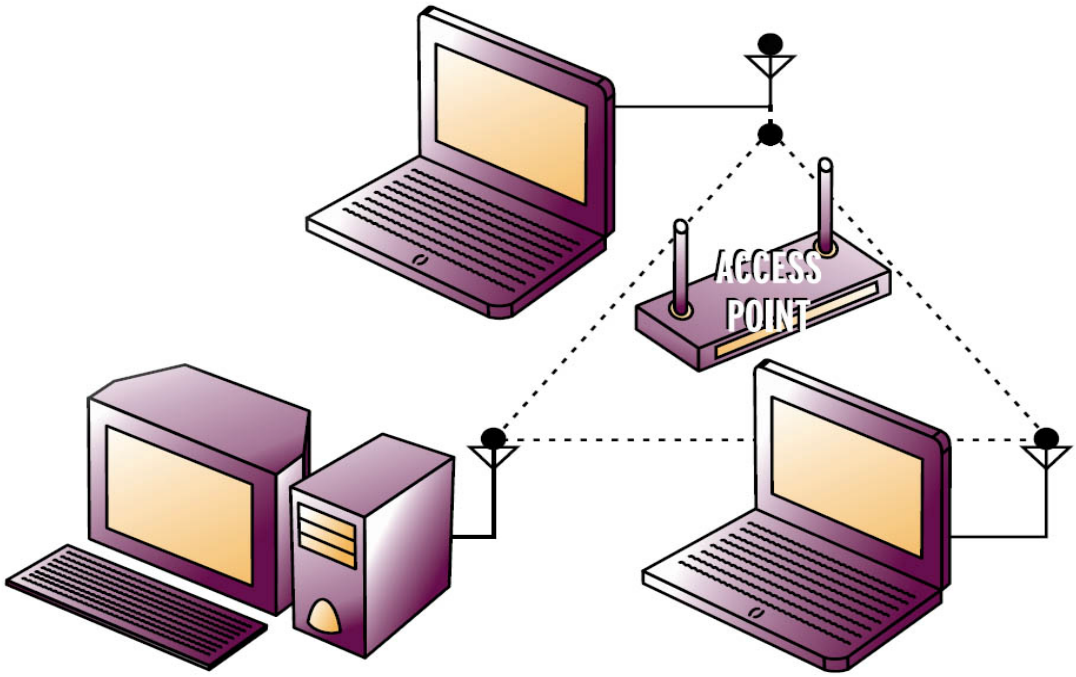
ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ
ΤΕΙ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΔΙΟΙΚΗΣΗΣ

ΓΙΑΝΝΗΣ ΖΕΡΒΑΣ

'ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ'



ΑΡΤΑ ΟΚΤΩΒΡΙΟΣ 2005

ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

ΣΠΟΥΔΑΣΤΗΣ: ΖΕΡΒΑΣ ΙΩΑΝΝΗΣ
ΥΠΕΥΘΥΝΟΣ ΚΑΘΗΓΗΤΗΣ: ΜΑΡΓΑΡΙΤΗ ΣΠΥΡΙΔΟΥΛΑ

ΑΡΤΑ ΟΚΤΩΒΡΙΟΣ 2005

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 4

ΚΕΦΑΛΑΙΟ 5

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Η δυνατότητα για πρόσβαση σε πληροφορίες από οπουδήποτε και οποτεδήποτε φαίνεται ότι θα χαρακτηρίσει τη πληροφορική και τη κοινωνία του 21ου αιώνα. Η δυνατότητα αυτή υποστηρίζεται από συστήματα ψηφιακών ασύρματων επικοινωνιών βασισμένα στις τεχνολογίες κινητής τηλεφωνίας, προσωπικών συστημάτων επικοινωνίας (Personal Communication Systems - PCS), δορυφορικών επικοινωνιών (περιλαμβανόμενης και ασύρματης υψηλής ταχύτητας πρόσβασης στο Διαδίκτυο μέσω δορυφόρων) και **ασύρματων τοπικών δικτύων (Wireless Local Area Networks - WLAN)**. Οι τεχνολογίες αυτές έχουν τη δυνατότητα να αλλάξουν δραματικά τη κοινωνία καθώς επιτρέπουν στον άνθρωπο να αποδεσμευτεί από τη "*με βάση τη γεωγραφική θέση επικοινωνία*" και *πρόσβαση* σε πηγές πληροφορίας ώστε να κινείται ελευθέρα παγκοσμίως χωρίς να μειώνεται η αποτελεσματικότητά του.

Τα ασύρματα δίκτυα υπολογιστών αναπτύχθηκαν στα τέλη της δεκαετίας του '90, κυρίως λόγω 1) της ανάγκης για διασύνδεση απομακρυσμένων ενσύρματων τοπικών δικτύων (LAN) με μεγάλες ταχύτητες μεταφοράς δεδομένων, και 2) της απαίτησης των χρηστών για πρόσβαση σε υπηρεσίες (που τα κοινά ενσύρματα δίκτυα προσφέρουν) από οποιοδήποτε μέρος, οποιαδήποτε ώρα της ημέρας.

Προκείμενου λοιπόν να είναι εφικτή αυτή η διασύνδεση ενσύρματων τοπικών δικτύων και επιπλέον να μπορεί ο τελικός χρήστης να έχει πρόσβαση τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα με την χρήση μόνο ενός τερματικού (π.χ. PC), οι παγκόσμιοι οργανισμοί δημιουργίας προτύπων (Standardisation bodies) δημιούργησαν και θέσπισαν πρότυπα λειτουργίας τα οποία ένα ασύρματο δίκτυα πρέπει να ακολουθεί. Τέτοια πρότυπα (standards) είναι το IEEE 802.11xx, το HIPERLAN I και II, το Bluetooth, το HOME RF, κ.α., τα οποία περιγράφουν τον τρόπο λειτουργίας ενός ασύρματου δικτύου στο φυσικό επίπεδο (Physical Layer - PHY) και στο επίπεδο διασύνδεσης (Data Link Layer), και εστιάζονται στον τρόπο λειτουργίας του Medium Access Control (MAC) ημι-επιπέδου. Πιο συγκεκριμένα, για το PHY οι επιλογές που υπάρχουν είναι η χρήση τεχνικών διάσπαρτου φάσματος (Spread Spectrum) όπως η Frequency Hopping, η Direct Sequence, και η Orthogonal Frequency Division Multiplex (OFDM). Όπως είναι λοιπόν φυσικό, οι συσκευές που θα συνδέονται και θα λειτουργούν σε κάποιο ασύρματο δίκτυο, θα πρέπει να ακολουθούν κάποιο από αυτά τα standards στο PHY και στο MAC, ενώ θα μπορούν διατηρούν τον τρόπο λειτουργίας των παραπάνω επιπέδων (π.χ. Network Layer, Transport Layer, κτλ.).

Ωστόσο, το μεγαλύτερο πρόβλημα που αντιμετωπίζει κάποιος κατά την δημιουργία ενός ασύρματου δικτύου είναι αυτό της πολλαπλής πρόσβασης. Δηλαδή του τρόπο με τον οποίο πολλοί ταυτόχρονοι χρήστες θα έχουν πρόσβαση στο δίκτυο. Η λύση στο πρόβλημα αυτό είναι η χρησιμοποίηση τεχνικών πολλαπλής πρόσβασης. Τέτοιες τεχνικές είναι η Time Division Multiple Access (TDMA - πολύπλεξη χρόνου), η Frequency Division Multiple Access (TDMA- πολύπλεξη συχνότητας), και Code Division Multiple Access (CDMA- πολύπλεξη με διαίρεση κωδίκων), ή συνδυασμός αυτών (π.χ. FDMA/TDMA). Τα περισσότερα σημερινά τοπικά ασύρματα δίκτυα κάνουν χρήση της CDMA τεχνικής πολλαπλής πρόσβασης, ακολουθώντας το διεθνές πρότυπο IEEE 802.11 (Wireless Ethernet) το οποίο ορίζει στο Medium Access Control (MAC) ημι-επίπεδο την Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) τεχνικής αποφυγής collision, ενώ χρησιμοποιεί τεχνικές διάχυτου φάσματος στο PHY.

ΚΕΦΑΛΑΙΟ 2

2.1 ΕΙΣΑΓΩΓΗ ΣΤΑ ΑΣΥΡΜΑΤΑ ΤΟΠΙΚΑ ΔΙΚΤΥΑ

Ένα ασύρματο τοπικό δίκτυο (WLAN: Wireless Local Area Network) είναι ένα σύστημα επικοινωνίας, το οποίο καθιστά δυνατή την διασύνδεση (και μεταφορά δεδομένων) - μέσω ηλεκτρομαγνητικών κυμάτων - κινητών ή ακίνητων χρηστών. Η συνηθισμένη ακτίνα δράσης ενός τέτοιου δικτύου εκτείνεται σε αρκετά μέτρα, η οποία είναι ικανή να διασυνδέσει από τους ορόφους μιας εταιρίας μέχρι τα κτίρια μιας πανεπιστημιούπολης. Η σύνδεση ενός ασύρματου τοπικού δικτύου με ένα αντίστοιχο ενσύρματο μπορεί να αυξήσει σημαντικά την ακτίνα δράσης του ασύρματου δικτύου.

Η πρώτη προσπάθεια για τη σύνδεση των τεχνολογιών δικτύου με την επικοινωνία μέσω ραδιοκυμάτων ξεκίνησε το 1971 με την υλοποίηση ενός project του πανεπιστήμιου της Hawaii, το οποίο ονομάστηκε ALOHANET. Το ALOHANET ήταν ένα σύστημα όπου απομακρυσμένοι υπολογιστές επικοινωνούσαν μεταξύ τους μέσω ενός κεντρικού υπολογιστή χωρίς την χρησιμοποίηση των συμβατικών τηλεφωνικών καλωδίων, αλλά με τη βοήθεια ραδιοκυμάτων.

Το 1985, στην Αμερική, ο οργανισμός FCC (Federal Communications Commission) – ο οποίος καθορίζει το εύρος συχνοτήτων που θα χρησιμοποιείται για κάθε τηλεπικοινωνιακή εφαρμογή - εξουσιοδότησε την κοινή χρήση του φάσματος συχνοτήτων ISM (Instrumentation, Scientific, and Medical) στο οποίο στηρίχθηκε η μελλοντική κατασκευή όλων των τεχνολογιών WLAN.

Για την κατασκευή ενός WLAN σε μία χώρα, θα πρέπει να ληφθεί υπόψη η νόμιμη χρήση των συχνοτήτων αυτών από τους αντίστοιχους οργανισμούς της συγκεκριμένης χώρας.

Στα τέλη του 1980, το IEEE ξεκίνησε την ανάπτυξη του πρώτου Standard για WLANs, το οποίο ολοκληρώθηκε τελικά το 1997 και είναι γνωστό ως IEEE 802.11. Την προσπάθεια αυτή ακολούθησαν και άλλοι οργανισμοί ώστε να επιτύχουν την καλύτερη δυνατή απόδοση των ασύρματων τοπικών δικτύων.

Ανάλογα με τους χώρους στους οποίους μπορούμε να δούμε οφέλη από τη χρήση των WLAN συμπεριλαμβάνονται και οι παρακάτω:

Επιχειρήσεις: Με ένα WLAN οι εργαζόμενοι μπορούν να εκμεταλλευθούν το κινητό δίκτυο για e-mail, πρόσβαση σε αρχεία και αναζήτηση στο Internet, ανεξάρτητα από την περιοχή που βρίσκεται το γραφείο, αλλά και από το αν βρίσκονται στο γραφείο ή όχι.

Εκπαίδευση: Με τη χρήση WLAN από τα ακαδημαϊκά ινστιτούτα οι φοιτητές μπορούν να έχουν πρόσβαση μέσω laptops στο πανεπιστημιακό δίκτυο ενώ γίνεται πιο προσιτή και εφαρμόσιμη η τηλε-εκπαίδευση.

Υγεία: Με τη χρήση ασύρματων φορητών υπολογιστών για την επεξεργασία σε πραγματικό χρόνο, οι εργαζόμενοι στον τομέα υγείας αυξάνουν την παραγωγικότητά τους και την ποιότητα φροντίδας των ασθενών, καθώς εξαλείφονται προβλήματα όπως οι καθυστερήσεις και η γραφειοκρατία.

Επενδύσεις: Με ένα φορητό υπολογιστή ο οποίος συνδέεται με ένα ασύρματο τοπικό δίκτυο, οι επενδυτές μπορούν να δεχθούν πληροφορίες για τις τιμές απο μια βάση δεδομένων σε πραγματικό χρόνο, βελτιώνοντας έτσι την ταχύτητα και την ποιότητα των συναλλαγών.

2.2 Τεχνολογίες WLAN

Για την υλοποίηση ενός ασύρματου τοπικού δικτύου μπορεί να επιλεχθεί ένα από τα πολλά Standards που οι διάφοροι οργανισμοί και εταιρίες έχουν δημιουργήσει τα τελευταία χρόνια. Στη συνέχεια αναφέρουμε τα κυριότερα.

2.2.1 IEEE 802.11

Τον Νοέμβριο του 1997 η IEEE οριστικοποίησε το πρώτο της Standard για WLANs. Το 802.11 Standard καθορίζει ως συχνότητα λειτουργίας τα 2.4 GHz και υποστηρίζει ρυθμούς δεδομένων της τάξεως των 1 Mbps και 2 Mbps. Για την ασύρματη μεταφορά δεδομένων καθορίζονται οι λειτουργίες και οι υπηρεσίες ενός υποστρώματος MAC και τριών διαφορετικών φυσικών στρωμάτων. Το υπόστρωμα MAC έχει 2 τρόπους λειτουργίας:

- Μία κατανεμημένη (distributed) λειτουργία (CSMA/CA)
- Μια συντονισμένη (coordinated) λειτουργία (polling mode)

Στα τέλη του 1999 η IEEE κοινοποίησε δύο νέα συμπληρωματικά Standards για WLANs, τα 802.11a και 802.11b:

- Το 802.11a έχει καθοριστεί έτσι ώστε να υποστηρίζει ρυθμούς δεδομένων έως και 54 Mbps με χρήση της τεχνικής διαμόρφωσης OFDM (Orthogonal Frequency Division Multiplexing) στην μπάντα των 5 GHz.
- Το 802.11b είναι ουσιαστικά μια προέκταση του αρχικού 802.11 καθώς χρησιμοποιεί ως διαμόρφωση την τεχνική DSSS και λειτουργεί στα 2.4 GHz. Η διαφορά έγκειται στο γεγονός ότι μπορεί να υποστηρίξει ρυθμούς δεδομένων έως και 11 Mbps.

2.2.2 HiperLAN

Το HiperLAN καθιερώθηκε το 1996 από την ETSI (European Telecommunications Standards Institute). Η πρώτη έκδοση του Standard είναι το HiperLAN I. Το Standard αυτό λειτουργεί στην μπάντα από 5.1 έως 5.3 GHz, ενώ ο ρυθμός σηματοδοσίας φτάνει τα 24 Mbps. Το πρωτόκολλο χρησιμοποιεί μια παραλλαγή του CSMA/CA η οποία στηρίζεται στο χρόνο ζωής του πακέτου, την προτεραιότητα των πακέτων και τις αναμεταδόσεις στο επίπεδο MAC.

Η ETSI έχει καθορίσει και ένα νέο πρωτόκολλο που ονομάζεται HiperLAN II και λειτουργεί και αυτό στα 5 GHz (5.4 έως 5.7 GHz). Το HiperLAN II στηρίζεται στην τεχνική διαμόρφωσης OFDM (Orthogonal Frequency Digital Multiplexing), ενώ υποστηρίζει διάφορους ρυθμούς μετάδοσης (6, 9, 12, 18, 27, 36 και έναν εναλλακτικό ρυθμό των 54 Mbps). Το HiperLan II είναι ουσιαστικά ένα σύστημα ασύρματου ATM, ενώ το πρωτόκολλο που χρησιμοποιείται στο υπόστρωμα MAC στηρίζεται σε μια διαφοροποιημένη λειτουργία της τεχνικής TDMA.

2.2.3 OpenAir

Το OpenAir είναι ένα Standard που αναπτύχθηκε από την εταιρία Proxim. Είναι προγενέστερο του 802.11 και χρησιμοποιεί την τεχνική του Frequency Hopping επιτυγχάνοντας ρυθμούς δεδομένων 0.8 και 1.6 Mbps (χρησιμοποιώντας τεχνικές διαμόρφωσης 2FSK και 4FSK, αντίστοιχα). Το πρωτόκολλο που χρησιμοποιείται στο υπόστρωμα MAC είναι το CSMA/CA με MAC επαναμεταδόσεις και στηρίζεται στην ανταλλαγή RTS/CTS πακέτων.

2.2.4 HomeRF SWAP

Η HomeRF είναι μια ομάδα από μεγάλες εταιρίες που δημιουργήθηκε για να προωθήσει την χρήση των WLAN στο σπίτι και στα γραφεία. Η ομάδα αυτή έχει αναπτύξει ένα νέο πρωτόκολλο για τον σκοπό αυτό, το οποίο ονομάζεται SWAP (Shared Wireless Access Protocol).

Το SWAP χρησιμοποιεί στο υπόστρωμα MAC ένα νέο πρωτόκολλο, το οποίο συνδυάζει χαρακτηριστικά και λειτουργίες από το DECT (ένα Standard της ETSI για ψηφιακά ασύρματα τηλέφωνα) και το 802.11. Η συχνότητα λειτουργίας είναι τα 2.4 GHz, ενώ στο φυσικό στρώμα χρησιμοποιείται η τεχνική FHSS, υποστηρίζοντας ρυθμούς δεδομένων της τάξης των 1 Mbps και 2 Mbps.

2.2.5 Bluetooth

Το Bluetooth αποτελεί μια προδιαγραφή που εκδόθηκε από το Bluetooth Special Interest Group (SIG) με την ενίσχυση μερικών από τις μεγαλύτερες εταιρίες όπως οι Ericsson, IBM, Intel, Microsoft κ.ά. Το Bluetooth δεν αποτελεί ένα πρωτόκολλο για WLAN, αλλά βρίσκει εφαρμογές στα ασύρματα προσωπικά δίκτυα WPANs (Wireless Personal Area Networks), που αποτελούν μικρότερα σε έκταση δίκτυα από τα WLANs, με ακτίνα δράσης έως 10 μέτρα. Το Bluetooth λειτουργεί στα 2.4 GHz, χρησιμοποιεί ως τεχνική διαμόρφωσης την FHSS και φτάνει σε ρυθμούς δεδομένων ως το 1 Mbps.

	Bluetooth	**HomeRF**	**IEEE802.11**	**IEEE802.11b**	**IEEE802.11a**	**HiperLAN1**	**HiperLAN2**
Ταχύτητα	1Mbps	2Mbps	2Mbps	11Mbps	54Mbps	24Mbps	54Mbps
Εμβέλεια	10μ	50μ	100μ	100μ	100μ	50μ	30-150μ
Συχνότητα	2,4GHz	2,4GHz	2,4GHz	2,4GHz	5GHz	5GHz	5GHz
Διασύνδεση	Καμία	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet	Ethernet, ATM, IP, UMTS, Firewire, PPP
Κατάσταση	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο	Διαθέσιμο		Διαθέσιμο	
Υποστηρικτές	Ericsson, IBM, Toshiba, Intel, Nokia, Motorola	Proxim, Intel, HP, 3COM, Motorola		Cisco, Lucent, 3Com, Apple, Compaq, Zoom, Dell, Nokia		ETSI, Proxim, HP, Xircom, IBM, Nokia	ETSI, HP, Xircom, IBM, TI, Dell, Ericsson, Nokia, Proxim

Σχήμα 2.1 Πίνακας «Προτύπων επικοινωνίας»

2.3 Άλλες τεχνολογίες ασύρματων δικτύων

Οι ασύρματες τεχνολογίες μπορούν να χωρισθούν σε διάφορες κατηγορίες, σύμφωνα με κριτήρια όπως:

Το πρωτόκολλο που χρησιμοποιούν (ATM, IP ή άλλο)

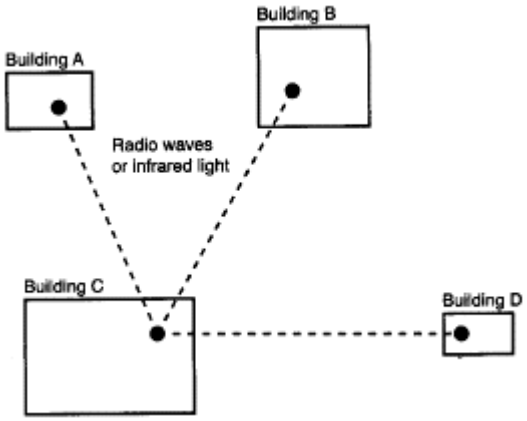
Το είδος σύνδεσης (point-to-point ή point-to-multipoint)

Το φάσμα συχνοτήτων στο οποίο λειτουργούν

Έτσι, ανάλογα με το είδος σύνδεσης υπάρχουν δύο κύριες κατηγορίες, οι οποίες αναπτύσσονται ξεχωριστά.

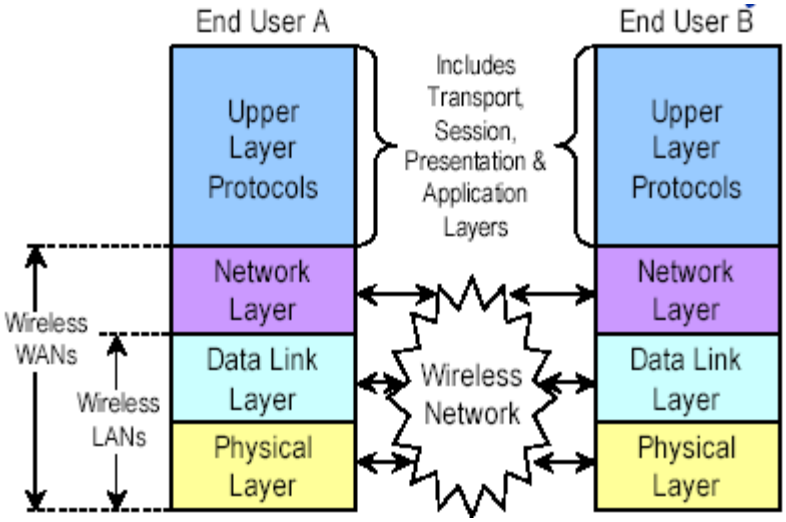
2.3.1 Ασύρματα Point-to-Point δίκτυα

Ο κυριότερος εκπρόσωπος των ασύρματων δικτύων με σύνδεση από σημείο-σε-σημείο (point-to-point) είναι τα ασύρματα μητροπολιτικά δίκτυα WMANs (Wireless Metropolitan Area Networks), τα οποία χρησιμοποιούν τεχνολογίες που μοιάζουν πολύ με αυτές των WLAN. Η σύνδεση που χρησιμοποιείται συνήθως φαίνεται στο επόμενο σχήμα.



Σχήμα 2.2 Η σύνδεση από σημείο σε σημείο μπορεί να συνδέσει πολλά απομακρυσμένα κτίρια μεταξύ τους.

Χρησιμοποιώντας κατευθυντικές κεραίες και τεχνικές διαμόρφωσης όπως η ‘spread spectrum’, τα δίκτυα αυτά μπορούν να υποστηρίξουν μετάδοση σε αποστάσεις μέχρι και 30 miles, απόσταση πάντως που μειώνεται αισθητά από διάφορους παράγοντες όπως οι καθυστερήσεις μετάδοσης και τα διάφορα εμπόδια και παρεμβολές. Ο ρυθμός μετάδοσης για τα WMAN μπορεί να φτάσει τα 11 Mbps για ζεύξεις των 2-3 miles. Η κυριότερη διαφορά μεταξύ τόσο των WMAN όσο και των WWAN (Wireless Wide Area Network, τα οποία εκτείνονται σε ακτίνα εκατοντάδων χιλιομέτρων) με τα WLAN έγκειται στο γεγονός ότι η λειτουργία των τελευταίων λαμβάνει χώρα στα δύο κατώτερα στρώματα του επιπέδου OSI (σχήμα 2.3), σε αντίθεση με τα δύο προηγούμενα, η λειτουργία των οποίων στηρίζεται επιπλέον και στο στρώμα δικτύου.



Σχήμα 2.3 WLAN και OSI model.

2.3.2 Ασύρματα Point-to-Multipoint δίκτυα

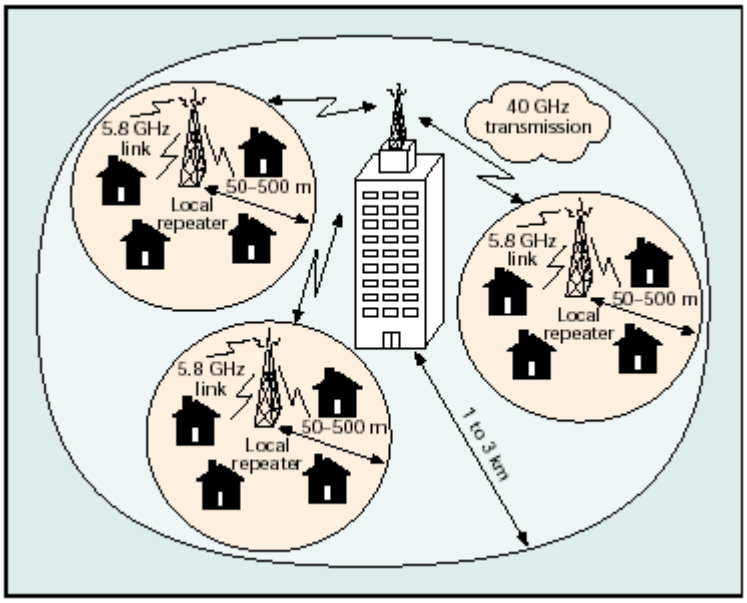
Τα δίκτυα αυτά στηρίζονται στην διασύνδεση ασύρματων (κινητών ή μη) χρηστών με μια σταθερή περιοχή στην οποία βρίσκεται ο παροχέας των υπηρεσιών (Service Provider), τις οποίες μοιράζονται οι ασύρματοι χρήστες. Δύο από τις πλέον αναπτυσσόμενες τεχνολογίες τέτοιου είδους ασύρματων δικτύων είναι και οι:

MMDS (Multichannel Multipoint Distribution Service), η οποία λειτουργεί στην περιοχή συχνοτήτων 2.1-2.7 GHz, ενώ μπορεί να υποστηρίξει ρυθμό δεδομένων έως και 10 Mbps σε ακτίνα 35 miles.

LMDS (local Multipoint Distribution Service), η οποία λειτουργεί σε διάφορες συχνότητες (από 24 μέχρι 40 GHz), ενώ μπορεί να υποστηρίξει ρυθμούς μέχρι και 155 Mbps σε ακτίνα λειτουργίας των 2 miles.

2.3.3 Η τεχνολογία LMDS

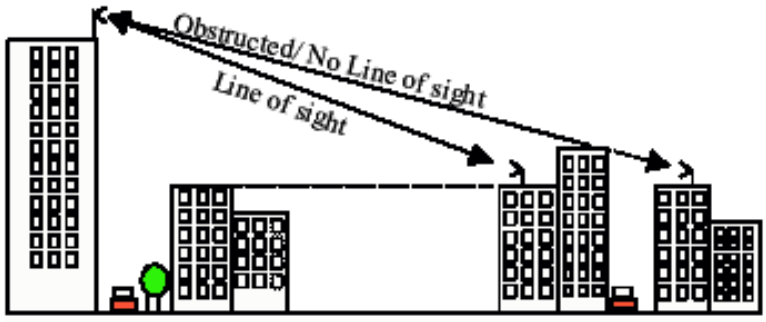
Η τεχνολογία LMDS (Local Multipoint Distribution System) είναι ένα ασύρματο σύστημα επικοινωνίας ευρείας ζώνης point-to-multipoint (σχήμα 2.4) και ανήκει σε μία κατηγορία ασύρματων τεχνολογιών που καλείται WLL (Wireless Local Loop) και λειτουργεί σε συχνότητες μεγαλύτερες των 20 GHz. Η τεχνολογία αυτή χρησιμοποιείται για την παροχή ψηφιακών αμφίδρομων υπηρεσιών όπως μετάδοση δεδομένων, φωνής, video και Internet.



Σχήμα 2.4 Τυπική αρχιτεκτονική της τεχνολογίας LMDS.

Τα δίκτυα LMDS (η τοπολογία των οποίων φαίνεται στο παραπάνω σχήμα) μοιάζουν πολύ με τα δίκτυα κινητής τηλεφωνίας όσον αφορά την τοπολογία, αλλά έχουν δύο σημαντικές διαφορές:

- Η τεχνολογία LMDS λειτουργεί σε πολύ υψηλές συχνότητες. Στην Ευρώπη η ζώνη συχνοτήτων στην οποία λειτουργεί το LMDS είναι μεταξύ 24 και 26 GHz, ενώ στις ΗΠΑ έχει δοθεί άδεια για λειτουργία και στα 38 GHz. Εξαιτίας των πολύ υψηλών συχνοτήτων τα σήματα μπορούν να μεταδοθούν μόνο σε μικρές αποστάσεις, οι οποίες συνήθως δεν ξεπερνάνε τα 3 Km. Επίσης, απαιτείται η ύπαρξη οπτικής επαφής (Line Of Sight) μεταξύ πομπού και δέκτη (όπως φαίνεται στο σχήμα 2.5), κάνοντας την τεχνολογία ευπαθή για τις κινητές εφαρμογές.
- Η τεχνολογία LMDS χρησιμοποιεί μεγάλα ποσά εύρους ζώνης. Σε σύγκριση με τα κυψελωτά (cellular) δίκτυα που συνήθως χρησιμοποιούν 25 με 30 MHz, τα δίκτυα LMDS μπορούν να χρησιμοποιήσουν περισσότερα από 1000 MHz, επιτρέποντας την μεταφορά τεράστιας ποσότητας πληροφορίας.



Σχήμα 2.5 Η τεχνολογία LMDS απαιτεί την ύπαρξη οπτικής επαφής μεταξύ πομπού και δέκτη.

Το βασικό δομικό στοιχείο μιας τέτοιας αρχιτεκτονικής είναι το κελί (cell) το οποίο φαίνεται στο σχήμα 2.6 και στο οποίο λαμβάνει χώρα η ασύρματη επικοινωνία. Κάθε κελί στο σύστημα έχει έναν σταθμό βάσης (AP: Access Point) ή hub, ο οποίος αναφέρεται και ως central hub και βρίσκεται στο CMN (Central Main Node). Σε κάθε

κελί υπάρχουν από λίγες έως πολλές απομακρυσμένες μονάδες (remote units) οι οποίες αντιπροσωπεύουν ουσιαστικά τους χρήστες. Η επικοινωνία και η διαχείριση των μονάδων αυτών γίνεται με τη βοήθεια του AP, η σύνδεση με τον οποίο γίνεται με την βοήθεια ενός SA (Station Adapter). Αξίζει να αναφέρουμε πως στο AP μπορεί να συνδεθεί και ένα ενσύρματο δίκτυο μέσω μιας ασύρματης γέφυρας (WB: Wireless Bridge).

Ένα σύστημα πολλαπλής προσπέλασης απαιτείται για να ρυθμίζει την επικοινωνία των απομακρυσμένων χρηστών με το AP. Κάποια τυπικά συστήματα που χρησιμοποιούνται για τον σκοπό αυτό είναι οι τεχνικές:

- FDMA (Frequency Division Multiple Access)
- TDMA (Time Division Multiple Access)
- CDMA (Code Division Multiple Access)

Το ασύρματο κανάλι μοιράζεται μεταξύ της απερχόμενης (upstream) και εισερχόμενης (downstream) στο CMN κίνησης, καθιστώντας έτσι αναγκαίο ένα 'duplexing scheme'. Οι τυπικές τεχνικές που χρησιμοποιούνται για τον σκοπό αυτό είναι οι:

- TDD (Time Division Multiplexing)
- FDD (Frequency Division Multiplexing)

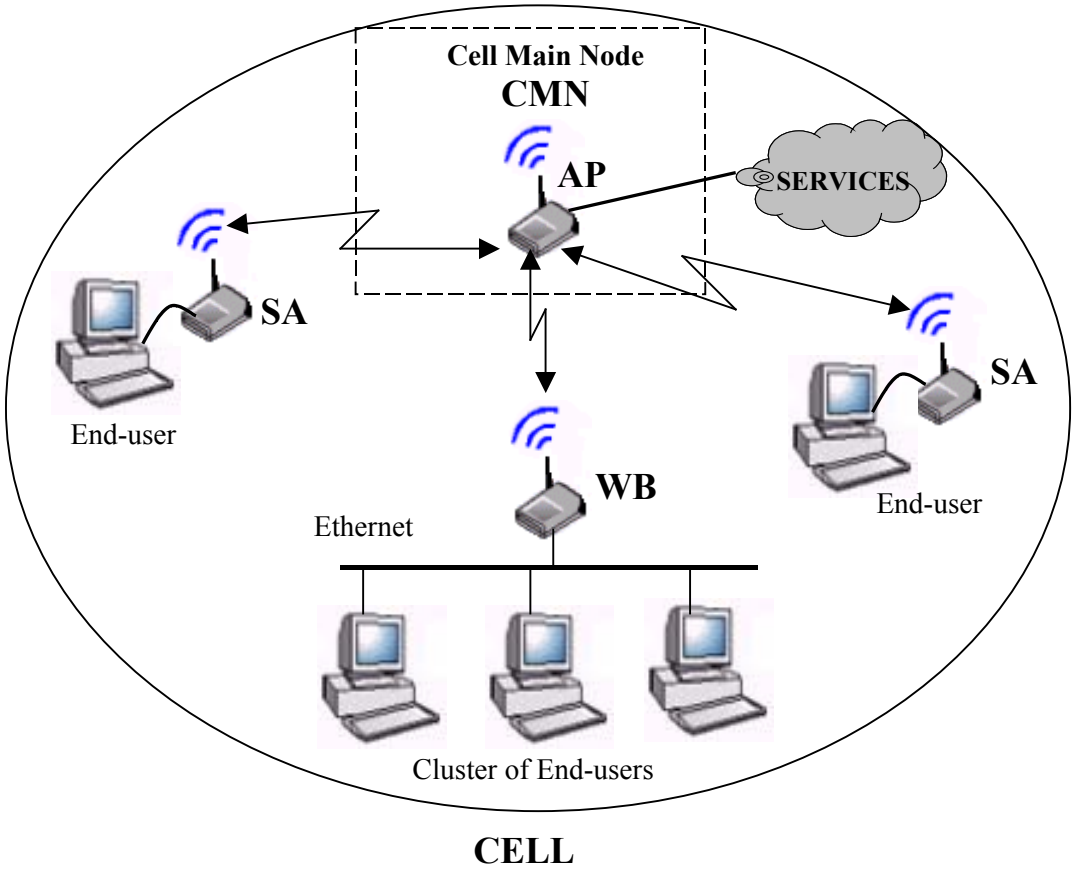
Είναι, επίσης, ενδιαφέρον να αναφέρουμε πως το ακρωνύμιο προκύπτει από τις παρακάτω λέξεις:

L (local): Δηλώνει την περιοχή κάλυψης ενός κελιού. Η συνήθης έκταση ενός κελιού είναι 12-15 χιλιόμετρα.

M (multipoint): Δηλώνει ότι τα σήματα μεταδίδονται με μία point-to-multipoint μέθοδο από το AP προς τους διάφορους χρήστες. Το ασύρματο κανάλι επιστροφής από τον συνδρομητή στον σταθμό βάσης είναι μια point-to-point μετάδοση.

D (distribution): Αναφέρεται στην κατανομή (distribution) των σημάτων η οποία μπορεί να αποτελείται από ταυτόχρονη μετάδοση φωνής, δεδομένων, Internet και video.

S (service): Δηλώνει την φύση της υπηρεσίας που προσφέρει ο διαχειριστής στον συνδρομητή η οποία υλοποιείται μέσω της συνδρομής του τελευταίου.



Σχήμα 2.6 Σχηματική αναπαράσταση ενός cell.

Ένα εκτεταμένο δίκτυο που χρησιμοποιεί την τεχνολογία LMDS μπορεί να περιέχει περισσότερα από ένα κελιά, τα APs των οποίων μπορούν να συνδέονται μεταξύ τους με συνδέσεις point-to-point. Κάθε κελί μπορεί να έχει όλα τα χαρακτηριστικά που περιγράφονται παραπάνω. Σύμφωνα με αυτή την αρχιτεκτονική του LMDS, ο service provider συνδέεται στα CMN κάθε κελιού, χρησιμοποιώντας point-to-point RF ζεύξεις, ενώ κάθε CMN επικοινωνεί με τους σχετιζόμενους χρήστες μέσω point-to-multipoint RF ζεύξεων.

Τα κυριότερα πλεονεκτήματα που προκύπτουν από την χρήση της τεχνολογίας LMDS αναφέρονται παρακάτω:

Αυξημένη απόδοση και χωρητικότητα. Σε μικρές αποστάσεις το LMDS μπορεί να υποστηρίξει ρυθμούς δεδομένων μεγαλύτερους του 1 Gbps, κάνοντας έτσι ικανή την ταυτόχρονη μετάδοση δεδομένων, video και φωνής μέσα από το ίδιο κανάλι.

Ευκολία και ευελιξία εγκατάστασης. Από τη στιγμή που θα εγκατασταθούν τα απαραίτητα στοιχεία στον server provider το περαιτέρω κόστος και η εγκατάσταση των APs διαφοροποιείται ανάλογα με τον αριθμό των χρηστών-συνδρομητών. Με τον τρόπο αυτό δεν επιβαρύνεται ο παροχέας των υπηρεσιών με επιπρόσθετο κόστος από την πρώιμη εγκατάσταση ανεκμετάλλευτων συσκευών.

Αποδοτικότητα στη χρησιμοποίηση του εύρους ζώνης. Όταν ένας συνδρομητής δεν χρησιμοποιεί το δίκτυο, η χωρητικότητα που του ‘αντιστοιχεί’ παρέχεται σε έναν άλλον χρήστη κάνοντας το συνολικό δίκτυο περισσότερο αποδοτικό και ευέλικτο.

2.3.4 WiMAX

Το WiMAX είναι μια νέα τεχνολογία που θα πραγματοποιήσει την ευρυζωνική πρόσβαση του τελευταίου μιλίου σε μια μεγαλύτερη γεωγραφική περιοχή από ότι το WLAN, παρέχοντας στους επιχειρησιακούς πελάτες ευρυζωνικές υπηρεσίες τύπου T1 (1.544 Mbps), ενώ στους απλούς χρήστες πρόσβαση ανάλογη του DSL. Με ακτίνα κάλυψης από 1.5 έως 9 km (ανάλογα με τις τιμές διαφόρων παραμέτρων), το WiMAX θα επιτρέψει μεγαλύτερη κινητικότητα στις εφαρμογές δεδομένων υψηλών ταχυτήτων . Με τέτοια χαρακτηριστικά, το WiMAX είναι σε θέση να προσφέρει backhaul για την υποδομή παρόχων, τις μεγάλες επιχειρήσεις και τα WLAN hotspots. Τα δίκτυα WiMAX προβλέπεται να αναπτυχθούν σε τρεις φάσεις. Σε πρώτη φάση, η τεχνολογία WiMAX, χρησιμοποιεί το πρότυπο IEEE 802.16d, θα επεκταθεί μέσω υπαίθριων κεραιών που στοχεύουν γνωστούς συνδρομητές σε μια σταθερή θέση. Σε δεύτερη φάση , θα χρησιμοποιήσει εσωτερικές κεραίες , οι οποίες θα δίνουν στους παρόχους τη δυνατότητα εύκολης εγκατάστασης στους χώρους των χρηστών . Σε τρίτη φάση, θα προωθήσει την IEEE 802.16e προδιαγραφή, στην οποία το WiMAX επικυρωμένο υλικό (WiMAX certified) θα είναι διαθέσιμο στις φορητές λύσεις για τους χρήστες , οι οποίοι θέλουν να κινούνται μέσα σε περιοχές υπηρεσιών, δυνατότητα που παρέχει το WLAN σήμερα.

2.4 Πλεονεκτήματα - Μειονεκτήματα Ασύρματων δικτύων

2.4.1 Πλεονεκτήματα

Μερικά από τα κυριότερα πλεονεκτήματα των ασύρματων τοπικών δικτύων είναι τα εξής:

Κινητικότητα (mobility): Τα WLAN μπορούν να παρέχουν τη δυνατότητα στους χρήστες για πρόσβαση σε πληροφορίες ενώ βρίσκονται σε κίνηση. Αυτή η ευχέρεια στην κίνηση υποστηρίζει την παραγωγικότητα και τις ευκαιρίες για εξυπηρέτηση οι οποίες δεν είναι δυνατές με ενσύρματα δίκτυα. Οι εφαρμογές που στηρίζονται στην κινητικότητα κατά τη χρήση συσκευών σε ένα WLAN συμπεριλαμβάνουν και αυτές που στηρίζονται στην πρόσβαση δεδομένων σε πραγματικό χρόνο-τα οποία είναι συνήθως αποθηκευμένα σε βάσεις δεδομένων. Μία τέτοια εφαρμογή συναντάμε στους αγώνες ταχύτητας. Τα αυτοκίνητα έχουν σύνθετα συστήματα επεξεργασίας που παρακολουθούν και ελέγχουν τα διάφορα όργανα που βρίσκονται στο αυτοκίνητο. Όταν το αυτοκίνητο περνάει μπροστά από τη βάση της ομάδας στα pit, οι πληροφορίες αυτές φορτώνονται στον κεντρικό υπολογιστή, καθιστώντας ικανή μια ανάλυση σε πραγματικό χρόνο της επίδοσης του αυτοκινήτου.

Ταχύτητα και ευελιξία εγκατάστασης: Η εγκατάσταση ενός WLAN εξαλείφει την ανάγκη της χρήσης των καλωδίων η οποία απαιτεί συνήθως κόπο και χρόνο, ενώ η ασύρματη τεχνολογία επιτρέπει τη διασύνδεση δικτύων η οποία υπό άλλες συνθήκες θα ήταν αδύνατη.

Μειωμένο κόστος κτήσης: Ενώ η αρχική επένδυση που απαιτείται για τον εξοπλισμό με ένα WLAN μπορεί σε μερικές περιπτώσεις να είναι υψηλότερη από το αντίστοιχο κόστος για μια ενσύρματη σύνδεση, το συνολικό κόστος λειτουργίας μπορεί να είναι σημαντικά χαμηλότερο, καθώς τα μακροπρόθεσμα κέρδη είναι πολύ

μεγαλύτερα σε δυναμικά περιβάλλοντα όπου απαιτούνται πολύ συχνές μετακινήσεις και αλλαγές.

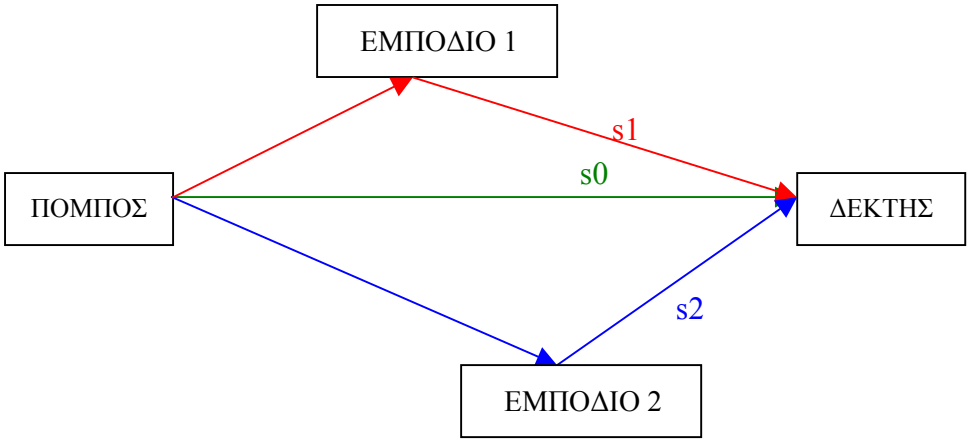
Συμβατότητα: Τα WLAN μπορούν να μεταβληθούν σε μια ποικιλία από τύπους για να ικανοποιήσουν τις ανάγκες συγκεκριμένων εγκαταστάσεων και εφαρμογών. Οι διαμορφώσεις αλλάζουν εύκολα και επεκτείνονται από μικρά δίκτυα κατάλληλα για έναν μικρό αριθμό χρηστών μέχρι πλήρως ανεπτυγμένα δίκτυα που καλύπτουν εκατοντάδες χρήστες.

2.4.2 Προβλήματα

Η χρήση των ηλεκτρομαγνητικών κυμάτων (ραδιοκυμάτων και υπέρυθρης ακτινοβολίας) για την μετάδοση των σημάτων κάνουν τα WLAN ευπαθή σε πολλά φαινόμενα παρεμβολής (interference) τα οποία αλλοιώνουν σε μικρότερο ή μεγαλύτερο βαθμό την επικοινωνία των ασύρματων χρηστών. Τα κυριότερα από αυτά τα προβλήματα αναφέρονται στη συνέχεια.

2. 4.2.1 Παρεμβολή λόγω πολλαπλών διαδρομών

Όπως φαίνεται και στο επόμενο σχήμα τα μεταδιδόμενα σήματα μπορούν να συνδυαστούν με τα ανακλώμενα από διάφορες επιφάνειες ή εμπόδια με αποτέλεσμα την φθορά ή καταστροφή του σήματος που ανιχνεύεται από τον δέκτη. Το φαινόμενο αυτό είναι γνωστό ως ‘παρεμβολή λόγω πολλαπλών διαδρομών’ ή ‘πολύοδη διάδοση’ (multipath propagation). Ο συνολικός χρόνος καθυστέρησης μεταξύ των ανακλώμενων σημάτων σε σχέση με το αρχικό σήμα (primary signal) αναφέρεται ως delay spread.



Σχήμα 2.7 Το φαινόμενο της ‘παρεμβολής λόγω πολλαπλών διαδρομών’.

Οι κατασκευαστές συσκευών για ασύρματα τοπικά δίκτυα ασχολούνται συνεχώς με την επεξεργασία διαφόρων τεχνικών για τον περιορισμό των προβλημάτων που προέρχονται από το συγκεκριμένο φαινόμενο, ενώ ανάμεσα στια άλλες μεθόδους που χρησιμοποιούνται είναι και οι equalization και antenna diversity.

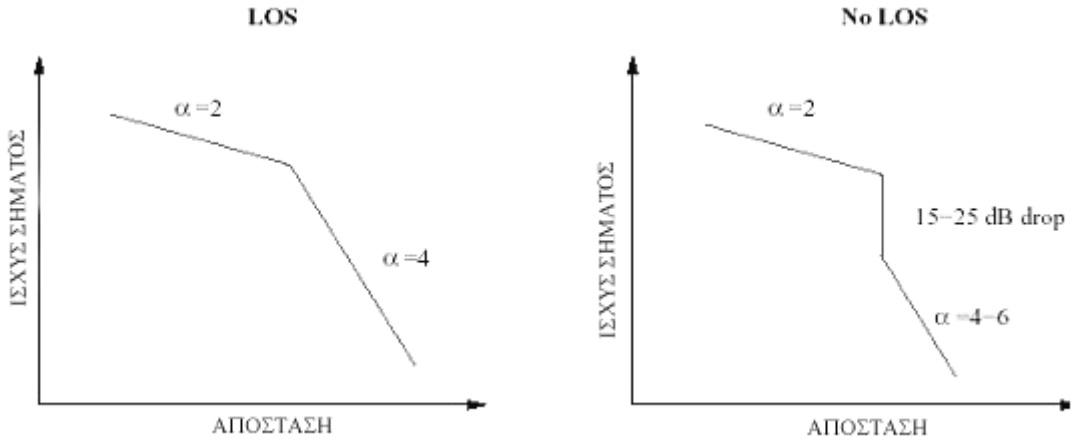
2. 4.2.2 Path loss

Το φαινόμενο του ‘path loss’ μεταξύ πομπού και δέκτη είναι ένα από τα σημαντικότερα στοιχεία που πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό ενός

WLAN. Τα αναμενόμενα επίπεδα του path loss, τα οποία βασίζονται στην απόσταση μεταξύ του πομπού και του δέκτη, παρέχουν πολύτιμες πληροφορίες για τον καθορισμό των επιπέδων στην ισχύ της εκπομπής, στην ευαισθησία του δέκτη και στον λόγο σήματος προς θόρυβο (SNR). Το πραγματικό path loss εξαρτάται από τη συχνότητα μετάδοσης και αυξάνει εκθετικά με την αύξηση της απόστασης μεταξύ του πομπού και του δέκτη. Για τυπικές εφαρμογές σε κλειστούς χώρους, το path loss αυξάνεται περίπου 20 dB ανά 100 πόδια.

Το path loss ισοδυναμεί, ουσιαστικά, με τον λόγο της ισχύος του δέκτη προς την ισχύ του πομπού. Για μία δεδομένη ισχύ μετάδοσης (από τον πομπό), ένα μοντέλο μπορεί να χρησιμοποιηθεί για την πρόβλεψη του επιπέδου της ισχύος στον δέκτη. Το πιο απλό μοντέλο που χρησιμοποιείται, συνήθως, είναι αυτό που στηρίζεται στην εξής εκθετική σχέση: Η ισχύς του λαμβανόμενου σήματος είναι ανάλογη με την ισχύ του μεταδιδόμενου σήματος και αντιστρόφως ανάλογη με το τετράγωνο της συχνότητας μετάδοσης και την απόσταση πομπού-δέκτη υψωμένη στην δύναμη ενός παράγοντα α, ο οποίος κυμαίνεται ανάμεσα στις τιμές 2 (για ελεύθερους χώρους) και 8 (για χώρους με πολλά εμπόδια).

Οι απώλειες από το φαινόμενο αυτό εξαρτώνται άμεσα από την ύπαρξη ή μη οπτικής επαφής (LOS: Line Of Sight) ανάμεσα στον πομπό και στον δέκτη και αποδίδονται παραστατικά στο επόμενο σχήμα.



Σχήμα 2.8 Η έλλειψη οπτικής επαφής μειώνει περισσότερο απότομα την ισχύ λήψης ενός ραδιοκύματος.

2. 4.2.3 Παρεμβολές ραδιοσημάτων

Η διαδικασία της εκπομπής και λήψης ραδιοσημάτων και σημάτων laser μέσω του αέρα καθιστά τα ασύρματα συστήματα ευπαθή από τον θόρυβο της ατμόσφαιρας και από τις μεταδόσεις άλλων συστημάτων που λειτουργούν στην ίδια μπάντα συχνοτήτων και λειτουργούν στον ίδιο φυσικό χώρο. Οι παρεμβολές από ραδιοσήματα (Radio Signal Interfernece) χωρίζονται σε:

Εσωτερικές (inward): Οι παρεμβολές αυτές προέρχονται από τις μεταδόσεις συστημάτων που χρησιμοποιούν τις ίδιες συχνότητες με αυτές ενός WLAN με το οποίο βρίσκονται στην ίδια περιοχή. Για παράδειγμα, πολλές συσκευές WLAN

λειτουργούν στην περιοχή των 2.4 GHz, στην οποία λειτουργούν και οι φούρνοι μικροκυμάτων με αποτέλεσμα η μία συσκευή να παρεμβάλλεται στην άλλη, γεγονός που οδηγεί σε καθυστερήσεις και σφάλματα στην μετάδοση.

Εξωτερικές (outward): Οι παρεμβολές αυτού του είδους προκύπτουν όταν το σήμα ενός ασύρματου δικτύου διακόπτει την μετάδοση ενός άλλου γειτονικού ασύρματου συστήματος, όπως είναι ένα WLAN. Οι παρεμβολές αυτές είναι σπάνιες καθώς τα προϊόντα των WLAN λειτουργούν, συνήθως, με ιδιαίτερα χαμηλή ισχύ (της τάξεως των μερικών mW).

Ένα μέρος των παρεμβολών προκύπτει, ακριβώς, από το γεγονός ότι τα προϊόντα που αποτελούν ένα WLAN λειτουργούν σε συχνότητες που δεν απαιτούν άδεια από τον FCC. Η αποφυγή και η μείωση τέτοιων παρεμβολών εναπόκειται στους κατασκευαστές των ασύρματων προϊόντων.

2. 4.2.4 Διαχείριση ενέργειας

Οι περισσότερες WLAN συσκευές από την πλευρά του χρήστη λειτουργούν με μπαταρίες που έχουν καθορισμένη διάρκεια ζωής. Η χρήση τους σε αυτές τις τηλεπικοινωνιακές εφαρμογές μειώνουν την αυτονομία τους. Έτσι οι περισσότεροι χρήστες δε θα ήταν ευχαριστημένοι αν ήταν υποχρεωμένοι να φορτίζουν συχνά τις μπαταρίες των συσκευών τους, ενώ υπάρχουν και περιπτώσεις που είναι σχεδόν αδύνατη η φόρτιση του υπολογιστή. Για τον λόγο αυτό θα πρέπει να γίνει επιλογή προϊόντων που να κάνουν σωστή διαχείριση ενέργειας (power management support), ώστε να μεγιστοποιείται η αυτονομία των μπαταριών και να ελαχιστοποιείται η αντικατάστασή τους.

2.4.2.5 Ασυμβατότητα συστημάτων

Στην κατασκευή ενός WLAN θα πρέπει να ληφθεί υπόψη η ασυμβατότητα (interoperability) μεταξύ προϊόντων διαφορετικών κατασκευαστών, διαφορετικά το δίκτυο δε θα λειτουργεί σωστά. Οι λόγοι ασυμβατότητας είναι οι εξής:

Διαφορετική τεχνολογία: Ένα σύστημα που χρησιμοποιεί την τεχνολογία διαμόρφωσης Frequency Hopping Spread Spectrum (FHSS) δε θα επικοινωνεί με ένα άλλο που βασίζεται στην τεχνολογία διαμόρφωσης Direct Sequence Spread Spectrum (DSSS).

Χρήση διαφορετικού φάσματος συχνοτήτων: Η επικοινωνία μεταξύ συσκευών που λειτουργούν σε διαφορετικές συχνότητες δεν είναι δυνατή ακόμα και αν χρησιμοποιείται η ίδια τεχνολογία.

Διαφορετική υλοποίηση: Ακόμα και να χρησιμοποιείται η ίδια τεχνολογία και το ίδιο φάσμα συχνοτήτων μπορεί να μην είναι δυνατή η επικοινωνία λόγω διαφορετικών παραμέτρων υλοποίησης από κάθε κατασκευαστή.

2. 4.2.6 Ασφάλεια δικτύου

Η λειτουργία ενός ασύρματου δικτύου αντιστοιχεί στα χαμηλότερα επίπεδα της αρχιτεκτονικής ενός δικτύου και δεν εμπεριέχει άλλες λειτουργίες όπως εγκατάσταση σύνδεσης από άκρο σε άκρο ή άλλες υπηρεσίες (π.χ. login) που προσφέρουν τα ανώτερα στρώματα. Για τον λόγο αυτό το μόνο θέμα που σχετίζεται με την ασφάλεια και απασχολεί τα ασύρματα δίκτυα έχει να κάνει με θέματα

ασφαλείας των χαμηλότερων στρωμάτων, όπως η κρυπτογράφηση (encryption) των δεδομένων.

Για τον λόγο αυτό, έχουν υλοποιηθεί διάφορες τεχνικές κωδικοποίησης οι οποίες καθιστούν εξαιρετικά δύσκολη την λήψη της μεταδιδόμενης πληροφορίας από κάποιον χρήστη πέραν του προοριζόμενου.

Τέτοιες τεχνικές είναι οι τεχνικές εξάπλωσης φάσματος (spread spectrum), ενώ εάν ο χρήστης απαιτεί περισσότερη ασφάλεια κατά τη μετάδοση των δεδομένων, το IEEE 802.11 Standard (το πιο διαδεδομένο ίσως πρωτόκολλο για WLAN στην περιοχή των 2.4 GHz), καθορίζει τη χρήση της κωδικοποίησης WEP (Wired Equivalent Privacy). Η κωδικοποίηση αυτή χρησιμοποιεί τον αλγόριθμο 'RSA Data Security Inc. RC4 encryption' για την κρυπτογράφηση των εκπεμπόμενων σημάτων.

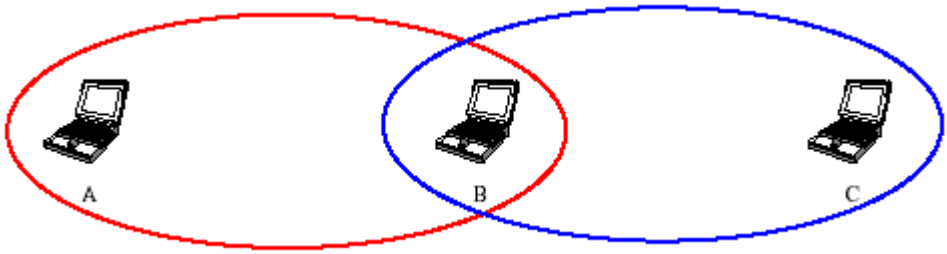
2. 4.2.7 Προστασία της υγείας των χρηστών

Το θέμα της προστασίας (safety) του χρήστη δεν έχει σημασία για τα ενσύρματα δίκτυα σε αντίθεση με τα ασύρματα. Τα ασύρματα LAN που χρησιμοποιούν την τεχνική μετάδοσης με υπέρυθρες ακτίνες, θα πρέπει να περιορίσουν την ισχύ του εκπεμπόμενου σήματος στο ανώτερο όριο των 2 Watts, για να αποφευχθούν ανεπιθύμητα οφθαλμολογικά προβλήματα.

Η ισχύς του εκπεμπόμενου σήματος από ένα πομπό ραδιοσυχνοτήτων (RF: Radio Frequency) των WLAN είναι πολύ μικρότερη (συνήθως μεταξύ 50 και 100 mWatt) από αυτή που εκπέμπει ένα κοινό κινητό τηλέφωνο (600 mWatt – 3 Watt). Έτσι καθώς η ισχύς των RF σημάτων μειώνεται με την αύξηση της απόστασης από τον πομπό, ελαχιστοποιείται ακόμα περισσότερο η ηλεκτρομαγνητική ακτινοβολία που δέχονται οι χρήστες που βρίσκονται στην περιοχή των ασύρματων δικτύων.

2. 4.2.8 Το πρόβλημα του κρυμμένου κόμβου

Ένας συνηθισμένος περιορισμός στην απόδοση των WLAN είναι το πρόβλημα που προκύπτει από την περιορισμένη ακτίνα δράσης των ραδιοκυμάτων και είναι γνωστό ως 'hidden node problem'. Το φαινόμενο αυτό προκύπτει όταν στο σύστημα υπάρχει ένας σταθμός που δεν μπορεί να ανιχνεύσει την μετάδοση ενός άλλου σταθμού ώστε να αναγνωρίσει ότι το μέσο χρησιμοποιείται. Στο επόμενο σχήμα, ο σταθμός Α θέλει να μεταδώσει στον σταθμό Β, όμως δεν μπορεί να ανιχνεύσει ότι και ο σταθμός C θέλει να μεταδώσει, με αποτέλεσμα να προκύψει σύγκρουση.



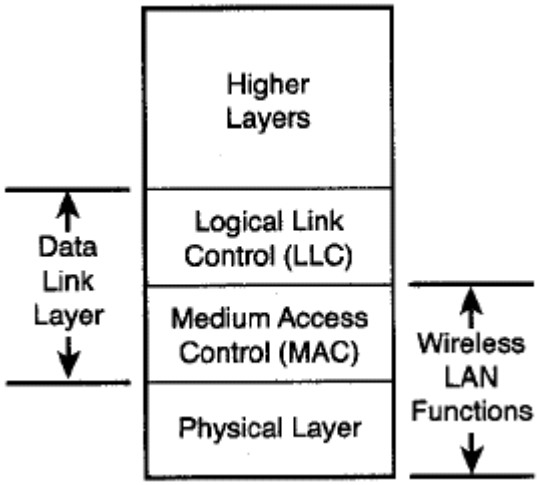
Σχήμα 2.9 Ο σταθμός Α δεν μπορεί να ανιχνεύσει την μετάδοση του σταθμού C, με αποτέλεσμα αν αποφασίσουν και οι δύο να μεταδώσουν προς τον Β να προκύψει μία σύγκρουση.

ΚΕΦΑΛΑΙΟ 3

3.1 ΕΙΣΑΓΩΓΗ ΣΤΟ 802.11

Το IEEE 802.11 Standard αποτελεί το πιο βασικό και αναγνωρισμένο Standard για WLAN, στις βασικές λειτουργίες του οποίου στηρίζονται τα τρέχοντα πρωτόκολλα του IEEE (802.11a και 802.11b) για ασύρματα τοπικά δίκτυα. Σύμφωνα με την αρχική διατύπωση του PAR (Project Authorization Request) για το 802.11 '…ο σκοπός του προτεινόμενου Standard είναι η ανάπτυξη μιας προδιαγραφής (specification) για την ασύρματη διασύνδεση σταθερών, φορητών (portable) και κινητών (moving) σταθμών μέσα σε μια τοπική περιοχή'.

Το τελικό Standard, που δημοσιεύθηκε το Νοέμβριο του 1997, καθορίζει την λειτουργία πρωτοκόλλων ικανών να υποστηρίξουν την από αέρος διαδικτύωση μιας τοπικής περιοχής. Όπως με άλλα Standards της οικογένειας IEEE 802 (όπως τα 802.3 και 802.5) η κύρια υπηρεσία του 802.11 είναι η μεταφορά των MSDU (MAC Service Data Unit) μεταξύ ομότιμων στρωμάτων ζεύξης δεδομένων. Οι λειτουργίες και οι υπηρεσίες που καθορίζονται από το 802.11 αφορούν τα επίπεδα MAC και PHY, όπως φαίνεται και στο επόμενο σχήμα.



Σχήμα 3.1 Το 802.11 καθορίζει τη λειτουργία των WLAN μέσω των επιπέδων MAC και PHY.

Το 802.11 λαμβάνει υπόψη του και τις επόμενες σημαντικές διαφορές ανάμεσα στα ενσύρματα και ασύρματα LAN:

Διαχείριση ενέργειας: Οι συσκευές που μπορούν να χρησιμοποιήσουν ένα δίκτυο 802.11 μπορεί να είναι είτε φορητές (portable, οι οποίες μπορούν να μετακινούνται, αλλά για να λειτουργήσουν πρέπει να βρίσκονται σε σταθερό σημείο) είτε κινητές (mobile, οι οποίες μπορούν να λειτουργούν ενώ είναι σε κίνηση). Και οι δύο αυτοί τύποι συσκευών απαιτούν την χρήση μπαταριών για την υποστήριξη των διάφορων ηλεκτρονικών στοιχείων, ενώ η χρήση των ασύρματων καρτών δικτύου εξαντλεί πιο γρήγορα τις μπαταρίες του υπολογιστή. Για τον λόγο αυτό, το 802.11 καθορίζει διάφορες λειτουργίες ελέγχου της ισχύος οι οποίες υλοποιούνται στο επίπεδο MAC.

Εύρος ζώνης: Το 802.11 εφαρμόζει διάφορες μεθόδους για να πετύχει τον υψηλότερο δυνατό ρυθμό δεδομένων στην μπάντα συχνοτήτων ISM.

Ασφάλεια: Τα ασύρματα δίκτυα μεταδίδουν τα σήματα σε πολύ μεγαλύτερες περιοχές (όσον αφορά την κατεύθυνση του σήματος) από αυτές που καλύπτει ένα

καλώδιο ή μια οπτική ίνα. Για την υψηλότερη ασφάλεια το 802.11 κάνει χρήση των πρωτοκόλλων που αναφέρονται στο 802.10, το οποίο σχετίζεται με μηχανισμούς ασφάλειας στα 802.x δίκτυα.

Διευθυνσιοδότηση: Η τοπολογία ενός ασύρματου δικτύου είναι δυναμική. Για τον λόγο αυτό η διεύθυνση προορισμού δεν ανταποκρίνεται πάντα στην ίδια φυσική θέση του προορισμού. Το πρόβλημα της δρομολόγησης πακέτων μεταξύ κινητών σταθμών μπορεί να λυθεί με τη χρήση διάφορων πρωτοκόλλων, το πιο γνωστό από τα οποία είναι το MobileIP που βασίζεται στο πρωτόκολλο μεταφοράς TCP/IP.

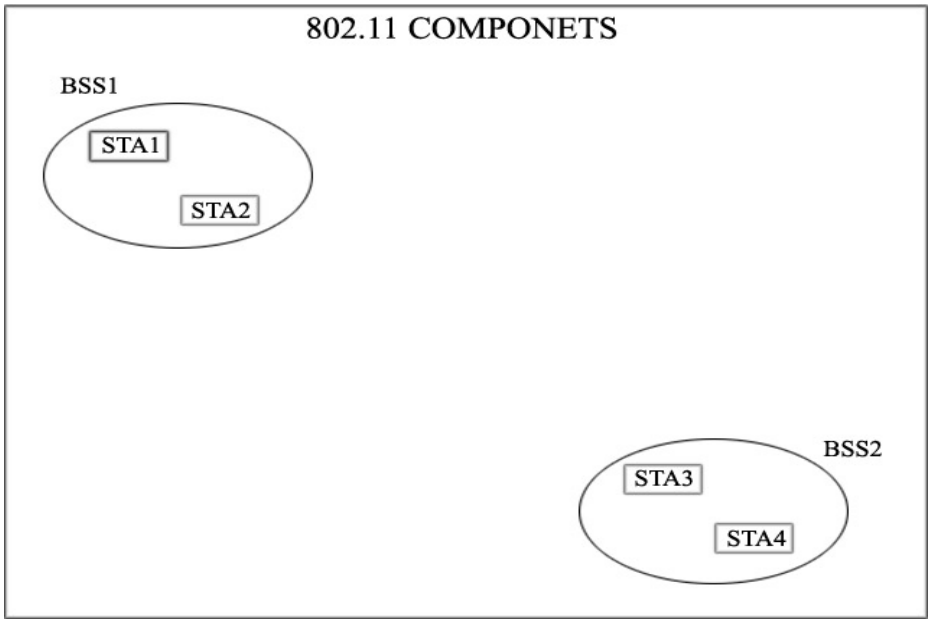
3.2 Η τοπολογία του 802.11

Η τοπολογία του 802.11 αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο που να παρέχει τη δυνατότητα μετακίνησης των σταθμών η οποία να μην γίνεται αντιληπτή από τα ανώτερα στρώματα, όπως το LLC (Logical Link Control). Ένας σταθμός (station) είναι κάθε συσκευή η οποία εμπεριέχει τις λειτουργίες του 802.11 (δηλαδή το επίπεδο MAC, το φυσικό στρώμα και μια διασύνδεση (interface) με το ασύρματο μέσο).

Οι λειτουργίες του 802.11 ενυπάρχουν (reside) σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card), το λογισμικό διασύνδεσης που οδηγεί την κάρτα NIC και τον σταθμό βάσης ή AP (Access Point).

3.2.1 BSS

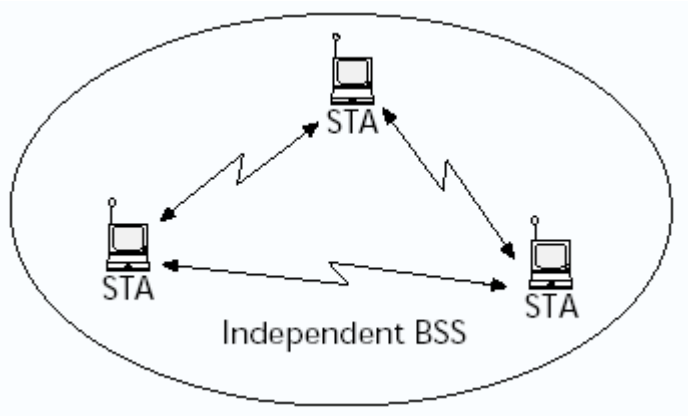
Το βασικό δομικό στοιχείο ενός IEEE 802.11 LAN είναι το BBS (Basic Service Set). Στο παρακάτω σχήμα φαίνονται 2 BSS, το καθένα από τα οποία έχει 2 σταθμούς (STA) οι οποίοι είναι μέλη του BSS. Αν ένας σταθμός μετακινηθεί έξω από το BSS στο οποίο ανήκει δεν μπορεί πλέον να επικοινωνεί άμεσα με τα άλλα μέλη του συγκεκριμένου BSS.



Σχήμα 3.2 Σχηματική αναπαράσταση δύο BSS.

3.2.2 IBSS

Ο πιο βασικός τύπος ενός 802.11 LAN είναι το IBSS (Independent BSS), όπου δύο ή περισσότεροι σταθμοί μπορούν να επικοινωνούν απευθείας μεταξύ τους. Στο παρακάτω σχήμα φαίνονται δύο IBSS ή όπως αλλιώς ονομάζονται ad-hoc δίκτυα.

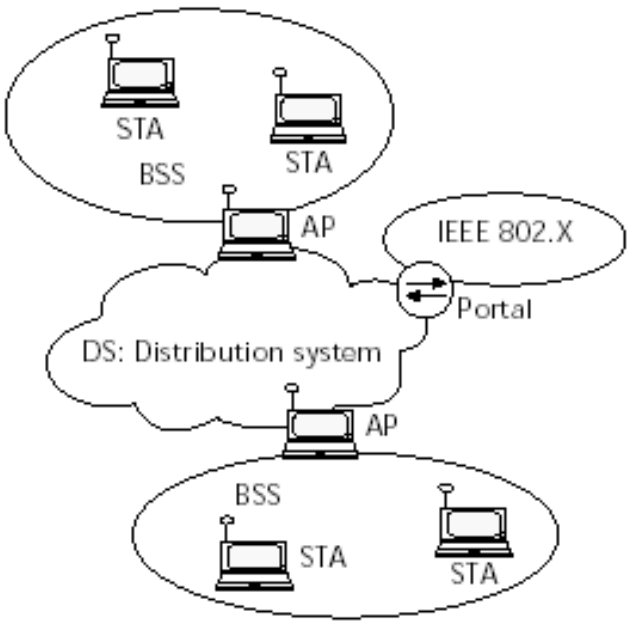


Σχήμα 3.3 Ένα ad-hoc δίκτυο

3.2.3 ESS

Όταν οι ανάγκες της διαδικτύωσης ξεπερνούν τα όρια του IBSS, το 802.11 καθορίζει τη δομή ενός πιο σύνθετου τοπικού δικτύου που ονομάζεται ESS (Extended Service Set) και στο οποίο είναι δυνατή η διασύνδεση και η επικοινωνία πολλών BSS μεταξύ τους. Το στοιχείο που χρησιμοποιείται για την διασύνδεση των BSS ονομάζεται DS (Distributed System). Το 802.11 κάνει διαχωρισμό μεταξύ του Ασύρματου Μέσου WM (Wireless Medium) από το DSM (Distributed System Medium).

Η πρόσβαση στο DS γίνεται με την βοήθεια ενός σταθμού που καλείται AP (Access Point) και ο οποίος παρέχει ουσιαστικά τη διασύνδεση των σταθμών που βρίσκονται σε διάφορα BSS στο DS. Η διασύνδεση αυτή φαίνεται στο επόμενο σχήμα.



Σχήμα 3.4 Η σύνδεση των BSSs με το DS γίνεται με την βοήθεια των APs.

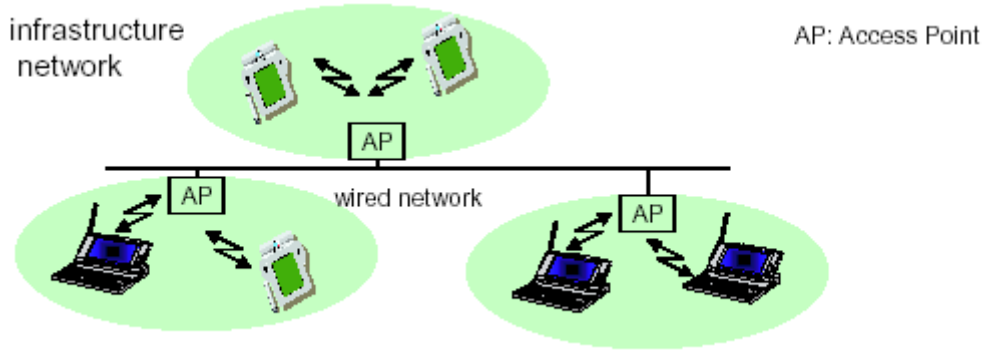
Τα δεδομένα μετακινούνται μεταξύ ενός BSS και του DS μόνο μέσω του AP, ενώ το DS υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές

να ελέγχουν την αντιστοίχηση (mapping) της διεύθυνσης στον προορισμό για κάθε σταθμό που μετακινείται.

Η κεντρική ιδέα της συγκεκριμένης τοπολογίας, είναι ότι ένα δίκτυο ESS εμφανίζεται το ίδιο σε ένα επίπεδο LLC όπως και ένα δίκτυο IBSS. Οι σταθμοί μέσα στο ίδιο ESS μπορούν να μετακινούνται από ένα BSS σε ένα άλλο διαφανώς ως προς το LLC. Τα ESS δίκτυα αναφέρονται και ως infrastructure δίκτυα, αν και τα τελευταία αποδίδουν συνήθως την τοπολογία όπου ένα BSS συνδέεται μέσω ενός AP σε ένα ενσύρματο δίκτυο.

Το Standard του 802.11 δεν περιορίζει τη σύνθεση του DS. Για τον λόγο αυτό μπορεί να είναι συμβατό με άλλα δίκτυα που είτε ανήκουν είτε όχι στην οικογένεια 802. Για την ενοποίηση της αρχιτεκτονικής του 802.11 με ένα παραδοσιακό ενσύρματο τοπικό δίκτυο χρησιμοποιείται ένα επιπλέον στοιχείο γνωστό ως πύλη (portal).

Η πύλη είναι το λογικό σημείο μέσω του οποίου τα MSDUs από ένα τοπικό δίκτυο διαφορετικό του 802.11 εισέρχονται στο DS του 802.11. Στην περίπτωση που το DS αποτελείται από τύπους δικτύων της οικογένειας 802 (όπως τα 802.3 και 802.5) η πύλη και το AP αποτελούν το ίδιο στοιχείο. Στο επόμενο σχήμα απεικονίζεται η διασύνδεση πολλών BSSs σε ένα ενσύρματο δίκτυο.



Σχήμα 3.5 Διασύνδεση ενός ενσύρματου δικτύου με 3 BSSs.

Το 802.11 αναγνωρίζει τους παρακάτω τύπους κίνησης:

Απουσία μετακίνησης: Ο τύπος αυτός αναφέρεται σε σταθμούς που δεν μετακινούνται και σε αυτούς που μετακινούνται μέσα σε ένα τοπικό BSS.

BSS μετακίνηση: Ο τύπος αυτός αναφέρεται σε σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο BSS μέσα στο ίδιο ESS.

ESS μετακίνηση: Αυτός ο τύπος μετακίνησης αναφέρεται σε σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο BSS το οποίο ανήκει σε διαφορετικό ESS.

Αξίζει να αναφέρουμε ότι το 802.11 ενώ υποστηρίζει ξεκάθαρα τους δύο πρώτους τύπους μετακίνησης, δεν εγγυάται την διατήρηση της σύνδεσης κατά την μετακίνηση σε διαφορετικό ESS.

3.3 Η ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ 802.11

Ενώ η τοπολογία καθορίζει τα αναγκαία μέσα για τη φυσική διασύνδεση του ασύρματου δικτύου, η αρχιτεκτονική καθορίζει τον τρόπο λειτουργίας του δικτύου. Έτσι, η αρχιτεκτονική του 802.11 η οποία εφαρμόζεται σε κάθε σταθμό, αποτελείται

από ένα υπόστρωμα MAC και 3 διαφορετικά φυσικά στρώματα PHY, τα οποία χρησιμοποιούν διαφορετικές τεχνικές διαμόρφωσης του εκπεμπόμενου σήματος.

3.3.1 ΤΟ ΥΠΟΣΤΡΩΜΑ MAC ΤΟΥ 802.11

Σκοπός του επιπέδου MAC είναι να παρέχει λειτουργίες ελέγχου πρόσβασης (στις οποίες συμπεριλαμβάνονται η διευθυνσιοδότηση, ο έλεγχος της σωστής σειράς των πλαισίων κ.ά.) στο μοιραζόμενο φυσικό κανάλι, όπως αυτό καθορίζεται από το Standard.

3.3.1.1 Λειτουργίες του υποστρώματος MAC

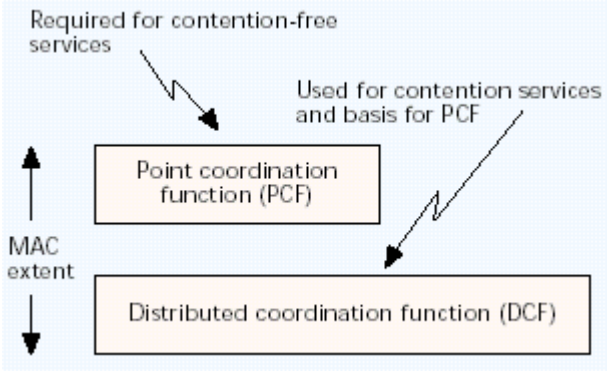
Κάθε σταθμός και AP σε ένα 802.11 WLAN υλοποιεί τις υπηρεσίες του υποστρώματος MAC η οποία παρέχει την δυνατότητα στις ομότιμες (peer) LLC οντότητες (entities) να ανταλλάσσουν MSDUs (MAC Service Data Units) μεταξύ των MAC SAPs (Service Access Points). Το υπόστρωμα MAC παρέχει 3 κύριες λειτουργίες:

- Πρόσβαση στο ασύρματο μέσο
- Προσχώρηση (joining) σε ένα δίκτυο
- Παροχή των λειτουργιών 'authentication' και 'privacy'

3.3.1.2 Πρόσβαση στο ασύρματο μέσο

Πριν ξεκινήσει η μετάδοση ενός πλαισίου, ένας σταθμός πρέπει πρώτα να επιτύχει την πρόσβαση στο μέσο. Για να το επιτύχει αυτό υπάρχουν δύο μέθοδοι, όπως καθορίζονται από την αρχιτεκτονική του Standard (σχήμα 3.6):

- DCF (Distributed Coordination Function): Το 802.11 καθορίζει τις επόμενες δύο κατηγορίες DCF:
  - *DCF CSMA/CA*: Η αρχή λειτουργίας της μεθόδου αυτής αυτού βασίζεται στον ανταγωνισμό και για την πρόσβαση στο μέσο χρησιμοποιείται η τεχνική CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance)
  - *DCF RTS/CTS*: Η αρχή λειτουργίας της μεθόδου αυτής στηρίζεται στην πρόσβαση στο μέσο με την βοήθεια πακέτων 'αίτησης' (RTS) και 'άδειας' (CTS) χρήσης του μέσου
- PCF (Point Coordination Function): Το πρωτόκολλο αυτό στηρίζεται στην πρόσβαση στο μέσο χωρίς ανταγωνισμό (χρήσιμο για infrastructure δίκτυα), ενώ κύριο ρόλο παίζει ένας ελεγκτής ο οποίος καλείται PC (Point Coordinator) και βρίσκεται στα APs.

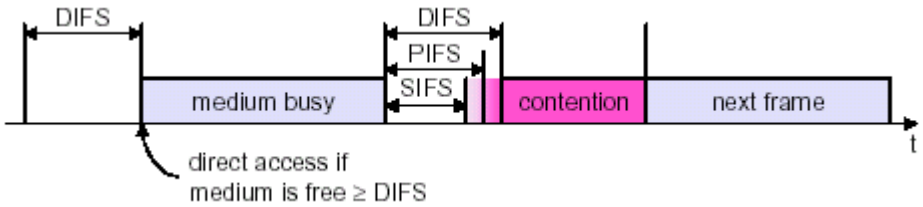


Σχήμα 3.6: Η αρχιτεκτονική του επιπέδου MAC του 802.11.

3.3.1.3 Χρονικά διαστήματα πρόσβασης

Το IEEE 802.11 καθορίζει την ύπαρξη χρονικών διαστημάτων για την μεσολάβηση μεταξύ των διαφόρων λειτουργιών αποστολής και λήψης πλαισίων ενός σταθμού. Το χρονικό διάστημα μεταξύ των πλαισίων (frames) καλείται **IFS** (Inter Frame Space). Τα 4 διαφορετικά IFSs που χρησιμοποιούνται για να καθορίσουν τα επίπεδα προτεραιότητας για την πρόσβαση στο ασύρματο μέσο φαίνονται στο επόμενο σχήμα. Η αναφορά γίνεται ξεκινώντας από αυτό με την μικρότερη διάρκεια:

A. SIFS: Short InterFrame Space
B. PIFS: PCF InterFrame Space
C. DIFS: DCF InterFrame Space
D. EIFS: Extended InterFrame Space



Σχήμα 3.7: Τα 3 κυριότερα IFS που χρησιμοποιούνται για τον καθορισμό των διάφορων πλαισίων που μετακινούνται μέσα στο 802.11 δίκτυο.

Τα διαφορετικά αυτά χρονικά διαστήματα πρέπει να είναι ανεξάρτητα από το ρυθμό bit ενός σταθμού, ενώ τα ίδια διαστήματα πρέπει να παραμένουν αμετάβλητα, σύμφωνα με τιμές που καθορίζονται από το φυσικό στρώμα. Στη συνέχεια αναλύουμε τις περιπτώσεις στις οποίες χρησιμοποιείται το κάθε IFS (η χρήση τους θα φανεί καλύτερα στις επόμενες παραγράφους):

- SIFS: Χρησιμοποιείται για τα ACK πλαίσια, τα CTS πλαίσια, το δεύτερο ή ένα διαδοχικό MPDU ενός 'fragment burst' και από έναν σταθμό που αποκρίνεται σε κάθε διαλογή (polling) μέσω του PCF. Το SIFS χρησιμοποιείται από έναν σταθμό όταν αυτός έχει καταλάβει το μέσο και χρειάζεται να το κρατήσει για την διάρκεια της μετάδοσης ενός πλαισίου. Έχοντας τη μικρότερη διάρκεια, εμποδίζει τους άλλους σταθμούς που θέλουν να μεταδώσουν, καθώς αυτοί πρέπει να περιμένουν για μεγαλύτερο διάστημα μέχρι να ανιχνεύσουν ότι το μέσο είναι ελεύθερο. Έτσι, δίνεται η δυνατότητα στον σταθμό που ήδη μεταδίδει να ολοκληρώσει τη διαδικασία μετάδοσης των πλαισίων που έχει προς μετάδοση.
- PIFS: Το PIFS μπορεί να χρησιμοποιηθεί από έναν σταθμό μόνο κατά τη λειτουργία του PCF για να κερδίσει την πρόσβαση στο μέσο, κατά την έναρξη του CFP. Ο υπολογισμός του γίνεται με βάση τον τύπο:

  PIFS = SIFSTime + SlotTime

- DIFS: Το DIFS μπορεί να χρησιμοποιείται από σταθμούς που λειτουργούν με DCF για την μετάδοση πλαισίων δεδομένων (MPDUs) και πλαισίων διαχείρισης (MMPDUs). Ο υπολογισμός του γίνεται με βάση τον τύπο:

  DIFS = SIFSTime + 2 x SlotTime

- EIFS: Το EIFS μπορεί να χρησιμοποιείται από σταθμούς που λειτουργούν με DCF, όποτε το φυσικό στρώμα υποδείξει στο MAC ότι η μετάδοση ενός πλαισίου είχε ξεκινήσει αλλά δεν κατέληξε στην σωστή παραλαβή ενός ολόκληρου MAC πλαισίου με τη σωστή τιμή FCS (Frame Check Sequence, το οποίο είναι ένα πεδίο στο πλαίσιο MAC που χρησιμοποιείται για έλεγχο λαθών με τη βοήθεια του αλγορίθμου CRC). Ο υπολογισμός του προκύπτει από τα SIFS, DIFS και τον χρόνο που χρειάζεται για να μεταδοθεί ένα ACK πλαίσιο ελέγχου με ρυθμό 1 Mbps, σύμφωνα με την εξίσωση:

EIFS = SIFSTime + (8 x ACKSize) + PreambleLength + PLCPHeaderLength + DIFS

Οι τιμές που δίνονται από το Standard, ανάλογα με το φυσικό επίπεδο που χρησιμοποιείται, φαίνονται στο επόμενο σχήμα

Interframe Space	DSSS	FHSS	DFIR
SIFS	10 μs	28 μs	7 μs
PIFS	30 μs	78 μs	15 μs
DFIS	50 μs	128 μs	23 μs
Slot time	20 μs	50 μs	8 μs

Σχήμα 3.8

3.3.1.4 Λειτουργία του μηχανισμού πρόσβασης DCF

Στην παράγραφο αυτή θα αναπτύξουμε τις δύο μεθόδους πρόσβασης DCF που καθορίζονται από το 802.11 Standard, δίνοντας ιδιαίτερη σημασία στην μέθοδο με χρήση της τεχνικής CSMA/CA.

3.3.1.4.1 Μηχανισμός ανίχνευσης φέροντος

Ένας συνδυασμός φυσικού και εικονικού μηχανισμού ανίχνευσης φέροντος ενεργοποιεί τη συνιστώσα 'MAC coordination' για να καθορίσει αν το μέσο είναι απασχολημένο ή αδρανές. Κάθε φυσικό στρώμα που καθορίζεται από το 802.11 παρέχει έναν συγκεκριμένο τρόπο ανίχνευσης του μέσου. Το αποτέλεσμα από την εκτίμηση του φυσικού καναλιού στέλνεται από την 'PHY coordination' στην 'MAC coordination' ως μέρος της πληροφορίας για τον καθορισμό της κατάστασης του μέσου.

Η 'MAC coordination' εκτελεί τον εικονικό μηχανισμό ανίχνευσης φέροντος που στηρίζεται στις πληροφορίες κράτησης που υπάρχουν στο πεδίο 'Duration' σε όλα τα πλαίσια RTS και CTS. Η πληροφορία αυτή ανακοινώνει σε όλους τους σταθμούς αν ένας σταθμός πρόκειται να χρησιμοποιήσει το μέσο. Η 'MAC coordination' ελέγχει τα πεδία 'Duration' σε όλα τα MAC πλαίσια και τοποθετεί την πληροφορία αυτή στο **NAV** (Network Allocation Vector) κάθε σταθμού αν η τιμή είναι μεγαλύτερη από την τρέχουσα NAV που έχει ο σταθμός. Ο NAV λειτουργεί ως ένας μετρητής, ξεκινώντας με μια τιμή ίση με την τιμή που υπήρχε στο πεδίο

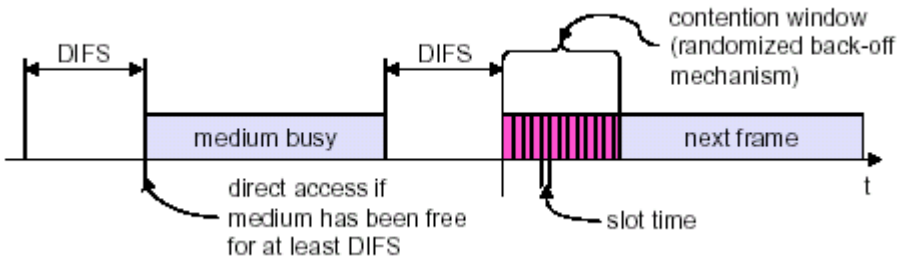
‘Duration’ του τελευταίου πλαισίου που ανιχνεύθηκε στο μέσο και μετρώντας αντίστροφα προς το 0.

Η ανίχνευση του φυσικού στρώματος και η λειτουργία του NAV παρέχουν ικανές πληροφορίες στο υπόστρωμα MAC για να αποφασίσει την κατάσταση του καναλιού. Για παράδειγμα, το φυσικό στρώμα μπορεί να έχει ανιχνεύσει ότι δεν υπάρχουν τρέχουσες μεταδόσεις στο μέσο, παρ’ όλα η τιμή στο NAV μπορεί να δηλώνει ότι μία μετάδοση που έλαβε χώρα αποτρέπει όλες τις μεταδόσεις για ένα καθορισμένο χρονικό διάστημα. Στην περίπτωση αυτή το MAC θα αναβάλλει όλες τις μεταδόσεις μέχρι να εκπνεύσει η περίοδος που καθορίζεται στο πεδίο ‘Duration’.

3.3.1.4.2 Λειτουργία του DCF με τη μέθοδο CSMA/CA

Ο βασικός μηχανισμός πρόσβασης καλείται DCF και ουσιαστικά είναι ένας μηχανισμός CSMA/CA (σχήμα 3.9). Ένα πρωτόκολλο CSMA λειτουργεί, γενικά, ως εξής: Ένας σταθμός που θέλει να μεταδώσει, αρχικά, ανιχνεύει το μέσο. Αν το μέσο είναι κατειλημμένο τότε ο σταθμός αναβάλλει την μετάδοση για αργότερα. Αν το μέσο ανιχνευθεί ελεύθερο τότε ο σταθμός επιτρέπεται να μεταδώσει. Πιο συγκεκριμένα η σειρά που ακολουθείται κατά την λειτουργία του CSMA/CA είναι η εξής:

1. Ένας σταθμός που θέλει να μεταδώσει ανιχνεύει αρχικά το μέσο για να διαπιστώσει αν ένας άλλος σταθμός μεταδίδει. Αν το μέσο είναι:
   - κατειλημμένο, αναβάλλει την μετάδοση μέχρι το τέλος της τρέχουσας μετάδοσης. Μετά την αναβολή (deferral) ή πριν προσπαθήσει να μεταδώσει αμέσως μετά από μια επιτυχή μετάδοση, ο σταθμός πρέπει να επιλέξει ένα τυχαίο διάστημα οπισθοχώρησης (backoff) πριν ξαναπροσπαθήσει να μεταδώσει.
   - ελεύθερο για ένα συγκεκριμένο χρονικό διάστημα (το οποίο είναι ίσο με DIFS) τότε επιτρέπεται στον σταθμό να μεταδώσει.
2. Ο σταθμός λήψης ελέγχει το CRC του ληφθέντος πακέτου και στέλνει ένα πακέτο επαλήθευσης (ACK). Η λήψη του πακέτου επαλήθευσης δηλώνει στον πομπό ότι δεν συνέβη σύγκρουση. Αν ο αποστολέας δεν λάβει το πακέτο επαλήθευσης ξαναστέλνει το τεμάχιο μέχρι να λάβει την επαλήθευση. Η διαδικασία αυτή επαναλαμβάνεται για ένα συγκεκριμένο αριθμό επαναμεταδόσεων.

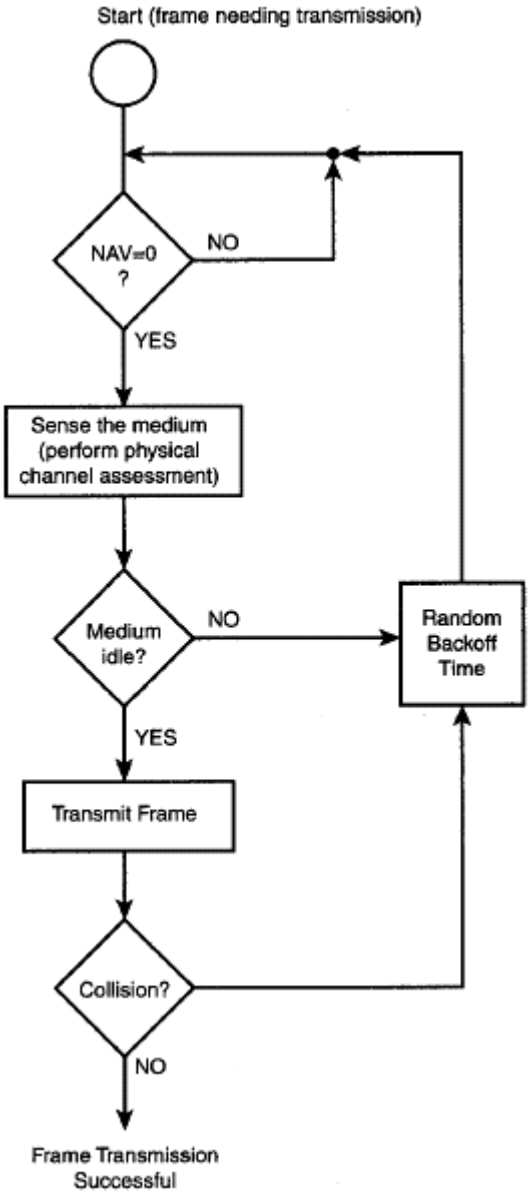


Σχήμα 3.9: Σχηματική αναπαράσταση του βασικού μηχανισμού πρόσβασης DCF.

Οι τυχόν συγκρούσεις που θα συμβούν πρέπει να ανιχνευθούν από το επίπεδο MAC ώστε η επαναμετάδωση των πακέτων να γίνει από το επίπεδο αυτό και όχι από κάποιο ανώτερο, γεγονός το οποίο θα προκαλούσε σημαντική καθυστέρηση.

Σε σταθμούς που χρησιμοποιούν στο φυσικό στρώμα την τεχνική της μεταπήδησης συχνότητας (FH: Frequency Hopping)), ο έλεγχος του καναλιού χάνεται

στο όριο του ‘dwell time’ και ο σταθμός πρέπει να ανταγωνιστεί για το κανάλι με το τέλος του παραπάνω διαστήματος. Είναι, επίσης, απαραίτητο οι σταθμοί που χρησιμοποιούν FH να έχουν ολοκληρώσει την μετάδοση ενός ολόκληρου MPDU και του αντίστοιχου ACK (αν απαιτείται) πριν το όριο του ‘dwell time’.



Σχήμα 3.10: Διάγραμμα ροής της λειτουργίας DCF σύμφωνα με τον αλγόριθμο CSMA/CA.

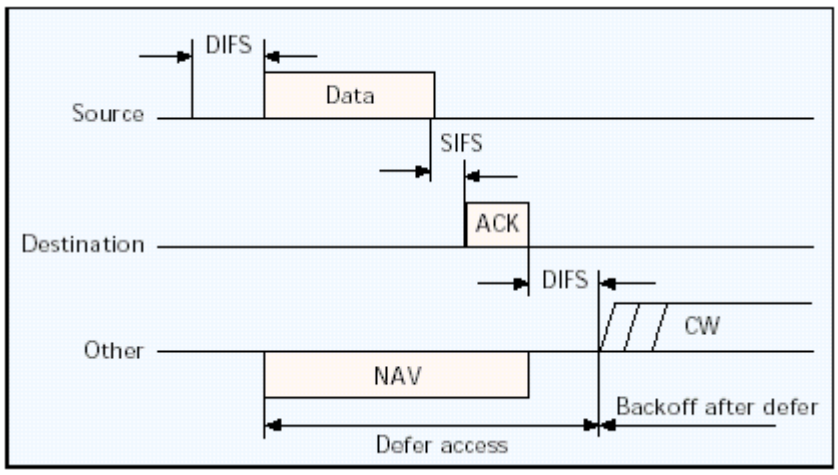
3.3.1.4.3 Διαδικασία επαλήθευσης από το υπόστρωμα MAC

Ένας σταθμός πρέπει να απαντήσει με μια επαλήθευση αν το CRC του ληφθέντος πλαισίου είναι σωστό. Αυτή η τεχνική είναι γνωστή ως ‘θετική επαλήθευση’. Η μη-λήψη ενός αναμενόμενου ACK πλαισίου είναι ένδειξη λάθους για τον σταθμό μετάδοσης. Παρ’ όλα αυτά, ο σταθμός λήψης μπορεί να έχει λάβει σωστά το πλαίσιο και το λάθος να έχει συμβεί στην λήψη του ACK, γεγονός που δεν μπορεί να διακρίνει ο σταθμός που ξεκίνησε την ανταλλαγή του πλαισίου.

Ύστερα από μια επιτυχή λήψη ενός πλαισίου που χρειάζεται επαλήθευση, η μετάδοση του ACK πλαισίου θα ξεκινήσει ύστερα από μια περίοδο SIFS (ώστε να

μην υπάρχει ανταγωνισμός) χωρίς να υπολογίζεται αν το μέσο είναι κατειλημμένο ή ελεύθερο.

Ένας σταθμός πρέπει να περιμένει για ένα χρονικό διάστημα το οποίο αναφέρεται ως 'ACKTimeout' χωρίς να έχει γίνει λήψη ενός ACK πλαισίου πριν προχωρήσει στο συμπέρασμα πως η μετάδοση του MPDU απέτυχε. Στο επόμενο σχήμα φαίνεται η λειτουργία της θετικής επαλήθευσης.



Σχήμα 3.11: Σχηματική αναπαράσταση της τεχνικής της θετικής επαλήθευσης.

3.3.1.4.4 Διαδικασία υποχώρησης

Αν το μέσο είναι κατειλημμένο, ο σταθμός πρέπει να αναβάλλει (defer) τη μετάδοση μέχρι το μέσο να γίνει ελεύθερο:

- για χρονική περίοδο ίση με DIFS, όταν το τελευταίο πλαίσιο που ανιχνεύθηκε στο μέσο λήφθηκε σωστά
- για διάστημα ίσο με EIFS, όταν το τελευταίο πλαίσιο που ανιχνεύθηκε στο μέσο δεν λήφθηκε σωστά

Μετά τα παραπάνω διαστήματα ο σταθμός θα δημιουργήσει μια τυχαία περίοδο υποχώρησης (**back off**) για έναν επιπρόσθετο χρόνο (ο οποίος χωρίζεται σε σχισμές) πριν την μετάδοση, εκτός αν ο μετρητής υποχώρησης (back off timer) περιέχει ήδη μια μη-μηδενική τιμή οπότε και η επιλογή του τυχαίου αριθμού δεν λαμβάνει χώρα. Αυτή η διαδικασία ελαχιστοποιεί τις συγκρούσεις κατά την διάρκεια του ανταγωνισμού (contention) μεταξύ πολλών σταθμών οι οποίοι ανέβαλλαν μία διαδικασία. Ο χρόνος υποχώρησης (που θα αποτελέσει την αρχική τιμή του μετρητή υποχώρησης) επιλέγεται με βάση τον τύπο:

Back off Time = Random x SlotTime

όπου Random είναι ένας ψευδοτυχαίος αριθμός που επιλέγεται από μία ομοιόμορφη κατανομή στο διάστημα [0,CW]. Το CW αντιπροσωπεύει το παράθυρο ανταγωνισμού και η λειτουργία του αναφέρεται στη συνέχεια.

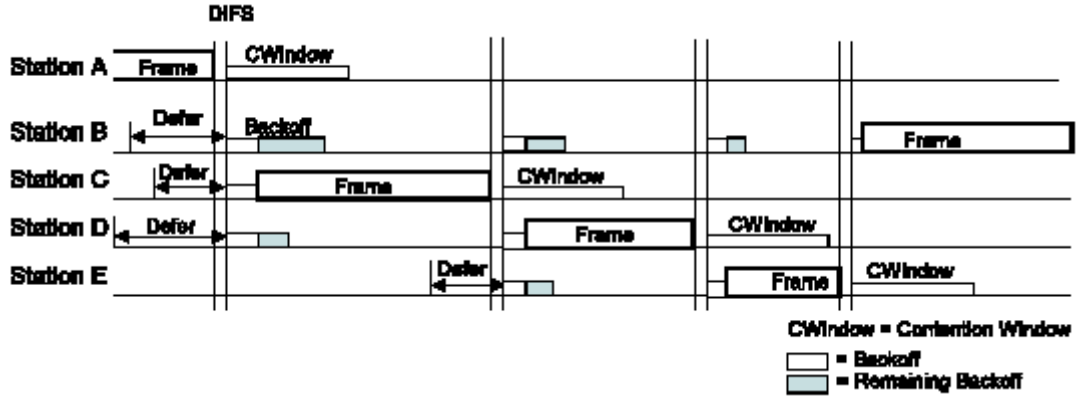
Ένας σταθμός που εκτελεί την διαδικασία υποχώρησης θα χρησιμοποιήσει τον μηχανισμό ανίχνευσης φέροντος (carrier sense) κατά τη διάρκεια κάθε σχισμής υποχώρησης (backoff slot). Αν δεν σημειωθεί καμία κίνηση στο μέσο κατά την περίοδο μιας συγκεκριμένης σχισμής υποχώρησης, τότε κατά την διαδικασία της υποχώρησης μειώνεται ο χρόνος υποχώρησης κατά SlotTime.

Αν το μέσο διαπιστωθεί ότι είναι απασχολημένο σε κάθε στιγμή κατά τη διάρκεια μιας σχισμής υποχώρησης τότε η διαδικασία της υποχώρησης

εγκαταλείπεται, δηλαδή ο μετρητής υποχώρησης δεν μειώνεται για τη σχισμή αυτή. Η μετάδοση μπορεί να ξεκινήσει όταν ο μετρητής υποχώρησης φτάσει το 0.

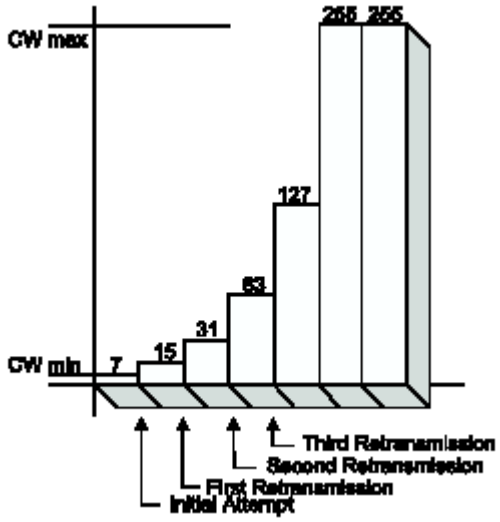
Στην περίπτωση επιτυχώς επαληθευμένων μεταδόσεων η διαδικασία της υποχώρησης ξεκινάει με το τέλος του ληφθέντος ACK πλαισίου. Στην περίπτωση ανεπιτυχών μεταδόσεων που απαιτούν επαλήθευση η διαδικασία της υποχώρησης ξεκινάει με το τέλος του χρόνου εκπνοής (**timeout interval**) του ληφθέντος ACK. Αν η μετάδοση είναι επιτυχής η τιμή του CW επιστρέφει στην τιμή CW_{min} πριν επιλεχθεί το νέο τυχαίο διάστημα υποχώρησης.

Το αποτέλεσμα της διαδικασίας υποχώρησης είναι ότι όταν πολλοί σταθμοί αναβάλλουν την μετάδοση και μπαίνουν στη διαδικασία της τυχαίας υποχώρησης, τότε ο σταθμός που επιλέγει το μικρότερο διάστημα υποχώρησης χρησιμοποιώντας την τυχαία συνάρτηση θα κερδίσει τον ανταγωνισμό.



Σχήμα 3.12: Η διαδικασία της υποχώρησης στην περίπτωση που 5 σταθμοί θέλουν να μεταδώσουν.

Το Παράθυρο Ανταγωνισμού **CW** (Contention Window) παίρνει αρχικά μία αρχική τιμή ίση με CW_{min}. Το CW θα πάρει την επόμενη τιμή κάθε φορά που μία ανεπιτυχής προσπάθεια για μετάδοση ενός MPDU γίνει η αιτία να αυξηθεί ο μετρητής επανάληψης (retry counter) του σταθμού, μέχρι το CW να φτάσει την τιμή CW_{max}. Από τη στιγμή που φτάσει την τιμή CW_{max}, το CW θα παραμείνει εκεί μέχρι να γίνει reset. Η συνηθέστερη περίπτωση στην οποία το CW θα γίνει reset στην τιμή CW_{min} είναι ύστερα από κάθε επιτυχή μετάδοση ενός MSDU ή MMPDU. Η εκθετική αύξηση του CW δίνεται στο επόμενο σχήμα.



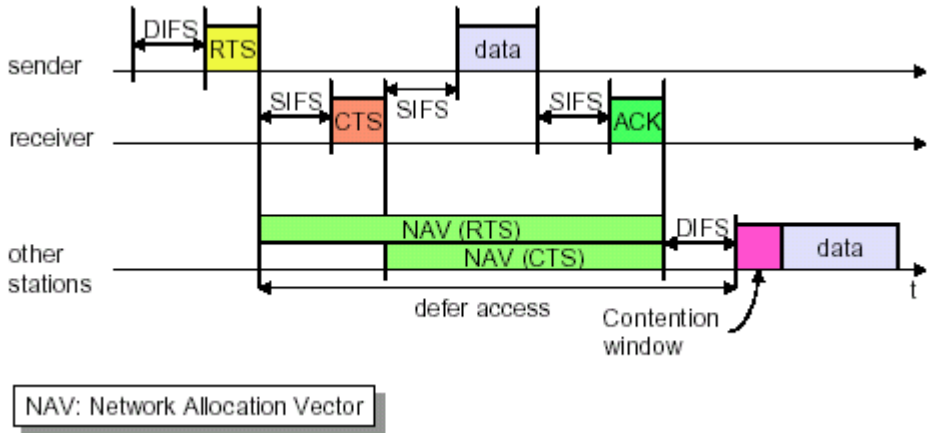
Σχήμα 3.13: Η εκθετική αύξηση του CW μετά από ανεπιτυχείς μεταδόσεις.

Το προηγούμενο σχήμα δίνει τις διαδοχικές τιμές του CW μετά από αναμεταδόσεις ενός σταθμού. Ο λόγος που το CW αυξάνεται εκθετικά είναι για να ελαχιστοποιηθούν οι συγκρούσεις και να μεγιστοποιηθεί το throughput τόσο για χαμηλή όσο και υψηλή χρησιμοποίηση του καναλιού. Για χαμηλή χρησιμοποίηση, οι σταθμοί δεν χρειάζεται να περιμένουν για μεγάλο χρονικό διάστημα πριν μεταδώσουν ένα πλαίσιο. Μετά την πρώτη ή την δεύτερη προσπάθεια, ένας σταθμός θα καταφέρει να μεταδώσει επιτυχώς μέσα σε ένα μικρό χρονικό διάστημα. Αν, όμως, η χρησιμοποίηση του δικτύου είναι υψηλή το πρωτόκολλο θα αναγκάσει τους σταθμούς να αναμένουν για μεγαλύτερες χρονικές περιόδους για να μειώσουν την πιθανότητα ταυτόχρονης μετάδοσης από 2 ή περισσότερους σταθμούς. Για υψηλή χρησιμοποίηση, η τιμή του CW αυξάνεται σε ιδιαίτερα υψηλές τιμές.

3.3.1.4.5 Λειτουργία του DCF με την χρήση RTS/CTS

Στην περίπτωση αυτή σημαντικό ρόλο παίζει ο εικονικός μηχανισμός ανίχνευσης που παρέχεται από το υπόστρωμα MAC. Η διαδικασία για την αποστολή πακέτων με την συγκεκριμένη μέθοδο φαίνεται στο παρακάτω σχήμα, ενώ η σειρά που ακολουθείται είναι η εξής:

1. Ο σταθμός που θέλει να στείλει δεδομένα στέλνει αρχικά ένα πακέτο RTS (Request To Send) με τις παραμέτρους κράτησης (reservation) του μέσου, αφού πρώτα περιμένει για ένα DIFS. Η κράτηση καθορίζει το χρονικό διάστημα που χρειάζεται για την αποστολή των δεδομένων.
2. Ο σταθμός λήψης επαληθεύει-αφού πρώτα περιμένει για ένα SIFS-μέσω ενός πακέτου CTS (Clear To Send) ότι είναι έτοιμος να κάνει λήψη των δεδομένων.
3. Ο σταθμός αποστολής μπορεί τώρα να στείλει άμεσα τα δεδομένα τα οποία θα επιβεβαιωθούν μέσω ACK.
4. Οι άλλοι σταθμοί αποθηκεύουν τις αλλαγές στις κρατήσεις του στρώματος που διανέμονται μέσω των RTS και CTS.



Σχήμα 3.14: Λειτουργία DCF με αποστολή και λήψη πακέτων RTS και CTS.

Η 'MAC coordination' εκτελεί την εικονική ανίχνευση φέροντος η οποία βασίζεται στην κρατημένη πληροφορία που βρίσκεται στο πεδίο διάρκειας (Duration) όλων των πλαισίων. Η πληροφορία αυτή αναγγέλλει (σε όλους τους σταθμούς) την επικείμενη χρησιμοποίηση του μέσου από έναν σταθμό. Η 'MAC coordination' ελέγχει το πεδίο διάρκειας σε όλα τα MAC πλαίσια και τοποθετεί την

πληροφορία αυτή στον NAV (Network Allocation Vector) του σταθμού εάν η τιμή είναι μεγαλύτερη από την τρέχουσα τιμή του NAV.

Ο NAV λειτουργεί ως ένας χρονομετρητής, ξεκινώντας με μια τιμή ίση με αυτή του πεδίου διάρκειας (Duration Field) του τελευταίου πλαισίου που μεταδόθηκε και ανιχνεύθηκε στο μέσο και μετρώντας αντίστροφα προς το 0. Από την στιγμή που ο NAV φτάσει το 0 (κάτι που δηλώνει ότι το μέσο δεν είναι κατειλημμένο), ο σταθμός είναι έτοιμος να μεταδώσει αν και εφόσον η 'PHY coordination' υποδείξει ότι το κανάλι είναι ελεύθερο.

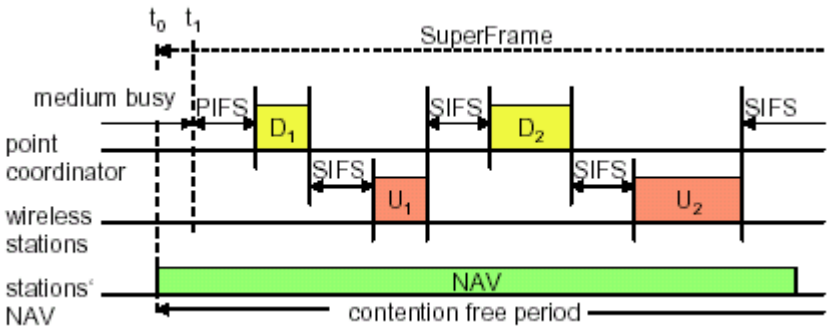
Ο NAV υποστηρίζει μια πρόβλεψη για την μελλοντική κίνηση στο δίκτυο η οποία βασίζεται στην πληροφορία διάρκειας που ανακοινώνεται στα RTS/CTS πλαίσια πριν από την ανταλλαγή των δεδομένων. Η πληροφορία της διάρκειας είναι επίσης διαθέσιμη στις MAC επικεφαλίδες (headers) όλων των πλαισίων που στέλνονται κατά τη διάρκεια του CP (εκτός των PS-Poll Control frames).

3.3.1.5 Λειτουργία του μηχανισμού πρόσβασης PCF

Η εναλλακτική μέθοδος PCF χρησιμοποιείται μόνο σε 'infrastructure' δίκτυα. Η μέθοδος αυτή κάνει χρήση ενός ελεγκτή που καλείται **PC** (Point Coordinator), ο οποίος λειτουργεί στο AP ενός BSS και καθορίζει ποιος σταθμός έχει την άδεια για να μεταδώσει την τρέχουσα χρονική στιγμή. Η λειτουργία είναι ουσιαστικά αυτή της διαλογής (polling), με το PC να παίζει το ρόλο του 'polling master'.

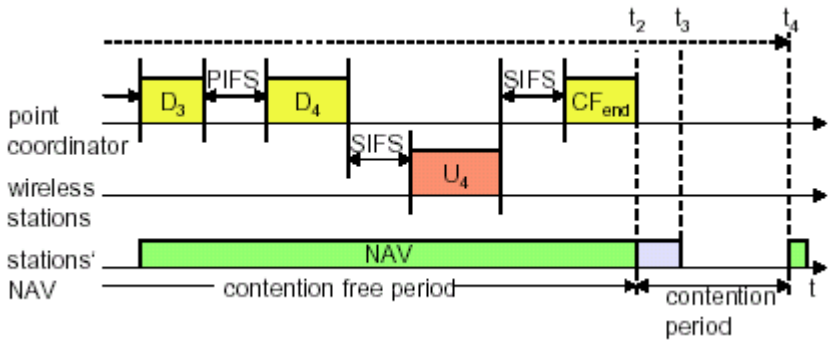
Το PCF χρησιμοποιεί τον εικονικό μηχανισμό ανίχνευσης φέροντος υποβοηθούμενο από ένα μηχανισμό ελέγχου προτεραιότητας. Ο PCF διανέμει τις απαραίτητες πληροφορίες μέσω των πλαισίων διαχείρισης 'Beacon' για να κερδίσει τον έλεγχο του μέσου θέτοντας σε λειτουργία το Network Allocation Vector (NAV). Συγκεκριμένα, ο PC ανιχνεύει το μέσο στην αρχή κάθε περιόδου **CFP** (Contention Free Period). Αν το μέσο είναι ελεύθερο για διάστημα ίσο με PIFS, το PC στέλνει ένα πλαίσιο Beacon, ώστε οι σταθμοί να ενημερώσουν τα NAV για την διάρκεια της CFP.

Επιπρόσθετα, όλες οι μεταδόσεις πλαισίων κάτω από τη λειτουργία του PCF μπορούν να χρησιμοποιούν ένα IFS το οποίο έχει μικρότερη διάρκεια από το αντίστοιχο IFS που χρησιμοποιείται με τη DCF. Αυτό σημαίνει ότι η κίνηση που στηρίζεται στη χρήση της PCF έχει προτεραιότητα στον έλεγχο του μέσου για σταθμούς που βρίσκονται σε υπερκαλυπτόμενα (overlapping) BSSs και κάνουν χρήση της DCF.



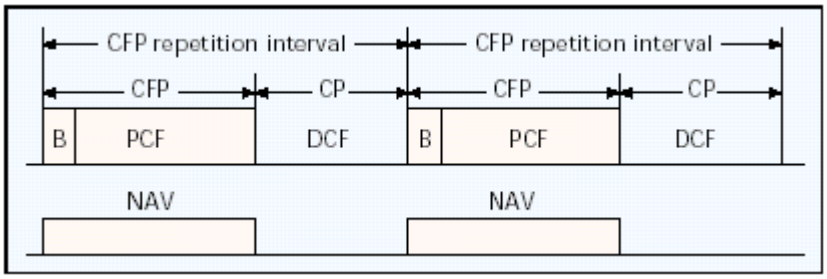
Σχήμα 3.15: Σχηματική αναπαράσταση της λειτουργίας του PCF.

Στο παράδειγμα του επόμενου σχήματος ο σταθμός 3 δεν έχει δεδομένα προς αποστολή. Έτσι, αφού περάσει ένα χρονικό διάστημα ίσο με PIFS, ο σταθμός 4 ο οποίος ελέγχει τώρα το μέσο μπορεί να μεταδώσει.



Σχήμα 3.16: Μετά το polling του σταθμού 3 (ο οποίος δεν έχει πακέτα προς μετάδοση) σειρά έχει ο σταθμός 4, ο οποίος μεταδίδει τα δεδομένα που θέλει (U4). Το πακέτο CF_{end} που αποστέλλεται από τον PC δηλώνει το τέλος της CFP.

Αξίζει να σημειώσουμε πως οι δύο τεχνικές που καθορίζονται από το Standard μπορούν να συνυπάρξουν μέσα στο ίδιο BSS. Όταν ένα PC λειτουργεί σε ένα BSS, οι 2 μέθοδοι πρόσβασης εναλλάσσονται, με την Contention Free Period (CFP) να ακολουθείται από μία Contention Period (CP), όπως φαίνεται στο επόμενο σχήμα.



Σχήμα 3.17: Διαδοχική λειτουργία των μεθόδων PCF και DCF.

3.3.1.6 Δομή του MAC πλαισίου

Το υπόστρωμα MAC του 802.11 καθορίζει τον σχηματισμό διαφόρων πλαισίων. Ο σχηματισμός αυτών των πλαισίων εξαρτάται από τη λειτουργία για την οποία προορίζονται, ενώ όπως θα δούμε στην επόμενη παράγραφο υποστηρίζεται και η δημιουργία μικρότερου μεγέθους πλαισίων σύμφωνα με μια τεχνική που καλείται τεμαχισμός.

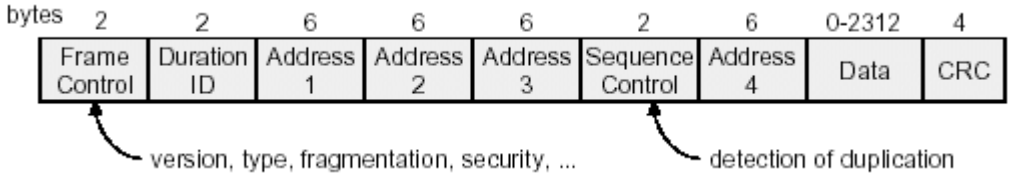
3.3.1.6.1 Κατηγορίες πλαισίων

Για την μεταφορά των MSDUs μεταξύ ομότιμων LLCs, το υπόστρωμα MAC χρησιμοποιεί 3 ειδών τύπους πλαισίου, οι οποίοι αναφέρονται παρακάτω:

- **Ελέγχου (Control)**: Μετά την εγκατάσταση των υπηρεσιών association και authentication μεταξύ σταθμών και APs τα πλαίσια ελέγχου είναι αυτά που θα βοηθήσουν στην σωστή παραλαβή των πλαισίων δεδομένων. Τέτοια πλαίσια είναι τα: RTS, CTS, ACK, PS Poll, CF End.

- **Διαχείρισης (Management)**: Ο σκοπός των πλαισίων διαχείρισης είναι η εγκατάσταση της αρχικής επικοινωνίας μεταξύ των σταθμών και των APs. Έτσι, τα πλαίσια αυτά παρέχουν υπηρεσίες όπως οι association και authentication.
- **Δεδομένων (Data)**: Ο κύριος σκοπός των πλαισίων αυτών είναι η μεταφορά πληροφορίας μεταξύ των ομότιμων LLCs.

Στο επόμενο σχήμα φαίνεται η γενική δομή ενός MAC πλαισίου που 'αντιστοιχεί' σε όλα τα πλαίσια που μεταδίδουν οι σταθμοί, ανεξάρτητα από τον τύπο του πλαισίου.



Σχήμα. 3.18: Η γενική δομή ενός MAC πλαισίου.

Τα πρώτα 30 bytes (όλα τα πεδία, δηλαδή, πριν αυτό των δεδομένων) αποτελούν την επικεφαλίδα (header) του MAC πλαισίου, ενώ μετά τα δεδομένα ακολουθεί ένα πεδίο το οποίο χρησιμοποιεί τον αλγόριθμο CRC για έλεγχο λαθών. Πιο συγκεκριμένα τα πεδία της επικεφαλίδας είναι τα εξής:

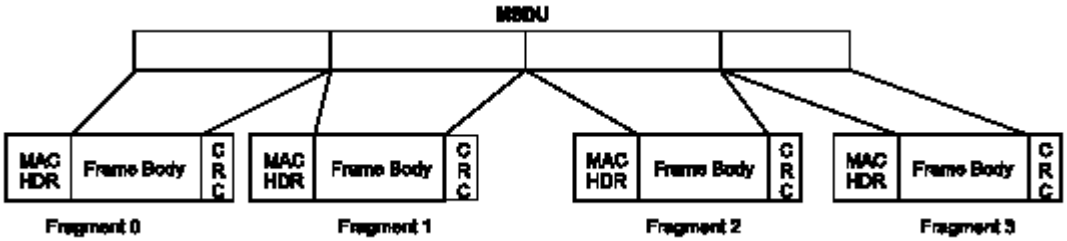
- Frame Control: Το πεδίο αυτό περιλαμβάνει πληροφορίες για τον τύπο του πλαισίου, για τον έλεγχο της ισχύος, για την κρυπτογράφηση κ.ά.
- Duration ID: Η πληροφορία στο πεδίο αυτό δηλώνει την διάρκεια του επόμενου πλαισίου προς μετάδοση.
- Address: Τα πεδία των διευθύνσεων παρέχουν τους διάφορους τύπους διευθύνσεων, όπως των σταθμών μετάδοσης και λήψης του πλαισίου, του BSS για το οποίο προορίζεται κ.ά.
- Sequence Control: Τα bytes στο πεδίο αυτό υποδεικνύουν τον αριθμό του πλαισίου ενός συγκεκριμένου MSDU.

3.3.1.6.2 Η τεχνική του τεμαχισμού

Η διαδικασία της διαίρεσης ενός MSDU ή ενός MMPDU σε μικρότερα MAC πλαίσια, τα MPDUs, ονομάζεται τεμαχισμός (fragmentation). Η διαδικασία αυτή γίνεται για να αυξηθεί η αξιοπιστία, μεγαλώνοντας την πιθανότητα επιτυχούς μεταφοράς ενός MSDU ή ενός MMPDU σε περιπτώσεις όπου τα χαρακτηριστικά του καναλιού περιορίζουν την αξιόπιστη μετάδοση για μεγαλύτερα πλαίσια. Η ανασυγκρότηση των MPDUs σε ένα MSDU ή ένα MMPDU ονομάζεται 'defragmentation'.

Όταν γίνεται λήψη ενός MSDU ή ενός MMPDU από το LLC από το υπόστρωμα διαχείρισης MAC (MLME) και το μήκος του MSDU είναι μεγαλύτερο από μια συγκεκριμένη τιμή η οποία καλείται κατώφλι τεμαχισμού (Fragmentation Threshold), τότε το MSDU χωρίζεται σε MPDUs, όπως φαίνεται στο επόμενο σχήμα. Κάθε τεμάχιο δεν πρέπει να υπερβαίνει σε μέγεθος το κατώφλι τεμαχισμού.

Μόνο τα MPDUs με μία και μόνο διεύθυνση αποδοχέα (unicast receiver address) επιτρέπεται να υποστούν τεμαχισμό. Τα πλαίσια εκπομπής (broadcast) και πολλαπλής διανομής (multicast) δεν επιτρέπεται να υποστούν τεμαχισμό ακόμα κι αν το μήκος τους υπερβαίνει το κατώφλι τεμαχισμού.



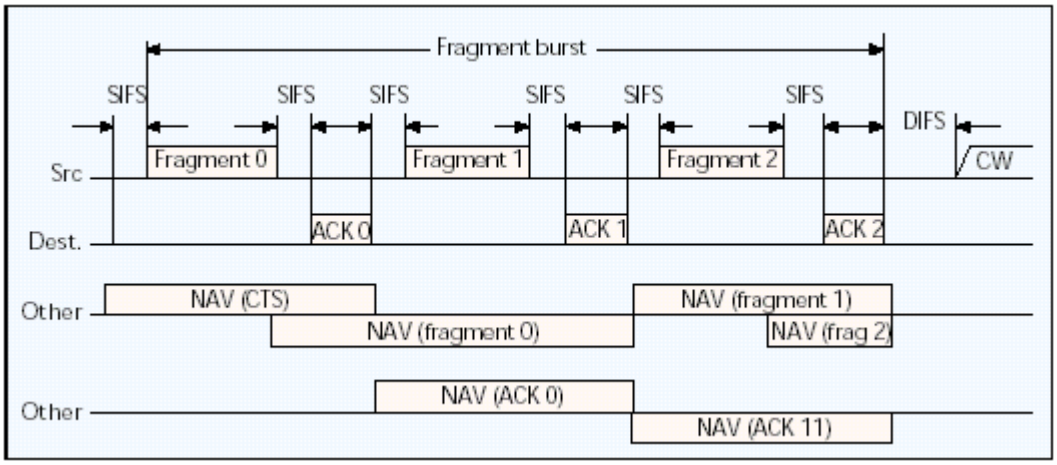
Σχήμα 3.19: Τεμαχισμός ενός MSDU σε μικρότερα πακέτα.

Τα MPDUs που προκύπτουν από τον τεμαχισμό ενός MSDU ή ενός MMPDU αποστέλλονται ως ανεξάρτητες μεταδόσεις και το καθένα από αυτά επαληθεύεται ξεχωριστά. Μετά τη λήψη ενός πακέτου επαλήθευσης ο σταθμός που μεταδίδει θα περιμένει για ένα χρονικό διάστημα ίσο με SIFS μέχρι να μεταδώσει το επόμενο τεμάχιο. Ένα πλαίσιο μπορεί να αποσταλεί με τη διαδικασία του τεμαχισμού χρησιμοποιώντας τόσο τον βασικό τρόπο μετάδοσης DCF όσο και τον τρόπο μετάδοσης DCF με τη χρήση των πακέτων RTS/CTS.

Από τη στιγμή που ένας σταθμός έχει ανταγωνιστεί για το κανάλι, θα συνεχίσει να στέλνει τεμάχια μέχρι να συμβεί ένα από τα παρακάτω γεγονότα:

1. Όλα τα τεμάχια ενός MSDU ή ενός MMPDU έχουν αποσταλεί.
2. Δεν έχει ληφθεί επιβεβαίωση.
3. Απαγορευθεί στο σταθμό να στείλει επιπλέον τεμάχια λόγω του ορίου του dwell time.

Στο επόμενο σχήμα φαίνεται η διαδικασία μετάδοσης ενός MSDU πολλών τεμαχίων (multiple-fragment), η οποία είναι γνωστή ως ‘fragment burst’.



Σχήμα 3.20: Διαδικασία αποστολής ενός πλαισίου με την μέθοδο του τεμαχισμού.

Κατά τη χρησιμοποίηση της μεθόδου του τεμαχισμού ισχύουν και οι επόμενοι κανόνες:

- Αν ο σταθμός εκπομπής κάνει λήψη μιας επιβεβαίωσης αλλά δεν υπάρχει αρκετός χρόνος για να μεταδώσει το επόμενο τεμάχιο λόγω του ορίου του dwell, θα ανταγωνιστεί για το κανάλι στο επόμενο dwell time.
- Αν ο σταθμός εκπομπής δεν κάνει λήψη μιας επιβεβαίωσης, θα προσπαθήσει να αναμεταδώσει το αποτυχημένο MPDU ή ένα άλλο MPDU, αφού εκτελέσει τη διαδικασία υποχώρησης και ανταγωνισμού.

- Από τη στιγμή που ο σταθμός έχει ανταγωνιστεί για το κανάλι για να επαναμεταδώσει ένα τεμάχιο ή ένα MSDU, θα ξεκινήσει τη μετάδοση με το τελευταίο τεμάχιο που δεν επιβεβαιώθηκε.

3.3.2 ΤΟ ΦΥΣΙΚΟ ΣΤΡΩΜΑ ΤΟΥ 802.11

Το 802.11 Standard καθορίζει την ύπαρξη, τον τρόπο λειτουργίας και τον καθορισμό τριών διαφορετικών φυσικών στρωμάτων, τα οποία αναπτύσσονται διεξοδικά στη συνέχεια.

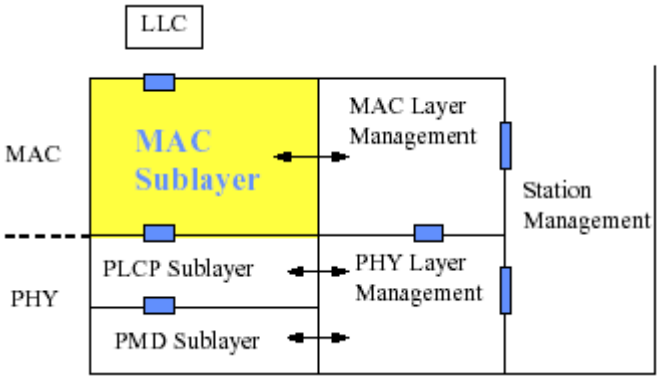
Το 802.11 καθορίζει διάφορα φυσικά στρώματα, καθώς γίνονται διαθέσιμες νέες τεχνολογίες. Έτσι, ενώ το αρχικό Standard υποστήριζε ρυθμούς μετάδοσης έως 2 Mbps, τα τρέχοντα Standard της οικογένειας 802.11 καθορίζουν φυσικά στρώματα με ρυθμούς μετάδοσης μέχρι και 54 Mbps, χρησιμοποιώντας κατάλληλες τεχνικές διαμόρφωσης.

3.3.2.1 Αρχιτεκτονική του φυσικού στρώματος

Η αρχιτεκτονική του φυσικού στρώματος αποτελείται από τα τρία επόμενα στοιχεία (components) για κάθε σταθμό:

- **PLM** (Physical Layer Management): Η συνιστώσα αυτή λειτουργεί σε συνεργασία με το υπόστρωμα διαχείρισης MAC και εκτελεί λειτουργίες διαχείρισης για το φυσικό στρώμα.
- **PLCP** (Physical Layer Convergence Procedure) υπόστρωμα: Το υπόστρωμα MAC επικοινωνεί με το PLCP μέσω στοιχείων υπηρεσίας (service primitives) με τη βοήθεια των SAPs (Service Access Points) του φυσικού στρώματος. Όταν το υπόστρωμα MAC δώσει εντολή, το PLCP ετοιμάζει τα **MPDUs** για μετάδοση. Το PLCP προσαρτίζει πεδία στο MPDU που περιέχουν πληροφορίες που χρειάζονται οι πομποί και οι δέκτες του φυσικού στρώματος. Το 802.11 αναφέρεται σε αυτό το σύνθετο πλαίσιο ως PPDU (PLCP Protocol Data Unit). Η δομή του **PPDU** πλαισίου παρέχεται για ασύγχρονη μεταφορά των MPDUs μεταξύ των σταθμών.
- **PMD** (Physical Medium Dependent) υπόστρωμα: Κάτω από την καθοδήγηση του PLCP, το PMD παρέχει την ουσιαστική μετάδοση και λήψη των οντοτήτων του φυσικού στρώματος μέσω του ασύρματου μέσου. Για την παροχή αυτής της υπηρεσίας, το PMD διασυνδέεται άμεσα με το ασύρματο μέσο (δηλαδή τον αέρα) και παρέχει διαμόρφωση και αποδιαμόρφωση των πλαισίων που μεταδίδονται. Τα PLCP και PMD επικοινωνούν μέσω των ‘primitives’ για τον έλεγχο των λειτουργιών μετάδοσης και λήψης.

Η συσχέτιση των παραπάνω στοιχείων τόσο μεταξύ τους όσο και με το υπόστρωμα MAC απεικονίζεται στο επόμενο σχήμα.



Σχήμα 3.21: Η αρχιτεκτονική του υποστρώματος MAC και του φυσικού στρώματος όπως αυτή καθορίζεται από το 802.11.

3.3.2.2 Λειτουργίες του φυσικού στρώματος (Physical Layer Operations)

Για την εκτέλεση των λειτουργιών του υποστρώματος PLCP, το 802.11 καθορίζει την χρήση των μηχανών κατάστασης (state machines). Κάθε μηχανή κατάστασης εκτελεί μία από τις παρακάτω λειτουργίες:

- Ανίχνευση φέροντος: Η λειτουργία αυτή αφορά τον καθορισμό της κατάστασης του μέσου
- Μετάδοση: Η λειτουργία αυτή αναφέρεται στην αποστολή των διαδοχικών bytes ενός πλαισίου δεδομένων.
- Λήψη: Η λειτουργία αυτή αναφέρεται στην λήψη διαδοχικών bytes ενός πλαισίου δεδομένων.

Παρακάτω αναφέρονται εκτενέστερα αυτές οι λειτουργίες.

3.3.2.2.1 Ανίχνευση φέροντος

Το φυσικό επίπεδο υλοποιεί την λειτουργία της ανίχνευσης φέροντος (**carrier sense**) κατευθύνοντας το PMD να ελέγξει αν το μέσο είναι απασχολημένο ή ελεύθερο. Το PLCP εκτελεί τις παρακάτω λειτουργίες όταν ο σταθμός δεν βρίσκεται σε διαδικασία μετάδοσης ή λήψης ενός πλαισίου:

- Ανίχνευση των εισερχόμενων σημάτων: Το PLCP μέσα στον σταθμό θα ανιχνεύει διαρκώς το μέσο. Όταν το μέσο γίνει απασχολημένο, το PLCP θα διαβάσει τα πεδία ‘preamble’ και ‘header’ του πλαισίου PLCP και θα επιχειρήσει συγχρονισμό του δέκτη στον ρυθμό μετάδοσης του σήματος.
- Καθορισμός ελεύθερου καναλιού (CCA: Clear Channel Assessment): Με τη λειτουργία αυτή καθορίζεται αν το μέσο είναι απασχολημένο ή όχι. Ο πιο συνηθισμένος τρόπος λειτουργίας του CCA είναι η μέτρηση, από το PMD, της ενέργειας στο μέσο. Ο καθορισμός του μέσου προκύπτει ανάλογα με το αν η μετρούμενη τιμή ξεπερνάει ένα συγκεκριμένο όριο, το οποίο αναφέρεται ως κατώφλι ανίχνευσης ενέργειας (ED: Energy Detection).

3.3.2.2.2 Λειτουργία μετάδοσης

Το PLCP θα αλλάξει το PMD σε κατάσταση μετάδοσης μετά την λήψη του κατάλληλου ‘service primitive’ (PHY-TXSTART.request) από το επίπεδο MAC. Το επίπεδο MAC στέλνει τον αριθμό των bytes (0-4095) και τις οδηγίες για τον ρυθμό

μετάδοσης μαζί με την παραπάνω αίτηση (request). Το PMD ανταποκρίνεται στέλνοντας το 'preamble' του πλαισίου στην κεραία μέσα σε 20 μs.

Ο πομπός στέλνει τα 'preamble' και 'header' με ρυθμό 1 Mbps. Αφού σταλεί το 'preamble' ο πομπός αλλάζει τον ρυθμό μετάδοσης σε αυτόν που καθορίζεται από το 'header'. Μετά την ολοκλήρωση της μετάδοσης, το PLCP στέλνει το κατάλληλο 'primitive' στο επίπεδο MAC, κλείνει τον πομπό και αλλάζει το κυκλωματικό (circuitry) του PMD σε κατάσταση λήψης.

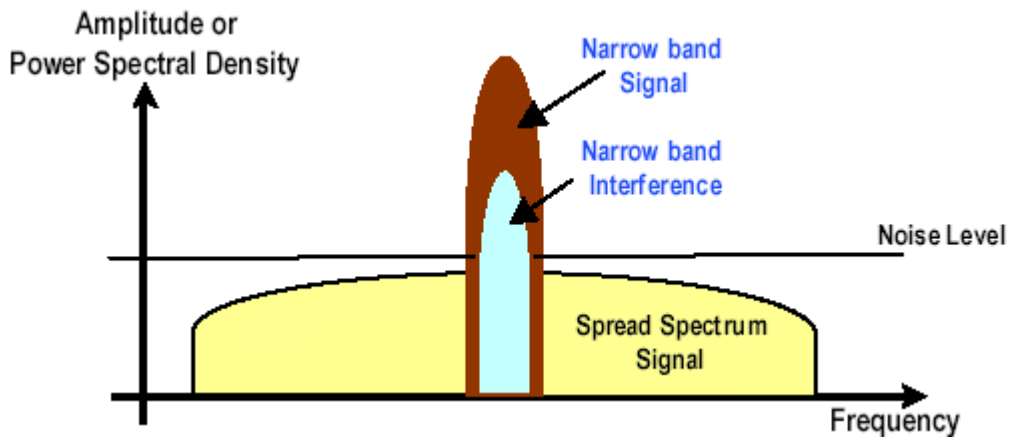
3.3.2.2.3 Λειτουργία λήψης

Αν ο καθορισμός του ελεύθερου καναλιού (CCA) ανακαλύψει ότι το μέσο είναι απασχολημένο και ανιχνεύσει ένα έγκυρο 'preamble' ενός εισερχόμενου πλαισίου τότε το PLCP θα ελέγξει την επικεφαλίδα (header) του πλαισίου. Το PMD θα υποδείξει ότι το μέσο είναι απασχολημένο όταν ανιχνεύσει ένα σήμα με ισχύ μεγαλύτερη από 85 dBm. Αν το PLCP καθορίσει ότι η επικεφαλίδα είναι χωρίς λάθη θα στείλει το κατάλληλο 'primitive' (PHY-RXSTART.indicate) στο επίπεδο MAC για να ειδοποιήσει για την επικείμενη λήψη ενός πλαισίου. Μαζί με αυτήν την ειδοποίηση το PLCP στέλνει τις πληροφορίες που βρίσκει στην επικεφαλίδα του πλαισίου (όπως ο αριθμός των bytes και ο ρυθμός μετάδοσης).

Το PLCP θέτει σε λειτουργία έναν μετρητή byte βασιζόμενο στην τιμή του πεδίου 'PSDU Length Word' που βρίσκεται στην επικεφαλίδα. Με την βοήθεια του μετρητή αυτού, το PLCP γνωρίζει πότε λαμβάνει χώρα το τέλος του πλαισίου. Καθώς το PLCP λαμβάνει τα δεδομένα, στέλνει τα bytes του PSDU στο επίπεδο MAC με τα κατάλληλα primitives.

3.3.2.3 Το Φυσικό Στρώμα του 802.11 με χρήση της τεχνικής Spread Spectrum

Το 802.11 καθορίζει δύο διαφορετικά φυσικά στρώματα τα οποία στηρίζονται στην τεχνική διαμόρφωσης που καλείται 'εξάπλωση φάσματος' (**SS**: Spread Spectrum). Η τεχνική αυτή 'εξαπλώνει' την ισχύ του σήματος σε μια ευρεία μπάντα συχνοτήτων, όπως φαίνεται στο σχήμα 3.22. Η διαδικασία αυτή κάνει το σήμα λιγότερο ευάλωτο στον θόρυβο και τις παρεμβολές από άλλες μεταδόσεις οι οποίες χρησιμοποιούν συνήθως ένα μικρό εύρος συχνοτήτων. Έτσι, η πιθανή προκύπτουσα παρεμβολή με το εξαπλωμένο σήμα θα οδηγεί σε λιγότερα λάθη κατά την αποδιαμόρφωση του σήματος από τον δέκτη.



Σχήμα 3.22: Η εξάπλωση του σήματος στην περιοχή των συχνοτήτων με τη χρήση της τεχνικής Spread Spectrum.

3.3.2.3.1 Το υπόστρωμα PMD FHSS

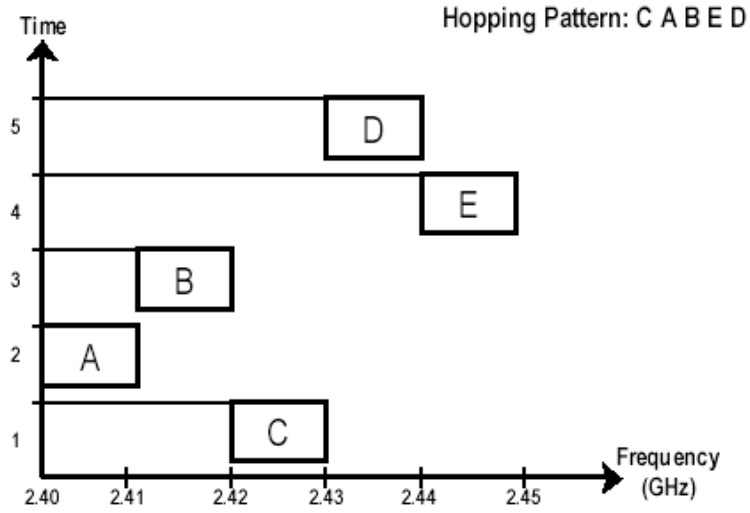
Το υπόστρωμα PMD (Physical Medium Dependent) εκτελεί την πραγματική μετάδοση και λήψη των PPDUs υπό την καθοδήγηση του PLCP. Για να εκτελέσει αυτήν την λειτουργία το FHSS PMD συνδέεται απευθείας με το ασύρματο μέσο (δηλαδή τον αέρα) και παρέχει την διαμόρφωση και αποδιαμόρφωση των πλαισίων που μεταδίδονται μέσω της τεχνικής FHSS.

Το PMD μεταφράζει την δυαδική αναπαράσταση των PPDUs σε ένα ραδιοσήμα ικανό για μετάδοση. Το FHSS PMD εκτελεί αυτές τις λειτουργίες μέσω της λειτουργίας μεταπήδησης συχνότητας (frequency hopping) και της τεχνικής διαμόρφωσης που ονομάζεται **FSK** (Frequency Shift Keying). Η επόμενη παράγραφος εξηγεί το FHSS PMD.

3.3.2.3.1α Η λειτουργία της μεταπήδησης συχνότητας

Το 802.11 καθορίζει έναν αριθμό καναλιών (79 για την Β. Αμερική και για τις περισσότερες χώρες της Ευρώπης) που ισοκατανέμονται στην μπάντα ISM στην συχνότητα των 2.4 GHz. Κάθε κανάλι έχει εύρος 1 MHz, κατά συνέπεια η κεντρική συχνότητα λειτουργίας (όσον αφορά τις ΗΠΑ) για το πρώτο κανάλι είναι τα 2.402 GHz, για το δεύτερο τα 2.403 GHz κ.ο.κ.

Το PMD που στηρίζεται στο FHSS μεταδίδει τα δεδομένα μεταπηδώντας από κανάλι σε κανάλι σύμφωνα με μια συγκεκριμένη ψευδό-τυχαία ακολουθία μεταπήδησης (hopping pattern) η οποία κατανέμει ομοιόμορφα το σήμα κατά μήκος της μπάντας συχνοτήτων. Από την στιγμή που η ακολουθία μεταπήδησης τεθεί σε ένα AP, οι σταθμοί αυτόματα συγχρονίζονται στην σωστή ακολουθία. Το 802.11 Standard καθορίζει έναν συγκεκριμένο αριθμό ακολουθιών, ώστε να αποφεύγεται η παρατεταμένη παρεμβολή μεταξύ των ακολουθιών αυτών. Μια τέτοια ακολουθία φαίνεται στο επόμενο σχήμα.



Σχήμα 3.23: Ακολουθία μεταπήδησης συχνότητας σε συνάρτηση με το χρόνο.

Για κάθε βήμα μεταπήδησης (hop) στην ακολουθία μεταπήδησης ο πομπός μεταδίδει σε μια συγκεκριμένη κεντρική συχνότητα λειτουργίας για ένα συγκεκριμένο χρονικό διάστημα το οποίο καλείται 'dwell time'. Ο ρυθμός μεταπήδησης (hop rate) είναι ρυθμιζόμενος, παρ' όλα αυτά υπάρχει ένας ελάχιστος ρυθμός που καθορίζεται από τους αρμόδιους οργανισμούς κάθε χώρας (π.χ. στις

Ηνωμένες Πολιτείες ο ελάχιστος ρυθμός είναι 2.5 hops/sec ο οποίος αντιστοιχεί σε ένα μέγιστο ;dwell time' ίσο με 400 ms). Επιπρόσθετα, η ελάχιστη απόσταση μεταπήδησης (hop distance) στην συχνότητα είναι 6 MHz για την Β. Αμερική και για το μεγαλύτερο μέρος της Ευρώπης και 5 MHZ για την Ιαπωνία.

3.3.2.3.1β Η λειτουργία διαμόρφωσης συχνότητας FHSS

Το PMD που στηρίζεται στο FHSS μεταδίδει τα δυαδικά δεδομένα με ρυθμό είτε 1Mbps είτε 2Mbps, χρησιμοποιώντας ένα συγκεκριμένο τύπο διαμόρφωσης για κάθε ρυθμό:

1. 1 Mbps: 2-level GFSK
2. 2 Mbps: 4-level GFSK

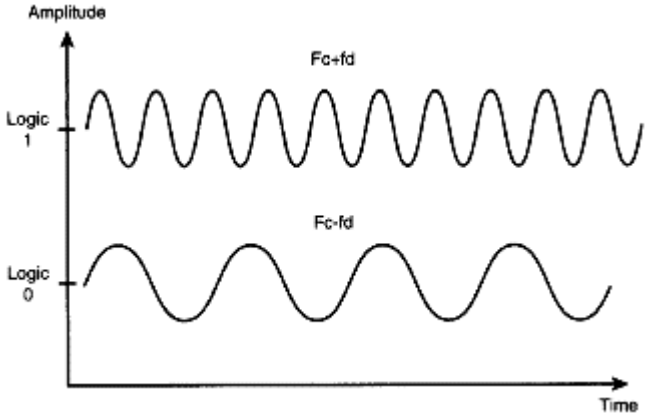
Για ρυθμό δεδομένων ίσο με 1Mbps, το PMD χρησιμοποιείται η 2-level Gaussian Frequency Shift Key (**GFSK**) διαμόρφωση, όπως φαίνεται στο σχήμα 3.24. Η ιδέα του GFSK είναι να μεταβάλει τη συχνότητα του φέροντος ώστε να αναπαριστά διαφορετικά δυαδικά σύμβολα.

Η είσοδος στον GFSK διαμορφωτή είναι 0 ή 1 όπως αυτά προέρχονται από το PLCP. Ο διαμορφωτής μεταδίδει τα δυαδικά δεδομένα μεταβάλλοντας τη συχνότητα μετάδοσης λίγο πάνω ή λίγο κάτω από την κεντρική συχνότητα λειτουργίας (Fc) για κάθε βήμα μεταπήδησης. Για να εκτελεστεί αυτήν την λειτουργία, χρησιμοποιούνται οι παρακάτω κανόνες:

- Συχνότητα μετάδοσης: Fc + fd, για την μετάδοση του bit 1
- Συχνότητα μετάδοσης: Fc – fd, για την μετάδοση του bit 0

Στις παραπάνω εξισώσεις, Fc είναι η κεντρική συχνότητα λειτουργίας (operating center frequency) για το συγκεκριμένο hop και fd είναι το μέγεθος της απόκλισης στη συχνότητα. Το 802.11 Standard εξηγεί τον τρόπο με τον οποίο υπολογίζονται οι ακριβείς τιμές για το fd, ενώ η ονομαστική τιμή είναι 160 KHz.

Στο επόμενο σχήμα φαίνεται η αντιστοίχηση των διαφορετικών συχνοτήτων μετάδοσης στα λογικά 1 και 0.



Σχήμα 3.24: Η διαμόρφωση GFSK χρησιμοποιεί 2 δυνατές συχνότητες για κάθε hop ώστε να δηλώνει αν ένα bit δεδομένων είναι 1 ή 0.

Για ρυθμό δεδομένων ίσο με 2 Mbps, το PMD χρησιμοποιεί τη 4-level Gaussian Frequency Shift Key (GFSK) διαμόρφωση. Για τη λειτουργία αυτή, η είσοδος στον διαμορφωτή είναι συνδυασμός 2 bit (00, 01, 10, 11) που προέρχονται από το PLCP. Κάθε ένα από αυτά τα σύμβολα των 2 bit στέλνεται με ρυθμό 1 Mbps, κάτι που σημαίνει ότι κάθε bit στέλνεται με ρυθμό 2 Mbps. Έτσι, με την τεχνική αυτή

διπλασιάζεται ο ρυθμός δεδομένων ενώ παραμένει ίδιο το baud rate, όπως αυτό ενός σήματος που μεταδίδεται με ρυθμό 1 Mbps. Ο πομπός μπορεί τώρα να μεταδώσει σε 4 πιθανές συχνότητες, κάθε μία για έναν συνδυασμό από bit. Στην περίπτωση αυτή υπάρχουν 2 διαφορετικές τιμές fd που μεταβάλλουν τη συχνότητα μετάδοσης πάνω και κάτω από τη συχνότητα Fc.

Το 802.11 περιορίζει την μέγιστη ισχύ του πομπού στα 100 mWatts για ισοτροπικά ακτινοβολούμενη ισχύ (κάτι που σημαίνει ότι οι μετρήσεις έγιναν για κεραία χωρίς ενίσχυση). Η πραγματική ισχύς, ωστόσο, θα είναι μεγαλύτερη με τη χρήση κεραιών οι οποίες προσφέρουν μεγαλύτερη κατευθυντικότητα και άρα απολαβή ή ενίσχυση (gain).

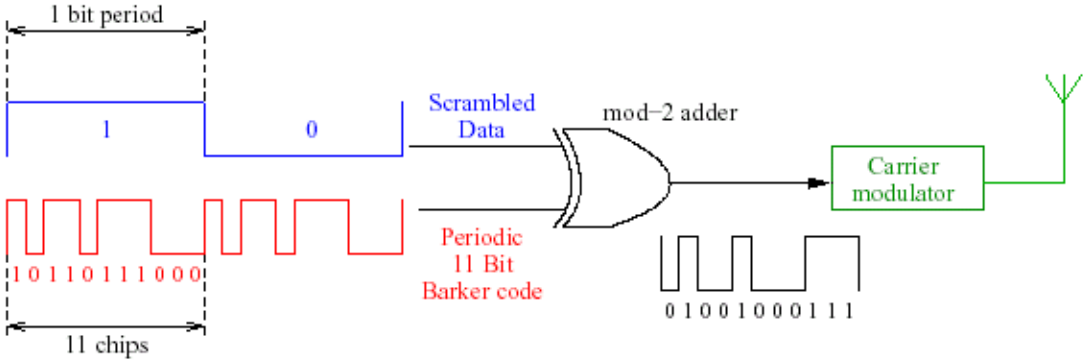
3.3.2.3.2 Το υπόστρωμα PMD DSSS

Όπως και με τα άλλα δύο φυσικά στρώματα που καθορίζονται από το 802.11 Standard, το DSSS PMD εκτελεί την ουσιαστική μετάδοση και λήψη των PPDUs υπό την καθοδήγηση του PLCP με χρήση της τεχνικής διαμόρφωσης **DSSS** (Direct Sequence Spread Spectrum). Η λειτουργία του DSSS PMD μεταφράζει την δυαδική αναπαράσταση των PPDUs σε ένα ραδιοσήμα κατάλληλο για μετάδοση. Το φυσικό στρώμα που χρησιμοποιεί την τεχνική DSSS εκτελεί αυτήν την λειτουργία πολλαπλασιάζοντας ένα φέρον (radio frequency carrier) με ένα **PN** (pseudo-noise) ψηφιακό σήμα. Το προκύπτον σήμα εμφανίζεται ως θόρυβος αν σχεδιαστεί στην περιοχή των συχνοτήτων. Το μεγαλύτερο εύρος ζώνης του 'direct sequence' σήματος δίνει την δυνατότητα στην ισχύ του θορύβου να πέσει κάτω από το όριο θορύβου χωρίς να υπάρξει καθόλου απώλεια πληροφορίας, όπως φαίνεται και στο σχήμα 3.22.

Όπως και με το FHSS, το φυσικό στρώμα DSSS λειτουργεί στις συχνότητες από 2.4 GHz έως 2.4835 GHz. Το 802.11 καθορίζει μέχρι 14 κανάλια διαφορετικών συχνοτήτων, με το καθένα να έχει εύρος 22 MHz.

3.3.2 3.2α Η λειτουργία του DSSS

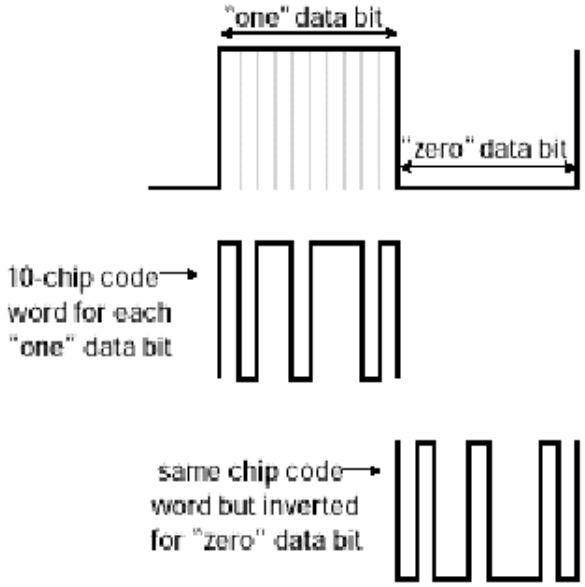
Η κεντρική ιδέα της τεχνικής DSSS είναι, αρχικά, να εξαπλωθεί ψηφιακά το μη διαμορφωμένο PPDU της βασικής ζώνης (baseband) και έπειτα να διαμορφωθούν τα εξαπλωμένα δεδομένα σε μια συγκεκριμένη συχνότητα. Το σχήμα 5.25 δείχνει τα στοιχεία που αποτελούν έναν DSSS πομπό.



Σχήμα 3.25: Σχηματική αναπαράσταση ενός DSSS πομπού.

Ο πομπός εξαπλώνει το PPDU συνδυάζοντας το PPDU ('Scrambled Data) με έναν Pseudo-Noise (PN) κώδικα (ο οποίος συχνά αναφέρεται ως chip code ή spreading sequence, ενώ στο σχήμα αναφέρεται ως 'Periodic 11 Bit Barker code') με την βοήθεια ενός modulo-2 αθροιστή (mod-2 adder). Η PN ακολουθία (PN sequence)

αποτελείται από μία ακολουθία θετικών και αρνητικών ‘1’. Μία τέτοια ακολουθία δίνεται στο επόμενο σχήμα.



Σχήμα 3.26: Αναπαράσταση ενός bit από μια ακολουθία θετικών και αρνητικών μονάδων (1).

Ο κώδικας που χρησιμοποιείται στο 802.11 DSSS αναφέρεται στη βιβλιογραφία ως 11-chip Barker sequence και δίνεται παρακάτω, με το bit που βρίσκεται πιο αριστερά να εφαρμόζεται πρώτο στο PPDU.

+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1

Η έξοδος του mod-2 αθροιστή είναι ένα DSSS σήμα με υψηλότερο ρυθμό σηματοδοσίας από αυτόν του αρχικού σήματος. Ένα PPDU με ρυθμό 1 Mbps στην είσοδο θα καταλήξει σε ένα εξαπλωμένο σήμα με ρυθμό 11 Mbps στην έξοδο του αθροιστή. Στη συνέχεια, ο διαμορφωτής (‘Carrier modulator’) μεταφράζει το σήμα της βασικής ζώνης σε ένα αναλογικό σήμα στην συχνότητα λειτουργίας της μετάδοσης του επιλεγμένου καναλιού. Αν και η ‘spreading sequence’ είναι η ίδια για όλους τους χρήστες, υπάρχει η ελευθερία επιλογής οποιουδήποτε καναλιού συχνότητας, ώστε να υποστηρίζεται η ταυτόχρονη μετάδοση.

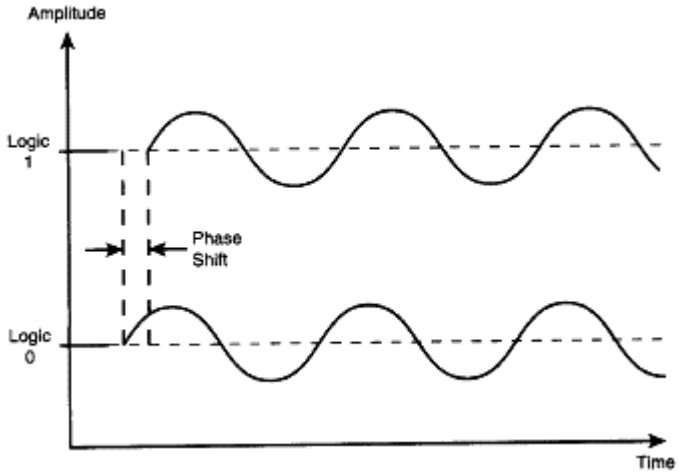
3.3.2.3.2β Η λειτουργία διαμόρφωσης συχνότητας DSSS

Ένας διαμορφωτής διαμορφώνει το εξαπλωμένο PPDU συνδυάζοντάς το με ένα φέρον ρυθμισμένο (set) στη συχνότητα μετάδοσης. Το DSSS PMD μεταδίδει το αρχικό PPDU με ρυθμό 1 Mbps ή 2 Mbps χρησιμοποιώντας διαφορετικό τύπο διαμόρφωσης, ανάλογο με το ποιος ρυθμός έχει επιλεχθεί:

1. 1 Mbps: DBPSK (Differential Binary Phase Shift Keying)
2. 2 Mbps: DQPSK (Differential Quadrature Phase Shift Keying)

Η λειτουργία της τεχνικής **PSK** (Phase Shift Keying) μεταβάλλει τη φάση της συχνότητας του φέροντος ώστε να αναπαραστήσει διαφορετικά σύμβολα. Έτσι, οι αλλαγές στη φάση διατηρούν τις πληροφορίες που βρίσκονται στο σήμα. Καθώς ο θόρυβος συνήθως επηρεάζει το πλάτος του σήματος και όχι τη φάση, η χρήση του συγκεκριμένου τύπου διαμόρφωσης μειώνει τις παρεμβολές (interference). Η είσοδος στον διαμορφωτή DBPSK είναι είτε 0 είτε 1, όπως αυτά προέρχονται από το PLCP.

Το επόμενο σχήμα δείχνει πως ο διαμορφωτής μεταδίδει τα δεδομένα μεταβάλλοντας τη φάση του φέροντος.



Σχήμα 3.27: Μετάδοση δεδομένων με χρήση της τεχνικής DBPSK.

Στην περίπτωση του DQPSK (για ρυθμό μετάδοσης 2 Mbps), η είσοδος στον διαμορφωτή είναι ένας συνδυασμός 2 bit (00, 01, 10, 11) που προέρχονται από το PLCP. Καθένα από αυτά τα σύμβολα των 2 bit στέλνονται με ρυθμό 1 Mbps, καταλήγοντας σε ένα ρυθμό δεδομένων ίσο με 2 Mbps. Έτσι, η τεχνική αυτή διπλασιάζει το ρυθμό δεδομένων ενώ διατηρεί το ίδιο baud rate με αυτό ενός σήματος με ρυθμό 1 Mbps.

Τα επίπεδα ισχύος για μετάδοση με DSSS είναι:

1. 1000 mWatts για τις ΗΠΑ
2. 100 mWatts για την Ευρώπη
3. 10 mWatts για την Ιαπωνία

Τα επίπεδα αυτά αναμένεται να είναι υψηλότερα χρησιμοποιώντας κεραίες με μεγαλύτερη κατευθυντικότητα.

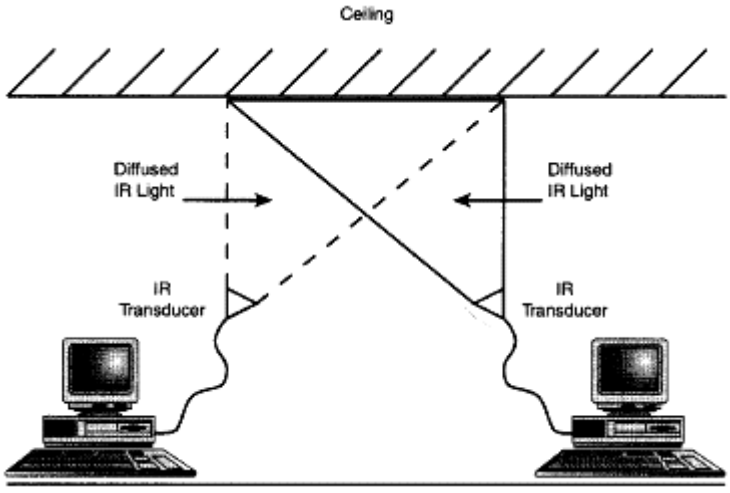
3.3.2.4 Το Φυσικό Στρώμα του 802.11 με χρήση υπέρυθρης ακτινοβολίας (Infrared-IR)

Το φυσικό επίπεδο που στηρίζεται στις υπέρυθρες ακτίνες χρησιμοποιεί μια τεχνική διαμόρφωσης που καλείται **PPM** (Pulse Position Modulation) με ρυθμούς δεδομένων 1 Mbps και 2 Mbps, οι οποίοι επιτυγχάνονται μέσω ανάκλασης των υπέρυθρων ακτινών στην οροφή της εγκατάστασης που βρίσκεται το ασύρματο δίκτυο. Ο συγκεκριμένος τρόπος λειτουργίας δεν τυγχάνει μεγάλης υποστήριξης από τις διάφορες εταιρίες.

3.3.2.4.1 Το υπόστρωμα IR PMD

Η λειτουργία του PMD μεταφράζει την δυαδική αναπαράσταση των PPDUs σε ένα σήμα υπέρυθρης ακτινοβολίας κατάλληλο προς μετάδοση. Το συγκεκριμένο φυσικό στρώμα λειτουργεί χρησιμοποιώντας μη-κατευθυντική μετάδοση, εξαλείφοντας την ανάγκη για LOS λειτουργία. Η μετάδοση αυτή είναι γνωστή ως ‘diffused infrared’.

Εξαιτίας αυτού του τρόπου μετάδοσης (σχήμα 3.28), η λειτουργία του συγκεκριμένου φυσικού στρώματος περιορίζεται σε εσωτερικούς χώρους όπου η ύπαρξη οροφής δίνει τη δυνατότητα ανάκλασης των σημάτων. Το τυπικό εύρος μετάδοσης είναι 10 με 20 μέτρα (ανάλογα με το ύψος της οροφής).



Σχήμα 3.28: Η μετάδοση των σημάτων με χρήση υπέρυθρης ακτινοβολίας γίνεται μέσω ανακλάσεων στην οροφή του χώρου στον οποίο είναι εγκατεστημένο το ασύρματο δίκτυο.

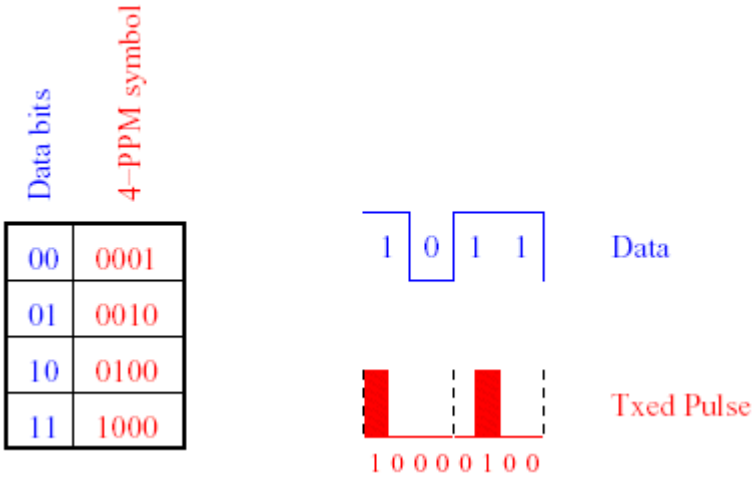
3.3.2.4.2 Η λειτουργία διαμόρφωσης PPM

Το IR PMD μεταδίδει τα δυαδικά δεδομένα με ρυθμό 1 Mbps ή 2 Mbps χρησιμοποιώντας διαφορετικό τύπο διαμόρφωσης, ανάλογο με το ποιος ρυθμός έχει επιλεχθεί:

- 1 Mbps: 16-PPM
- 2 Mbps: 4-PPM

Η τεχνική διαμόρφωσης PPM στηρίζεται στην αλλαγή θέσης ενός παλμού για την αναπαράσταση διαφορετικών δυαδικών συμβόλων. Το bit 1 σε ένα σύμβολο 16-PPM αντιστοιχεί στη θέση ενός παλμού ο οποίος αναπαριστά μία συγκεκριμένη ομάδα από 4 PPDU bits. Για παράδειγμα, η ομάδα (0110) αντιστοιχεί στο σύμβολο (0000000000001000).

Στο επόμενο σχήμα φαίνεται ο τρόπος μετάδοσης των δεδομένων με 4-PPM διαμόρφωση.



Σχήμα 3.29: Κάνοντας χρήση της διαμόρφωσης 4-PPM, η σειρά δεδομένων 1011.

Το φυσικό στρώμα που χρησιμοποιεί υπέρυθρες ακτίνες μεταδίδει τα σήματα στο κοντινό ορατό φάσμα (850-950 nm) με το μέγιστο όριο ισχύος μετάδοσης να φτάνει τα 2 Watt.

3.3.3 ΥΠΗΡΕΣΙΕΣ ΤΟΥ 802.11

Το 802.11 καθορίζει τις υπηρεσίες που παρέχουν τις απαιτούμενες λειτουργίες για την αποστολή των MSDU ανάμεσα σε δύο ομότιμα στρώματα LLC. Αυτές οι υπηρεσίες, που υλοποιεί το στρώμα MAC, χωρίζονται σε δύο κατηγορίες:

Station Services: Σε αυτές περιλαμβάνονται οι Authentication, Deauthentication και Privacy.

Distribution System Services: Σε αυτές περιλαμβάνονται οι Association, Disassociation, Distribution, Integration και Reassociation.

3.3.3.1 Station Services

Το 802.11 καθορίζει υπηρεσίες για την παροχή λειτουργιών μεταξύ των σταθμών. Για την παροχή αυτών των λειτουργιών οι σταθμοί πρέπει να στείλουν και να λάβουν MSDUs και να καθορίσουν επαρκή επίπεδα ασφάλειας. Οι υπηρεσίες αυτές αναφέρονται στη συνέχεια.

Authentication

Κάθε σταθμός, είτε είναι μέρος ενός IBSS ή ενός ESS δικτύου, πρέπει να χρησιμοποιήσει την υπηρεσία της ‘επικύρωσης’ (authentication) πριν την εγκατάσταση μιας σύνδεσης (η οποία στο 802.11 αναφέρεται ως ‘σύνδεση’ ή association) με έναν άλλον σταθμό με τον οποίο θέλει να επικοινωνήσει. Οι σταθμοί που εκτελούν την υπηρεσία της authentication στέλνουν ένα ‘unicast management authentication’ πλαίσιο στον αντίστοιχο σταθμό.

Το 802.11 καθορίζει τις ακόλουθες δύο υπηρεσίες επικύρωσης:

Επικύρωση ανοικτού συστήματος (open system authentication): Αυτή είναι η προκαθορισμένη μέθοδος επικύρωσης του 802.11. Σύμφωνα με αυτή, ο σταθμός που θέλει να χρησιμοποιήσει την υπηρεσία στέλνει ένα πλαίσιο ελέγχου με την ταυτότητα

του αποστολέα και ο σταθμός που το λαμβάνει στέλνει ως απάντηση ένα πλαίσιο με το οποίο αναγνωρίζει ή όχι την ταυτότητα του αποστολέα.

Shared key authentication: Αυτός ο τύπος επικύρωσης προϋποθέτει ότι όλοι οι σταθμοί έχουν λάβει μέσω ενός καναλιού (ανεξάρτητου από το 802.11 δίκτυο) ένα μυστικό κλειδί, με τη χρήση του οποίου λαμβάνει χώρα η επικύρωση. Για την χρήση αυτής της μεθόδου εφαρμόζεται ο αλγόριθμος WEP (Wired Equivalent Privacy).

Deauthentication

Όταν ένας σταθμός θέλει να αποσυνδεθεί (disassociate) από έναν άλλον σταθμό χρησιμοποιεί την υπηρεσία που καλείται 'deauthentication'. Η υπηρεσία αυτή είναι μια ειδοποίηση και δεν μπορεί να απορριφθεί από έναν σταθμό που λαμβάνει το ανάλογο πλαίσιο ελέγχου το οποίο ενημερώνει για την επικείμενη αποσύνδεση του σταθμού-αποστολέα.

Privacy

Η υπηρεσία αυτή εφαρμόζεται σε όλα τα πλαίσια δεδομένων και σε μερικά πλαίσια ελέγχου επικύρωσης και βασίζεται στον αλγόριθμο WEP. Ο αλγόριθμος αυτός κρυπτογραφεί τα μηνύματα (με την χρήση του αλγορίθμου κρυπτογράφησης RC4) που στέλνονται δια μέσου του ασύρματου δικτύου. Αξίζει να αναφέρουμε ότι όλες οι 'επικεφαλίδες' (headers) των πλαισίων του φυσικού στρώματος δεν κρυπτογραφούνται, ώστε όλοι οι σταθμοί να μπορούν να κάνουν λήψη των πληροφοριών ελέγχου για την σωστή διαχείριση του δικτύου.

3.3.3.2 Distribution System Services

Οι υπηρεσίες του DS, όπως καθορίζονται από το 802.11, παρέχει λειτουργίες δια μέσου του DS. Οι υπηρεσίες για την σωστή μεταφορά των MSDUs μέσω των DS είναι οι εξής:

Associaiton

Κάθε σταθμός πρέπει αρχικά να θέσει σε λειτουργία την υπηρεσία της σύνδεσης (association) με ένα AP πριν στείλει οποιαδήποτε πληροφορία μέσω του DS. Η σύνδεση αυτή αντιστοιχίζει έναν σταθμό στο DS μέσω ενός AP. Κάθε σταθμός μπορεί να συνδεθεί με ένα μόνο AP, ενώ ένα AP μπορεί να συνδεθεί με περισσότερους του ενός σταθμούς.

Disassociaiton

Η υπηρεσία αυτή τερματίζει μια υπάρχουσα σύνδεση. Οι σταθμοί πρέπει να αποσυνδέονται όταν εγκαταλείπουν ένα δίκτυο και τα AP όταν χρειάζονται συντήρηση.

Distribution

Ένας σταθμός χρησιμοποιεί την υπηρεσία αυτή κάθε φορά που θέλει να στείλει MAC πλαίσια δια μέσου του DS. Το 802.11 δεν καθορίζει τον τρόπο με τον οποίο το DS διανέμει τα δεδομένα. Η μόνη πληροφορία που δίνει η υπηρεσία στο DS είναι ο καθορισμός του BSS για το οποίο προορίζεται το πλαίσιο.

Integration

Η υπηρεσία της ενοποίησης (integration) κάνει εφικτή την διανομή των MAC πλαισίων μέσω μιας πύλης (portal) μεταξύ ενός DS και ενός LAN που δεν ανήκει στην οικογένεια 802.11.

Reassociation

Η υπηρεσία αυτή της επανασύνδεσης (reassociation) καθιστά ικανό ένα σταθμό να αλλάζει την τρέχουσα κατάσταση σύνδεσης από ένα AP σε ένα άλλο. Με τον τρόπο αυτό υποστηρίζεται η μετάβαση μεταξύ διαφορετικών BSS.

Το 802.11 υποστηρίζει, μεταξύ των άλλων υπηρεσιών, την περιαγωγή (roaming) ενός σταθμού μεταξύ πολλών APs, τα οποία χρησιμοποιούν το ίδιο ή διαφορετικό κανάλι. Για την υποστήριξη της λειτουργίας αυτής, κάθε AP μεταδίδει σε συγκεκριμένα χρονικά διαστήματα (συνήθως κάθε 100 ms) ένα σήμα (που καλείται beacon signal) και το οποίο ενημερώνει τον κάθε σταθμό για την τρέχουσα ισχύ της σύνδεσής του με το ανάλογο AP. Αν ο σταθμός ανιχνεύσει ένα ασθενές σήμα, μπορεί να εφαρμόσει την υπηρεσία της επανασύνδεσης, ώστε να συνδεθεί με ένα AP που να εκπέμπει ένα ισχυρότερο σήμα.

ΚΕΦΑΛΑΙΟ 4

Δομικά στοιχεία ενός WLAN

Ένα ασύρματο τοπικό δίκτυο αποτελείται από διάφορα στοιχεία (components) που βοηθούν στην σωστή μετάδοση, λήψη και επεξεργασία του σήματος από τον χρήστη. Στα στοιχεία αυτά συμπεριλαμβάνονται τόσο το κατάλληλο λογισμικό (software) όσο και το ανάλογο υλικό εξοπλισμού (hardware). Οι κατηγορίες των στοιχείων αυτών αναφέρονται στη συνέχεια.

4.1 Συσκευές χρηστών (End-user devices)

Όπως με κάθε σύστημα, έτσι και στα WLANs πρέπει να υπάρχει ένας τρόπος διασύνδεσης των διαφόρων εφαρμογών και υπηρεσιών με τους χρήστες. Είτε το δίκτυο είναι ασύρματο ή ενσύρματο, μία συσκευή αποτελεί τη διασύνδεση μεταξύ του χρήστη και του δικτύου. Τέτοιες συσκευές που χρησιμοποιούνται σε ασύρματα δίκτυα είναι και οι επόμενες:

- Laptop computers
- Palmtop computers
- Handheld PCs and printers
- Personal Digital Assistants (PDAs)
- Hanheld printers and scanners

4.2 Λογισμικό δικτύου (Network Software)

Ένα ασύρματο δίκτυο είναι δομημένο με το κατάλληλο λογισμικό που βρίσκεται σε διάφορα μέρη του δικτύου. Ένα σύστημα διαχείρισης δικτύου (NOS: Network Operating System), όπως είναι για παράδειγμα το Microsoft NT Server, παρέχει διαφόρων ειδών υπηρεσίες, όπως μεταφορά δεδομένων, εκτύπωση κ.ά. Πολλά τέτοια συστήματα στηρίζονται στην ύπαρξη ενός server, στον οποίο βρίσκονται οι βασικές συσκευές λογισμικού και οι βάσεις δεδομένων στις οποίες έχουν πρόσβαση οι διάφορες συσκευές τις οποίες ελέγχει ο χρήστης. Οι τελευταίες ‘τρέχουν’ το δικό τους λογισμικό (client software), το οποίο κατευθύνει τις εντολές του χρήστη στον server.

4.3 Ασύρματες κάρτες δικτύου (Wireless NICs)

Η ασύρματη κάρτα δικτύου (Wireless Network Interface Card) χρησιμοποιείται για την μετάδοση του ψηφιακού σήματος ενός υπολογιστή μέσω του ασύρματου μέσου σε έναν άλλο υπολογιστή. Στην διαδικασία αυτή συμπεριλαμβάνεται η διαμόρφωση και η ενίσχυση του σήματος.

Οι ασύρματες κάρτες δικτύου συνδέονται με τη συσκευή του χρήστη μέσω ενός διαύλου υπολογιστή όπως είναι οι ISA (Industry Standard Architecture), η PCI και PCMCIA (Personal Computer Memory Card International Association). Μερικές εταιρίες παράγουν κάρτες οι οποίες συνδέονται με τον υπολογιστή μέσω μιας USB θύρας.

Η διασύνδεση της ασύρματης κάρτας με την συσκευή του χρήστη συμπεριλαμβάνει και έναν οδηγό λογισμικού (software driver) που συνδέει το

λογισμικό του NOC στην κάρτα. Τα κυριότερα Standards για τους παραπάνω οδηγούς είναι τα εξής:

- NDIS (Network Driver Interface Specification)
- ODI (Open Datalink Interface)
- PDS (Packet Driver Specification)

a	*b*

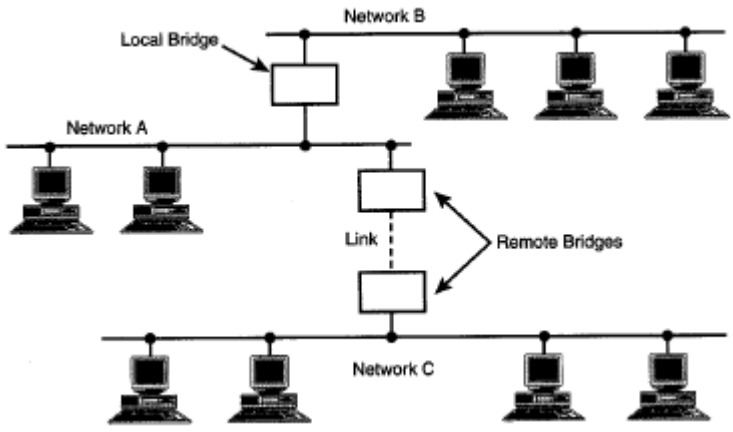
Σχήμα 4.1 Ασύρματες κάρτες δικτύου (Wireless NICs) . a)PCI card b) USB card

4.4 Ασύρματες Τοπικές Γέφυρες (Wireless Local Bridges)

Οι γέφυρες δικτύων αποτελούν ένα σημαντικό μέρος της τοπολογίας ενός δικτύου καθώς συνδέουν πολλά LANs μεταξύ τους στο επίπεδο του υποστρώματος MAC, με αποτέλεσμα την διαμόρφωση ενός εκτενέστερου και πιο λειτουργικού δικτύου. Οι γέφυρες χωρίζονται σε δύο είδη (τα οποία παρουσιάζονται και στο επόμενο σχήμα):

Local bridges: Συνδέουν τοπικά δίκτυα που βρίσκονται σε κοντινή απόσταση.

Remote bridges: Συνδέουν δίκτυα που χωρίζονται από αποστάσεις μεγαλύτερες από αυτές που μπορούν να υποστηρίξουν τα πρωτόκολλα των τοπικών δικτύων.



Σχήμα 4.2 Διασύνδεση δικτύων με local και remote γέφυρες.

Στην ορολογία των ασύρματων δικτύων οι γέφυρες αναφέρονται ως APs (Access Points), τα οποία είναι συσκευές απαραίτητες για τη διασύνδεση ενός WLAN με ένα ενσύρματο δίκτυο, αλλά και τη διασύνδεση πολλών WLAN μεταξύ τους.

4.5 Access Point (Σημεία Πρόσβασης)

Τα access point χρησιμοποιούνται όταν θέλουμε να αυξήσουμε την εμβέλεια του ασύρματου δικτύου μας, να δημιουργήσουμε ένα ασύρματο δίκτυο με αρκετούς υπολογιστές ή όταν θέλουμε να συνδέσουμε ένα ασύρματο δίκτυο με ένα ενσύρματο δίκτυο. Στην απλούστερη μορφή τους, προσφέρουν μια θύρα δικτύου RJ-45 για την σύνδεσή τους με το ενσύρματο τοπικό δίκτυο και πολλές φορές ενσωματώνουν DHCP server για το αυτόματο μοίρασμα διευθύνσεων TCP/IP στους υπολογιστές που συνδέονται ασύρματα με αυτό. Να σημειώσουμε ότι ορισμένα access point διαθέτουν σειριακή θύρα για τη ρύθμιση της συσκευής μέσω ενός υπολογιστή που δεν διαθέτει κάρτα δικτύου.

Σχήμα 4.3: Συσκευή Access Point

4.6 Ασύρματα ADSL Router

Η κατηγορία αυτή αποτελείται από Access point που ενσωματώνουν και ADSL modem. Έτσι, οι συσκευές αυτές μπορούν να συνδεθούν μόνες τους στο διαδίκτυο μέσω της γρήγορης σύνδεσης ADSL και να προσφέρουν internet σε όσους υπολογιστές συνδέονται ασύρματα με αυτές. Εκτός από τις δυνατότητές τους ως Access point και το μοίρασμα μιας γραμμής ADSL, οι συσκευές αυτής της κατηγορίας συνήθως ενσωματώνουν 4θυρα ή 5θυρα switches (επιτρέπουν ενσύρματη σύνδεση υπολογιστών), Firewall, DHCP Server, NAT ή και άλλα χαρακτηριστικά. Ορισμένα μοντέλα διαθέτουν επίσης μια θύρα USB για την σύνδεση και το μοίρασμα στο ασύρματο δίκτυο ενός εκτυπωτή. Διακρίνονται σε μοντέλα Annex A, τα οποία χρησιμοποιούνται για τη σύνδεση ADSL σε απλή τηλεφωνική γραμμή PSDN, και σε μοντέλα Annex B, τα οποία χρησιμοποιούνται για τη σύνδεση ADSL σε τηλεφωνική γραμμή ISDN

Σχήμα 4.4: Ασύρματο ADSL Router

4.7 Κεραίες (Antennas)

Η κεραία εκπέμπει το διαμορφωμένο σήμα μέσω του αέρα ώστε αυτό να φτάσει στον προορισμό του. Γενικά, οι κεραίες διακρίνονται σε πολλά είδη και μεγέθη και χαρακτηρίζονται από τις παρακάτω παραμέτρους:

- Μοντέλο διάδοσης (propagation pattern)
- Ευαισθησία (Gain)
- Ισχύς μετάδοσης (Transmit power)
- Εύρος ζώνης (Bandwidth)

Το μοντέλο διάδοσης μιας κεραίας καθορίζει την περιοχή κάλυψης (coverage area) της κεραίας. Για την μετάδοση του σήματος στα WLAN χρησιμοποιούνται κυρίως δύο είδη κεραιών:

Μια πολυκατευθυντική (omnidirectional) κεραία, η οποία διοχετεύει την ισχύ της προς κάθε κατεύθυνση.

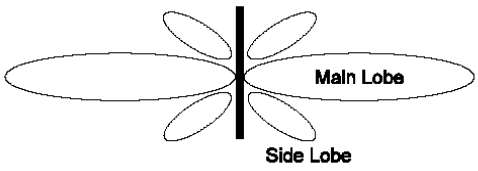
Μια μονοκατευθυντική (directional) κεραία, η οποία συγκεντρώνει το μεγαλύτερο μέρος της ισχύος της σε μία μόνο κατεύθυνση.

4.7.1 Πολυκατευθυντικές κεραίες

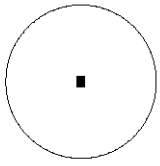
Οι κεραίες αυτές μπορεί να έχουν κάθετη ή οριζόντια πόλωση και είναι ιδανικές για την κάλυψη τετραγωνικών ή περίπου τετραγωνικών και κυρίως εσωτερικών χώρων. Τα συνηθέστερα είδη πολυκατεθυντικών κεραιών που χρησιμοποιούνται είναι:

- Place antenna
- Ceiling mount dipole antenna
- Rubber duck dipole antenna
- Short rubber duck dipole antenna
- Spectrum24 Sandra “D” antenna

Η πολυκατευθυντική κεραία εκπέμπει και λαμβάνει το ίδιο καλά σε όλες τις διευθύνσεις του αζιμουθίου (Azimuth). Στο σχήμα 4.5 φαίνεται το διάγραμμα ακτινοβολίας μιας πολυκατευθυντικής κεραίας με τους πλευρικούς της λοβούς σε πολική μορφή.



Πλευρική όψη



Άποψη

Σχήμα 4.5: Διάγραμμα ακτινοβολίας πολυκατευθυντικής κεραίας

Οι πολυκατευθυντικές κεραίες χρησιμοποιούνται σε εσωτερικούς δικτυακούς χώρους και οι περισσότερες εγκαθίστανται με ευκολία σε τοίχους και οροφές. Μπορεί να χρησιμοποιούνται δύο κεραίες σε κάθε AP για τη βελτιστοποίηση της κάλυψης (η οποία είναι της μορφής doughnut-shaped). Επίσης τέτοιου είδους κεραίες χρησιμοποιούνται για point to multipoint εφαρμογές καθώς και για εφαρμογές όπου υπάρχει ανάγκη κινητικότητας με τη θέση των σταθμών εργασίας να μεταβάλλεται συνεχώς. Η πόλωση της κεραίας πρέπει να είναι του ίδιου τύπου τόσο στην πλευρά του πομπού όσο και σε αυτή του δέκτη. Στις περισσότερες εφαρμογές χρησιμοποιούνται κεραίες κάθετης πόλωσης.

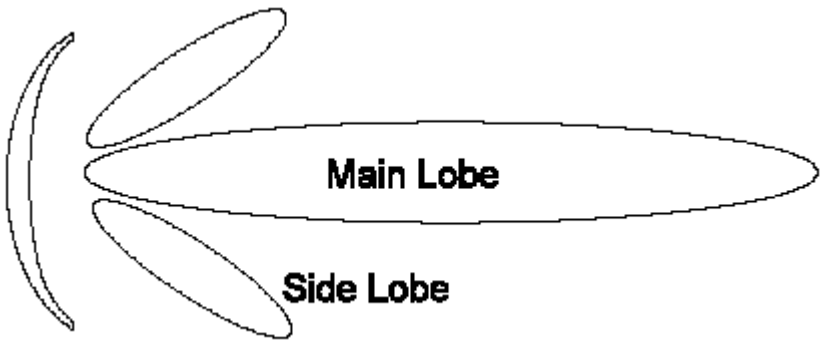
(α) (β)

Σχήμα 4.6: Πολυκατευθυντικές 'spread spectrum' κεραίες: (α) οριζόντιας πόλωσης, (β) κάθετης πόλωσης

4.7.2 Μονοκατευθυντικές κεραίες

Εκπέμπει και λαμβάνει την μεγαλύτερη ισχύ του σήματος σε μια μόνο κατεύθυνση. Στο σχήμα 4.7 φαίνεται το διάγραμμα ακτινοβολίας μιας μονοκατευθυντικής κεραίας, καθώς επίσης και οι πλευρικοί της λοβοί σε πολικές συντεταγμένες. Η κατευθυντικότητα της κεραίας καθορίζεται από τη γωνία και το εύρος της δέσμης ακτινοβολίας (beam width Τυπικές γωνίες αρχίζουν από 10° (μεγάλη κατευθυντικότητα) έως 90° (πολύ μικρή κατευθυντικότητα). Τέτοιου είδους κεραίες χρησιμοποιούνται για μακρύτερους αλλά στενότερους χώρους και σε εφαρμογές point-to-point. Τα συνηθέστερα είδη των μονοκατευθυντικών κεραιών που χρησιμοποιούνται είναι:

- Yagi antenna (30° beam)
- Patch antenna (70° beam)
- Panel antenna (22° beam)



Σχήμα 4.7: Διάγραμμα ακτινοβολίας μιας κατευθυντικής κεραίας

Αναφερόμενοι γενικά στις κεραίες, ένα μέγεθος που σχετίζεται με τη δυνατότητα κάλυψης είναι η ευαισθησία της κεραίας (antenna gain) και μετράται με τιμές decibel (db). Όσο μεγαλύτερη είναι η ευαισθησία, τόσο μεγαλύτερη είναι η ισχύς του σήματος και επομένως η κάλυψη γίνεται σε μεγαλύτερο βαθμό. Για βήμα αύξησης 1 db της ευαισθησίας της κεραίας, η κάλυψη αυξάνει κατά 2.5%. Ειδικά για εξωτερικούς χώρους χωρίς εμπόδια, αύξηση της ευαισθησίας κατά 1 db επιφέρει αύξηση στην κάλυψη κατά 5%. Τα αποτελέσματα αυτά μπορούν να διαφέρουν ανάλογα με τον τύπο του χώρου και τα φυσικά εμπόδια που υπάρχουν σ' αυτόν.

Η σωστή τοποθέτηση και ο κατάλληλος προσανατολισμός της κεραίας σε ένα δικτυακό χώρο συμβάλλει στην αύξηση της κάλυψης και στη βελτιστοποίηση της απόδοσης του ασύρματου συστήματος. Γενικά, οι κεραίες θα πρέπει να τοποθετούνται σε ψηλά σημεία και σε περιοχές που δεν υπάρχουν φυσικά εμπόδια (όσο αυτό βέβαια είναι εφικτό). Μέγιστη απόδοση έχουμε στην περίπτωση που ο πομπός και ο δέκτης βρίσκονται στο ίδιο ύψος και υπάρχει οπτική επαφή ανάμεσά τους.

Ο συνδυασμός της ισχύος μετάδοσης και της ευαισθησίας μιας κεραίας καθορίζει την απόσταση που μπορεί να μεταδοθεί το σήμα. Για μεταδόσεις σε μεγάλη απόσταση απαιτείται υψηλή τιμή ισχύος και μοντέλα κατευθυντικής μετάδοσης (directive radiation patterns), ενώ οι μεταδόσεις σε μικρές αποστάσεις γίνονται εφικτές με λιγότερη ισχύ και ευαισθησία. Γενικά, στα ασύρματα δίκτυα η ισχύς μετάδοσης είναι σχετικά χαμηλή, συνήθως κάτω από 1 Watt.

Ανάλογα με τις εφαρμογές τις οποίες υποστηρίζει ένα ασύρματο τοπικό δίκτυο οι κεραίες μπορούν να χωριστούν σε 3 είδη:

Snap-on antenna: Η κεραία αυτή συνδέεται κατευθείαν στην ασύρματη κάρτα και είναι ιδανική για εφαρμογές που απαιτούν συνεχή κίνηση.

Dipole antenna: Η κεραία αυτή συνδέεται με την ασύρματη κάρτα μέσω ενός μικρού καλωδίου και χρησιμοποιείται κυρίως από μεταφερόμενους (portable) σταθμούς, οι οποίοι μπορούν να κινούνται αλλά για να λειτουργήσουν πρέπει να βρίσκονται σε σταθερό σημείο.

High-gain antenna: Αυτό το είδος κεραίας προσαρτάται σε έναν τοίχο ή υψηλό μέρος ενός κτιρίου με τη βοήθεια ενός μεγάλου καλωδίου. Η κεραία αυτή είναι ιδανική για APs και σταθερούς σταθμούς.

(α) (β)

Σχήμα 4.8: Μονοκατευθυντικές spread spectrum κεραίες (α) 22° beam width (β) 7,5° beam width

ΚΕΦΑΛΑΙΟ 5

5.1 Εισαγωγή

Η δημοτικότητα των WLANs θα αναπτυχθεί σε μερικά χρόνια, σε εταιρίες, σε σπίτια και στο δημόσιο, όταν οι πελάτες θα αισθάνονται τα WLANs ασφαλή.

Όταν η ασφάλεια ενός ασύρματου δικτύου αποτύχει, κάνει κακό στη φήμη ολόκληρης της βιομηχανίας των ασύρματων δικτύων. Όλοι εγγυούνται ενός υψηλού επιπέδου ασφαλείας .

Για να επιτευχθεί αυτό, τα τελευταία χρόνια , η βιομηχανία έχει βελτιώσει την ασφάλεια με ποικίλες μετρήσεις. Σε αυτό το σημείο η κρυπτογραφία και τα πρωτόκολλα πιστοποίησης είναι σε θέση να φτάσουν την ασφάλεια των ασύρματων δικτύων στο ίδιο υψηλό επίπεδο όπως των ενσύρματων δικτύων. Αυτά τα πρωτόκολλα έχουν εγκριθεί από επίσημα σώματα ή είναι μόνιμα.

Οι μέθοδοι είναι διαθέσιμοι να αποτρέπουν κάθε γνωστό είδος επίθεσης πάνω στα ασύρματα δίκτυα συμπεριλαμβανομένων των ακολούθων :

- ***Eavesdropping :*** Ο επιτιθέμενος ελέγχει την κυκλοφορία μεταξύ ενός ασύρματου σταθμού και ενός σημείου σύνδεσης για να κλέψει ευαίσθητα δεδομένα.
- ***Mac spoofing:*** Ο επιτιθέμενος αναγνωρίζει και αντιγράφει τις (MAC) διευθύνσεις, των γνωστών σταθμών για να κερδίσει την πρόσβαση στο δίκτυο.
- ***Rogue Access points:*** Ο επιτιθέμενος υποδύεται ένα νόμιμο σημείο πρόσβασης ώστε να μάθει ευαίσθητες πληροφορίες όπως συνδυασμούς των username και password.
- ***Theft of service:*** Ο επιτιθέμενος, κερδίζει την πρόσβαση στο internet μέσω της εταιρικής ή σπιτικής υποδομής με συνέπεια τη σπατάλη των ISP για την παράνομη χρήση των e-mails που στέλνονται από το δίκτυο.
- ***Denial of service:*** Είναι το μόνο είδος επίθεσης που μπορεί να απειλήσει την προστασία των Ασύρματων Δικτύων και παραμένει άλυτο. Ο επιτιθέμενος αποτρέπει τους νόμιμους χρήστες να εισέλθουν στο δίκτυο με το να γεμίζει το δίκτυο με κίνηση.

Αν και τα πρωτόκολλα ασφαλείας και μηχανισμοί είναι διαθέσιμοι, παρόλα αυτά, πολλά Ασύρματα Δίκτυα δεν είναι προστατευμένα. Κατανοώντας τα σύνθετα ζητήματα, είναι το πρώτο βήμα για την επίτευξη της απαραίτητης προστασίας. Παρακάτω θα περιγράψουμε τις ασφαλείς μεθόδους που είναι διαθέσιμοι σήμερα, από τα παλαιότερα τρωτά πρωτόκολλα ως τα νεότερα πρωτόκολλα, που παρέχουν την ασφάλεια που οι πελάτες επιθυμούν.

5.2 ΣΥΝΟΠΤΙΚΗ ΙΣΤΟΡΙΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

5.2.1 WIRED EQUIVALENT PRIVACY (WEP)

Το 1999, Η ομάδα εργασίας του IEEE 802.11 πρότεινε ένα εναλλακτικό μηχανισμό ασφάλειας που ονομάζεται πρωτόκολλο WEP. Το πρωτόκολλο WEP επιδίωκε να παρέχει ένα επίπεδο ασφάλειας για τα Ασύρματα Δίκτυα όμοιο με αυτό

των ενσύρματων δικτύων, με το να μεταδίδει κρυπτογραφημένα δεδομένα και αποτρέποντας παράνομους χρήστες να συνδεθούν. Το πρωτόκολλο WEP δεν είναι το υποχρεωτικό μέρος του IEEE 802.11b, εν τούτοις, και τα περισσότερα προϊόντα του 802.11b δεν έχουν την υπολογιστική ισχύει να τρέξουν την κρυπτογράφηση WEP χωρίς να γίνει σημαντική υποβάθμιση απόδοσης. Κατά συνέπεια, πολλοί χρήστες έχουν κλείσει την ασφάλεια WEP στα δίκτυά τους. Κατά το πέρασμα του χρόνου, πολλοί χρήστες αναγνώρισαν την σημασία της ασφάλειας των Ασύρματων Δικτύων και άρχισαν να ενεργοποιούν την κρυπτογράφηση WEP.

Ατυχώς, το WEP έχει αποδειχθεί ανεπαρκή για την ασφάλεια των Ασύρματων Δικτύων. Πολλοί εμπειρογνώμονες ασφάλειας, τόσο στον ακαδημαϊκό κόσμο όσο και στην ιδιωτική βιομηχανία έχουν προσδιορίσει τις ‘τρύπες’ της προδιαγραφής WEP οι οποίες είναι:

- Αδυναμία του WEP λόγω της βασικής επαναχρησιμοποίησής του και της ανεπαρκούς επικύρωσης μηνυμάτων.
- Αδυναμία των μηχανισμών έλεγχου πρόσβασης του 802.11.
- Αδυναμία του πρωτοκόλλου WEP λόγω της ανάρμοστης χρήσης του βασικού αλγόριθμου RC4.

Λαμβάνοντας υπόψη αυτές τις ανεπάρκειες, πολλοί πωλητές αύξησαν το μήκος του WEP κλειδιού στα προϊόντα τους από 40 σε 152 bits και εμπορεύτηκαν αυτή την αλλαγή ως ασφαλέστερη κρυπτογράφηση WEP. Όμως, ένα πιο μεγάλο κλειδί κρυπτογράφησης είναι ευεργετικό μόνο εάν το βασικό σύμβολο κρυπτογράφησης είναι ασφαλές. Επειδή το WEP είναι από την φύση του μη ασφαλές, αυξάνοντας το μέγεθος του κλειδιού WEP απλά αυξάνεις το χρόνο που χρειάζεται ένας hacker για να μπει στο δίκτυο.

Ομοίως, καθώς στα παλιά προϊόντα των Ασύρματων δικτύων είχαν μόνο τέσσερα διαμοιραζόμενα κλειδιά για ολόκληρο το δίκτυο, διάφοροι προμηθευτές υποστήριζαν τώρα το μοναδικό κλειδί του πρωτοκόλλου WEP, ανά-χρηστών ή ανά-συνόδου. Αυτή η προσέγγιση αυξάνει τον χρόνο διάρρηξης των hackers, με το να τους αναγκάζει να συλλέξουν τα απαραίτητα στοιχεία από έναν χρήστη παρά από όλους τους χρήστες, αλλά το WEP κλειδί ανά-χρηστών ή ανά-συνόδου είναι ακόμα ευαίσθητο στις βασικές αδυναμίες του αλγόριθμου WEP.

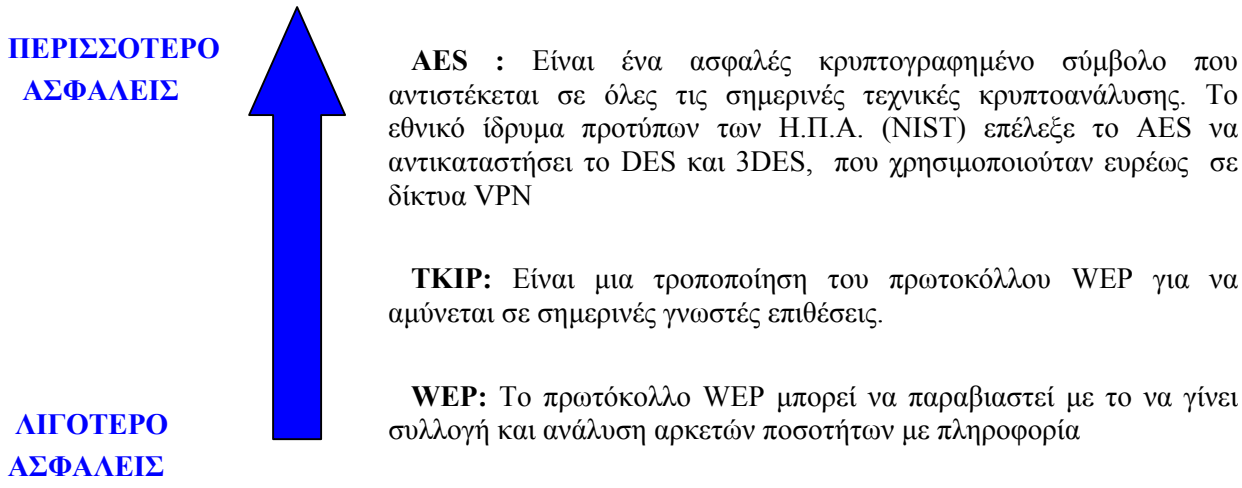
5.2.2 IEEE 802.11i

Αμέσως μετά από τα ελαττώματα του WEP, η ομάδα της IEEE 802.11i

διαμορφώθηκε για να καθιερώσει μια περιεκτικότερη λύση για την ασφάλεια των Ασύρματων Δικτύων. Αυτή η ομάδα έχει σχεδόν ολοκληρώσει το πρότυπο RSN (Robust Security Network). Αυτό το πρότυπο περιέχει δυο μέρη:

- Το πρότυπο AES (Advanced Encryption Standard) που χρησιμοποιείται για την κρυπτογραφία της κυκλοφορίας στα Ασύρματα Δίκτυα.
- Το πρότυπο IEEE 802.1x (port-based Network Authentication) που χρησιμοποιείται για την επικύρωση των χρηστών ενός Ασύρματου Τοπικού Δικτύου και την βασική διαχείρισή τους.

Η ομάδα του IEEE 802.11i επίσης, πρότεινε μια σειρά από διορθώσεις για το πρωτόκολλο WEP που θα διευκόλυνε τα προϊόντα του 802.11b τα οποία δεν υποστηρίζουν αναβάθμιση του AES, λόγω των περιορισμών της σχεδίασης. Αυτές οι διορθώσεις απαρτίζουν το πρωτόκολλο TKIP (Temporal Key Integrity Protocol)



Σχήμα 5.1: Διαβάθμιση διαφορετικών τύπων κρυπτογράφησης, στην ασφάλειας των Ασύρματων Τοπικών Δικτύων

5.2.3 Κρυπτογραφία AES

Η διεθνής κρυπτογραφική κοινότητα συμμετέχει ενεργά στην ομάδα 802.11i για την εύρεση ενός αλγόριθμου κρυπτογράφησης και επιλέχτηκε το AES επειδή αντιστέκεται σε όλες τις γνωστές τεχνικές κρυπτοανάλυσης. Στην πραγματικότητα οι κρυπτογράφοι έχουν τόσο μεγάλη εμπιστοσύνη στο πρωτόκολλο AES, που το διεθνές ίδρυμα προτύπων και τεχνολογίας της Αμερικής το διάλεξε για να αντικαταστήσει το πρωτόκολλο DES που χρησιμοποιούταν στις εφαρμογές των δικτύων VPN, σε τραπεζικές λύσεις και σε ένα μεγάλο πλήθος από ευαίσθητες εφαρμογές.

5.2.4 Κρυπτογραφία TKIP

Όπως είπαμε νωρίτερα, η ομάδα IEEE 802.11i έκανε μερικές διορθώσεις για την ανεπάρκεια του πρωτοκόλλου WEP ώστε να υποστηρίζει τα προϊόντα του 802.11b.Η κύρια σκέψη για την ασφάλεια των περισσοτέρων προϊόντων του 802.11b είναι ότι γενικά χρησιμοποιούσαν αργόστροφες ενσωματωμένες CPUs(κεντρικές μονάδες επεξεργασίας) με περιορισμένο ελεύθερο χώρο, για να υπολογιστεί η εντατική ασφάλεια. Δουλεύοντας πάνω σ'αυτό τον περιορισμό, η ομάδα διατύπωσε το πρωτόκολλο TKIP ως μια βραχυπρόθεσμη λύση, που προσφέρει έναν λογικό συμβιβασμό μεταξύ της προσθήκης , της ασφάλειας και του περιορισμού της απόδοσης της υπάρχουσας CPU που περιορίζει τα προϊόντα του 802.11b.

Το πρωτόκολλο TKIP αποτελείται από 4 patches του αλγόριθμου WEP:

1. Ένας έλεγχος ακεραιότητας μηνυμάτων, που καλείται στο πρωτόκολλο σαν 'Michael'
2. Αντίμετρα που διαγράφουν το τρέχον κλειδί επικύρωσης και κρυπτογράφησης εάν ανιχνευτεί μια επίθεση
3. Μια λειτουργία μίξης κλειδιού ανά πακέτο
4. Μία επαναληπτική προστασία.

Είναι σημαντικό να σημειώσουμε ότι το TKIP δεν εξασφαλίζει το επίπεδο ασφαλείας που πετυχαίνει το AES. Στην πραγματικότητα, το τρέχον σχέδιο της προδιαγραφής 802.11b δηλώνει ξεκάθαρα : 'Λόγω της αδυναμίας του, η ομάδα IEEE

802.11 συνιστά να μην χρησιμοποιείται το TKIP μόνο ως Patch του προ-RSN εξοπλισμού'.

5.2.5 ΠΡΟΔΙΑΓΡΑΦΗ 802.1x

Το 802.1x είναι ένα ανοιχτό πλαίσιο εργασίας για να πιστοποιεί ασύρματους σταθμούς, με έναν Server πιστοποίησης πάνω στο ενσύρματο δίκτυο δια μέσου ενός ασύρματου access point. Συχνά ο Server πιστοποίησης είναι ο ίδιος RADIUS Server (Remote Authentication Dial-up User Service) που χρησιμοποιείται από μια εταιρία για να πιστοποιεί τους χρήστες που συνδέονται.

Το πλαίσιο εργασίας του 802.1x είναι βασισμένο στο πρωτόκολλο EAPOL (Extensible Authentication Protocol Over Lan) και υπάρχει ένας αριθμός από αλγόριθμους πιστοποίησης EAPOL που μπορούν να χρησιμοποιηθούν. Οι πιο συνήθης εφαρμοσμένοι τύποι επικύρωσης περιλαμβάνουν EAP-MD5, EAP-TLS, EAP-TTLS, LEAP και PEAP.

ΤΥΠΟΣ ΠΡΟΔΙΑΓΡΑΦΗΣ EAP	ΣΧΟΛΙΑ
EAP-MD5 Message Digest 5)	Το EAP-MD5 είναι μια μέθοδος πιστοποίησης βασισμένη στο συνθηματικό το οποίο δεν χρησιμοποιείται ευρέως διότι δεν εξασφαλίζει έναν μηχανισμό για την ασφαλή ανταλλαγή νέου κλειδιού
EAP- TLS (Transport Layer security)	Το EAP- TLS μπορεί να είναι αρκετά σύνθετο για να στηθεί αλλά δεν έχει καμία γνωστή αδυναμία στην ασφάλεια. Απαιτεί την χρησιμοποίηση, ενός RADIOUS Server και του ψηφιακού πιστοποιητικού, και στο σταθμό και στον RADIOUS Server.Η ψηφιακή πιστοποίηση μπορεί να εγκατασταθεί χρησιμοποιώντας μια σπιτική αρχή πιστοποίησης (π.χ. Microsoft internet access server) ή πληρώνοντας τρίτο για την παροχή ψηφιακού πιστοποιητικού (π.χ. Verising ή entrust). Ένα σημαντικό πλεονέκτημα στη χρησιμοποίηση EAP- TLS είναι ότι η Microsoft υποστηρίζει TLS στα Windows XP και παρέχει την υποστήριξη EAP- TLS στα πακέτα αναβάθμισης για τα Windows 2000,98,ME και NT4. Ο κεντρικός υπολογιστής πρόσβασης της Microsoft, περιέχει, και τον RADIOUS Server και την αρχή πιστοποίησης που χρειάζεται για να δημιουργήσει μια 802.1x EAP-TLS υποδομή.
LAEP (EAP Cisco Wireless)	Το LEAP παρέχει έναν αποτελεσματικό τρόπο για να ασφαλίσει το ασύρματο δίκτυο καθώς χρησιμοποιεί ακόμα συσκευές που βασίζονται στο πρωτόκολλο WEP. Αποτελείται από μια αμοιβαία προδιαγραφή που βασίζεται στο password και έναν RADIOUS server και συχνή ανανέωση του WEP κλειδιού ώστε να αποτρέψει τους εισβολείς από το να σπάσουν το κλειδί. Καθώς ο μηχανισμός ζήτησης του LEAP είναι διαθέσιμος με έναν μεγάλο αριθμό κατασκευαστικών προϊόντων, ο μηχανισμός πιστοποίησης access point, περιορίζεται στον εξοπλισμό της Cisco.
EAP-TTLS(Tunneled TLS) PEAP (Protected EAP)	Το EAP-TTLS και το PEAP είναι όμοιοι τύποι πιστοποίησης EAP και υποστηρίζεται από έναν ευρύ κύκλο εταιριών στην βιομηχανία των Ασύρματων Τοπικών Δικτύων. Αυτά τα πρωτόκολλα χρησιμοποιούν ψηφιακή πιστοποίηση όπως το EAP-TLS, αλλά απαιτεί πιστοποιήσεις μόνο στον RADIOUS server. Ο σταθμός πιστοποιεί τον RADIOUS server χρησιμοποιώντας την ψηφιακή πιστοποίηση του server, τότε ένα ασφαλές τούνελ δημιουργείται μεταξύ του σταθμού και του RADIOUS server και δια μέσου αυτού ο RADIOUS server μπορεί να πιστοποιήσει τον σταθμό.

Σχημα: 5.2: Οι διάφοροι τύποι αλγορίθμων πιστοποίησης EAP πάνω σε Δίκτυα

Όταν ένας σταθμός προσπαθεί να συνδεθεί σ'ένα Ασύρματο Τοπικό Δίκτυο μέσω του 802.1x, το access point επιτρέπει στο σταθμό να συνδεθεί αλλά τον αναγκάζει σε παράνομη δήλωση στην οποία μόνο το πρωτόκολλο EAP περνάει δια μέσου του RADIUS Server. Χρησιμοποιώντας EAP μηνύματα, είτε με κωδικό είτε με δημόσιο ή ιδιωτικό κλειδί ο RADIUS Server πιστοποιεί τον σταθμό. Ο RADIUS Server τροφοδοτεί το access point με ένα αρχικό κρυπτογραφημένο κλειδί, το οποίο έχει προέρθει από τον σταθμό μέσω της διαδικασίας πιστοποίησης. Το access point τότε δημιουργεί ένα δεύτερο κλειδί για επικοινωνιακή χρήση με το σταθμό, κρυπτογραφεί το δεύτερο κλειδί χρησιμοποιώντας το αρχικό κλειδί και το στέλνει στο σταθμό. Το access point τότε στέλνει καινούργια κλειδιά στο σταθμό ώστε να είναι σίγουρο ότι η ασφάλεια δεν παραβιάστηκε.

5.3 ΕΝΑΛΛΑΚΤΙΚΑ ΠΡΩΤΟΚΟΛΛΑ ΑΠΟ ΤΟ 802.11i

5.3.1 LEAP (EAP Cisco Wireless)

Το Δεκέμβρη του 2000, η Cisco παρουσίασε το πρωτόκολλο LEAP που διόρθωνε τα προβλήματα της ασφάλειας WEP. Το LEAP βασίζεται στην WEP κρυπτογράφηση αλλά παρέχει πιστοποίηση του χρήστη και λειτουργία ξανακλειδώματος για να αποφύγει μερικά ρίσκα της ασφάλειας WEP. Το access point της Cisco εφαρμόζει το LEAP πρωτόκολλο με το να κάνει πιστοποίηση στο σταθμό με την βοήθεια ενός Cisco RADIUS server και με το να ανανεώνει τα WEP κλειδιά σε συνεχή βάση.

Βασιζόμενο στην βαριά κάλυψη των αδυναμιών του WEP και στο ισχυρό όνομα του Cisco, το Cisco Leap βρήκε μεγάλη επιτυχία στην αγορά των επιχειρήσεων του WLAN. Την ίδια στιγμή, έχε στο νου σου δύο σημαντικά θέματα όταν σκέφτεσαι την εφαρμογή LEAP: Ενώ η Cisco διαθέτει το LEAP για τις λύσεις **(solutions)** πολλών σταθμών προμηθευτών, μόνο τα access point της Cisco μπορούν να τρέξουν το πρωτόκολλο LEAP. Επιπλέον, αντί να χρησιμοποιεί δημόσια/ ιδιωτικά κλειδιά κρυπτογράφησης για εξασφάλιση της γνησιότητας, το LEAP βασίζεται σε κωδικούς πρόσβασης **(passwords).** Οι χρήστες επομένως μπορεί να είναι ευάλωτοι σε **dictionary** επιθέσεις κατά τις οποίες ο επιτιθέμενος προσπαθεί να σπάσει το κλειδί WEP καταγράφοντας μία σειρά από **frames** , και μετά προσπαθεί απλά χρησιμοποιώντας κωδικούς offline μέχρι κάποιος να είναι ο κατάλληλος. Αυτή η ευπάθεια υπονοεί ότι οι διαχειριστές του IT θα ήταν σωστό να χρησιμοποιούν μεγάλους / σύνθετους κωδικούς όταν εφαρμόζεται η αυθεντικότητα του Cisco LEAP.

5.3.2 WI-FI PROTECTED ACCESS (WPA)

Η συμμαχία (Alliance) Wi-Fi προωθεί ένα καινούριο δεδομένο το επονομαζόμενο WI- Fi Protected Access(WPA). Βασιζόμενο σε ένα πληροφοριακό κείμενο σε ένα πρόσφατο σχέδιο της 802.11i προδιαγραφής, το WPA είναι μία προτεινόμενη πρακτική για το υλικό pre-802.11i αλλά δεν συμπεριλαμβάνεται σαν μέρος του απαιτούμενου 802.11ι προτύπου. Προϊόντα που εφαρμόζουν WPA ξεκίνησαν να κυκλοφορούν το πρώτο μισό του 2003, και περιλάμβαναν υποστήριξη για WEP, TKIP και δεδομένα κρυπτογράφησης AES καθώς και αυθεντικότητα του χρήστη 802.1x μαζί με ένα WPA- ειδικό EAPol αλγόριθμο.

Ενώ ή προδιαγραφή για το WPA περιλαμβάνει υποστήριξη για κρυπτογράφηση AES , οι συνήγοροι της αρχικής βιομηχανίας WPA αναζητούν μία **stopgap** λύση για να βελτιώσουν την ασφάλεια σε μία εγκατεστημένη βάση από 802.11b προϊόντα. Συνεπώς, η αρχική δοκιμή για τη δια-λειτουργικότητα και την πιστοποίηση θα επικεντρωθεί στη διαπίστωση ασφάλειας του TKIP το οποίο μπορεί να εφαρμοστεί ως βελτίωση του λογισμικού(software) / firmware σε εκείνα τα προϊόντα .

Για χρήστες που δουλεύουν στο σπίτι και οι οποίοι είναι απίθανο να έχουν ένα RADIUS server για να επικυρώνει τους σταθμούς, το WPA παρέχει ένα μηχανισμό PRE-SHARED KEY (PSK). Για να χρησιμοποιήσεις το PSK, ο χρήστης εισάγει μία φράση-εισόδου στα δύο σημεία πρόσβασης και στο σταθμό. Αυτή η φράση εισόδου χρησιμοποιείται για να επικυρώνει όποιο σταθμό προσπαθεί να συνδεθεί. Το σημείο πρόσβασης παρέχει τότε στο σταθμό ένα κλειδί συνόδου (session) το οποίο ανανεώνεται σε τακτά χρονικά διαστήματα. Η διαπίστωση της WI-FI Alliance για τη βάση-TKIP WPA ξεκίνησε το καλοκαίρι του 2003.

Η WPA βελτιώνεται επάνω στο επίπεδο ασφάλειας που είναι διαθέσιμο από το WEP στα υπάρχοντα ασύρματα δίκτυα, ειδικά όταν χρησιμοποιείται η κρυπτογράφηση AES. Υπάρχουν πολλοί σημαντικοί περιορισμοί που πρέπει να παρθούν υπ' όψιν, ωστόσο: Πρώτον, η WPA απαιτεί την εισαγωγή ενός νέου σταθμού 802.1x-WPA supplicants. Ενώ, η Microsoft έχει δεσμευθεί για ένα Windows XP supplicant για το WPA, δεν είναι ξεκάθαρο εάν η Microsoft θα εφοδιάσει τα WPA supplicants στα λειτουργικά συστήματα των νόμιμων επιχειρήσεων (σε αντίθεση, η Microsoft επιτρέπει τη χρήση του 802.11i υποστηρίζοντας την εγχώρια 802.1x EAP-TLS στα Windows XP και με τις βελτιώσεις μπαλωμάτων για τα Windows 98, Windows ME, Windows NT 4.0 και τα Windows 2000.) Δεύτερον, η υποστήριξη για το WPA απαιτεί μία βελτίωση firmware στους υπάρχοντες σταθμούς 802.11b και στα σημεία πρόσβασης. Πολλοί καταναλωτές καθώς και οι διευθυντές IT έχουν ιστορικά αποφύγει τέτοιες βελτιώσεις επειδή είναι δύσκολο και επικίνδυνο να καταστραφεί το προϊόν εάν κατά τη διαδικασία παρουσιαστούν οποιεσδήποτε δυσλειτουργίες (ή απότομες μεταβολές τάσης). Τέλος, η ικανότητα διαπραγμάτευσης της κρυπτογράφησης που διευκρινίζεται από το WPA επιτρέπει στους wep-based clients να λειτουργήσουν σε ένα ανάμικτο WEP/WPA δίκτυο. Συμπεριλαμβάνοντας WEP έστω και σε ένα σταθμό παρέχει ασφάλεια για ολόκληρο το δίκτυο, εξαλείφοντας τα οποιαδήποτε οφέλη με το να τρέχουν TKIP και AES στους άλλους σταθμούς.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. www.americasnetwork.com
2. stdsbbs.ieee.org/802/11/index.html
3. www.proxim.com
4. www.hiperlan2.com
5. www.3com.com/wireless
6. www.atheros.com/
7. www.weca.net
8. www.wi-fi.com
9. www.broadcom.com
10. www.awmn.gr
11. www.salonicawireless.net
12. www.serreswireless.net
13. www.nokia.com/nokia/0,1522,,00.html?orig=/corporate/wlan/
14. www.iss.net/wireless/WLAN_FAQ.php
15. h18004.www1.hp.com/products/wireless/wlan/
16. PC magazine (Δεκέμβριος 2002)
17. RAM (Μάιος, Νοέμβριος, Δεκέμβριος 2003)
18. RAM (Ιανουάριος, Αύγουστος-Σεπτέμβριος 2004)