε επιχειρήσεις, οι διαχειριστές δικτύων ελαχιστοποιούν τα γενικά έξοδα που προκαλούνται κατά επεκτάσεις στα δίκτυα και άλλες

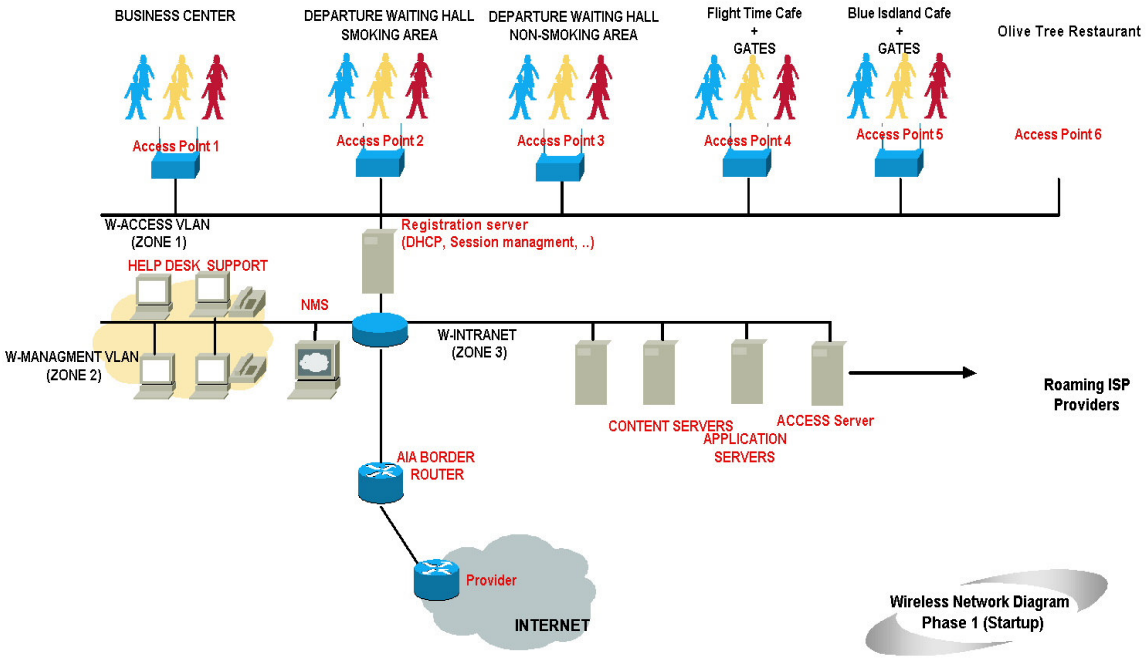
αλλαγές, και μπορούν να επαναπροσδιορίσουν την τοπολογία δικτύων δυναμικά με αποτέλεσμα να αποκτήσουν οι υπάλληλοι ευελιξία στις κινήσεις τους αφού θα αποκτήσουν την δυνατότητα να συνδέονται στο εταιρικό δίκτυο από οποιοδήποτε σημείο μέσα στο κτήριο της εταιρίας. Οι διαχειριστές δικτύων που εγκαθιστούν τους υπολογιστές δικτύων στα παλαιότερα κτήρια (όπως τα παλαιά νοσοκομεία) διαπιστώνουν ότι τα δίκτυα Wi-Fi είναι μια οικονομικώς αποδοτική λύση υποδομής δικτύων δεδομένου ότι εξαλείφουν την ανάγκη για επιθετικές αλλαγές στο περιβάλλον (τρύπες στους τοίχους, μεγάλα καλώδια, κ.λ.π.).

5.3 Τα δίκτυα Wi-Fi στην εκπαίδευση.

Άλλη μία εφαρμογή των δικτύων Wi-Fi είναι στο χώρο της εκπαίδευσης. Με την εγκατάσταση ενός δικτύου Wi-Fi σε έναν εκπαιδευτικό χώρο, όπως τα πανεπιστήμια και τα Τ.Ε.Ι. (Τεχνολογικά Εκπαιδευτικά Ιδρύματα), οι σπουδαστές μπορούν να έχουν συνεχώς πρόσβαση στο δίκτυο σε οποιοδήποτε χώρο του ιδρύματος, με αποτέλεσμα να ενημερώνονται ανά πάσα στιγμή για ανακοινώσεις και θέματα που τους ενδιαφέρουν, και να έχουν πρόσβαση στο internet και τη δυνατότητα να βρουν ανά πάσα στιγμή πληροφορίες που τους ενδιαφέρουν και χρειάζονται.

5.4 Τα δίκτυα Wi-Fi συνδέουν τους ταξιδιώτες.

Με την δημιουργία "hot spot" σε χώρους όπως αεροδρόμια και λιμάνια και ακόμα σε καταστήματα καφέ ή και δημόσιοι χώροι δίνεται η δυνατότητα στους οι επισκέπτες και στους ταξιδιώτες να έχουν με μία μικρή χρέωση ή και ακόμα δωρεάν πρόσβαση στο internet και στα εταιρικά τους δίκτυα μέσω των VPNs. Παράδειγμα αυτών των δυνατοτήτων στην Ελλάδα είναι το δίκτυο Wi-Fi που έχει εγκατασταθεί στους χώρους του αεροδρομίου της Αθήνας όπου οι επισκέπτες και οι ταξιδιώτες με τα laptop και τα PDA τους μπορούν να συνδεθούν στο internet με διάφορους τρόπους πληρωμής (προπληρωμένες κάρτες και πιστωτικές κάρτες κ.τ.λ.), το μοντέλο αυτό αποκαλείται "Neutral Host" που αποτελείται από Access Point, κεραίες, διοικητικό λογισμικό εργασιών, firewalls και δρομολογητές (σχήμα 5.1)



Σχήμα 5.1 : Αρχιτεκτονική του δικτύου Wi-Fi στο Αεροδρόμιο Αθηνών.

5.5 Τα δίκτυα Wi-Fi στα νοσοκομεία.

Υπάρχει ένα ευρύ φάσμα των εφαρμογών κατάλληλων για τα δίκτυα Wi-Fi μέσα σε ένα νοσοκομείο. Ένα παράδειγμα είναι οι πληροφορίες ασθενών, που επιτρέπουν στους γιατρούς και τις νοσοκόμες να χρησιμοποιήσουν τα PDAs ή τα palmtop με την χρήση του δικτύου Wi-Fi να λάβουν και να ενημερώσουν τις πληροφορίες ασθενών. Ένα άλλο παράδειγμα της χρήσης της ασύρματης τεχνολογίας των δικτύων Wi-Fi σε ένα νοσοκομείο είναι η ένταξη του κλινικού εργαστηριακού εξοπλισμού στο σύστημα πληροφοριών. Αυτό επιτρέπει στους διαφορετικούς τύπους εξοπλισμών να κινηθούν από ένα δωμάτιο νοσοκομείου προς άλλο και οι αναγνώσεις τους να διαβιβάζονται μέσω των ασύρματων επικοινωνιών στο δίκτυο Wi-Fi των νοσοκομείων, όπου οι πληροφορίες των βάσεων δεδομένων ασθενών μπορούν να ενημερωθούν. Φυσικά, τέτοιες πληροφορίες περισσότερο από πιθανές χρησιμοποιούνται επίσης από το σύστημα τιμολόγησης για να εξασφαλίσουν ότι οι ασθενείς τιμολογούνται για τις διαφορές εξετάσεις.

5.6 Ποιότητα υπηρεσιών στα Wi-Fi δίκτυα (QoS).

Όπως και κάθε εφαρμογή έτσι και τα δίκτυα Wi-Fi χρειάζονται την ποιότητα υπηρεσιών για την σωστή τους λειτουργία στις διάφορες εφαρμογές τους.

Η QoS (Quality of Services) επιτρέπει στα Access Point των Wi-Fi να δώσουν προτεραιότητα στην κυκλοφορία και να βελτιστοποιήσουν τον τρόπο διαμοιρασμού των

πόρων του δικτύου που διατίθεται μεταξύ των διαφορετικών εφαρμογών. Χωρίς την QoS, όλες οι εφαρμογές που τρέχουν σε διαφορετικές συσκευές έχουν ίση ευκαιρία να διαβιβάσουν τα πλαίσια δεδομένων. Το πρότυπο IEEE 802.11 , αν και έχει γίνει το αδιαμφισβήτητο standard όσον αφορά τα πρωτόκολλα MAC για τα Wi-Fi δίκτυα, παρέχει μια πολλή βασική μέθοδο για την διαφοροποίηση της προτεραιότητας των πλαισίων (PCF Point Coordination Function). Η μέθοδος DCF στηρίζεται στο περιοδικό polling των ασύρματων κόμβων που θα μεταδώσουν από έναν κεντρικό κόμβο, τον επονομαζόμενο point coordinator. Ο point coordinator ελέγχει τη σειρά με την οποία θα μεταδοθούν τα πλαίσια στο ασύρματο δίαυλο, ρυθμίζοντας την ποιότητα υπηρεσίας του κάθε κόμβου. Εκτός από τη μέθοδο PCF η οποία στηρίζεται στην κεντρικό έλεγχο της πρόσβασης στον δίαυλο, έχουν προταθεί και κατανεμημένες μέθοδοι, μερικές από τις οποίες είναι :

- Διαφοροποίηση στην συνάρτηση αύξησης του contention window γιαδιαφορετικές κλάσεις πλαισίων.
- Διαφοροποίηση ως προς το ελάχιστο contention window που αντιστοιχεί στην κάθε κλάση.
- Διαφοροποίηση ως προς την καθυστέρηση μετάδοσης (DIFS) για διαφορετικές κλάσεις πλαισίων.
- Διαφοροποίηση του μέγιστου μήκους πλαισίου για κάθε κλάση

Επίσης έχει προταθεί μια μέθοδος υποστήριξη εφαρμογών πραγματικού χρόνου , η οποία παρέχει εγγύηση για τη μέγιστη καθυστέρηση κάθε πλαισίου, με εκπομπή καταιγισμού θορύβου (black burst) πριν την εκπομπή κάθε πλαισίου πραγματικού χρόνου, η οποία οδηγεί στον προσδιορισμό του σταθμού που πρέπει να εκπέμψει.

Στις παραπάνω μεθόδους για παροχή ποιότητας υπηρεσίας πάνω στο IEEE 802.11, η πιθανότητα κατάληψης του διαύλου καθορίζεται από το μέγεθος του πλαισίου προς εκπομπή. Έχουν επίσης αναπτυχθεί μέθοδοι διαφοροποίησης των υπηρεσιών, στις οποίες η πιθανότητα κατάληψης του διαύλου εξαρτάται και από άλλες παραμέτρους, όπως η διαφοροποίηση της καθυστέρησης στην πρόσβαση ανάλογα με τον αριθμό των σκυταλών ενός token bucket κτλ.

6. Η ΕΞΕΛΙΞΗ ΤΟΥ Wi-Fi

Τα Wi-Fi δίκτυα έχουν πλέον μπει μέσα στις επιχειρήσεις και στα σπίτια καθώς οι πωλήσεις των συσκευών Wi-Fi έχουν αυξηθεί κατά 60% τα τελευταία χρόνια. Οι επαγγελματίες που απαιτούν να έχουν πρόσβαση σε δεδομένα από παντού απαιτούν την δημιουργία "hotspot" δημόσιας πρόσβασης που θα τους παρέχουν ασύρματη πρόσβαση σε τοποθεσίες όπως τα εστιατόρια, καφετέριες, μαγαζιά, αεροδρόμια, ξενοδοχεία και τηλεφωνικούς θαλάμους. Ο αριθμός τους αυξάνεται ραγδαία και αναμένεται μέχρι το 2007 ο αριθμός των "hotspot" στην Αμερική θα 530.000, στην Ευρώπη περίπου 800.000 και πάνω από ένα εκατομμύριο στην Ασία.

Εν' τούτοις η δημόσια πρόσβαση Wi-Fi δεν είναι χωρίς πρόκληση. Η ανησυχία για την ασφάλεια και η δυσκολία να εδραιωθεί ασύρματη πρόσβαση την ίδια στιγμή για πολλούς χρήστες. Η έλλειψη ομοφωνίας πλοήγησης επιβάλει στους χρήστες να διατηρούν πολλαπλούς λογαριασμούς ή χρέωση υπηρεσιών ορισμένου χρόνου ώστε να μπορούν να έχουν πρόσβαση στο internet από οποιοδήποτε δημόσιο "hotspot". Αυτά τα ζητήματα αντιπροσωπεύουν σημαντικά εμπόδια στην ευρέως αποδοχή των δικτύων Wi-Fi δημόσιας πρόσβασης. Μέχρι να επιλυθούν, οι πλήρεις δυνατότητες των δικτύων Wi-Fi δημόσιας πρόσβασης δεν μπορούν να πραγματοποιηθούν και η πανταχού παρών πρόσβαση θα παραμείνει περισσότερο όραμα παρά πραγματικότητα.

6.1 Η επιτυχία του πρότυπου 802.11

Αναγνωρίζοντας τις προοπτικές στην αγορά του πρότυπου 802.11 πολλές ηγετικές εταιρίες ενώθηκαν για να κάνουν το 802.11 ως το μοναδικό αποδεκτό πρότυπο για μεγάλες ταχύτητες για τοπικά ασύρματα δίκτυα . Για αυτόν το σκοπό δημιουργήθηκε ο οργανισμός Wi-Fi Alliances. Με την δημιουργία του οργανισμού Wi-Fi Alliances και του προγράμματος Wi-Fi CERTIFIED, που διασφάλισε την γρήγορη αποδοχή των προϊόντων βασισμένων στο 802.11b , άνοιξε τις πόρτες σε μία έκρηξη αγοράς προϊόντων Wi-Fi σε σπίτια και σε εταιρίες. Τα δίκτυα Wi-Fi έγιναν γρήγορα και ευρέως αποδεκτά από κατασκευαστές και καταναλωτές ομοίως. Πρόσφερε σε κατασκευαστές, προμηθευτές υπηρεσιών και σε υπεύθυνου ανάπτυξης ένα μοναδικό πρότυπο ασύρματης πλατφόρμα για την ανάπτυξη προϊόντων που δημιούργησε ένα κύμα από εισαγωγές νέων προϊόντων.

Χάρης την εκκίνηση του προγράμματος Wi-Fi CERTIFIED το Μάρτιο του 2000 ο οργανισμός Wi-Fi Alliances έχεί πιστοποιήσει πάνω από 1000 προϊόντα. Σήμερα το λογότυπο Wi-Fi αναγνωρίζετε παντού ως ένα σύμβολο δια-λειτουργικότητα και εμπιστοσύνης καταναλωτών στην τεχνολογία ασύρματων τοπικών δικτύων. Και το πρότυπο IEEE 802.11,

όπως η Wi-Fi Alliances σκόπευε, παρουσιάζεται ως το κυρίαρχο πρότυπο για ασύρματα τοπικά δίκτυα παγκοσμίως.

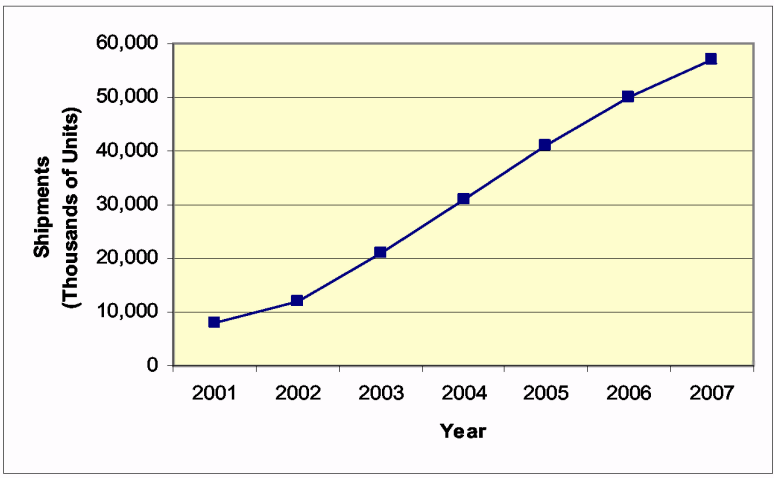
Η βαθιά προσιτότητα του Wi-Fi στο σπίτι και στις εταιρικές τοποθετήσεις έχει επεκταθεί στους δημόσιους χώρους. Η γρήγορη υιοθέτηση του προτύπου και η διαδεδομένης δημοτικότητας του Wi-Fi κέντρισε την ανάπτυξη ασύρματων φορέων παροχής υπηρεσιών internet (WISPs, Wireless Internet Services Providers). Αυτός ο νέος τύπος φορέα παροχής υπηρεσιών αγκάλιασε τα πρότυπα για να δημιουργήσει ένα εξ ολοκλήρου νέο επιχειρησιακό μοντέλο, χτίζοντας δημόσιες υποδομές Wi-Fi για να παρέχει την ασύρματη πρόσβαση internet στους διακινούμενους επιχειρησιακούς χρήστες.

Σήμερα αυτό το μοντέλο εξελίσσεται ως άλλους φορείς παροχής υπηρεσιών, τηλεπικοινωνίες και κινητοί χειριστές, πρόθυμοι να εμπλουτίσουν τις προσφορές τους με ασύρματη συνδεσιμότητα internet, να κάνουν τις δημόσιες υπηρεσίες πρόσβασης Wi-Fi διαθέσιμες προς στους πελάτες τους.

Δεδομένου ότι η αγορά εξελίσσεται, με αυτόν τον τρόπο πραγματοποιούνται οι προσπάθειες της Wi-Fi Alliances. Εκτός από την εργασία της για να εξετάσει και να πιστοποιήσει τη διαλειτουργικότητα των συσκευών Wi-Fi, η Wi-FI Alliances έχει πάρει το προβάδισμα στις πρωτοβουλίες που στοχεύουν στην ενίσχυση και την απλούστευση της εμπειρίας των χρηστών, προωθεί μία τυποποίησης για να μειώσει το κόστος της κατασκευή υποδομής στο δημόσιο χώρο πρόσβασης, και ωθεί την αποδοχή της αγοράς στην δημόσιας πρόσβασης Wi-Fi και προσπαθεί να αναβαθμίσει την ποιότητα και της υπηρεσίες του προτύπου καθιερώνοντας τα πρωτόκολλα 802.11g και 802.11e που προσφέρουν μεγαλύτερες ταχύτητες και ασφάλεια καθώς και τις υπηρεσίες Wi-Fi multimedia όπως την Voice over Internet Protocol (VoIP), Video Streaming και ψυχαγωγικά παιχνίδια.

6.2 Επιτυχία στην αγορά.

Ο ζωηρός ανταγωνισμός μεταξύ των κατασκευαστών των συσκευών Wi-Fi οδήγησε σε μείωση των τιμών στην αγορά που, στη συνέχεια, κατέστησε τη νέα τεχνολογία προσιτή τόσο που ήταν ελκυστική από τους καταναλωτές. Χωρίς καλώδια δικτύων που έδεναν τους υπολογιστές τους στα γραφεία τους, οι χρήστες ήταν τώρα ικανοί να μεταφέρουν τα lap-top ή άλλες φορητές συσκευές τους για να εργαστούν ποίο παραγωγικά, σε συνεργασία και άνετα σε μια ποικιλία από διαφορετικές ρυθμίσεις.



Σχήμα 6.1: Πρόβλεψη πωλήσεων συσκευών Wi-FI

Μέχρι το 2000, η παγκόσμια αγορά για τα προϊόντα WLAN είχε φθάσει σε 785 εκατομμύρια δολάρια. Εκτίμηση των Gartner/Dataquest αναλυτών αγοράς ότι οι παγκόσμιες αποστολές των WLAN adapters θα φθάσουν σε 26,5 εκατομμύρια μονάδες μέχρι το τέλος του 2003, επάνω από 15,5 εκατομμύριο μονάδες από το 2002, και το εισόδημα από εκείνες τις πωλήσεις, πρόβλεψη του Gartner, θα πλησιάσει τα 2,8 δισεκατομμύρια δολάρια (Σχήμα 6.1).

Αυτές οι πωλήσεις έχουν αυξηθεί σημαντικά στην καταναλωτική αγορά. Τα Wi-Fi, η διαλειτουργικότητα, η τυποποίηση, η ογκώθης παραγωγή, η απαιτήσεις και ο ανταγωνισμός έχουν οδηγήσει την τιμολόγηση των προϊόντων WLAN σε ένα επίπεδο που καθένα μπορεί να αντέξει οικονομικά. Σήμερα, είναι δυνατό για ένα πρόσωπο να "αποκτήσει" με κόστος περίπου 80 δολάρια ένα Access Point (AP) 802.11b που επιτρέπει τις επικοινωνίες δικτύων Wi-Fi μέσα σε μια εμβέλεια 100 έως 300 ποδιών. Οι τιμές μίας 802.11b κάρτας διασύνδεσης ασύρματου δικτύου (WNICs, Wireless network interface cards), που επιτρέπουν στα lap-top ή σε άλλες φορητές συσκευές να συνδέσουν με ένα AP και να αποκτήσουν ασύρματη πρόσβαση στο internet, είναι τώρα κάτω από 30 δολάρια. Αυτές οι μειώσεις τιμών κεντρίζουν τις πωλήσεις ακόμα υψηλότερα. Ο Gartner προβλέπει ότι οι αποστολές των Wi-Fi συσκευών σε πελάτες θα πλησιάσουν τα 70 εκατομμύρια στο 2006.

6.2.1 Εμφάνιση της δημόσιας πρόσβασης αγορά

Οι χρήστες είναι τώρα εξοικειωμένοι με την ελευθερία και την κινητικότητα που το Wi-Fi προσφέρει. Απαιτούν υψηλής ταχύτητας ασύρματη πρόσβαση internet σε όλα τα περιβάλλοντα όπου λειτουργούν και παίζουν. Και το αποκτούν.

Το φράγμα χαμηλού κόστους των δικτύων Wi-Fi και η ευκολία με τα οποία τα ιδρύματα μπορούν να τα εγκαταστήσουν έχουν βοηθήσει να κεντράρουν την υιοθέτησή τους σε περιοχές που συχνάζουν οι επιχειρησιακοί ταξιδιώτες και, όλο και περισσότερο, στους δημόσιους χώρους που το ευρύ κοινό συχνάζει. Μπορούν να βρεθούν παντού από τις

περιοχές αναμονής στους διεθνείς αερολιμένες, στις εγκαταστάσεις συνεδρίων, στις παγκόσμιες αλυσίδες ξενοδοχείων και στα εστιατόρια γρήγορων φαγητών.

Αυτά τα δημόσιας πρόσβασης "hotspots" αναπηδούν επάνω σε ένα πολύ γρήγορο ποσοστό για να ικανοποιήσουν τα αιτήματα συνδεσιμότητας των χρηστών που, είναι εξοικειωμένοι με πρόσβαση Wi-Fi, απαιτούν εύκολη ΠΡΌΣΒΑΣΗ, πανταχού παρούσα συνδεσιμότητα όταν ταξιδεύουν μακριά από το σπίτι ή το γραφείο. Αυτά τα hotspot, μέσα στις Ηνωμένες Πολιτείες και σε μεγάλη πλειοψηφία σε όλο τον κόσμο, χρησιμοποιούν τον εξοπλισμό 802.11b. Παρέχουν υψηλής ταχύτητας ασύρματη πρόσβαση internet μέσω ποικίλων προμηθευτών, συμπεριλαμβανομένου WISPs, των παραδοσιακών φορέων παροχής υπηρεσιών, των τηλεπικοινωνιών και των κινητών χειριστών σε προπληρωμένη αμοιβή ή σε "δωρεάν" βάση.

Η Boingo Wireless, ένα διεθνές aggregator των φορέων παροχής υπηρεσιών Wi-Fi, περιγράφει το μέλλον ως "αρπαγή εδάφους" και υπολογίζει ότι υπάρχουν τουλάχιστον 2 εκατομμύρια πιθανές θέσεις hotspot στις Ηνωμένες Πολιτείες μόνο. Αυτές περιλαμβάνουν:

- 212 κέντρα συνεδρίων
- 3.032 σταθμοί τραίνων
- 5.352 αερολιμένες
- 53.500 ξενοδοχεία
- 72.720 επιχειρησιακά κέντρα
- 202.600 βενζινάδικα
- 480.298 εστιατόρια, μπαρ και καφετέριες
- 1.111.300 λιανικά καταστήματα

Αυτοί οι διάφοροι τόποι συναντήσεως βρίσκουν την υπηρεσία Wi-Fi να είναι ένας ελκυστικός αδιαφοροποίητης στην προσέλκυση νέων και συνάμα ίδιας θέσης εισοδήματα. Ένα παράδειγμα είναι δημοφιλές καφέ Starbucks στις Ηνωμένες Πολιτείες. Το Starbucks έγινε ένα από τα πρώτα λιανικά καταστήματα που παρείχαν πρόσβαση Wi-Fi στο internet όταν συνεργάστηκαν το 2001 με το τώρα διεθνές δίκτυο MobileStar για να παρέχουν hotspot σε περισσότερες από 2000 θέσεις. Η MobileStar, τα οποία είχαν επενδύσει βαριά στην ασύρματη υποδομή αρχικά, αρχειοθετημένα για πτώχευση αργότερα εκείνο το έτος. Σήμερα η T-Mobile εξυπηρετεί τα hotspot Starbucks. Και η εμπειρία MobileStar's στέκεται ως μάθημα μέσα σε μια βιομηχανία που αγωνίζεται ακόμα να καθορίσει στερεά επιχειρησιακά πρότυπα σε μια νέα και φυτρώνοντας αγορά που φωνάζει για αυτά.

Δύο βασικά ζητήματα στέκονται εμπόδιο στο δρόμο της διαδεδομένης καταναλωτικής υιοθέτησης και την επιτυχία αυτών των μοντέλων. Αυτά περιλαμβάνουν:

- Μια έλλειψη συνειδητοποίησης μεταξύ των καταναλωτών ότι οι δημόσια προσιτές ασύρματες συνδέσεις υπάρχουν.
- Καταναλωτική ανικανότητα να παραληφθεί το είδος ενός ενιαίου/ λογαριασμού υπηρεσία έχει έρθει να αναμένουν από τους χειριστών κινητών IP που τους παρέχουν τώρα ασύρματη κυψελοειδής τηλεφωνική υπηρεσία.

6.2.2 Συνειδητοποίηση συνδέσεων

Σύμφωνα με τις εκτιμήσεις Gartner, περισσότεροι από 59 εκατομμύρια κινητοί εργαζόμενοι πήραν το δρόμο μέσα το 2002. Πολλοί από αυτούς τους επιχειρησιακούς ταξιδιώτες στηρίζονται στη συνδεσιμότητα δικτύων για να κάνουν τις εργασίες τους. Πολλοί έχουν αρχίσει να προγραμματίζουν το ταξίδι τους (συμπεριλαμβανομένου του ψυχαγωγικού ταξιδιού) και τις στεγάσεις τους γύρω από την διαθεσιμότητα πρόσβασης υψηλών ταχυτήτων στο internet. Αυτοί είναι άνθρωποι που θα επιλέξουν συχνά ένα ξενοδοχείο πέρα από ένα άλλο για να αποφύγουν τη δαπάνη και την περιορισμένη παραγωγικότητα των αργών dial-up συνδέσεων, ή που θα συχνάσουν σε μία καφετέρια ή σε ένα εστιατόριο με πρόσβαση Wi-Fi για να ελέγξουν το ηλεκτρονικό ταχυδρομείο τους κατά τη διάρκεια του μεσημεριανού γεύματος και των διαλειμμάτων τους. Είναι οι προφανείς πελάτες των Wi-Fi δημόσιας πρόσβασης.

Εντούτοις, μια καταναλωτική αγορά για Wi-Fi δημόσιας πρόσβασης, που οδηγείται από τις συνεχώς αυξανόμενες πωλήσεις των συσκευών Wi-Fi στο σπίτι, φαίνεται ακόμα μεγαλύτερη. Οποιοσδήποτε χρήστης με ένα lap-top με δυνατότητα Wi-Fi ή ένα PDA μπορεί να έχει πρόσβαση στο internet μέσω ενός Hotspot δημόσιας πρόσβασης. Τα hotspot αρχίζουν να πολλαπλασιάζονται, ακόμη και στις θέσεις που οι επιχειρησιακοί ταξιδιώτες δεν συχνάζουν, για να εξυπηρετήσουν εκείνη την ευρύτερη απαίτηση. Σήμερα, μπορούν να βρεθούν στα θέρετρα, στις κατασκηνώσεις, στις μαρίνες και στα κρουαζιερόπλοια.

Η εταιρία Arizona, υπολογίζει ότι μέχρι το 2007 ο αριθμός hotspot θα αυξηθεί σε 530.000 στις Ηνωμένες Πολιτείες, σχεδόν 800.000 στην Ευρώπη και περισσότερο από ένα εκατομμύριο στην Ασία.

Όλο και περισσότερο, όλο και περισσότερα lap-top στέλνονται με ενσωματωμένη τεχνολογία Wi-Fi πάνω τους. Πλέον δεν θα απαιτείται η αγορά μιας χωριστής κάρτας Wi-Fi. Υπολογίζεται ότι 40-50% όλων των νέων lap-top θα έχουν ενσωματωμένη τεχνολογία Wi-Fi. Αυτό θα οδηγήσει τη χρήση του Wi-Fi στο σπίτι, αλλά θα οδηγήσει επίσης την απαίτηση για τη χρήση δημόσιας πρόσβασης από τους επιχειρησιακούς ταξιδιώτες. Περαιτέρω, αναμένεται ότι το Wi-Fi θα είναι τόσο κοινό όσο ένα modem σε ένα lap-top στα επερχόμενα έτη.

Ακόμα, ακόμη και καθώς όλο και περισσότεροι χρήστες γίνονται αποδέκτες Wi-Fi μέσω των αγορών των νέων συσκευών, είναι ανίκανοι να το χρησιμοποιήσουν πλήρως και να απολαύσουν την υπηρεσία Wi-Fi hotspot. Τα πολυάριθμα εμπόδια στέκονται στο δρόμο τους.

Ο αρχηγός μεταξύ αυτών των εμποδίων είναι συνειδητοποίηση των χρηστών της υπηρεσίας Wi-Fi. Οι πιθανοί πελάτες θα μπορούσαν ήδη να είναι σε μια περιοχή με τις υπηρεσίες Wi-Fi και να το μην το ξέρουν. Αντίθετα από επιλογές επάνω από έναν μετρητή ή ένα προϊόν σε ένα ράφι, ένα Wi-Fi δημόσιας πρόσβασης που προσφέρει σε ένα εστιατόριο ή ένα κατάστημα λιανικής που υπάρχει στον αέρα είναι αόρατα σε έναν καταναλωτή. Όχι μόνο είναι οι χρήστες απληροφόρητοι ότι η πρόσβαση Wi-Fi στο internet είναι διαθέσιμη σε μια θέση, συχνά δεν ξέρουν εάν θα υπάρξει ένα hotspot στον προορισμό ταξιδιού τους, πώς να το προσδιορίσουν όταν φθάνουν εκεί, ή πώς να κάνουν σύνδεση εάν υπάρχει.

Αυτό το πρόβλημα της συνειδητοποίησης υπηρεσιών θέτει ένα σοβαρό εμπόδιο στην αύξηση της βιομηχανίας. Τα εργαστήρια Forrester επιφυλάζονται ότι τα δημόσια WLAN hotspot θα φτάσουν σε περίπου 7,7 εκατομμύρια χρήστες μέχρι το 2008.

Η Wi-Fi Alliances εξετάζει αυτό το πρόβλημα μέσω του προγράμματος Wi-Fi ZONE της, το οποίο επεκτείνει την αναγνώριση της συμμαχίας στο ευρέως πρόγραμμα διαβεβαίωσης διαλειτουργικότητας στα δημόσιας πρόσβασης hotspot.

Η πιστοποίηση Wi-Fi ZONE έχει ως σκοπό να βελτιώσει την πληροφόρηση των χρηστών για τα Wi-Fi hotspot και να οδηγήσει στην απαίτηση για δημόσιες υπηρεσίες πρόσβασης Wi-Fi που προσφέρονται από τους ασύρματους φορείς παροχής υπηρεσιών internet (WISPs), τους aggregators, τις τηλεπικοινωνίες και τους κινητούς χειριστές, ακριβώς όπως η πιστοποίηση Wi- Fi έχει κάνει για την πώληση των συσκευών Wi-Fi.

Το Wi-Fi ZONE λέει στους χρήστες πού να βρουν εγκεκριμένο Wi-Fi, δημόσια προσιτή ασύρματη υπηρεσία internet με την προσφορά ενός online καταλόγου που μπορούν να χρησιμοποιήσουν για να βλέπουν την τοποθεσία των Wi-Fi ZONE στον προορισμό τους. Επίσης παρέχει εμπορικά σήματα Wi-Fi ZONE, και επιτρέπει στους χειριστές των τόπων συναντήσεως κυρίως να επιδείξουν τα παγκοσμίως αναγνωρισμένα διακριτικά Wi-Fi για να παρουσιάσει στους πελάτες ότι η υπηρεσία Wi-Fi είναι διαθέσιμη στη θέση τους και ότι η υπηρεσία τους έχει πιστοποιηθεί από την Wi-FI Alliances για να είναι διαλειτουργική με τον Wi-Fi CERTIFICATION εξοπλισμό του χρήστη.

6.2.3 Πλοήγηση

Υψηλού προφίλ hotspot όπως τα Starbucks και τα McDonalds δίνουν σημασία στην δυνατότητα της πανταχού παρούσας διαθεσιμότητας υπηρεσιών. Αλλά παρά την αφθονία των

τίτλων αυτών των hotspot που έχουν παράγει, η πρόσβαση των διάφορων WISP (Wireless Internet Service Provider) δικτύων δεν είναι ούτε συνεχής ούτε εύκολη όπως οι πρώτοι χρήστες αυτών των δικτύων μπορούν να βεβαιώσουν. Οι χρήστες που προσπαθούν να συνδεθούν από τους διαφορετικούς προμηθευτές hotspot αντιμετωπίζουν μια σειρά επιλογών σύνδεσης και σχεδίων τιμολόγησης από διαφορετικούς προμηθευτές. Αυτοί οι προμηθευτές χρησιμοποιούν ποικίλα σχέδια να επικυρώσουν τους χρήστες προκειμένου να εγκρίνουν την χρήση και η τιμολόγηση της σύνδεσης. Αυτό περιπλέκει αυτό που πρέπει να είναι μια απλή διαδικασία. Μια τυποποιημένη διαδικασία σύνδεσης απαιτείται.

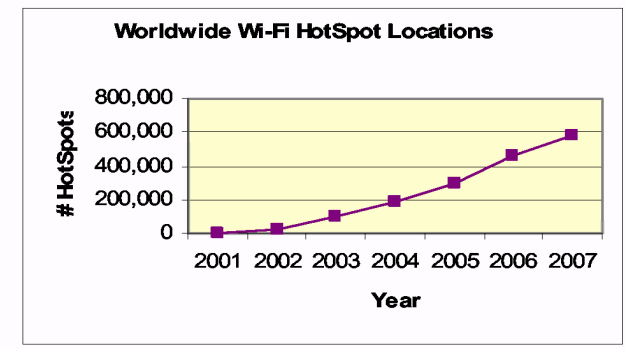
Πολλοί προμηθευτές έχουν αρχίσει να εξετάζουν το πρόβλημα μέσω των συμφωνιών πλοήγησης ο ένας με τον άλλον, και με τούς aggregators και τα γραφεία συμψηφισμού. Με τις συμφωνίες πλοήγησης σε ισχύ, είναι σε θέση να συμφιλιώσουν τις ανόμοιες διαδικασίες σύνδεσης και τιμολογούν με ένα ενιαίο λογαριασμό σύνδεσης τις δαπάνες των λογαριασμών πίσω στον εγχώριο προμηθευτή του χρήστη.

Δεδομένου ότι η αγορά συνεχίζει να εξελίσσεται και περισσότεροι προμηθευτές αγκαλιάζουν τις συμφωνίες πλοήγησης ενιαίου-λογαριασμού, οι χρήστες θα απολαύσουν την απλουστευμένη "ενιαία σύνδεση απολογισμού" στις διάφορες θέσεις και όλες οι δαπάνες θα τιμολογηθούν πίσω σε αυτούς μέσω των μεμονωμένων προμηθευτών τους.

Πολλή δουλειά παραμένει να γίνει. Αλλά σε πολλές μεγάλες πόλεις όπου οι χρήστες περιπλανώνται από hotspot σε hotspot καθώς ταξιδεύουν μέσω των ξενοδοχείων και περιοχών συμβάσεων, είναι ήδη δυνατό στην αναλαμπή στο μέλλον της απεριόριστης δυνατότητας πλοήγησης.

6.2.4 Πανταχού παρών κινητικότητα

Τελικά, η αγορά δημόσια πρόσβασης Wi-Fi είναι ισορροπημένη για να παρέχει την εμπειρία κάλυψης για τους επιχειρησιακούς ταξιδιώτες σε μια άνευ ραφής μόδα πέρα από το "διάδρομο επιχειρησιακού ταξιδιού." Η αύξηση του αριθμού των hotspot Wi-Fi παρουσιάζει τη δυνατότητα για τους χρήστες να περιπλανούνται από hotspot σε hotspot (Σχήμα 6.2).



Σχήμα 6.2: Πρόβλεψη αύξησης σημείων hotspot

Η πανταχού παρούσα κινητικότητα θα προκαλέσει σε νέες ασύρματες εφαρμογές και επιχειρησιακές ευκαιρίες, όπως στην ψυχαγωγία και σε εφαρμογές φωνής και τηλεοπτικές, οι οποίες θα υποστηρίζουν κινητά IP –like sessions (η ψηφιακή πλοήγηση που παρέχει συνεχή συνδεσιμότητα και άνευ ραφής hands-off, με τον ίδιο τρόπο όπου οι εφαρμογές φωνής πάνω στην τηλεφωνική κυψελοειδή υπηρεσία λειτουργεί σήμερα). Αυτή η σύγκλιση, και οι ευκαιρίες που αντιπροσωπεύει, δεν μπορούν να συνειδητοποιηθούν πλήρως έως ότου είναι σε θέση η αγορά δημόσιας πρόσβασης Wi-Fi να παρέχει μια ποίο απλουστευμένη και άνευ ραφής εμπειρία στο χρήστη από ότι είναι διαθέσιμη σήμερα.

6.3 Η αλυσίδα αξίας της δημόσιας πρόσβασης

Το τοπίο της δημόσιας πρόσβασης είναι τεμαχισμένο. Εντούτοις, διάφοροι βασικοί φορείς που καταλαμβάνουν θέσεις μέσα στη αλυσίδα αξίας της δημόσιας πρόσβασης (Σχήμα 6.3) εργάζονται για να ενθαρρύνουν νέες αγορές και επιχειρησιακά πρότυπα καθώς η ζήτηση για υπηρεσίες Wi-Fi αυξάνονται. Αυτοί κυμαίνονται από τους ιδιοκτήτες hotspot που παρέχουν τους τόπους συναντήσεως των πελατών στους aggregators που ανήκουν στους πελάτες και στους φορείς παροχής υπηρεσιών που τους ανήκει η υποδομή.

Κάθε σύνδεσμος της αλυσίδας έχει μια μοναδική προσέγγιση και ένα μοναδικό σύνολο επιχειρησιακών οδηγιών. Κάθε ένας παρέχει επίσης μια κλιμακωτή αγορά προστιθεμένης αξίας υπηρεσιών που κυμαίνονται από τους ειδικούς του IT που παρέχουν και εξασφαλίζουν το δίκτυο στα γραφεία συμψηφισμού που παρέχουν την επικύρωση των χρηστών και τη συμφιλίωση τιμολόγησης για τους προμηθευτές.

Σχήμα 6.3: Η αλυσίδα αξίας της δημόσιας πρόσβασης

Πολλοί συμμετέχουν επίσης σε ένα δίκτυο συνεργασιών και στρατηγικών σχέσεων σχεδιασμού με σκοπό για να επεκτείνουν γρήγορα και να ενισχύσουν τις προσφορές στους πελάτες τους. Η Wi-Fi Alliances λειτουργεί με κάθε ένα από αυτούς τους φορείς για να διευκολύνει την ανάπτυξη απλουστευμένων, εφαρμόσιμων επιχειρησιακών μοντέλων που κινούν τη βιομηχανία μπροστά.

6.3.1 Ιδιοκτήτες ενώσεών & συνεργάτες

Οι λιανικοί τόποι συναντήσεως διαπιστώνουν ότι η πρόσβαση Wi-Fi στο Inetrnet μπορεί να είναι ένας ισχυρός μαγνήτης που προσελκύει νέους πελάτες, κρατά την πίστη στους πελάτες και αυξάνει τις πωλήσεις στα καταστήματα. Τα hotspot χρησιμοποιούν πολλά διαφορετικά πρότυπα εισοδήματος για να οδηγήσουν αυτήν την επιχείρηση.

Αυτοί που επιλέγουν είναι κατά ένα μεγάλο μέρος μια συνάρτηση από την βάσης πελατών τους, μαρκάρουν και τη φύση της επιχείρησης τους και επιδιώκουν να τους προσελκύσουν. Ένας Πρόεδρος τμήματος στα εστιατόρια Mc Donald's, παραδείγματος χάριν, προσδιόρισε τον επιχειρησιακό οδηγό εκεί όταν ανήγγειλε ένα rollout hotspot, "εμείς θέλουμε τα Golden Archers να είναι η πρώτη επιλογή για ένα μεγάλο γεύμα και μια θέση για να πάει ασύρματα". Σε αντίθεση, ο περιφερειακός γίγαντας των αμερικανικών τηλεπικοινωνιών, Verizon, χρησιμοποιεί τα Wi-Fi για να ενισχύσει την προσφορά στους απευθείας σύνδεσης DSL πελάτες. Και σε πολλές θέσεις, οι εθελοντές πολίτες, συμπεριλαμβανομένων των μελών του NYCWireless στις Ηνωμένες Πολιτείες και του Elecktrosmog στη Σουηδία, παρέχουν hotspot ως δωρεάν υπηρεσία στις κοινότητές τους.

Η Wi-Fi Alliances έχει αναγνωρίσει οργανώσεις που αντιπροσωπεύουν τις υψηλών απαιτήσεων τόπων συναντήσεως και εργάζονται μαζί τους. Μερικοί από αυτούς είναι:

- Η Ασύρματη ένωση αερολιμένων (WAA, Wireless Airport Association) και η Διεθνής ένωση-ασφάλειας, διαδικασίες & υποδομή αεροπορικών μεταφορών (IATA - SO&I, International Air Transport Association-Safety, Operations & Infrastructure).
- Η National Multi-Housing Council - Multi-family Information and Transactions Standards (NMHC-MITS).
- Η Εθνική ένωση εστιατορίων.
- Το Αμερικάνικο υπουργείο μεταφορών , η ομοσπονδιακή διοίκηση αεροπορίας και η διοίκηση ασφάλειας μεταφορών.

Το WAA και το IATA - SO&I, παραδείγματος χάριν, καθορίζουν προς το παρόν τα πρότυπα για την υπηρεσία Wi-Fi αερολιμένων και λειτουργούν για να καλύψουν την ασφάλειας και τις ανάγκες των καταναλωτών, των επιβατών, των υπαλλήλων και των μισθωτών στους αερολιμένες. Το NMHC - MITS λειτουργούν για να αναπτύξουν τα πρότυπα για τις συναλλαγές στη βιομηχανία της κατοικίας.

6.3.2 Aggregators & γραφεία συμψηφισμού

Η βοήθεια των Aggregators παρέχει μια άνευ ραφής εμπειρία στους χρήστες hotspot με τη συνάθροιση των υπηρεσιών πολλών διαφορετικών WISP δικτύων για να προσφέρει μία

σφαιρική πρόσβαση Wi-Fi στο πλαίσιο των ενιαίων σχεδίων τιμολόγησης. Οι Aggregators χαρακτηριστικά πωλούν τις υπηρεσίες στους και στις χονδρικές και λιανικές αγορές, στοχεύοντας στις επιχειρήσεις και τα άτομα που απαιτούν σφαιρική συνδεσιμότητα. Η πρόκλησή τους είναι να αναπτύξουν μια συνεπή προσφορά στους πελάτες με την καλλιέργεια των συμφωνιών πλοήγησης πέρα από ένα διαφορετικό σύνολο επιχειρησιακών συνεργατών.

Οι Aggregators αντιπροσωπεύουν τους βασικούς συνεργάτες στους WISPs που τους ανήκει η υποδομής και επιδιώκουν να μεταπωλήσουν τη συνδεσιμότητά στους μεταφορείς τηλεπικοινωνιών, καθώς επίσης και στους εικονικούς χειριστές δικτύων Wi-Fi (WVNOs, Wi-Fi Virtual Network Operators) που προσφέρουν τις υπηρεσίες συνδεσιμότητας και τους ανήκουν οι πελάτες αλλά δεν τους ανήκει η υποδομή. Οι Aggregators προσφέρουν στους πελάτες των WVNOs την δυνατότητα να περιπλανώνται εύκολα και αόρατα μεταξύ των συνεταιρικών δικτύων.

Ομοίως, οι aggregators συνεργάζονται με τους παραδοσιακούς μεταφορείς, που παρέχουν τις τηλεπικοινωνίες DSL και στους προμηθευτές καλωδίων την ευκαιρία να συσσωρεύσουν την πρόσβαση Wi-Fi στις σε απευθείας σύνδεση προσφορές τους. Αυτές οι συνεργασίες όχι μόνο ενισχύουν τις υπηρεσίες που ο μεταφορέας προσφέρει στους πελάτες, αλλά επιτρέπουν στον μεταφορέα να επεκτείνει γρήγορα το δίκτυο των hotspot όπου οι πελάτες τους μπορούν να έχουν άμεση πρόσβαση.

Τα γραφεία συμψηφισμού είναι γραφεία υπηρεσιών τρίτων που παρέχουν την τακτοποίηση, την τιμολόγηση, τον έλεγχο πρόσβασης, την επικύρωση και τις λογιστικές υπηρεσίες στα περισσότερα από τα μέλη στην αλυσίδα αξίας, συμπεριλαμβανομένων των χονδρικών πελατών, των χειριστών δικτύων και των ικανοποιημένων προμηθευτών, ISPs και διεθνείς χειριστές δικτύων. Το δίκτυο των συνεργασιών τους περιλαμβάνει χαρακτηριστικά άλλα γραφεία συμψηφισμού και aggregators οι οποίοι παρέχουν ενσωματωμένη συνδεσιμότητα και επιλογές ασφάλειας, καθώς επίσης και άλλες υπηρεσίες τεχνολογίας.

Όπως με τους aggregators, το επιχειρησιακό πρότυπο των γραφείων συμψηφισμού εξελίσσεται. Προς το παρόν, περιπλέκεται από μια έλλειψη προτύπων και ασυμβίβαστων μεθοδολογιών συλλογής δεδομένων. Αλλά αυτό το πρότυπο, επίσης, κινείται προς ένα που υπόσχεται στους καταναλωτές την προβλέψιμη και συνεπή τιμολόγηση για τις υπηρεσίες hotspot καθώς περιπλανώνται από μια θέση του φορέα παροχής υπηρεσιών σε άλλη.

Η παρούσα κατάσταση δεν είναι αντίθετη από τις αρχικές ημέρες της κυψελοειδούς τηλεφωνικές υπηρεσίες όταν οι χρήστες έπρεπε να πληκτρολογούν κωδικούς καθώς κινούνται μεταξύ των δικτύων διαφορετικών προμηθευτών και λαμβάνουν χωριστούς λογαριασμούς από κάθε προμηθευτή. Ακριβώς όπως η βιομηχανία κυψελοειδή τηλεφώνων εργάστηκε γρήγορα για να ξεπεράσουν οι χρήστες τη δυσκολία τη χειρωνακτική επέμβαση

καθώς περιπλανούνται από μια περιοχή του φορέα παροχής υπηρεσιών σε άλλη, η βιομηχανία Wi-Fi εργάζεται προς την παροχή στους πελάτες τους έναν ενιαίο λογαριασμό που παγιώνει τις δαπάνες στα δίκτυα.

6.3.3 Προμηθευτές υπηρεσιών

Οι WISPs είναι οι κυρίαρχοι ιδιοκτήτες της υποδομής δημόσιας πρόσβασης WLAN. Με μεγάλο κόστος, επέκτειναν ευρέως την τεχνολογία WLAN για να δημιουργήσουν μια προσφορά που να ανταγωνίζεται άμεσα τους προμηθευτές με καλώδιο και DSL για την παράδοση ευρυζωνικών υπηρεσιών internet. Οι WISPs επεκτείνουν και διεκπεραιώνουν ασύρματες υπηρεσίες internet για τους τόπους συναντήσεως και για τη διάσπαση του εισοδήματος μεταξύ τους.

Εντούτοις, οι ημέρες της ογκώδους κατασκευής της υποδομής για την παροχή αυτής της υπηρεσία τελειώνουν. Πολλοί πρώτοι φορείς έχτισαν τις δαπανηρές υποδομές για να παρέχουν "backhaul" το οποίο εξασφάλιζε εγγυημένα επίπεδα απόδοσης στον τόπο συναντήσεως. Διάφοροι πρώτοι φορείς, συμπεριλαμβανομένου της MobileStar και της hereUare, λύγισαν κάτω από το κόστος και πτώχευσαν. Εντούτοις, άλλοι όπως η Wayport έχουν χτίσει τις επιτυχείς επιχειρήσεις μέσω των συνεργασιών, που επικυρώνουν το WISP πρότυπο και που παρέχουν την ώθηση για τους νέους παίκτες να μπουν μέσα στο παιχνίδι. Νεοφερμένοι όπως Starhub στην Ασία και η The Cloud στη δυτική Ευρώπη μόλις μπήκαν.

6.4 Διαθέσιμες τεχνολογίες - φόρουμ και ενσωματωμένα πρότυπα

Ένας αριθμός από διάφορα φόρουμ εφαρμοσμένης μηχανικής και οργανώσεις βιομηχανίας συνεργάζονται μαζί στις βασικές περιοχές για να αναπτύξουν τα διαλειτουργικά πρότυπα που θα γεφυρώσουν τα συμφέροντα όλων αυτών των φορέων και θα προσκρούσουν άμεσα στην εξέλιξη της δημόσιας πρόσβασης Wi-Fi. Αυτοί περιλαμβάνουν:

- Το Ίδρυμα ηλεκτρικών και μηχανικών ηλεκτρονικής (IEEE), το ευρωπαϊκό πρότυπο τηλεπικοινωνιών Institute/Broadband Radio Access Networks (ETSI/BRAN European Telecommunications Standards Institute/Broadband Radio Access Networks) και η πολυμέσική κινητή πρόσβασης επικοινωνίας σύστημάτων-υψηλής ταχύτητας ασύρματη πρόσβασης υποεπιτροπή (MMAC-HSWA Multimedia Mobile Access Communication Systems-High Speed Wireless Access Subcommittee). Αν και δεν συμμετέχουν συγκεκριμένα σε δραστηριότητες σχετικές με τη δημόσια πρόσβαση, η IEEE, το ETSI και το MMAC εμπλέκονται ζωτικά στον καθορισμό των προτύπων για WLANs. Υποστηρίζουν από κοινού την αλληλεπιδρώντας ομάδα WLAN (WIG, WLAN Interworking Group), η οποία εξετάζει τα αλληλεπιδρώντας θέματα. Η WIG λειτουργεί για να καθορίσει μια γενική διεπαφή μεταξύ του τοπικού δικτύου Wi-FI και των δημόσιων (κυψελοειδών) δικτύων.

• Η ομάδα εργασίας εφαρμοσμένης μηχανικής internet (IETF, internet Engineering Task Force) εργάζεται για να καθιερώσει τα πρωτόκολλα που χρησιμοποιούνται για την επικύρωση των χρηστών στα δίκτυα.

• Το 3ο πρόγραμμα συνεργασίας παραγωγής (3GPP, Generation Partnership Project) και το 3GPP2. Το 3GPP λειτουργεί για να τυποποιήσει την αρχιτεκτονική και να διευκρινίσει τα πρωτόκολλα για τα WLAN-3GPP την αλληλεπίδραση που περιλαμβάνει τον έλεγχο πρόσβασης, την επικύρωση και τη λογιστική. Το 3GPP2 άρχισε μόλις να λειτουργεί στην αλληλεπίδραση των WLAN-3GPP2. Αυτοί οι δύο οργανισμοί επιδιώκουν να συγκλίνουν τα ευρύτατα επεκταμένα κυψελοειδή πρότυπα GSM (Groupe Speciale Mobile) και το CDMA μέσω της τρίτης γενιάς κυψελοειδούς τεχνολογίας (3G).

• Η οργάνωση πρωτοκόλλου internet λεπτομερών αρχείων (IPDR, Internet Protocol Detail Record) εργάζεται για να καθιερώσει μια λογιστικής και τακτοποίηση προδιαγραφή που θα προωθήσει την πλοήγηση στα hotspot. Η λογιστικής ασύρματου τοπικού LAN και η ομάδα εργασίας τακτοποίησης επιδιώκει να τυποποιήσει την οικονομική επεξεργασία μεταξύ των ασύρματων χειριστών.

6.5 Εμπόδια στη μαζική υιοθέτηση

Αν και οι φορείς στην αλυσίδα αξίας σφυρηλατούν γρήγορα τα επιχειρησιακά πρότυπα για να οδηγήσουν την αγορά της δημόσια πρόσβασης, παραμένουν τα πολυάριθμα εμπόδια στη μαζική υιοθέτηση που πρέπει να εξεταστούν προτού μπορέσει να επιτευχθεί η πανταχού παρούσα κινητικότητα. Αυτά τα εμπόδια περιλαμβάνουν την περιορισμένη δημόσια πληροφόρηση των συνδέσεων Wi-Fi, ασυμβίβαστα τεχνικά πρότυπα καθώς οι χρήστες κινούνται από hotspot σε hotspot, η έλλειψη ομοιόμορφων διαδικασιών επικύρωσης και συμφωνιών πλοήγησης ενιαίου-λογαριασμού, όπως αναφέρεται ανωτέρω.

6.5.1 Δημόσια πληροφόρηση

Το Wi-FI μπορεί να είναι παντού, αλλά εάν δεν προσδιορίζεται από έναν κοινώς αναγνωρισμένο προμηθευτή υπηρεσιών είναι αόρατο στους χρήστες. Η Telcos και άλλοι χειριστές δικτύων που συνεργάζονται μαζί, και μεταπωλούν, τις υπηρεσίες των aggregator κάτω από τα δικά τους εμβλήματά έχουν κάνει καλή δουλειά στη διαφήμιση των προσφορών δημόσιας πρόσβασης τους, και οδηγούν την πληροφόρηση των χρηστών και τις απαιτήσεις τους για υπηρεσίες hotspot. Αυτοί οι προμηθευτές προσφέρουν πληροφορίες στους πελάτες τους για το πώς να συνδεθούν και να έχουν πρόσβαση σε ένα δημόσιο hotspot, καθώς επίσης και για τους online καταλόγους των hotspot στα δικά τους δίκτυά και εκείνα των συνεργατών τους. Αλλά αυτοί δεν αγκαλιάζουν άλλα ανταγωνιστικά δίκτυα για να προσφέρουν στους

χρήστες μια πλήρη επισκόπηση των επιλογών τους με τον τρόπο όπου το πρόγραμμα Wi-Fi ZONE κάνει, ιδιαίτερα ως σφαιρικός δείκτης της διαθεσιμότητας υπηρεσιών.

Πολύ δουλειά παραμένει να γίνει στον τομέα της εκπαίδευσης και της υποστήριξης. Πολλοί χρήστες το βρίσκουν ακόμα δύσκολο να κάνουν μια σύνδεση. Αν και πολλά hotspot λειτουργούν με το Wi-Fi NICs των χρηστών, επιτρέποντας τους συνδεθούν αυτόματα όταν ενεργοποιούν τον φυλλομετρητή τους, άλλα απαιτούν από τους χρήστες να διαμορφώσουν με το χέρι τη δικιά τους σύνδεση για πρόσβασή. Μερικά λειτουργικά συστήματα στερούνται την αυτόματη ανακάλυψη των δικτύων Wi-Fi, απαιτούν από τους χρήστες να εκτελέσουν τις χειροκίνητη ανίχνευση για να βρουν το δίκτυο. Ανάλογα με ποιο Wi-Fi NIC χρησιμοποιούν, οι χρήστες μπορεί να πρέπει να τρέξουν ένα Wi-FI πρόγραμμα διαχείρισης και να δημιουργήσουν μια νέα θέση δικτύου. Αυτό δεν είναι εύκολο για τον αμύητο.

6.5.2 Ανησυχία για την ασφάλεια

Το σενάριο περιπλέκεται περαιτέρω από την ανοικτή φύση των δικτύων Wi-Fi δημόσιας πρόσβασης και η ανησυχίας των χρηστών ότι τα στοιχεία τους μπορούν να εκτεθούν. Τα μέτρα ασφάλειας όπως η Wi-Fi Protected Access (WPA) και η Wired Equivalent Privacy (WEP) απαιτούν κλειδιά που δεν διανέμονται εύκολα στα hotspot. Προκειμένου να προωθηθούν η ανεμπόδιστη πρόσβαση και η μέγιστη χρήση των hotspot τους, οι ιδιοκτήτες των τόπων συναντήσεως ενργοποιούν σπάνια αυτά τα μέτρα ασφάλειας.

Αν και η μεγάλη πλειοψηφία των φορέων παροχής υπηρεσιών χρησιμοποιεί την ασφάλεια ασφαλή υποδοχών επιπέδων (SSL, Secure Socket Layer) για να προστατευθούν οι μεταδόσεις των στοιχείων πιστωτικής κάρτας και σύνδεσης, άλλα δεδομένα συμπεριλαμβανομένου του ηλεκτρονικού ταχυδρομείου κατεβαίνουν και φορτώνονται χαρακτηριστικά στον αέρα. Μερικοί φορείς παροχής υπηρεσιών προειδοποιούν για αυτό το γεγονός και συστήνουν στους πελάτες τους να επεκτείνουν προσωπικά Firewall και κρυπτογράφηση εικονικών ιδιωτικών δικτύων (VPN, Virtual Private Network) εάν είναι διαθέσιμα. Οι χρήστες που επιθυμούν να χρησιμοποιήσουν την κρυπτογράφηση VPN αντιμετωπίζουν συχνά την ποιο περίπλοκη πρόκληση του να πρέπει να εγκατασταθεί και να ενεργοποιηθεί λογισμικό κρυπτογράφησης.

6.5.3 Σύνθετα πρότυπα τιμολόγησης

WISPs και οι μεταφορείς προσφέρουν συνήθως μία λίστα από επιλογές σχεδίων τιμολόγησης για τους πελάτες Wi-Fi, συμπεριλαμβανομένου κάποιου συνδυασμού σταθερών αμοιβών, αμοιβών χρήσης και αμοιβών υπηρεσιών.

Οι σταθερές αμοιβές καλύπτουν τις βασικές χρεώσεις υπηρεσιών και αγοράζονται συνήθως ανά την ημέρα, είτε ως εικοσιτετράωρη περίοδος κυλίσματος από τον χρόνο αγοράς

είτε σταθερή καθημερινή δαπάνη, είτε ως μηνιαίο σχέδιο. Σχεδόν όλες οι υπηρεσίες συνδρομής προσφέρουν ομαλής μηνιαίας αμοιβής, χρεώνοντας μία φορά τον μήνα. Άλλες δαπάνες μπορούν να προστεθούν, όπως οι αμοιβές για τον αριθμό των συσκευών που έχουν πρόσβαση στα δίκτυα ή δαπάνες θέσης που αξιολογούνται από τα hotspot.

Ο υπολογισμός των αμοιβών υπολογίζονται χρεώνοντας τις αυξήσεις των αριθμών των byte που χρησιμοποιούνται, του χρονικού διαστήματος που ξοδεύεται on-line ή (στην περίπτωση των προμηθευτών όπως οι aggregators που δεν διατηρούν άμεσα το δίκτυο) του αριθμού των επιτυχών επικυρώσεων.

Οι αμοιβές των υπηρεσιών προστίθενται συχνά στη χρήση ή τις σταθερές αμοιβές καθώς η αξία της υπηρεσίας βελτιώνεται. Παραδείγματος χάριν, οι ανά λεπτού δαπάνες μπορούν να προστεθούν ως διαθέσιμες αυξήσεις εύρους ζώνης. Τα ποιο κοινά πρότυπα τιμολόγησης περιλαμβάνουν συγκεκριμένες δαπάνες πρόσβασης για τη διαθεσιμότητα εύρους ζώνης, το ηλεκτρονικό ταχυδρομείο ή τις ειδικές υπηρεσίες όπως τα VPN, και τις δαπάνες για τις υπηρεσίες add-on όπως το streaming video ή voice-over IP.

Ενώ αυτά τα σχέδια τιμολόγησης προσφέρουν στους χρήστες έναν ευπρόσδεκτα μεγάλο αριθμό επιλογών, η έλλειψη προσφορών "σφαιρικών υπηρεσιών ενιαίου λογαριασμού" ανατρέπουν ακόμα τους χρήστες που δεν θέλουν να διαπραγματευτούν μαζί με ένα πλήθος διαφορετικών δαπανών από διαφορετικούς φορείς παροχής υπηρεσιών.

6.5.4 Δυσκολία στην πλοήγηση

Η σύνδεση με το internet μέσω των hotspot σε διάφορες θέσεις μπορεί να είναι δύσκολη. Είναι συχνά αδύνατο για έναν πελάτη ενός WISP να συνδεθεί σε μια τοποθεσία hotspot που συντηρείται από έναν άλλον χωρίς το άνοιγμα ενός εξ ολοκλήρου νέου λογαριασμού, και να έχει πέρα δώσε με ένα εξ ολοκλήρου διαφορετικού συνόλου διαδικασιών σύνδεσης και επικύρωσης. Η κατάσταση συγκρίνεται με τις αρχές των ημερών των κυψελοειδών τηλεφώνων όταν ήταν αδύνατο να γίνει μια σύνδεση ενώ ταξίδευες έξω από την καλώντας περιοχή του μεταφορέα σας.

Η βιομηχανία πάσχει προς το παρόν από μια έλλειψη ενοποιημένων συμφωνιών πλοήγησης μεταξύ των διάφορων προμηθευτών που συντηρούν τα hotspot. Αν και μια κηρήθρα των επιχειρησιακών σχέσεων εξελίσσεται για να υπερνικήσει αυτό το πρόβλημα, οι ταξιδιώτες που έχουν πρόσβαση στο internet μέσω των ασύρματων hotspot αντιμετωπίζουν ακόμα την ανάγκη να ανοίξουν διαφορετικούς λογαριασμούς στις διάφορες υπηρεσίες, συνήθως με την είσοδο του αριθμού της πιστωτικής τους κάρτας στην αρχική σελίδα του τόπου συναντήσεως. Οι διάφοροι φορείς στο χώρο της δημόσιας πρόσβασης Wi-Fi έχουν αναπτύξει επιχειρησιακά πρότυπα που αγκαλιάζουν την πλοήγηση και επεκτείνουν τη

δημόσια πρόσβαση Wi-Fi για τους πελάτες τους. Η Wi-Fi Alliances εργάζεται σε ποικίλες πρωτοβουλίες για να ενισχύσει και να επιταχυνθεί αυτή η τάση. Αυτές οι πρωτοβουλίες θα ενοποιήσουν το τοπίο δημόσιας πρόσβασης και θα επιτρέψουν τη μελλοντική αύξηση.

6.6. Wi-Fi Alliance - Διευκολύνει το μέλλον της δημόσιας πρόσβασης

Η Wi-Fi Alliances υποστηρίζει μια κεντρική θέση, και είναι δεσμευμένη, στη διευκόλυνση του μέλλοντος της δημόσιας πρόσβασης Wi-Fi. Δεσμευμένη με το καταστατικό της για να πιστοποιήσει τη διαλειτουργικότητα των προϊόντων 802.11 και να τα προαγάγει στην παγκόσμια αγορά, η Wi-Fi Allinces εστιάζει στη δημόσια πρόσβαση σε τρεις βασικές περιοχές:

- Η ανάπτυξη προγραμμάτων πιστοποίησης δημόσιας πρόσβασης που θα ενισχύσουν την εμπειρία των χρηστών.
- Η ανάπτυξη των διεθνών προτύπων για να προωθήσει τη διαλειτουργικότητα και να επιτρέψει την πλοήγηση.
- Η ανάπτυξη ενός πλαισίου για τα υγιή επιχειρησιακά πρότυπα που θα επιτρέψει τη συνεχή αύξηση της βιομηχανίας.

6.6.1 Wi-Fi ZONE

Ως τμήμα της δέσμευσής της για την παγκόσμια αγορά υπηρεσιών δημόσιας πρόσβασης, η Wi-Fi Alliances εισήγαγε το πρόγραμμα Wi-Fi ZONE τον Μάρτιο του 2003. Το Wi-Fi ZONE επηρεάζει την σφαιρική επιτυχία του εμπορικού σήματος Wi-Fi και του λογότυπου που εισήχθη με το πρόγραμμα πιστοποίησης διαλειτουργικότητας Wi-Fi το 1999. Κάθε NIC και AP που έχει περάσει τη δοκιμή διαλειτουργικότητας Wi-Fi για να κερδίσει την πιστοποίηση Wi-Fi φέρουν το λογότυπο Wi-Fi. Σήμερα, το λογότυπο αναγνωρίζεται σε όλο τον κόσμο.

Το πρόγραμμα Wi-Fi ZONE επιτρέπει στους προμηθευτές να χρησιμοποιήσουν αυτό το διεθνώς αναγνωρισμένο σύμβολο ως μέσο να διαφημιστούν οι δημόσιες υπηρεσίες πρόσβασης Wi-Fi τους. Συγχρόνως, απαιτεί από τους προμηθευτές να προσαρμοστούν σε ένα ελάχιστο σύνολο κριτηρίων απόδοσης για να κερδίσούν την πιστοποίηση Wi-Fi ZONE.

Οι συμμετέχοντες προμηθευτές λαμβάνουν decals φέροντας το λογότυπο Wi-Fi ZONE που μπορεί να χρησιμοποιηθεί με τα εμπορικά λογότυπά τους για να χτίσει μια ταυτότητα εμπορικών σημάτων. Αυτό επιτρέπει στους χρήστες να προσδιορίσουν εύκολα τα Wi-Fi hotspot δημόσιας πρόσβασης. Αν και η υποστήριξη των χρηστών πρέπει να είναι διαθέσιμη για έναν τόπο συναντήσεως για να κερδίσει την πιστοποίηση Wi-Fi, μπορεί να μεταφερθεί και δεν είναι απαραίτητο να παρασχεθεί άμεσα από τον προμηθευτή του τόπου συναντήσεως.

Το ομοιόμορφο μαρκάρισμα του λογότυπου Wi-Fi ZONE φέρνει ένα υψηλό επίπεδο συνοχής και εμπιστοσύνης από τους χρήστες στο διαφορετικό τοπίο Wi-Fi. Μόνο οι τόποι συναντήσεως που συμμετέχουν στο πρόγραμμα Wi-Fi ZONE μπορούν να επιδείξουν το λογότυπο Wi-Fi ZONE στα hotspot τους, στην ιστοσελίδα τους ή στα διαφημιστικά υλικά τους. Το πρόγραμμα προσφέρει πολυάριθμα οφέλη στους συμμετέχοντες φορείς παροχής υπηρεσιών, συμπεριλαμβανομένης της πρόσθετης κυκλοφορίας πελατών που παράγει. Οι χρήστες παντού στον κόσμο μπορούν να ψάξουν το λογότυπο Wi-Fi ZONE και να είναι βέβαιοι για μια σύνδεση Wi-Fi που λειτουργεί.

Το πρόγραμμα Wi-Fi ZONE παρέχει επίσης μια ελεύθερη εξερευνήσιμη σε απευθείας σύνδεση βάση δεδομένων των Wi-Fi ZONEs που ενημερώνεται τακτικά. Οποιοσδήποτε χρήστης μπορεί να έχει πρόσβαση στον ανιχνευτή Wi-Fi ZONE για να προσδιορίσει τις Wi-Fi ZONEs στις περιοχές όπου θα ταξιδεύουν. Ο κατάλογος μπορεί να βρεθεί στο http://www.wi-fizone.org. Οι χρήστες επιλέγουν απλά τη χώρα, το κράτος και την πόλη τους από έναν εξελισσόμενο κατάλογο. Ο ανιχνευτής επιστρέφει έναν κατάλογο όλων των δυναμικών ζωνών σε εκείνη την περιοχή, μαζί με τις διευθύνσεις των hotspot, τις πληροφορίες σύνδεσης και τα ονόματα των προμηθευτών που τις συντηρούν. Οι χρήστες μπορούν επίσης να τυπώσουν τους καταλόγους των hotspot που ταιριάζουν με τις απαιτήσεις τους και παίρνουν τους καταλόγους μαζί τους όταν ταξιδεύουν.

Σαν πελάτης αντιμετωπίζοντας το πρόγραμμα, το Wi-Fi ZONE βεβαιώνει τους χρήστες σε καταστάσεις πλοήγησης ότι ο Wi-Fi CERTIFICATION εξοπλισμός τους θα επικοινωνήσει με αυτόν στους τόπους συναντήσεως που επισκέπτονται. Προσφέρει άμεσα οφέλη στους φορείς παροχής υπηρεσιών Wi-Fi ZONE και στους χειριστές των τόπων συναντήσεως. Όχι μόνο αυξάνει τη δυνατότητά τους να προσελκύσουν νέους συνδρομητές και πελάτες, παρέχει τη μεγαλύτερη διαφάνεια των υπηρεσιών και των εμπορικών σημάτων τους, και χαμηλώνει τις λειτουργικές δαπάνες τους μέσω της τυποποίησης.

Ακόμα καλύτερα, αυτό είναι ένα ελεύθερο πρόγραμμα για τους φορείς παροχής υπηρεσιών που καλύπτουν τις απαιτήσεις του προγράμματος. Οι προμηθευτές μπορούν να πάνε στην διεύθυνση http://www.wi-fizone.org/zoneSignup.asp?TID=7 για να εισαχθούν στο πρόγραμμα.

6.6.2 Διευκόλυνση της πλοήγησης από την Wi-Fi Alliances

Η Wi-Fi Alliances εργάζεται επίσης για να καθιερώσει ένα ενιαίο σύνολο προτύπων από την τιμολόγηση και την εφαρμογή στις διαδικασίες κλιμάκωσης για όλα τα hotspot Wi-Fi, σαν την προδιαγραφή των κυψελοειδή τηλεφώνων GSM (Groupe Speciale Mobile ή

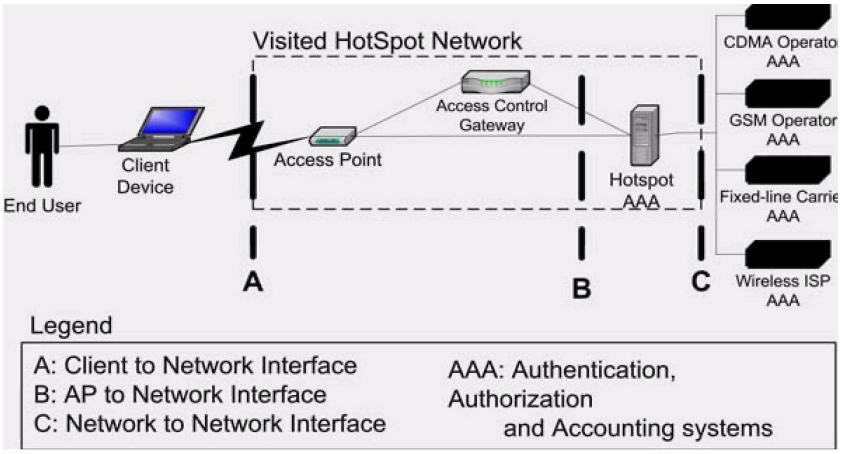
σφαιρικό σύστημα, Global System, για την κινητή επικοινωνία) που καθιέρωσε κοινά πανευρωπαϊκά πρότυπα για την κινητή επικοινωνία.

Στις αρχές του τρέχοντος έτους, η Wi-Fi Alliances δημοσίευσε ένα σύνολο καλύτερων πρακτικών που χρησιμοποιούνται από τους WISPs στην ανάπτυξη των επιχειρησιακών προτύπων πλοήγησης τους. Οι έχουσες το δικαίωμα καλύτερες τρέχουσες πρακτικές για τους φορείς παροχής υπηρεσιών ασύρματης πλοήγησης internet (ή WISPr), συστήνουν λειτουργικές πρακτικές, τεχνική αρχιτεκτονική και επικύρωσης, έγκρισης και λογιστικού πλαισίου που απαιτούνται για να επιτραπεί η πλοήγηση στους συνδρομητές στους WISPs βασισμένους σε Wi-Fi.

Η Wi-Fi Alliances στηρίζεται σε αυτήν την εργασία για να αναπτύξει ένα συνιστώμενο έγγραφο πρακτικής που θα εξηγήσει πώς να εφαρμοστεί η Wi-Fi Protected Access και επικύρωση 802.1x, στα περιβάλλοντα δημόσια πρόσβασης.

Επιπλέον, η Wi-Fi Alliaces λειτουργεί για να επεκτείνει το εξεταστικό πρόγραμμα πιστοποίησης του εξοπλισμού της για να καλύψει τις απαιτήσεις της αγοράς δημόσιας πρόσβασης. Αυτή η σημαντική πρωτοβουλία στρέφεται στις ανάγκες των φορέων παροχής υπηρεσιών και θα επαινέσει το πρόγραμμα Wi-Fi ZONE.

Αυτή η πρωτοβουλία θα μειώσει την πολυπλοκότητα, το κόστος και το χρόνο που παίρνει για να επεκτείνει την δημόσια πρόσβαση Wi-Fi σε μια μεγαλύτερη βάση πελατών.



Σχήμα 6.4: Διαδικασία σύνδεσης ενός χρήστη σε ένα hotspot

Όπως φαίνεται στο σχήμα 6.4, χειριστές όλων των τύπων, από τους κυψελοειδείς μεταφορείς στους παραδοσιακούς φορείς τηλεπικοινωνιών σε τυχάρπαστο ασύρματο ISPs, θα είναι σε θέση να συνδέσει με ένα τυποποιημένο και επικυρωμένο δίκτυο hotspot.

Αυτό το πρόγραμμα πιστοποίησης θα καθιερώσει τις απαιτήσεις της αγοράς όπως η υποστήριξη για την πλοήγηση και την πολλαπλή επικύρωση, έγκριση και τις λογιστικές μεθόδους. Προσφέρει τις απαιτήσεις βασικών γραμμών για τους χειριστές να συμμετέχουν σε ένα οικοσύστημα Wi-Fi των δημόσιων πρόσβασης hotspot που προωθούν την ασφάλεια, εύχρηστες και παγκοσμίως προσιτές συνδέσεις για τους χρήστες κάτω από το σχέδιο ενιαίας-

τιμολόγησης. Το πρόγραμμα θα επιτρέψει στο φορείς υπηρεσιών να εξασφαλίσουν ότι οι χρήστες τους εξοπλισμένοι με Wi-FI μπορούν να αγοράσουν τις υπηρεσίες στα βιομηχανικά τυποποιημένα δίκτυα.

6.7 Συμπεράσματα

Η Wi-Fi Alliances αναγνωρίζει ότι υπάρχουν δαπανηρά προβλήματα που πρέπει να λυθούν εάν η αγορά Wi-Fi πρόκειται να αυξηθεί και να ευημερήσει. Η συμμαχία έχει υιοθετήσει μια στρατηγική κατεύθυνση για να εξασφαλίσει ένα επίπεδο τυποποίησης και να παρέχει μια άνευ ραφής, ικανοποιητική και κερδοφόρα εμπειρία για όλα τα συμβαλλόμενα μέρη που συμμετέχουν στη δημόσια πρόσβαση Wi-Fi.

Με την προώθηση των προτύπων βιομηχανίας μέσω του Wi-Fi ZONE και των άλλων προγραμμάτων πιστοποίησής της, η Wi-Fi Alliances λειτουργεί για να το καταστήσει γρηγορότερο, ευκολότερο, και οικονομικώς ποιο αποδοτικό για τους χειριστές και τους μεταφορείς να δημιουργήσουν δίκτυα δημόσιας πρόσβασης Wi-FI και να επιτρέψουν την εξέλιξης της πλοήγησης ενιαίων-λογαριασμών. Με την πιστοποίηση των δημόσιων σημείων πρόσβασης, η Wi-Fi Alliances επεκτείνει το όραμα της διαλειτουργικότητας στην κοινότητα των φορέων παροχής υπηρεσιών. Η προοπτική των επικυρωμένων "βιομηχανικών προτύπων" hotspot μειώνει τα εμπόδια στις συμφωνίες επέκτασης και πλοήγησης μεταξύ των χειριστών και των aggregators που ήδη έχουν ισχυρές σχέσεις στους ασύρματους πελάτες τους.

Επιπλέον, η Wi-Fi Alliances εργάζεται για να προσδιορίσει και να καθορίσει τα πρότυπα τιμολόγησης για τη βιομηχανία και παίρνει έναν συντονίζοντας ρόλο μεταξύ των διάφορων οργανώσεων για να παραδώσει μια μήτρα των προμηθευτών που χρησιμοποιούν εκείνα τα πρότυπα επιτυχώς. Μεταδίδοντας μέσω των όλων της προσπαθειών η συμμετοχή της Wi-Fi Alliances με τους φορείς της βιομηχανίας, οι συνεταιρισμοί και οι οργανώσεις ρύθμισης των προτύπων που προσκρούουν στο μέλλον της δημόσιας πρόσβασης Wi-Fi.

Σαν τρέχουσα αρχή πιστοποίησης των υπηρεσιών Wi-Fi, η Wi-Fi Alliances τοποθετείται μεμονωμένα για να παρέχει παγκόσμια ηγεσία στην αναζήτηση των κοινών στόχων που θα αυξήσουν την υιοθέτηση, θα μειώσουν τις γενικές δαπάνες στους προμηθευτές μέσω της εμμονής στα πρότυπα, και θα βεβαιώσουν μία ασφαλή, ποιοτική και συνεπή εμπειρία για τους χρήστες οπουδήποτε και όποτε έχουν ασύρματη πρόσβαση στο internet. Είναι δεσμευμένη στο πρότυπο, είναι μεγάλη διεθνής μέλος και δίκτυο συμμαχία μαζί με όλες τις βασικές οργανώσεις ρύθμισης των προτύπων, κατασκευαστής, φορέας παροχής υπηρεσιών, χειριστής τόπος συναντήσεως και η ένωση που τους αντιπροσωπεύει , τοποθετεί την Wi-Fi Alliances στην πύλη ενός μέλλον που υπόσχομαι πανταχού παρών ασύρματη κινητικότητα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- A Technical Tutorial on the IEEE 802.11 Protocol By Pablo Brenner, 1997
- Wi-Fi – 802.11b Μια μελέτη του κραταιού πρωτοκόλλου ασύρματης δικτύωσης
- Wi-Fi and Beyond, K. Βυρσόκινος & Ε. Αγγελόπουλος
- The Peer to Peer Wireless Network Confederation: Enabling Global Wi-Fi Roaming, Ηλία Ευσταθίου & Γιώργος Πολύζος
- Wireless Lan: Origins, capabilities & uses by NEuW Technology Brief, Μάιος 2003
- Enabling the Future of Wi-Fi Public Access by Wi-Fi Alliances, 2 Φεβρουάριος 2004
- Wireless Fidelity (Wi-Fi) Technology Reaching the Home Market in 2004
- Wi-Fi CERTIFIED for WMM – Support for Multimedia Applications with Quality of Service in Wi-Fi Network by Wi-Fi Alliances, 1 Σεπτεμβρίου 2004
- White Paper Security Problems and Solution for Wireless LANs by ActivCard
- Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for today's Wi-Fi networks by Wi-Fi Alliances, 29 Απριλίου 2003
- Wi-Fi is everywhere Wi-Fi Protected Access Web cost, 11 Ιουνίου 2003
- Data Over Wireless Network Bluetooth, WAP & Wireless LANs by Gil Held
- Μελέτη και κατασκευή εργαλείου διαχείρισης για ασύρματα δίκτυα τεχνολογίας 802.11b και 802.11a από τον Ζουμπούρλου Α. Αλέξανδρο, Εκδόσεις Ε.Μ.Π., Ιούλιος 2003

Ιστοσελίδες

- WWW.Wi-Fi.org
- WWW.IEEE.org
- Wifi.think.gr/index.html
- WWW.hellascams.gr/grc/products/wireless/index.html
- WWW.ActivCard.com

ΧΡΟΝΟΔΙΑΓΡΑΜΜΑ

ΗΜΕΡΟΜΗΝΙΑ	ΔΡΑΣΤΗΡΙΟΤΗΤΑ
18-8-2004	Ανάληψη θέματος
15-8-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για διευκρινίσεις σχετικές με το θέμα της πτυχιακής
5-9-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για την δομή της πτυχιακής εργασίας
29-9-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για την τελική δομή της πτυχιακής εργασίας
14-10-2004	Αποστολή $1^{ου}$ κεφαλαίου πτυχιακής εργασίας
26-10-2004	Διορθώσεις $1^{ου}$ κεφαλαίου και αποστολή του $2^{ου}$ κεφαλαίου
20-11-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για τις διορθώσεις του $2^{ου}$ κεφαλαίου και διευκρινήσεις για τα υπόλοιπα κεφάλαια
11-11-2004	Αποστολή $4^{ου}$ κεφάλαίου
20-11-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για τις διορθώσεις του $4^{ο}$ κεφαλαίου
7-12-2004	Αποστολή του $3^{ου}$ κεφαλαίου
22-1-2004	Αποστολή του $5^{ου}$ και $6^{ου}$ κεφαλαίου
5-2-2004	Συζήτηση με την υπεύθυνη καθηγήτρια για τις τελικές διορθώσεις για την πτυχιακή εργασία.
18-2-2004	Τέλος πτυχιακής εργασίας.