Πανεπιστήμιο Αιγαίου

Ασύρματα Δίκτυα Επικοινωνιών

Πρότυπο 802.11

Δημοσθένης Βουγιούκας (dvouyiou@aegean.gr)

Αναπληρωτής Καθηγητής

Τμήμα Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.
- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.

Χρηματοδότηση

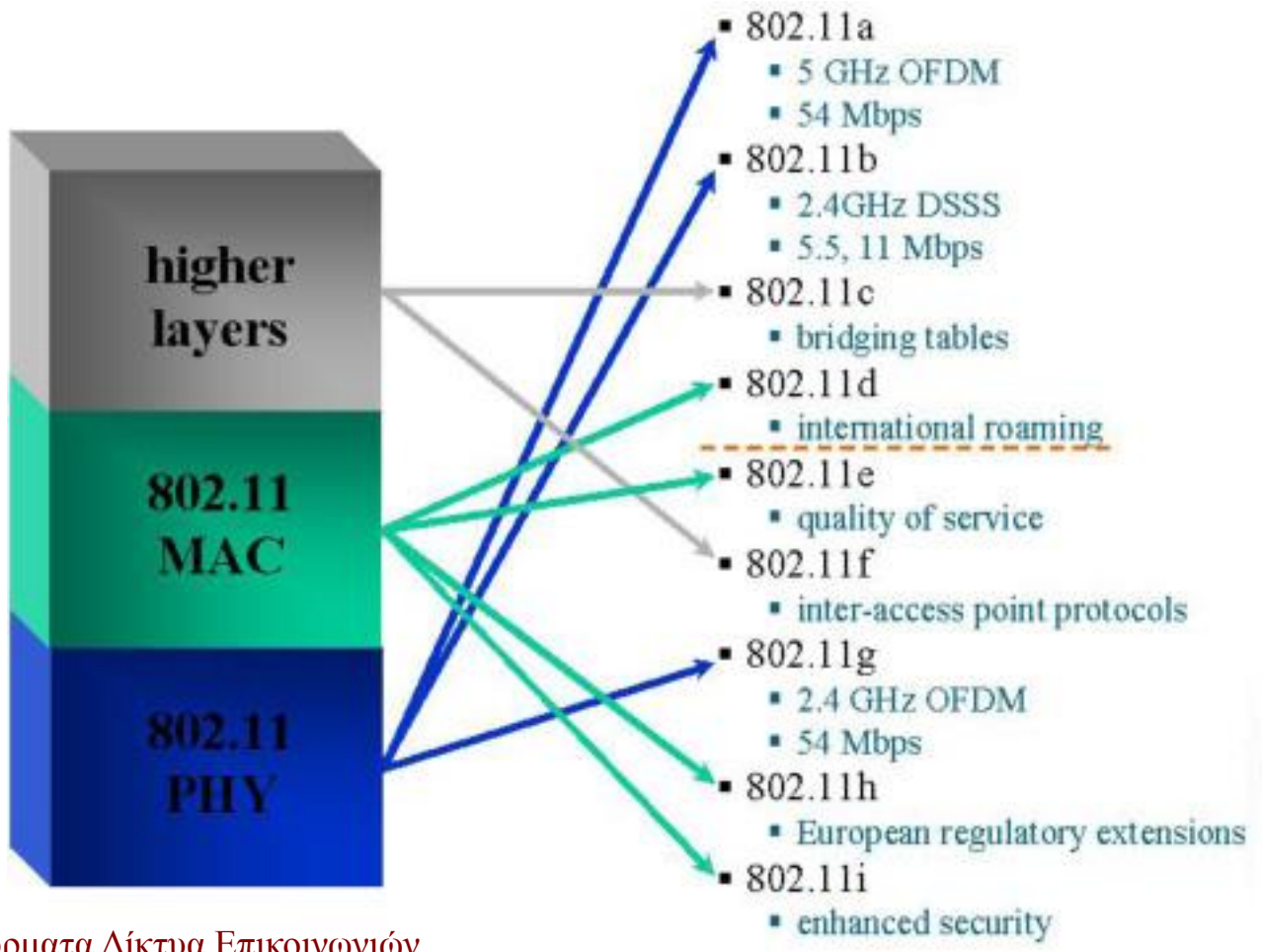
- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Αιγαίου**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Δομή της διάλεξης

- Εισαγωγή στο 802.11
- Τοπολογία 802.11
- Φυσικό στρώμα και λειτουργίες του
- Υπηρεσίες 802.11
- Υποστρώμα MAC
  - Λειτουργίες MAC
  - Δομή πλαισίων
  - Ασφάλεια

IEEE 802.11


higher layers
802.11 MAC
802.11 PHY
802.11a
5 GHz OFDM
54 Mbps
802.11b
2.4GHz DSSS
5.5, 11 Mbps
802.11c
bridging tables
802.11d
international roaming
802.11e
quality of service
802.11f
inter-access point protocols
802.11g
2.4 GHz OFDM
54 Mbps
802.11h
European regulatory extensions
802.11i
enhanced security

IEEE 802.11

- IEEE 802.11j: Extensions for Japan (2004)
- IEEE 802.11-2007: A new release of the standard that includes amendments a, b, d, e, g, h, i & j. (July 2007)
- IEEE 802.11k: Radio resource measurement enhancements (2008)
- IEEE 802.11n: Higher throughput improvements using MIMO (multiple input, multiple output antennas) (September 2009)
- IEEE 802.11p: WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working—June 2010)
- IEEE 802.11r: Fast BSS transition (FT) Working "Task Group r" (2008)
- IEEE 802.11s: Mesh Networking, Extended Service Set (ESS) (working—September 2010)
- IEEE 802.11u: Interworking with non-802 networks (for example, cellular) (working—September 2010)
- IEEE 802.11v: Wireless network management (working—June 2010)
- IEEE 802.11w: Protected Management Frames (September 2009)
- IEEE 802.11y: 3650–3700 MHz Operation in the U.S. (2008)
- IEEE 802.11z: Extensions to Direct Link Setup (DLS) (August 2007 – December 2011)
- IEEE 802.11aa: Robust streaming of Audio Video Transport Streams (March 2008 – June 2011)
- IEEE 802.11mb: Maintenance of the standard. Will become 802.11-2011. (Expected publication 8/02/11)
- IEEE 802.11ac: Very High Throughput <6 GHz; potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase); wider channels (80 or even 160MHz), multi user MIMO; (September 2008 – December 2012)
- IEEE 802.11ad: Very High Throughput 60 GHz (December 2008 – December 2012)
- IEEE 802.11ae: QoS Management
- IEEE 802.11af: TV Whitespace

IEEE 802.11a

- Υψηλός ρυθμός PHY, 6-54 Mbps.
- 5 GHz UNII-band (Unlicensed National Information Infrastructure).
- OFDM (Orthogonal Frequency Division Multiplexing).
- Υψηλή διεκπεραιωτικότητα (throughput).
- Μεγάλος αριθμός καναλιών.
- Καλή προστασία από γειτονικές παρεμβολές.
- Εκδόθηκε το 1999.

IEEE 802.11b

- Υψηλός ρυθμός PHY, 5.5-11 Mbps.
- 2.4 GHz ISM-band (Industrial, Science, Medical).
- 83 MHz, 3x22 MHz channels (14 overlapped channels).
- CCK (Complementary Code Keying).
- Πιθανότητα γειτονικών παρεμβολών από πολλούς χρήστες λόγω χρησιμοποίησης τριών μόνο καναλιών.
- Εκδόθηκε το 1999.

IEEE 802.11c

- Σύσταση (recommendation) σχετικά με τη λειτουργία των διαδικασιών γεφύρωσης (bridge).
- Χρησιμοποιείται από τους κατασκευαστές AP (Access Point).
- Διαλειτουργικότητα των APs.
- Εκδόθηκε το 1998.

IEEE 802.11d

- Συμπληρωματικό του MAC επιπέδου.
- Επιτρέπει την επικοινωνία των AP στα επιτρεπτά κανάλια με αποδεκτά επίπεδα ισχύος για τους χρήστες.
- Προσθέτει χαρακτηριστικά και περιορισμούς για τη λειτουργία του 802.11 σε όλες τις χώρες.
- Ειδικά στην Ευρώπη λειτουργεί στα 5 GHz.
- Εκδόθηκε το 2001.

IEEE 802.11e

- Συμπληρωματικό του MAC επιπέδου για την παροχή QoS υποστήριξης για LAN εφαρμογές.
- Εφαρμόζει στο 802.11 τα φυσικά πρότυπα a,b και g.
- Παρέχει κατηγορίες υπηρεσιών για διαφορετικά επίπεδα QoS για εφαρμογές δεδομένων, φωνής και εικόνας.
- Χειρισμός πακέτο-ανά-πακέτο.
- Μετάδοση πολλαπλών πακέτων.
- Μετάδοση client-to-client.
- Εκδόθηκε το 2002.

IEEE 802.11f

- Χρησιμοποιείται για να πετύχει δια-λειτουργικότητα μεταξύ δικτύων WLAN πολλαπλών κατασκευαστών (multi-vendor).
- Επικοινωνία μεταξύ διαφορετικών APs.
- Περιαγωγή μεταξύ multi-vendors APs.
- Fast hand-off.
- Εκδόθηκε το 2002.

IEEE 802.11g

- Υψηλός ρυθμός PHY για 2.4 GHz ISM-band
- >20 Mbps (max 54 Mbps).
- Συμβατό με το πρότυπο 802.11b (μέσω CCK και PBCC – Packet Binary Convolutional Coding).
- Απαραίτητα CCK και OFDM.
- Υποστηρίζει και άλλες τεχνικές διαμόρφωσης.
- Εκδόθηκε το 2002.

IEEE 802.11h

- Συμπληρωματικό του MAC επιπέδου για τη συμμόρφωση με τους ευρωπαϊκούς κανονισμούς στα 5 GHz WLAN.
- Προσαρμόζει κατάλληλα το IEEE 802.11a.
- Περιλαμβάνει DFS (Dynamic Frequency Selection) και TPC (Transmit Power Control).
- Εκδόθηκε το 2002.

IEEE 802.11i

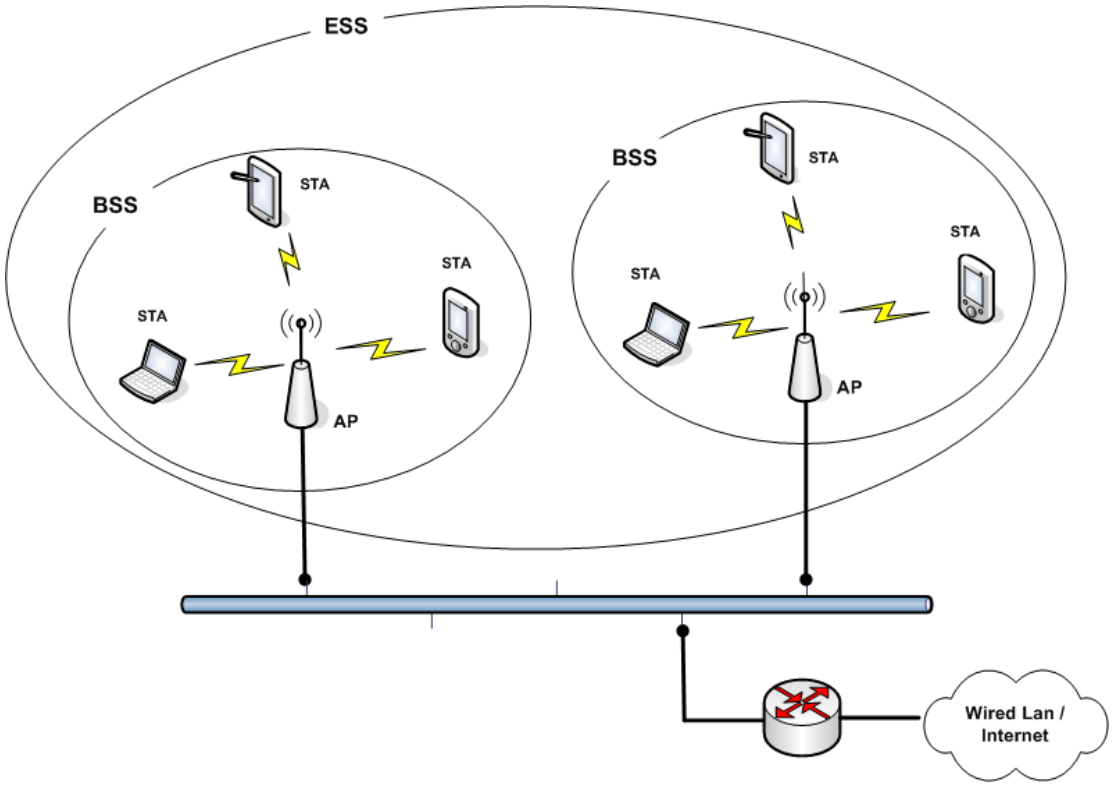
- Συμπληρωματικό του MAC επιπέδου για τη βελτίωση της ασφάλειας.
- Εφαρμόζει στο 802.11 τα φυσικά πρότυπα a,b και g.
- Εμπλουτίζει την ασφάλεια και την πιστοποίηση (authentication) με νέες μεθόδους κρυπτογράφησης.
- Διαφορετικό από το WEP.
- Εκδόθηκε το 2002.

IEEE 802.11n

- At least 100 Mbps at MAC user layer ⇒ 200+ Mbps at PHY ⇒ 4x to 5x faster than 11a/g(802.11a/g have 54 Mbps over the air and 25 Mbps to user)
- Uses multiple input multiple output antenna (MIMO)
- Data rate and range are enhanced by using spatial multiplexing (N antenna pairs) plus antenna diversity
- Occupies one WLAN channel, and in compliance with 802.11
- Backwards compatible with 802.11 a,b,g
- One access point supports both standard WLAN

Διατάξεις WLAN

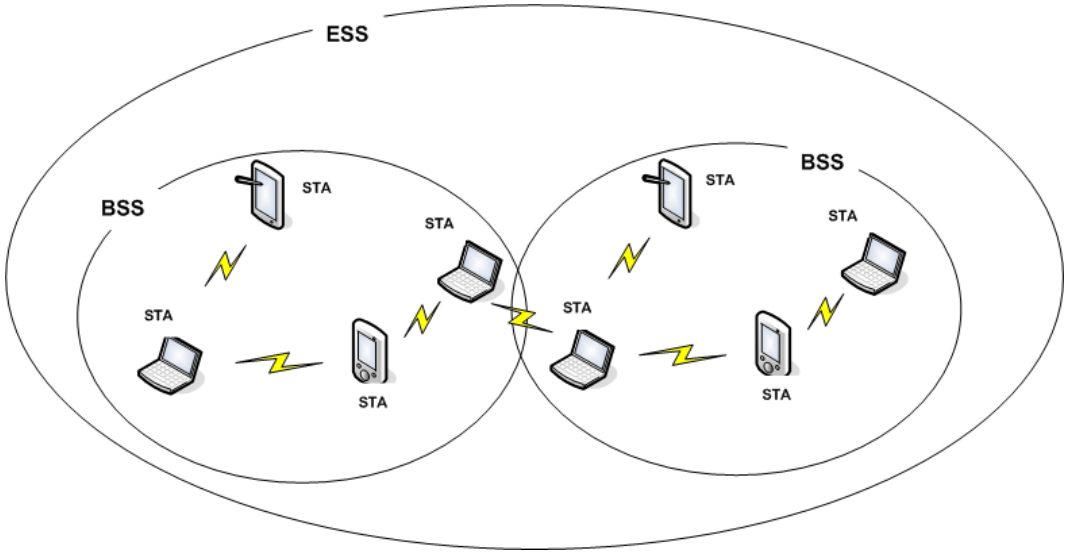
- Infrastructure WLAN



AP: Access Point
STA: Station
BSS: Basic Service Set
ESS: Extended Service Set

Διατάξεις WLAN

- Ad-hoc WLAN

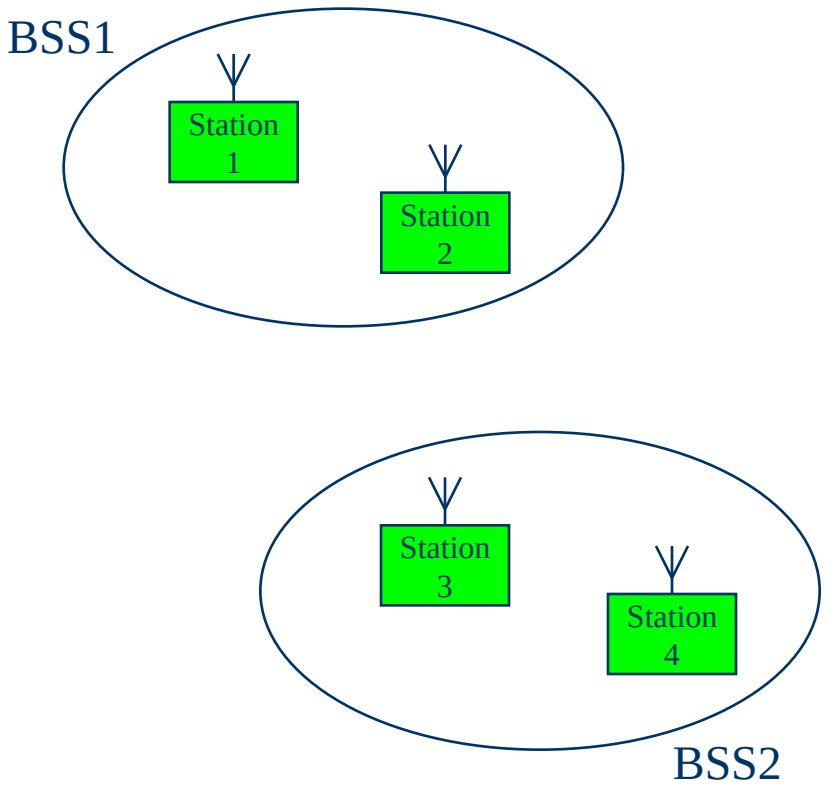


- Δεν περιλαμβάνονται APs.
- Τα τερματικά επικοινωνούν μεταξύ τους απευθείας (peer-to-peer).
- Κάθε τερματικό επικοινωνεί με τα υπόλοιπα μέσω ενός μονοπατιού που συντίθεται από τα τερματικά ενός ή περισσότερων BSS.

Τοπολογία 802.11

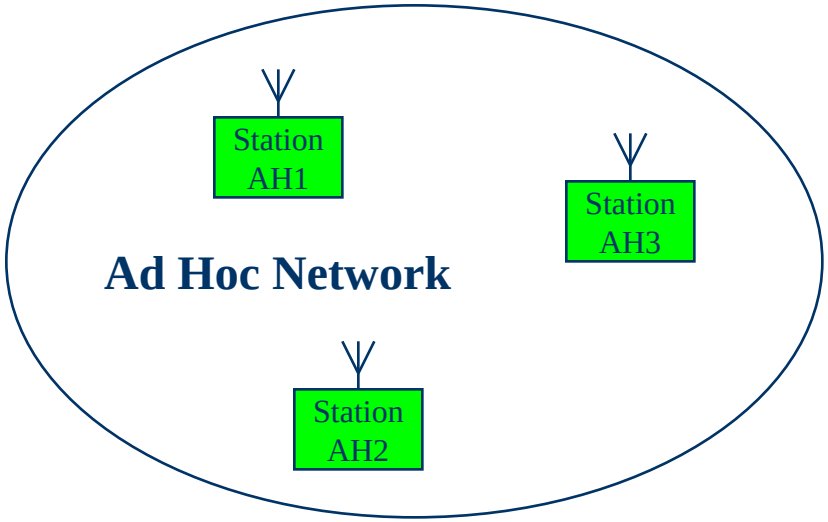
- Αποτελείται από στοιχεία που αλληλεπιδρούν ώστε να παρέχουν ένα ασύρματο τοπικό δίκτυο που να παρέχει τη δυνατότητα μετακίνησης των σταθμών η οποία να μην γίνεται αντιληπτή από τα ανώτερα στρώματα, όπως το LLC.
- Οι λειτουργίες του 802.11 ενυπάρχουν (reside) σε μια ασύρματη κάρτα δικτύου NIC (Network Interface Card), το λογισμικό διασύνδεσης που οδηγεί την κάρτα NIC και τον σταθμό βάσης ή AP (Access Point).
- BSS (Basic Service Set)
- IBSS (Independent BSS)
- ESS (Extended Service Set)

Τοπολογία BSS



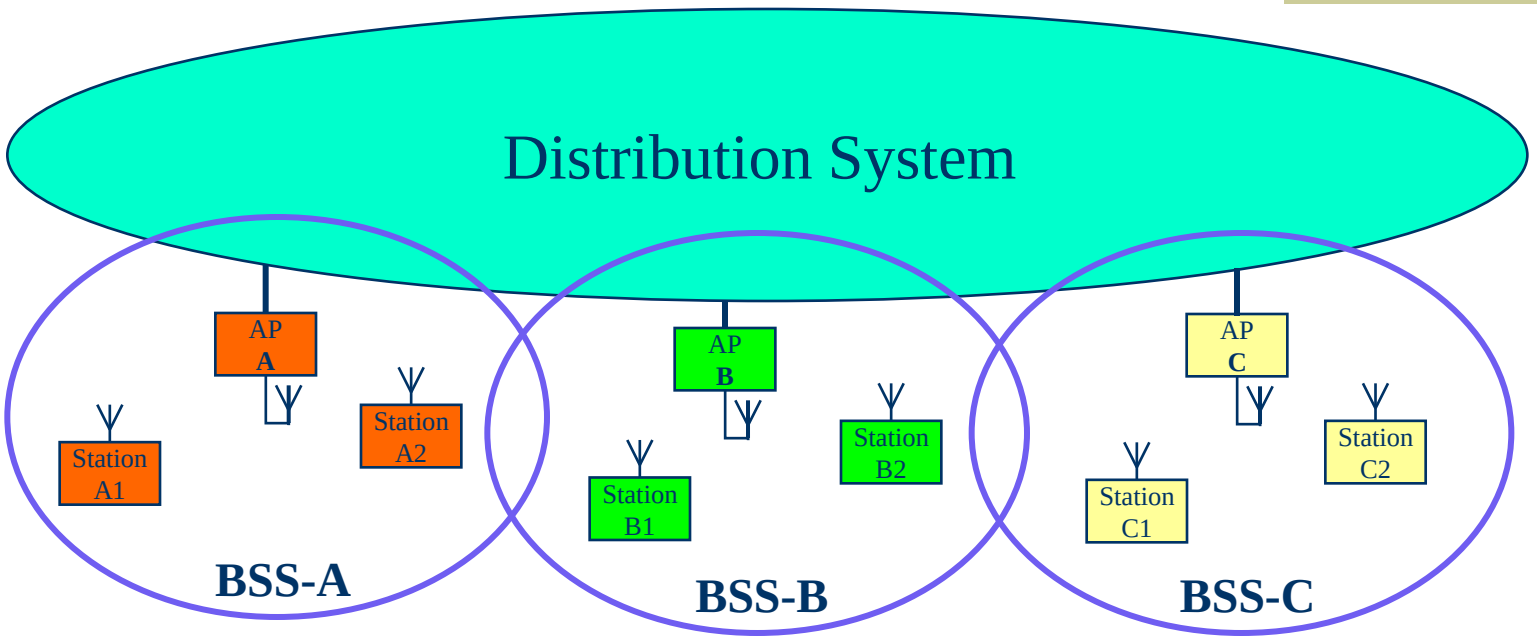
- Βασικό δομικό στοιχείο.
- Κάθε BSS έχει δύο σταθμούς οι οποίοι είναι μέλη του BSS.
- Αν κάποιος σταθμός μετακινηθεί έξω από το BSS στο οποίο ανήκει δεν μπορεί πλέον να επικοινωνεί με άμεσα με τα άλλα μέλη του συγκεκριμένου BSS.

Τοπολογία IBSS



- Ένα "Basic Service Set", BSS
- "Ad Hoc" δίκτυο
- Απευθείας επικοινωνία
- Περιορισμένη ραδιοκάλυψη

Τοπολογία ESS



- Σύνθετο δίκτυο όπου είναι δυνατή η διασύνδεση των BSSs μέσω του DS.
- Το 802.11 κάνει διαχωρισμό μεταξύ του ασύρματου μέσου WM (wireless medium) από το DSM (Distributed System Medium).
- Τα δεδομένα μετακινούνται μεταξύ ενός BSS και του DS μόνο μέσω του AP.

Τοπολογία ESS

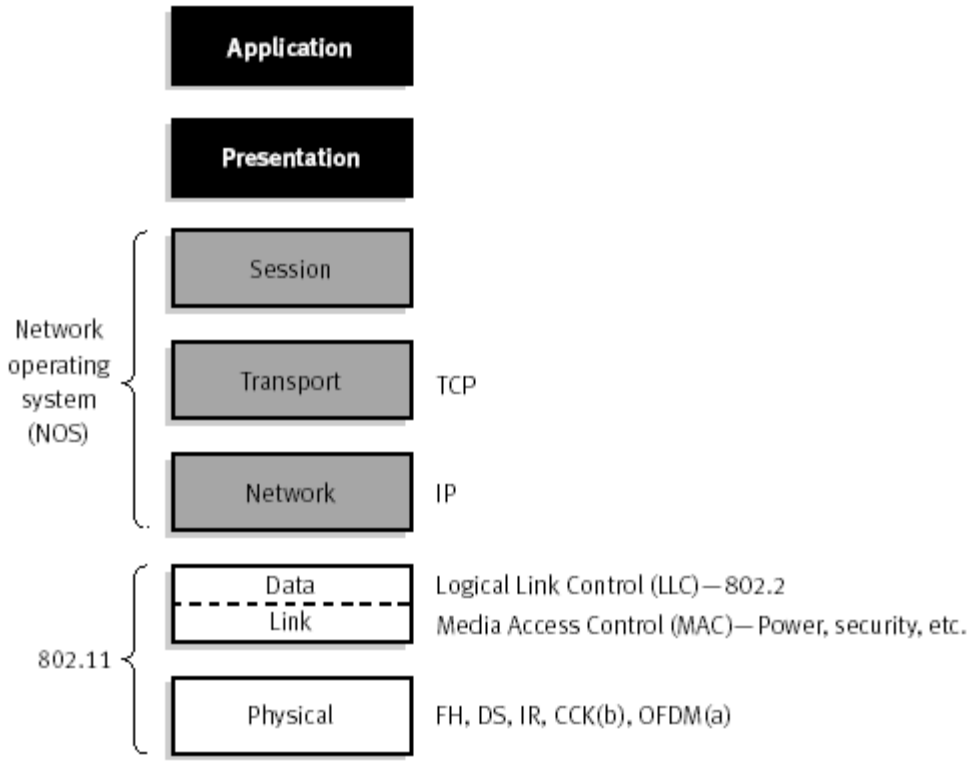
- Το DS υποστηρίζει τους τύπους κίνησης του 802.11 παρέχοντας υπηρεσίες ικανές να ελέγχουν την αντιστοίχιση (mapping) της διεύθυνσης στον προορισμό για κάθε σταθμό που μετακινείται.
- Οι σταθμοί μέσα στο ίδιο ESS μπορούν να μετακινούνται από ένα BSS σε ένα άλλο διαφανώς ως προς το LLC (Logical Link Control).
- Τα ESS δίκτυα αναφέρονται και ως infrastructure δίκτυα.
- 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.

Τοπολογία 802.11

- 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 BSSμέσα 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.

Πρωτόκολλα WLAN



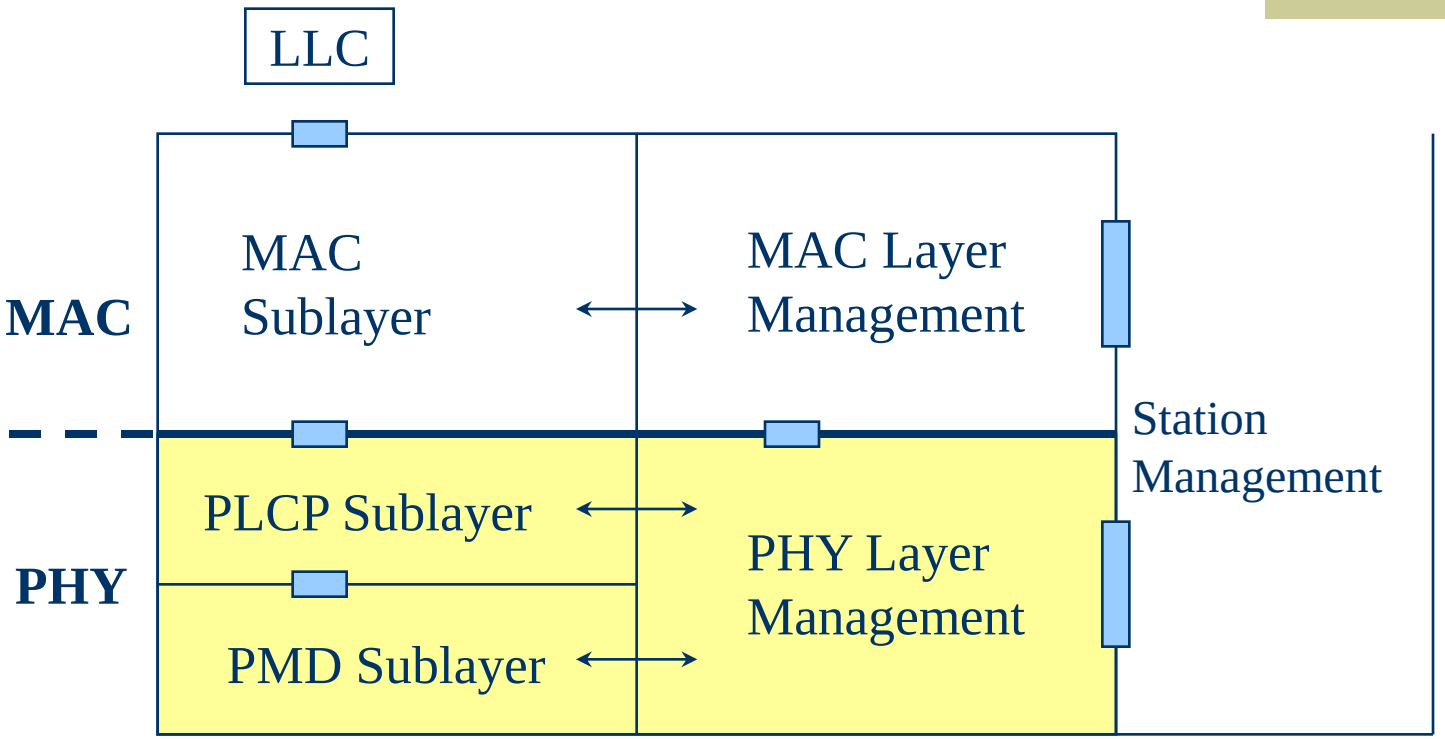
Data Link Layer

- LLC: Logical Link Control
- MAC: Medium Access Control

Physical Layer

- PLCP: Physical Layer Convergence Protocol
- PMD: Physical Medium Dependent

Αρχιτεκτονική Φυσικού Στρώματος



PHY : Physical Layer
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent

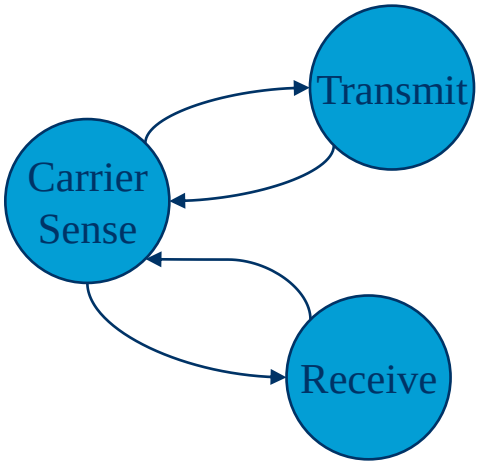
Αρχιτεκτονική Φυσικού Στρώματος

- **PLM** (Physical Layer Management)
  - Η συνιστώσα αυτή λειτουργεί σε συνεργασία με το υποστρώμα διαχείρισης MAC και εκτελεί λειτουργίες διαχείρισης για το φυσικό στρώμα.
- **PLCP** (Physical Layer Convergence Procedure) υποστρώμα
  - Το υποστρώμα MAC επικοινωνεί με το PLCP μέσω στοιχείων υπηρεσίας (service primitives) με τη βοήθεια των SAPs (Service Access Points) του φυσικού στρώματος. Όταν το υποστρώμα MAC δώσει εντολή, το PLCP ετοιμάζει τα **MPDUs (**MAC Protocol Data Units) 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) υποστρώμα
  - 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.

Λειτουργίες Φυσικού Στρώματος

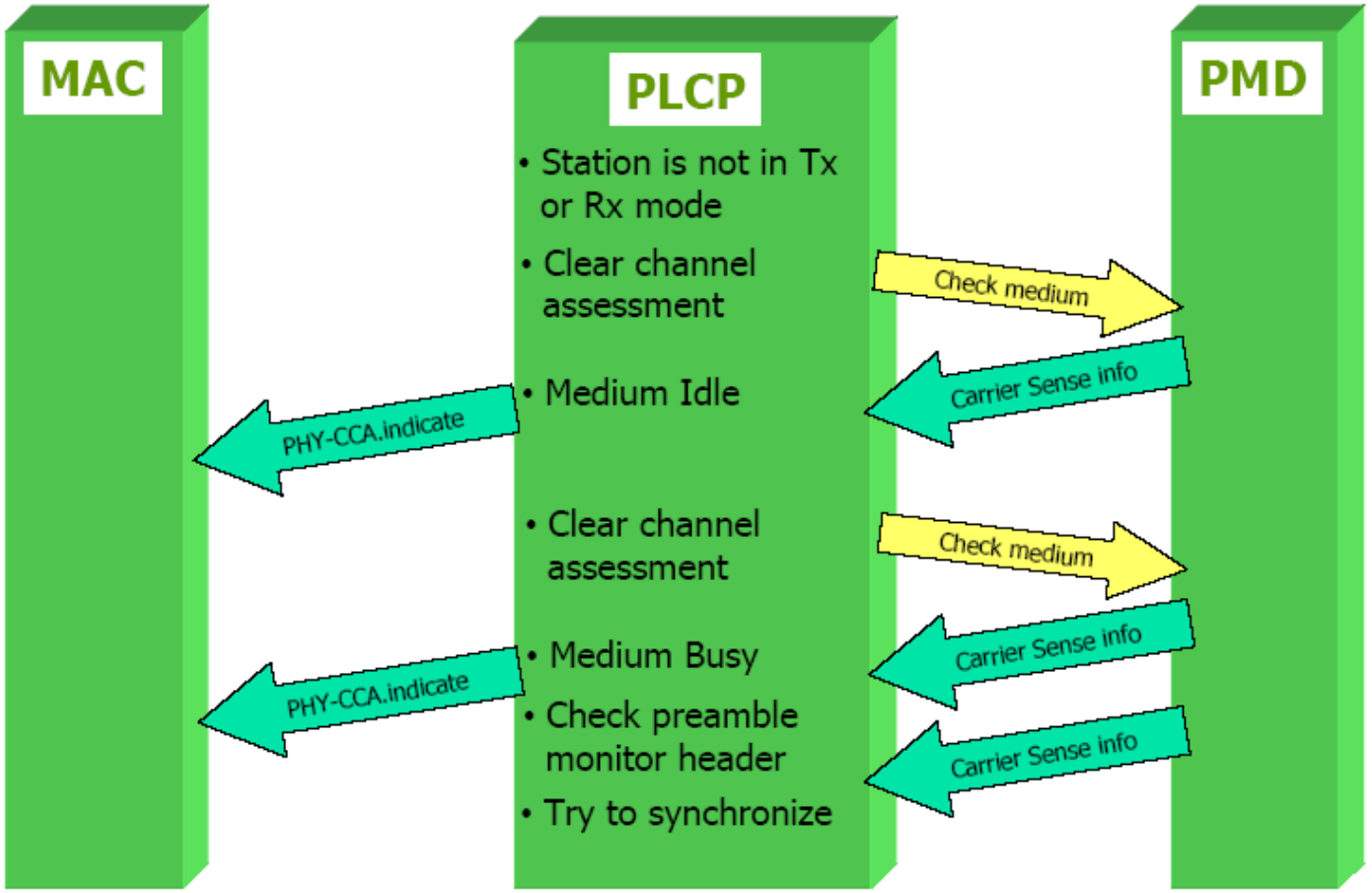
- Για την εκτέλεση των λειτουργιών του υποστρώματος PLCP, το 802.11 καθορίζει την χρήση των μηχανών κατάστασης (state machines). Κάθε μηχανή κατάστασης εκτελεί μία από τις παρακάτω λειτουργίες:
  - Ανίχνευση φέροντος: Η λειτουργία αυτή αφορά τον καθορισμό της κατάστασης του μέσου
  - Μετάδοση: Η λειτουργία αυτή αναφέρεται στην αποστολή των διαδοχικών bytes ενός πλαισίου δεδομένων.
  - Λήψη: Η λειτουργία αυτή αναφέρεται στην λήψη διαδοχικών bytes ενός πλαισίου δεδομένων



Λειτουργία Ανίχνευσης 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).

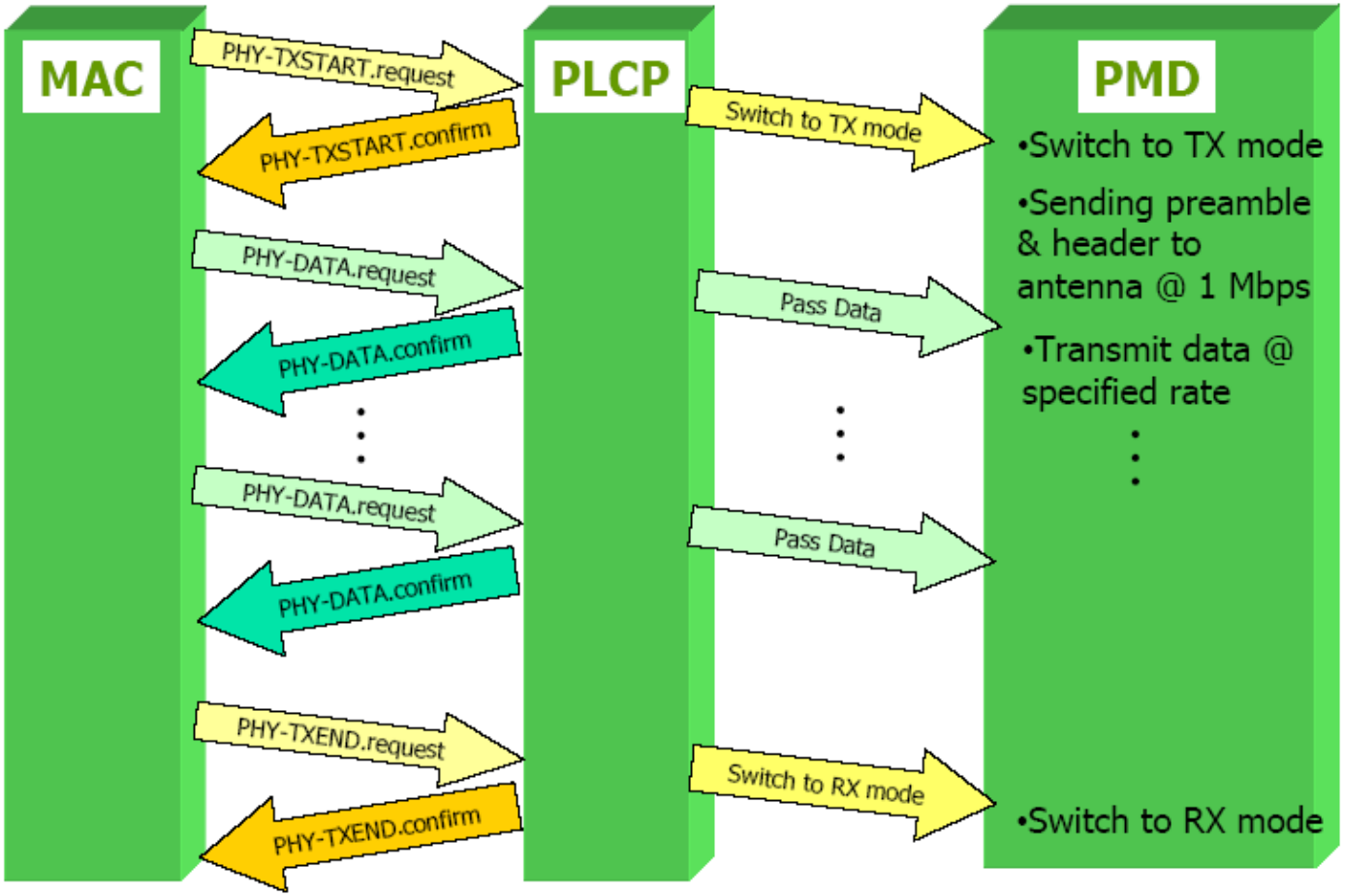
Λειτουργία Ανίχνευσης Φέροντος



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.

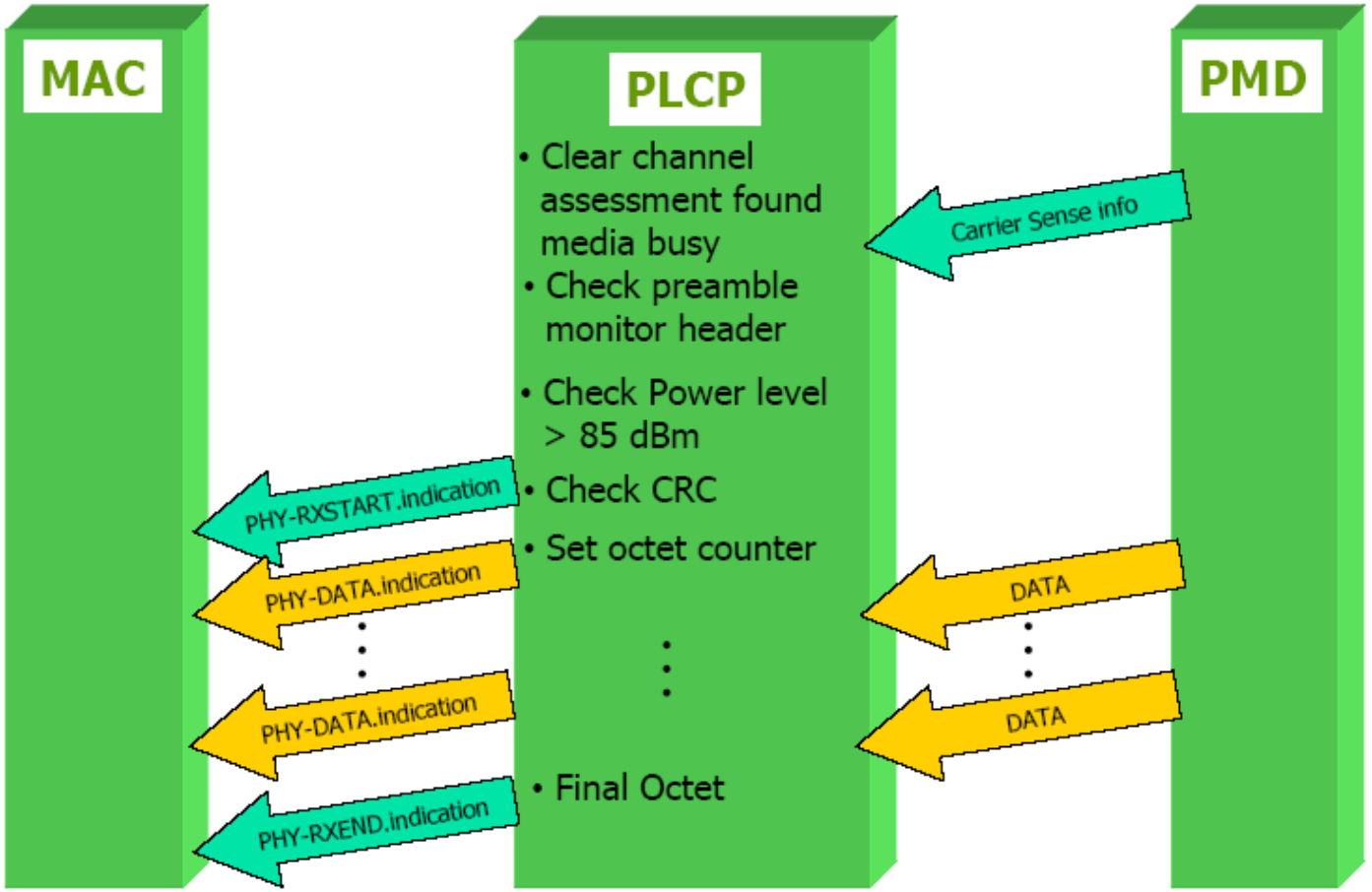
Λειτουργία Μετάδοσης



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 ‘PLCP Service Data Unit (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.

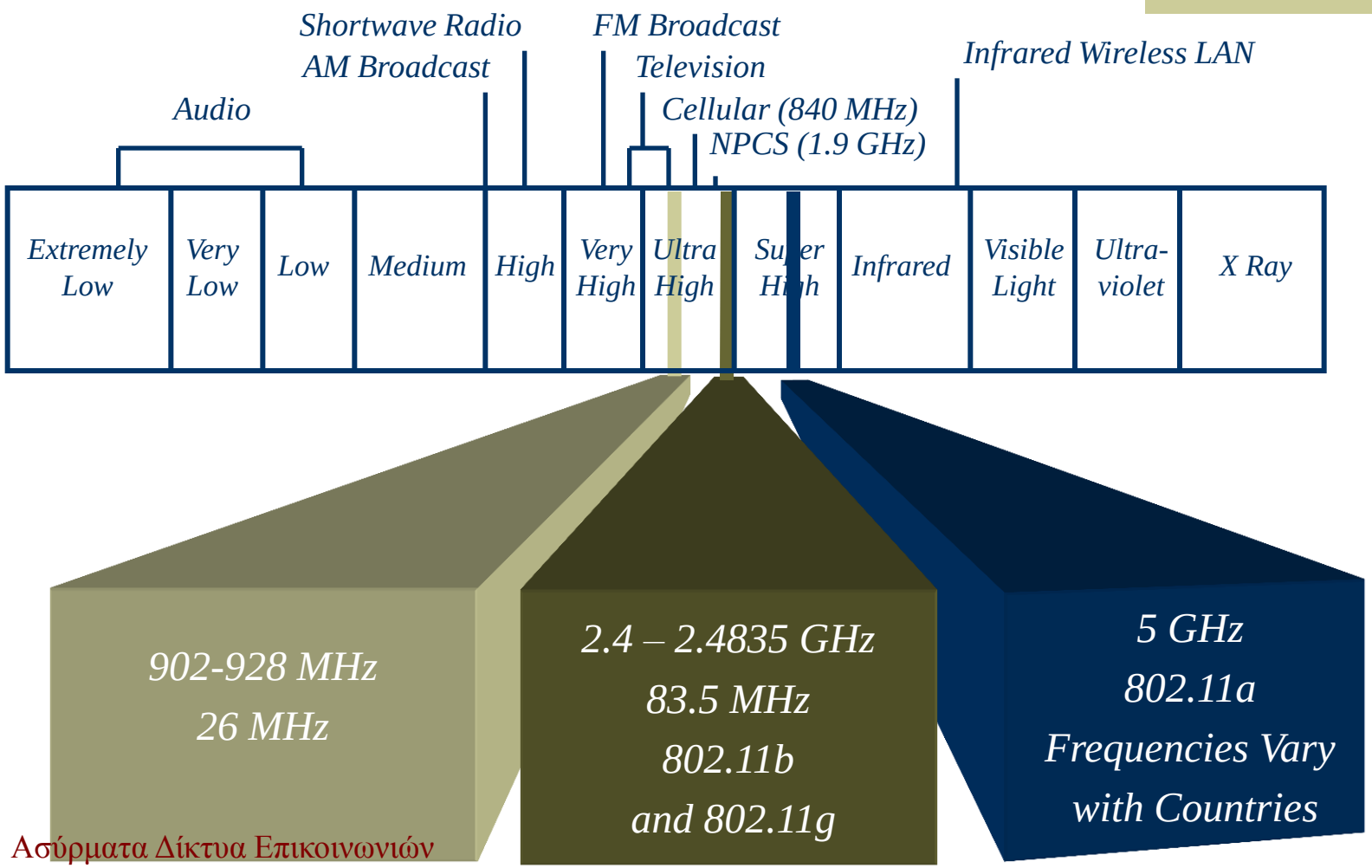
Λειτουργία Λήψης



Μέσα Μετάδοσης WLAN

- Μέσο μετάδοσης
  - Radio frequency (RF)
  - Infrared (IR)
- Direct Sequence Spread Spectrum (DSSS)
  - 2.4GHz band, 1, 2, 5.5 or 11 Mbps transmission
  - DBPSK, DQPSK
  - 11 chip Barker sequence
- Frequency Hop Spread Spectrum (FHSS)
  - 2.4GHz band, 1 and 2 Mbps transmission
  - 2GFSK, 4GFSK
  - Hop over 79 channels (North America)
- Orthogonal Frequency Division Multiplexing (OFDM)
  - 2.4GHz & 5GHz, 6 to 54 Mbps
  - No Spread Spectrum
- Baseband IR
  - Diffuse infrared
  - 1 and 2 Mbps transmission, 16-PPM and 4-PPM

ISM Band (Industrial Scientific Medical)



Οικογένεια Προτύπων 802.11

	802.11b	802.11a	802.11g
Μέγιστος ρυθμός μετάδοσης (Mbps)	11	54	54
Τύπος διαμόρφωσης	CCK	OFDM	CCK & OFDM
Υποστηριζόμενοι ρυθμοί μετάδοσης	1, 2, 5.5, 11Mbps	6, 9, 12, 18, 24, 36, 48, 54Mbps	OFDM: 6, 9, 12, 18, 24, 36, 48, 54Mbps CCK: 1, 2, 5.5, 11Mbps
Συχνότητες	2.4 – 2.497 GHz	5.15-5.35GHz 5.425-5.675GHz 5.725-5.875GHz	2.4 – 2.497 GHz

CCK: Complementary Code Keying

Οικογένεια Προτύπων 802.11

		802.11b @2.4 GHz		802.11g @2.4 GHz		802.11a @5.2 GHz	
Rate, Mbps	Single/Multi Carrier	Mandatory	Optional	Mandatory	Optional	Mandatory	Optional
1	Single	Barker		Barker			
2	Single	Barker		Barker			
5.5	Single	CCK	PBCC	CCK	PBCC		
6	Multi			OFDM	CCK-OFDM	OFDM	
9	Multi				OFDM, CCK-OFDM		OFDM
11	Single	CCK	PBCC	CCK	PBCC		
12	Multi			OFDM	CCK-OFDM	OFDM	
18	Multi				OFDM, CCK-OFDM		OFDM
22	Single				PBCC		
24	Multi			OFDM	CCK-OFDM	OFDM	
33	Single				PBCC		
36	Multi				OFDM, CCK-OFDM		OFDM
48	Multi				OFDM, CCK-OFDM		OFDM
54	Multi				OFDM, CCK-OFDM		OFDM

PBCC: Packet Binary Convolutional Code

Γιατί διαφορετικές διαμορφώσεις;

- Έχουμε τέσσερις (4) διαφορετικές διαμορφώσεις.
- Όσο πάμε προς μεγαλύτερες διαμορφώσεις αυξάνεται ο αριθμός των bits που μεταφέρονται σε κάθε σύμβολο, τόσο αυξάνεται ο ρυθμός μετάδοσης της πληροφορίας, αφού η διάρκεια κάθε συμβόλου είναι η ίδια (4μsec).
- Από την άλλη τόσο αυξάνεται η ισχύς που απαιτείται να έχει το σήμα (δηλαδή η ευαισθησία του δέκτη γίνεται χειρότερη), αφού έχουμε περισσότερες τιμές για ένα σύμβολο, άρα πιο δύσκολο για το δέκτη να ξεχωρίσει τα σύμβολα .
- Υπάρχει δηλαδή ένα trade-off ρυθμού μετάδοσης, ισχύος ή ρυθμού μετάδοσης – εμβέλειας.
- Βασικό χαρακτηριστικό των 802.11b/a/g η προσαρμογή του ρυθμού (rate adaptation) με το οποίο μπορούμε να ανταλλάξουμε ρυθμό για εμβέλεια ή/και ποιότητα ζεύξης.

Υποστρώμα PMD DSSS

- 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.
- 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.
- Τα επίπεδα ισχύος για μετάδοση με DSSS είναι:
  - 1000 mWatts για τις ΗΠΑ
  - 100 mWatts για την Ευρώπη
  - 10 mWatts για την Ιαπωνία

Υποστρώμα PMD DSSS

- Μηχανισμός Direct Sequence Spread Spectrum
  - Τα σύμβολα του χρήστη πολλαπλασιάζονται (XOR) με μία ψευδοτυχαία (PN) ακολουθία ή ακολουθία chip.
  - Τα σύμβολα έχουν περίοδο t_s
  - Τα chips έχουν περίοδο t_c
  - Spreading factor ή processing gain $G= t_s/ t_c$
  - Αν το αρχικό σήμα θέλει εύρος W, το απλωμένο σήμα θέλει εύρος GW.
- Τα WLANs που χρησιμοποιούν DSSS (αλλά όχι CDMA) χρειάζονται μικρό σχετικά spreading factor.
  - π.χ., οι χρήστες 802.11 χρησιμοποιούν μία 11-bit PN ακολουθία.

Υποστρώμα PMD DSSS

- Ένας διαμορφωτής διαμορφώνει το εξαπλωμένο PPDU συνδυάζοντάς το με ένα φέρον ρυθμισμένο 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 Mbps: DBPSK (Differential Binary Phase Shift Keying)
  - 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.
- Οι αλλαγές στη φάση διατηρούν τις πληροφορίες που βρίσκονται στο σήμα.
- Η χρήση του συγκεκριμένου τύπου διαμόρφωσης μειώνει τις παρεμβολές (interference), καθώς ο θόρυβος συνήθως επηρεάζει το πλάτος του σήματος και όχι τη φάση.

Υποστρώμα PMD FHSS

- Το υποστρώμα PMD (Physical Medium Dependent) εκτελεί την πραγματική μετάδοση και λήψη των PPDUs υπό την καθοδήγηση του PLCP.
- 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).
- Καθορίζει έναν αριθμό καναλιών (79 για την Β. Αμερική και για τις περισσότερες χώρες της Ευρώπης) που ισοκατανέμονται στην ISM-Band 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.

Υποστρώμα PMD FHSS

- Το συνολικό διαθέσιμο εύρος συχνοτήτων χωρίζεται σε μικρότερα ευρυζωνικά κανάλια (μαζί με τα guard spaces).
- Ο πομπός και ο δέκτης ‘μεταπηδούν’ (“hop”) μεταξύ διαφορετικών καναλιών.
  - Ο χρόνος σε κάθε κανάλι είναι το dwell time, t_D
  - Η μορφή του καναλιού (channel pattern) είναι η ακολουθία hopping.
- Διατάξεις (schemes)
  - Slow hopping: μερικά σύμβολα εκπέμπονται πριν την αλλαγή καναλιών ($t_D = n \times t_S$) (*Απλούστερο hardware με πολλές αντοχές, άρα μικρό κόστος*).
  - Fast hopping: μερικά σύμβολα χρειάζονται για την εκπομπή ενός συμβόλου ($t_S = n \times t_D$) (*Απαιτεί πολύ καλό συγχρονισμό, άρα υψηλό κόστος, αλλά ανοχή σε παρεμβολές στενής ζώνης και στο frequency selective fading*).
- Στις ΗΠΑ ο ελάχιστος ρυθμός είναι 2.5 hops/sec ο οποίος αντιστοιχεί σε ένα μέγιστο dwell time ίσο με 400 ms.
- 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.

Υποστρώμα PMD 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 Mbps: 2-level GFSK
  - 2 Mbps: 4-level GFSK
- Για ρυθμό δεδομένων ίσο με 1Mbps, το PMD χρησιμοποιείται η 2-level Gaussian Frequency Shift Key (**GFSK**) διαμόρφωση. 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

Σύγκριση DSSS και FHSS

Σύστημα	Πλεονεκτήματα	Μειονεκτήματα
DSSS	- Μεγαλύτερες ανοχές σε multipath και fading - Δυσκολότερα ανιχνεύεται και παρεμβάλλεται - Δυνατότητες για CDMA και adaptive τεχνικές	- Πιο μεγάλο κόστος - Χρειάζεται ευρυζωνικό κανάλι - Απαιτεί μεγάλο χρόνο ανάκτησης - Πρόβλημα near/far
FHSS	- Χρησιμοποιεί μόνο μέρος του φάσματος - Ευκολότερη υλοποίηση - Μικρό κόστος υλοποίησης	- Σύνθετος frequency synthesizer - Ανώφελο για μετρήσεις range-rate - Χρειάζεται Error correction

OFDM

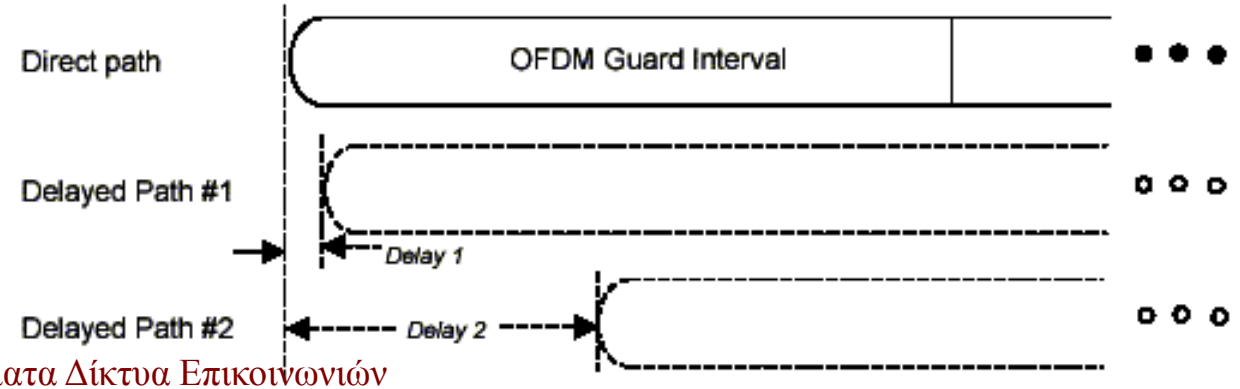
- Η μέθοδος OFDM που προτιμήθηκε από την IEEE 802.11a είναι παρόμοια με την τεχνική διαμόρφωσης που υιοθετήθηκε από την προδιαγραφή ETSI HIPERLAN II 5 GHz radio PHY.
- Η βασική αρχή είναι ο διαχωρισμός του σήματος high-speed binary και η μετάδοσή του σε έναν αριθμό από subcarriers μικρότερου ρυθμού.
- Υπάρχουν 48 data subcarriers και 4 carrier pilot subcarriers για ένα σύνολο από 52 μη-μηδενικά subcarriers προσδιορισμένα στην IEEE 802.11a. Κάθε ένα από τα lower data rate bit stream χρησιμοποιείται στη διαμόρφωση ενός ξεχωριστού subcarrier από ένα εκ των καναλιών στη ζώνη των 5 GHz.
- Η διασυμβολική παρεμβολή (Intersymbol interference - ISI) δεν είναι γενικά πρόβλημα για lower speed carrier, αλλά τα subchannels μπορούν να υποπέσουν σε frequency selective fading. Έτσι, διεμπλοκή (bit interleaving) και συνελικτική κωδικοποίηση (convolutional encoding) χρησιμοποιούνται για να βελτιωθεί η απόδοση του bit error rate.

OFDM

- Η διάταξη χρησιμοποιεί ακέραια πολλαπλάσια του πρώτου subcarrier, τα οποία είναι ορθογώνια μεταξύ τους.
- Πριν τη μετάδοση τα PPDU κωδικοποιούνται χρησιμοποιώντας ρυθμό συνέλιξης (convolutional code) R=1/2, και τα bits αναδιατάσσονται και διεμπλέκονται (bit interleaved) για τον επιθυμητό ρυθμό. Κάθε bit τότε αντιστοιχίζονται (mapped) σε ένα μιγαδικό αριθμό σύμφωνα με τον τύπο διαμόρφωσης και υποδιαιρούνται σε 48 data subcarriers και 4 pilot subcarriers.
- Τα subcarriers ενώνονται χρησιμοποιώντας τον Inverse Fast Fourier Transform (IFFT) και εκπέμπονται.
- Στον δέκτη, το φέρον μετατρέπεται σε ένα multicarrier lower data rate form χρησιμοποιώντας τον FFT. Τα lower data subcarriers συνδυάζονται για να σχηματίσουν το high rate PPDU.

OFDM - Guard Interval

- Κάθε παλμός – σύμβολο OFDM που εκπέμπεται περιέχει ένα χρονικό διάστημα ασφαλείας (guard interval, GI).
- Η λειτουργία αυτή είναι κρίσιμη για τη λειτουργία του OFDM.
- Το χρονικό περιθώριο αυτό επιλέγεται να είναι μεγαλύτερο από τη διαφορά στις καθυστερήσεις στις διάφορες ραδιοδιαδρομές.
- Το περιθώριο αυτό επιλέγεται να είναι 800nsec.
- Κατά την επεξεργασία του σήματος στο δέκτη το GI απορρίπτεται.
- Ο παλμός που παραμένει έχει διάρκεια 3200ns=3.2μs.



Γιατί Guard Interval ;

- Ο παλμός των 3.2μsec στο δέκτη μετά την αφαίρεση του GI, είναι παντελώς ελεύθερος από διασυμβολική παρεμβολή.
- Παραμόρφωση λόγω πολλαπλών διαδρομών είναι πιθανό πλέον να συμβεί μόνο από το ίδιο σύμβολο.
- Τα αποτελέσματα των πολλαπλών διαδρομών μπορούν πλέον να αντιμετωπιστούν στο πεδίο συχνότητας.
- Αν κάποια φέρουσα έχει υποστεί αλλοίωση με ενίσχυση της και διόρθωση της φάσεως (τα οποία είναι σταθερά στην ίδια υποφέρουσα καθ' όλη τη διάρκεια του παλμού) γίνεται αντιστάθμιση του multipath φαινομένου.

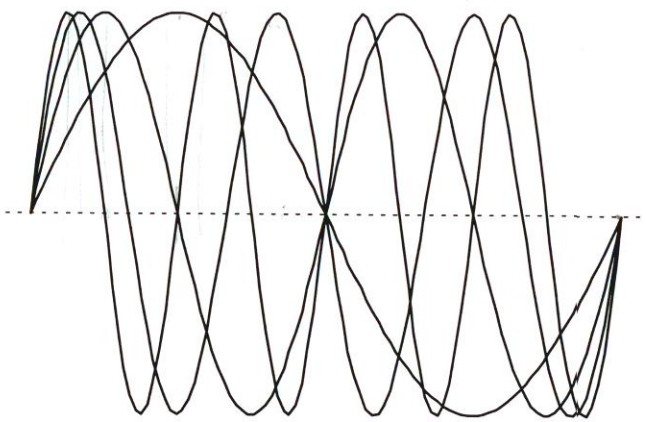
Τι είναι η ορθογωνιότητα;

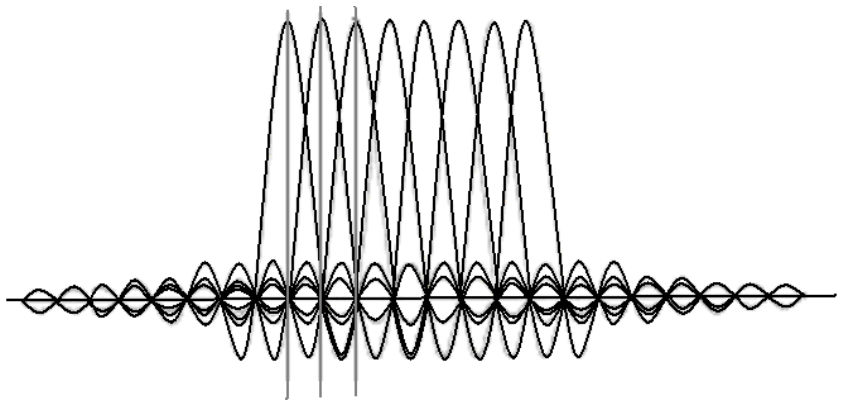
- Αν δύο σήματα είναι ορθογώνια, τότε το ολοκλήρωμα του γινομένου τους είναι μηδενικό.
- Στο πεδίο της συχνότητας ο ορθογώνιος παλμός έχει τη μορφή sinc(x) με μηδενισμούς που αντιστοιχούν σε απόσταση 1/3200ns=312.5kHz.
- Οι φέρουσες είναι σε απόσταση 312.5kHz απόσταση.
- Ο αριθμός αυτός προέκυψε διαιρώντας τον ρυθμό δειγματοληψίας του FFT, 20MHz με τον συνολικό αριθμό bins που χρησιμοποιούνται στον FFT, που είναι 64.
- Οι υποφέρουσες εκπέμπονται αφού μορφοποιηθούν με μια συνάρτηση sinx/x.
- Με την προϋπόθεση ότι οι υποφέρουσες τοποθετούνται στα σημεία μηδενισμού της συνάρτησης sinx/x, οι υποφέρουσες δεν αλληλοπαρεμβάλονται.
- Γενικά τα συστήματα με πολλές φέρουσες (multicarrier) είναι πιο αξιόπιστα στη μετάδοση από το μονής φέρουσας (single carrier).

Τι είναι η ορθογωνιότητα;

- Για να είναι ορθογώνια μεταξύ τους πρέπει να χωράει ακριβώς ακέραιος αριθμός κύκλων σε ένα χρονικό διάστημα Τ.
- Έτσι η απόσταση ανάμεσα στις συχνότητες πρέπει να είναι ακέραιο πολλαπλάσιο του 1/Τ.
- Οι φέρουσες που είναι ορθογώνιες δεν παρεμβάλουν μεταξύ τους (intercarrier interference).

Four subcarriers in one OFDM symbol





Παράμετροι Μετάδοσης

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

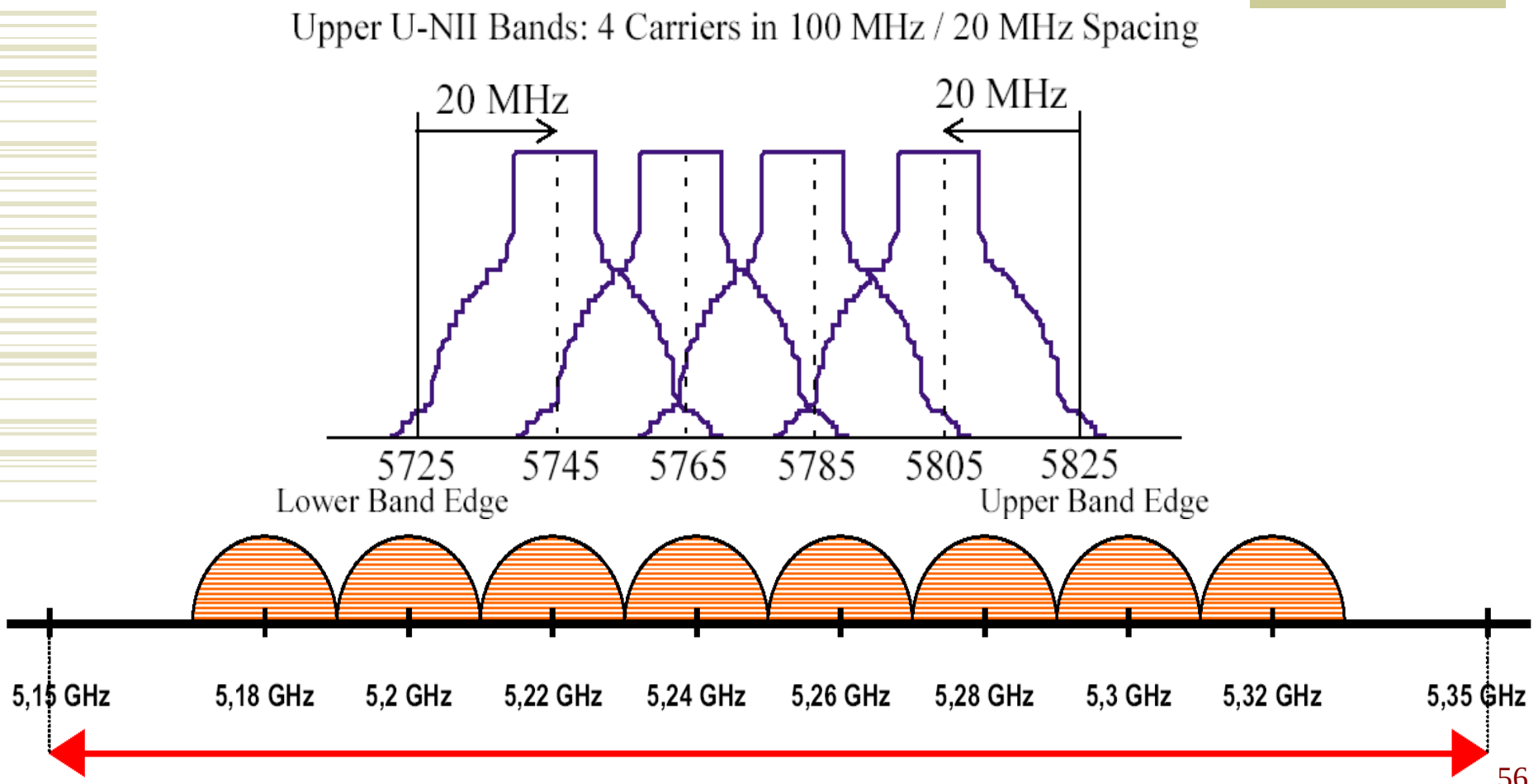
Παράμετροι Μετάδοσης

Parameter	Value
N_{SD}: Number of data subcarriers	48
N_{SP}: Number of pilot subcarriers	4
N_{ST}: Number of subcarriers, total	52 ($N_{SD} + N_{SP}$)
Δ_F: Subcarrier frequency spacing	0.3125 MHz (=20 MHz/64)
T_{FFT}: IFFT/FFT period	3.2 μs ($1/\Delta_F$)
$T_{PREAMBLE}$: PLCP preamble duration	16 μs ($T_{SHORT} + T_{LONG}$)
T_{SIGNAL}: Duration of the SIGNAL BPSK-OFDM symbol	4.0 μs ($T_{GI} + T_{FFT}$)
T_{GI}: GI duration	0.8 μs ($T_{FFT}/4$)
T_{GI2}: Training symbol GI duration	1.6 μs ($T_{FFT}/2$)
T_{SYM}: Symbol interval	4 μs ($T_{GI} + T_{FFT}$)
T_{SHORT}: Short training sequence duration	8 μs ($10 \times T_{FFT}/4$)
T_{LONG}: Long training sequence duration	8 μs ($T_{GI2} + 2 \times T_{FFT}$)

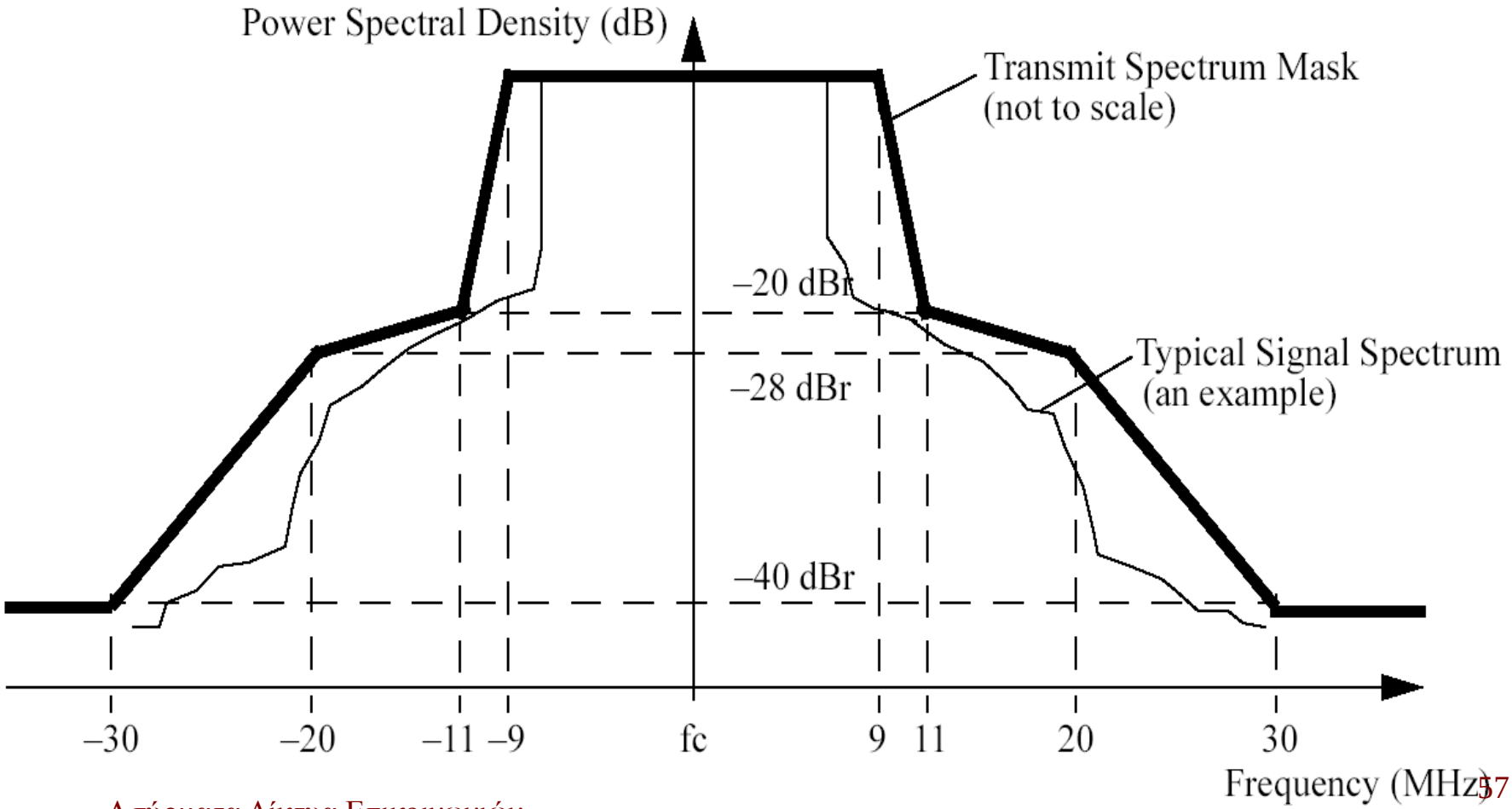
Πόσα κανάλια είναι διαθέσιμα;

- 802.11b/g
  - 11 κανάλια (Ν Αμερική) – 13 κανάλια (Ευρώπη) , κάθε κανάλι έχει εύρος 22MHz, έχουν απόσταση 5MHz μεταξύ τους
  - Κεντρικές συχνότητες 2.412MHz ... 2.462GHz
  - Τρία μόνο κανάλια δεν επικαλύπτονται, τα 1, 6 ,11
- 802.11a
  - 12 κανάλια, εύρους 20MHz, σε απόσταση 20MHz μεταξύ τους σε τρεις ζώνες συχνοτήτων:
    - lower-middle → 5.180GHz-5.320GHz
    - upper → 5.745GHz-5.805GHz
  - Δεν υπάρχει επικάλυψη ανάμεσα στα κανάλια
  - Η χαμηλότερη ζώνη προορίζεται για χρήση σε εσωτερικό χώρο, ενώ η υψηλότερη σε εξωτερικό
  - Δεν είναι υποχρεωτικό για μια συσκευή να καλύπτει και τις τρεις ζώνες

802.11a, Lower & Middle U-NII bands



802.11a/g, μάσκα φάσματος συχνοτήτων πομπού



Ελάχιστες προδιαγραφές δέκτη 802.11a/g

Data rate (Mbits/s)	Minimum sensitivity (dBm)	Adjacent channel rejection (dB)	Alternate adjacent channel rejection (dB)
6	–82	16	32
9	–81	15	31
12	–79	13	29
18	–77	11	27
24	–74	8	24
36	–70	4	20
48	–66	0	16
54	–65	–1	15

Ελάχιστες προδιαγραφές δέκτη 802.11a/g

- Ορίζεται η ευαισθησία για ρυθμό λανθασμένων πακέτων – PER, packet error rate 10% με μέγεθος πακέτου 1000 bytes, ο οποίος και αντιστοιχεί σε ρυθμό λαθών περίπου BER=$10^{-5.}$
- Η IEEE δίνει τιμές υποθέτοντας δέκτη με NF=10 dB και κατασκευαστικό περιθώριο υλοποίησης 5 dB (λόγω ανοχών στα στοιχεία, ατελειών στην υλοποίηση, κτλ.).
- Μετράται η απόρριψη γειτονικού καναλιού, θέτοντας την ισχύ σε επίπεδο 3dB μεγαλύτερο από την ευαισθησία του δέκτη, όπως ορίζεται στον πίνακα, και αυξάνοντας την ισχύ του γειτονικού καναλιού μέχρι να παρατηρηθεί ρυθμός λανθασμένων πακέτων (1000bytes), PER = 10% .
- Η διαφορά στη ισχύ του γειτονικού καναλιού από το κανάλι λήψης ορίζεται τότε ως η απόρριψη γειτονικού καναλιού.
- Ως alternate adjacent channel rejection ορίζεται η εναλλακτική απόρριψη του γειτονικού καναλιού (+16dBr).

Πόσο αποδοτικά χρησιμοποιούμε το φάσμα;

- Σημαίνει αν η διαμόρφωση, η τεχνολογία και τα υλικά είναι τέτοιων προδιαγραφών, ώστε η ισχύς που απαιτούν οι συσκευές για να αποδιαμορφώσουν είναι κοντά στη βέλτιστη τιμή.
- Το ερώτημα είναι βασικό διότι το φάσμα είναι ακριβό (άσχετα αν είναι ελεύθερο για χρήση) και είναι πεπερασμένος πόρος.

Θεώρημα Shannon

- Ο ρυθμός πληροφορίας R (bits/sec) που μπορεί να σηκώσει ένας δίαυλος με εύρος BW (Hertz) δίνεται από τη σχέση:

$$R=BW \log (1+S/N) ,$$

- Όπου S/N είναι ο σηματοθορυβικός λόγος στο δίαυλο, δηλαδή η ισχύς του χρήσιμου σήματος προς το θόρυβο.

Διαμορφώσεις και απαιτούμενο SNR (BER 10^{-6})

Δηλαδή πόση πρέπει να είναι η διαφορά του χρήσιμου σήματος από το θόρυβο ώστε να γίνεται αποδιαμόρφωση του σήματος με ένα συγκεκριμένο ρυθμό λαθών.

FSK	2-state	13.4	B
	3-state	15.9	B
	4-state	23.1	B/2
PSK	2-state	10.5	B
	4-state	13.5	B/2
	8-state	18.8	B/3
	16-state	24.4	B/4
QAM	16-QAM	20.5	B/4
	32-QAM	23.5	B/5
	64-QAM	26.5	B/6
	128-QAM	29.5	B/7
	256-QAM	32.5	B/8
	512-QAM	35.5	B/9
FEC (QAM) WITH BLOCK CODES r=6.7%	16-QAM	17.6	B/4(1+r)
	32-QAM	20.6	B/5(1+r)
	64-QAM	23.6	B/6(1+r)
	128-QAM	26.7	B/7(1+r)
	256-QAM	29.8	B/8(1+r)
	512-QAM	32.4	B/9(1+r)
BCM	16BCM-8D	18.5	B/3.75
	80BCM-8D	28.4	B/6
	88BCM-6D	28.8	B/6
	96BCM-4D	29	B/6
	128BCM-8D	28.2	B/6
TCM	16TCM-2D	14.3	B/3
	32TCM-2D	17.6	B/4
	64TCM-4D	21.9	B/5.5
	128TCM-2D	23.6	B/6
	128TCM-4D	24.9	B/6.5
	512TCM-2D	29.8	B/8
	512TCM-4D	31.1	B/8.5
MLCM	32-MLCM-2D	18.3	B/4.5
	64-MLCM-2D	21.7	B/5.5
	128-MLCM-2D	24.5	B/6.5

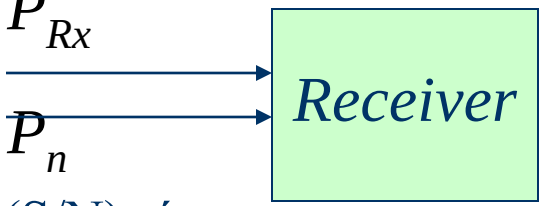
Ευαισθησία δέκτη

- P_{Rx} είναι η ισχύς του χρήσιμου σήματος στην είσοδο του δέκτη σε dBm
- P_n είναι η ισχύς θορύβου ανηγμένη στην είσοδο του δέκτη σε dBm.
- Υπολογίζεται αθροίζοντας όλες τις πηγές θορύβου εντός του δέκτη και βρίσκοντας την ισοδύναμη πηγή θορύβου στην είσοδο του δέκτη
- Αν το εύρος του διαύλου είναι BW και NF ο συντελεστής θορύβου, τότε:

$$P_n = NF \cdot K \cdot T \cdot BW$$

- ή σε dBm

$$P_n(dBm) = NF(dB) - 113.8 + 10\log(BW(MHz))$$



- Έτσι ο σηματοθορυβικός λόγος Signal to Noise (S/N) είναι :

$$S/N(dB) = P_{RX} - P_n = P_{RX} - \left(NF(dB) - 113.8 + 10\log(BW(MHz))\right)$$

Κατώφλι δέκτη

- Κάθε τρόπος διαμόρφωσης απαιτεί ένα ελάχιστο S/N για την αποδιαμόρφωση του σήματος με ένα μέγιστο ρυθμό λαθών
- Το κατώφλι του δέκτη (για έναν συγκεκριμένο ρυθμό λαθών) μπορεί να βρεθεί ως εξής :

$$P_{rx\_threshold} = NF - 113.8 + 10\log(BW(MHz)) + S/N_{\min}$$

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #1 (θόρυβος ενεργών στοιχείων)
  - Θεωρούμε ότι λόγω περιορισμών στα ηλεκτρονικά το καλύτερο NF που μπορούμε να έχουμε είναι 2dB. Θα εξετάσουμε διάφορα παραδείγματα κρατώντας σε όλα αυτόν τον περιορισμό
- Περιορισμός #2 (εύρος καναλιού)
  - Το εύρος του κάθε καναλιού είναι 20MHz, από τα οποία μόνο τα 16.5MHz έχουν χρήσιμη πληροφορία, τα υπόλοιπα μπαίνουν για να μην επικαλύπτονται τα κανάλια μεταξύ τους
  - Θεωρούμε επικοινωνία με τους προηγούμενους περιορισμούς και ιδανική διαμόρφωση αντίστοιχη της 64-QAM, αλλά με S/N όσο ορίζει το θεώρημα του Shannon (δηλαδή έχοντας την ιδανική διαμόρφωση)
  - Τότε 99Mbps=16.5MHz $\log_2(1+S/N)$ → S/N = 18dB, BER=10^{-6}
  - $P_{threshold}$ = 2-113.8+10log16.5+18 = -81.6dBm , BER=10^{-6} και R=99Mbps

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #3 (διαμόρφωση)
  - Ας θεωρήσουμε μια διαμόρφωση η οποία είναι τεχνικά εφικτή. Η 64-MLCM-2D (Multilevel Code Modulation) είναι μια διαμόρφωση που χρησιμοποιείται σε εμπορικά συστήματα υψηλής χωρητικότητας και είναι γνωστή για την αποτελεσματικότητα της
  - Χρειάζεται S/N=21.7dB, ώστε να επιτύχει ρυθμό R=BW*5.5=91, BER=10^{-6} δηλαδή με ένα μικρό αντίτιμο στο ρυθμό, πετυχαίνει μια σημαντική βελτίωση στο SNR που απαιτείται

Έτσι:

- $P_{threshold}$ = 2-113.8+10log$_2$16.5+21.7 = -77.7dBm , BER=$10^{-6,}$ R=91Mbps

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #4 (κόστος διαμορφωτή)
  - Τέτοιες διαμορφώσεις είναι ακριβές να υλοποιηθούν, προτιμάμε μια απλούστερη όπως η 64-QAM
  - Αυτή χρειάζεται S/N=26.3dB, ώστε να επιτύχει ρυθμό R=BW*6, BER=10^{-6}

  Έτσι:

  - $P_{threshold}$ = 2-113.8+10log$_2$16.5+26.5 = -73.1dBm , BER=$10^{-6,}$ R=99Mbps

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #5 (αντιμετώπιση σφαλμάτων φάσης)
  - Προκειμένου να αντιμετωπίσουμε διάφορα προβλήματα ακριβούς χρονισμού, χρησιμοποιούμε για τη μεταφορά πληροφορίας μόνο τα 15MHz, από τα 16.5MHz
  - Έτσι ο ρυθμός γίνεται 90Mbps
- Περιορισμός #6 (αντιμετώπιση διασυμβολικής παρεμβολής)
  - Για την αντιμετώπιση του φαινομένου εισάγεται ένα περιθώριο ασφαλείας – GI, Guard Interval
  - Το αποτέλεσμα είναι ότι ο ρυθμός ελαττώνεται κατά 3.2μs/4μs 90Mbps = 72Mbps

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #7 (αντιμετώπιση σφαλμάτων ραδιοεπαφής)
  - Επειδή σφάλματα θα συμβούν (η ραδιοεπαφή είναι μη αξιόπιστο μέσο μετάδοσης), εισάγουμε κώδικα διόρθωσης λαθών. Το αντίτιμο που πληρώνουμε είναι το περισσότερο overhead.
  - Έτσι, με R=3/4 (δηλ στα 3bits πληρώνουμε ένα παραπάνω) ο καθαρός ρυθμός μετάδοσης που μένει είναι R=3/4*72Mbps=54Mbps
  - Για τη θυσία αυτή έχουμε κερδίσει όμως περίπου 4dB ευαισθησία στο δέκτη που είναι τώρα $P_{threshold}$ = -77dBm , BER=10^{-6}
  - Αυτό ισοδυναμεί με περίπου $P_{threshold}$ = -78dBm , BER=10^{-5} , αντίστοιχο σε PER=10% - 1000bytes/packet

Τελικά είναι αποδοτική η 802.11g ;

- Περιορισμός #8 (κοινό μέσο πρόσβασης)
  - Επειδή έχουμε κοινό μέσο, υλοποιούμε επίπεδο ελέγχου της πρόσβασης σε αυτό (MAC)
  - Η υλοποίηση αυτή θα μειώσει ακόμα περαιτέρω τον καθαρό ρυθμό που μένει για τη μεταφορά δεδομένων σε περίπου 30Mbps
- Περιορισμός #9 (κόστος υλοποίησης)
  - Προκειμένου να απλοποιήσουμε περισσότερο τη σχεδίαση και να ρίξουμε το κόστος, αν επιτρέψουμε NF=10dB και επιπλέον απώλειες 5dB λόγω υλοποίησης θα έχουμε περαιτέρω υποβάθμιση του κατωφλιού κατά 13dB
  - Όποτε έχουμε: $P_{threshold}$ = -65dBm , PER=10% - 1000bytes/packet, R=30Mbps
  - Όσο δηλαδή δίνει η προδιαγραφή της IEEE

Τελικά είναι αποδοτική η 802.11g ;

- Από την προηγούμενη ανάλυση φαίνεται ότι οι ανοχές που έχουν δοθεί είναι πραγματικά τεράστιες και η υλοποίηση του προτύπου και των συσκευών του απέχει μακρά από τη βέλτιστη.
- Έτσι οι συσκευές που ήδη κυκλοφορούν στο εμπόριο, μπορούμε να πούμε ότι είναι σπάταλες με την έννοια ότι ρυπαίνουν πολύ περισσότερο το φάσμα για το ίδιο αποτέλεσμα (μεταφορά δεδομένων) από μία βέλτιστη τεχνικά λύση.
- Ας μην ξεχνάμε ότι η 802.11 οικογένεια προδιαγράφει συσκευές οι οποίες ουσιαστικά δεν είναι για εμπορική χρήση και για χρήση σε φάσμα το οποίο είναι ελεύθερο, και έτσι προς χάριν του κόστους και της δυνατότητας μαζικής παραγωγής, έχει επιτρέψει πολύ χαλαρές προδιαγραφές.
- Για σύγκριση παραθέτουμε τις προδιαγραφές ενός 802.11g συστήματος:

  $P_{threshold}$ = -65dBm , PER=10% - 1000bytes/packet, R=30Mbps

  και μίας SDH ραδιοεπαφής:

  $P_{threshold}$ = -72dBm , BER=10^{-6} , R=155.52Mbps

Μπορεί να γίνει κάτι;

- Ξεκινήσαμε από μία τεχνικά άψογη υλοποίηση η οποία θα είχε R=91Mbps, $P_{threshold}$ = - 77.7dBm , BER=10^{-6}
- Μετά από μία σειρά από συμβιβασμούς καταλήξαμε σε R=30Mbps, $P_{threshold}$ = -65dBm , PER=10% - 1000bytes/packet.
- Μπορούμε να περιμένουμε δέκτες οι οποίοι να είναι πολύ καλής ποιότητας και οι οποίοι φτάνουν σε ευαισθησία: $P_{threshold}$ = -75dBm , αντί για –65dBm.
- Να παρατηρήσουμε ότι αυτό σημαίνει άλλη υλοποίηση του τμήματος RF-IF.
- Τα υπάρχοντα chipsets υλοποιούν ευαισθησίες της τάξεως των –69dBm, προς χάριν της μείωσης του κόστους παραγωγής.
- Δεδομένου ότι το φάσμα είναι πλέον πολύτιμος πόρος για την υλοποίηση ασύρματων μητροπολιτικών δικτύων, συνίσταται εντόνως η μη χρήση τέτοιων συσκευών.

Μπορεί να γίνει κάτι;

- Μπορούμε να περιμένουμε κάποιον κατασκευαστή να υλοποιεί κάποιον αποτελεσματικό τρόπο διαμόρφωσης (και ακριβό – πολύπλοκο) κερδίζοντας άλλα 3dB ευαισθησίας.
- Μπορούμε να δούμε κάποιον κατασκευαστή να υλοποιεί ένα MAC επίπεδο, ουσιαστικά πιο αποδοτικό, πιο απογυμνωμένο, προορισμένο για p2p ζεύξεις, ανεβάζοντας έτσι τον καθαρό ρυθμό μετάδοσης.
- Προφανώς οι δύο τελευταίες λύσεις θα είναι σε βάρος της συμβατότητας – διαλειτουργικότητας.
- Παρ' ό,τι οι 802.11 υλοποιήσεις είναι σπάταλες όσον αφορά το φάσμα (εκπέμπουν περισσότερο απ' όσο θα χρειαζόταν μία state of the art υλοποίηση), αποτελούν μια συμφέρουσα επιλογή ανάμεσα στο κόστος και στην τεχνική αρτιότητα.
- Με απλά λόγια με τα χρήματα που κοστίζει ένας 802.11 εξοπλισμός αγοράζεις πολλαπλάσια αξίας τεχνολογία.

Σύγκριση Απόδοσης (Throughput)

	Data Rate (Mbps)	Προσεγγιστικό Throughput (Mbps)	Throughput ως ένα ποσοστό του 802.11b Throughput
802.11b	11	6	100%
802.11g (802.11b clients in cell)	54	8	133%
802.11g (no 802.11b clients in cell)	54	22	367%
802.11a	54	25	417%

- Το throughput αυξάνεται για το 802.11g όταν αυτό είναι σε λειτουργία mixed-mode και είναι σχετικά μέτρια συγκρινόμενο με το 802.11b.
- Η λειτουργία mixed-mode είναι ένα μέρος του παρεχόμενου μέρους του throughput που παρέχεται στο 802.11g όταν δεν υποστηρίζει legacy clients.

Υποστρώμα MAC

- Επιτελεί τις ακόλουθες λειτουργίες:
  - Association (passive/active scanning)
  - Data Transfer
    - CSMA / CA
    - Fragmentation / reassembly
    - Auto rate selection (fallback)
  - Authentication
  - Synchronization (beacon frames)
  - Security (Wireless Equivalent Privacy), RSA
  - Roaming / Reassociation

Υποστρώμα MAC

- **Association (passive/active scanning)**
  - Υπάρχουν δύο τρόποι ένταξης ενός νέου σταθμού σε μια κυψέλη, δηλαδή εντοπισμού του ενεργού AP καθώς και λήψης αναγκαίων στοιχείων συγχρονισμού.
    - Παθητική σάρωση (passive scanning): Ο σταθμός ανιχνεύει στο δίαυλο τα περιοδικά πλαίσια αναφοράς (beacon frames) που εκπέμπονται από τον AP.
    - Ενεργητική σάρωση (active scanning): Εκπέμπει ο ίδιος σταθμός δοκιμαστικά πλαίσια (probe frames) και περιμένει την αντίστοιχη απάντηση από τον AP.

Υποστρώμα MAC

- **Data Transfer**
  - *CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance)*
    - Χρησιμοποιείται αντί του CSMA/CD του 802.3 (Ethernet).
    - Ακούει πριν εκπέμψει (listen before transmit).
    - Δε βασίζεται στην αναγνώριση κατάστασης σύγκρουσης από τον εκπέμποντα σταθμό αλλά στην αποστολή πακέτων RTS/CTS και στην επιβεβαίωση σωστής λήψης (ACK) από το σταθμό προορισμού.
  - *Διαχωρισμός / επανένωση πακέτων* (*Fragmentation / reassembly*)
    - Ανάλογα με τις εκάστοτε συνθήκες θορύβου και παρεμβολών χωρίζεται δυναμικά σε δύο κατηγορίες:
      - Διαχωρισμός σταθερού μήκους πακέτα (fixed fragmentation)
      - Διαχωρισμός μεταβλητού μήκους πακέτα (adaptive fragmentation)
  - *Αυτόματη επιλογή ρυθμού* (*auto rate selection*)
    - Αύξηση του ρυθμού μετάδοσης μείωση της εμβέλειας και αντίστροφα.
    - Υποστήριξη πολλαπλών ρυθμών μετάδοσης.

Υποστρώμα MAC

- **Authentication**
  - Διαδικασία που έπεται χρονικά του επιτυχούς προσδιορισμού ενός AP.
  - Ανταλλάσσονται συνθηματικά πλαίσια μεταξύ του AP και SA (Station Adapter) για να επιβεβαιωθεί η ταυτότητα του τελευταίου.
- **Synchronization**
  - Επιτυγχάνεται με την περιοδική εκπομπή από το σταθμό βάσης (AP) πλαισίων συγχρονισμού (beacon frames) με στόχο τον συγχρονισμό των ρολογιών των σταθμών SA με αυτό του σταθμού βάσης.
- **Association process**
  - Είναι το σύνολο των διαδικασιών και ανταλλαγών των αντίστοιχων πλαισίων δεδομένων.
  - Με την ολοκλήρωση μπορεί ο σταθμός να προβεί στην αποστολή πλαισίων δεδομένων.

Υποστρώμα MAC

- **Security**
  - Χρησιμοποιεί την WEP βασισμένη στον αλγόριθμο κρυπτογράφησης RC4 της RSA.
  - Χρησιμοποιεί κλειδί μήκους 40-bits.
  - Καλύτερη ασφάλεια η υπέρυθρη πρόσβαση (LOS)
- **Roaming – Reassociation**
  - Μπορεί να συμβεί μόνο κατά το χρονικό διάστημα που μεσολαβεί μεταξύ δύο εκπομπών πακέτων.
  - Είναι πιθανό να υπάρξουν διαταραχές στο ρυθμό μετάδοσης λόγω των επανεκπομπών που θα εκτελεστούν από τα ανώτερα στρώματα (MAC).

Υπηρεσίες του 802.11

- Το 802.11 καθορίζει τις υπηρεσίες που παρέχουν τις απαιτούμενες λειτουργίες για την αποστολή των MSDU (MAC Service Data Unit) 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.

Station Services

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.

- **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): 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).

Station Services

- **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. 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.

Distribution System Services

- **Association**
  - 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.
- **Disassociation**
  - 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.

Distribution System Services

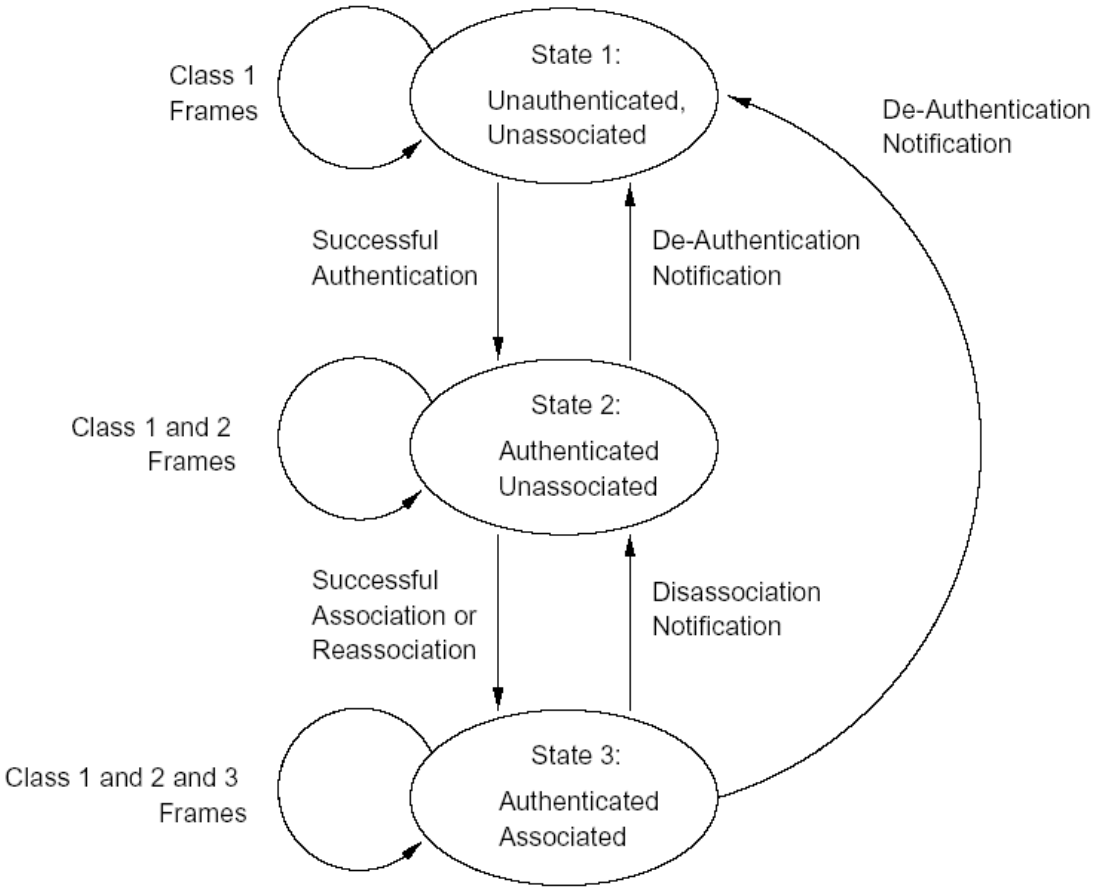
- **Integration**
  - Η υπηρεσία της ενοποίησης (integration) κάνει εφικτή την διανομή των MAC πλαισίων μέσω μιας πύλης (portal) μεταξύ ενός DS και ενός LAN που δεν ανήκει στην οικογένεια 802.11.
- **Reassociation**
  - Η υπηρεσία αυτή της επανασύνδεσης (reassociation) καθιστά ικανό ένα σταθμό να αλλάζει την τρέχουσα κατάσταση σύνδεσης από ένα AP σε ένα άλλο. Με τον τρόπο αυτό υποστηρίζεται η μετάβαση μεταξύ διαφορετικών BSS.

- Το 802.11 υποστηρίζει 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.

Αλληλεπίδραση μεταξύ ορισμένων Services

- Το IEEE 802.11 standard επισημαίνει ότι κάθε σταθμός πρέπει να υποστηρίζει δύο μεταβλητές οι οποίες εξαρτώνται από τις υπηρεσίες authentication, de-authentication και τις υπηρεσίες association, reassociation, disassociation.
- Οι μεταβλητές είναι οι καταστάσεις (state variables) **authentication** και **association**.
- Χρησιμοποιούνται σε μία απλή συσκευή η οποία προσδιορίζει το βαθμό ή τη σειρά με την οποία ορισμένες υπηρεσίες πρέπει να λειτουργήσουν.
- Χρησιμοποιούνται όταν ένας σταθμός αρχίζει την παράδοση υπηρεσιών δεδομένων (data delivery services).
- Ένας σταθμός μπορεί να είναι authenticated με πολλούς διαφορετικούς σταθμούς ταυτόχρονα.
- Ένας σταθμός μπορεί να είναι συνδεδεμένος με έναν άλλον σταθμό κάθε φορά.

Αλληλεπίδραση μεταξύ State Variables και Services



Αλληλεπίδραση μεταξύ State Variables και Services

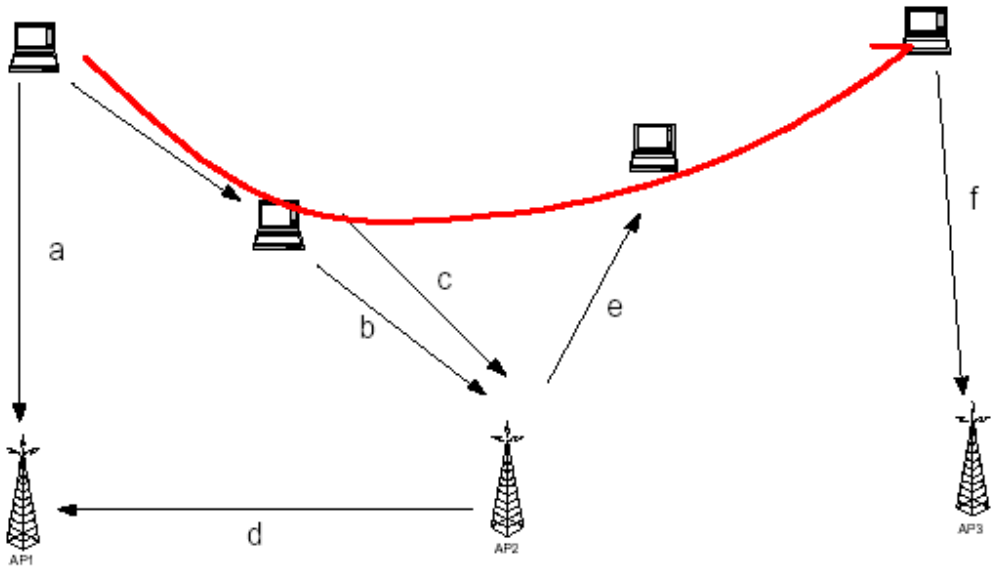
- Στην **κατάσταση 1**, ο σταθμός μπορεί να χρησιμοποιήσει ένα πολύ περιορισμένο αριθμό τύπων πλαισίων. Αυτά τα πλαίσια:
  - Βρίσκουν ένα IEEE 802.11 WLAN, ένα ESS και τους APs.
  - Ολοκληρώνουν την επικοινωνία μεταξύ των πρωτοκόλλων (μέσω των πλαισίων).
  - Υλοποιούν την υπηρεσία authentication.

    Αν ένας σταθμός είναι μέρος ενός IBSS, επιτρέπεται η υλοποίηση του data service στην κατάσταση 1.
- Στην **κατάσταση 2**, επιπλέον τύποι πλαισίων επιτρέπονται με σκοπό να δώσει τη δυνατότητα σε ένα σταθμό να υλοποιήσει τις υπηρεσίες association, reassociation και disassociation.
- Στην **κατάσταση 3**, όλοι οι τύποι πλαισίων επιτρέπονται και ο σταθμός μπορεί να χρησιμοποιήσει την υπηρεσία data delivery.

Αλληλεπίδραση μεταξύ State Variables και Services

- Ο σταθμός πρέπει να αντιδρά για κάθε λαμβανόμενο πακέτο σε κάθε κατάσταση, ακόμα και για αυτά που δεν επιτρέπονται σε κάποια κατάσταση.
- Ο σταθμός θα στείλει μία ειδοποίηση deauthentication σε οποιονδήποτε σταθμό με το οποίο δεν είναι authenticated, αν λάβει πλαίσια που δεν επιτρέπονται στην κατάσταση 1.
- Ο σταθμός θα στείλει μία ειδοποίηση disassociation σε οποιονδήποτε σταθμό με τον οποίο είναι authenticated, αλλά όχι associated, αν λάβει πλαίσια που δεν επιτρέπονται στην κατάσταση 2.
- Αυτές οι ειδοποιήσεις θα αναγκάσουν τον σταθμό που στέλνει τα μη επιτρεπτά πλαίσια να κάνει μία μετάβαση στην κατάλληλη κατάσταση και να επιτρέψει την ομαλή πρόσβαση προς την κατάσταση 3.

Αλληλεπίδραση μεταξύ State Variables και Services



(a) --- The station finds AP1, it will authenticate and associate.

(b) --- As the station moves, it may pre-authenticate with AP2.

(c) --- When the association with AP1 is no longer desirable, it may reassociate with AP2.

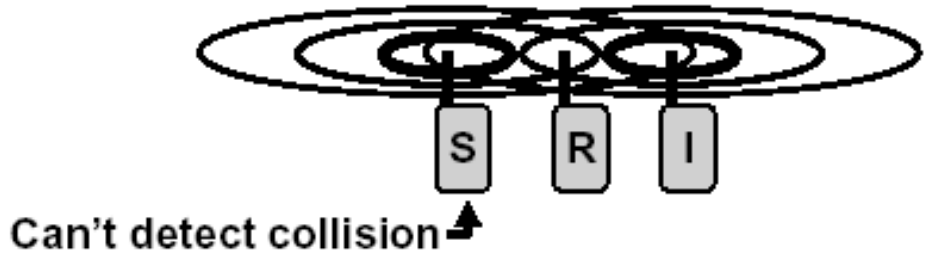
(d) --- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) --- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) --- The station find another access point and authenticate and associate.

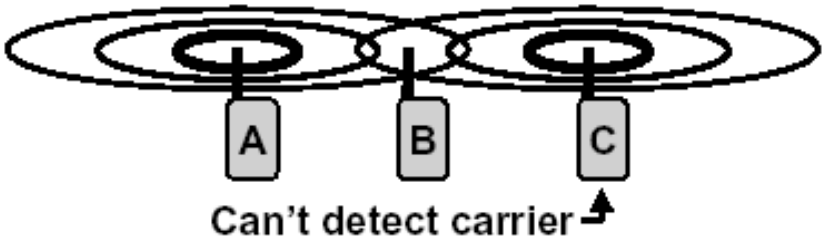
MAC προβλήματα για WLAN

- Το collision detection (CD) δε λειτουργεί σωστά λόγω των διαφορετικών επιπέδων ισχύων στο δέκτη και τον πομπό
  - π.χ., CSMA/CD βασίζεται στη δυνατότητα αναγνώρισης πιθανής σύγκρουσης στο δέκτη.
  - Δε λειτουργεί στα ασύρματα δίκτυα, λόγω των διαφορετικών επιπέδων ισχύων στο δέκτη.
  - Ο πομπός ακούει μόνο τον εαυτό του.



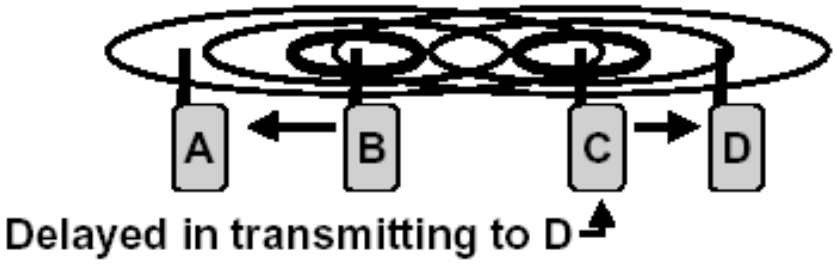
MAC προβλήματα για WLAN

- Η ανίχνευση φέροντος (carrier sensing) δε λειτουργεί λόγω του προβλήματος του κρυμμένου κόμβου (hidden terminal)
  - Ο σταθμός Α εκπέμπει στον σταθμό Β, αλλά δεν ακούγεται (ή ανιχνεύεται) στον C.
  - Ο σταθμός C μπορεί να εκπέμψει στον Β.
  - Ο σταθμός Α κρύβεται από τον C.
  - Αν εκπέμπει ο σταθμός Α, ο C δεν μπορεί να ανιχνεύσει το φέρον και μπορεί να αρχίσει να εκπέμπει.



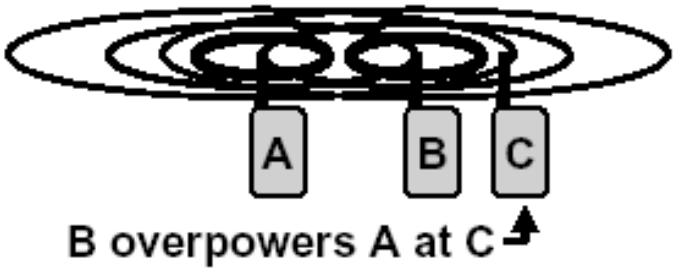
MAC προβλήματα για WLAN

- Η ανίχνευση φέροντος (carrier sensing) μπορεί να επιφέρει περιττές καθυστερήσεις λόγω του προβλήματος του εκτεθειμένου κόμβου (exposed terminal).
  - Οι σταθμοί A και C ακούν τον B.
  - Ο σταθμός A δεν μπορεί να ακούσει τον C.
  - Αν ο σταθμός B εκπέμψει στον A, ο σταθμός C καθυστερεί να εκπέμψει στον D.

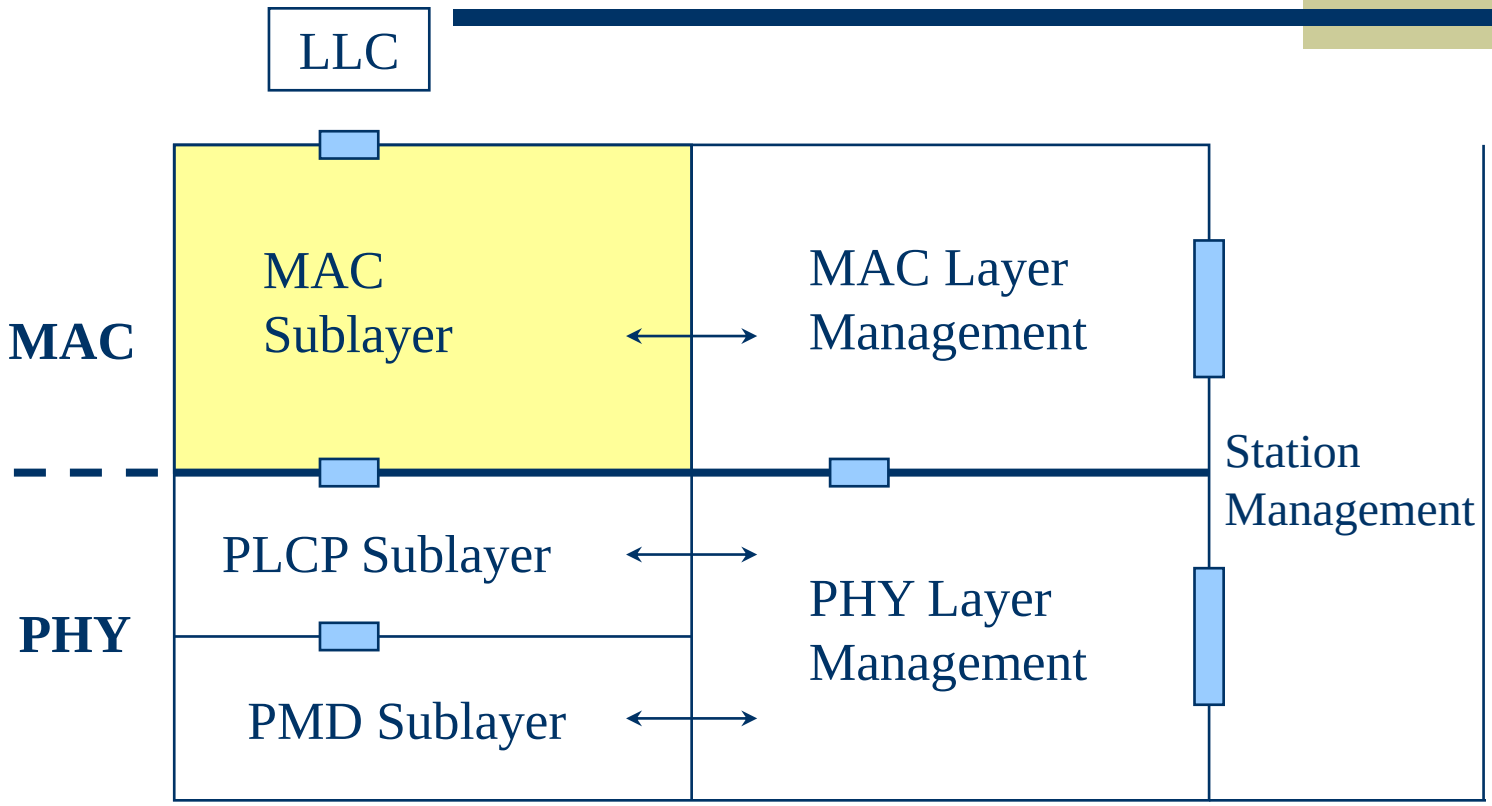


MAC προβλήματα για WLAN

- Ένας σταθμός μπορεί αποτελεσματικά να υποφέρει από έναν άλλον στο στρώμα MAC λόγω του προβλήματος near-far στο φυσικό στρώμα.
  - Ο σταθμός C λαμβάνει σήμα από τον σταθμό B πολύ πιο ισχυρό από το σήμα του A.
  - Τότε υπάρχει πρόβλημα αν η 'διαιτησία' του πρωτοκόλλου MAC εξαρτάται από τη λαμβανόμενη ισχύ, π.χ. CDMA.



Οντότητες MAC



PHY : Physical Layer
PLCP: Physical Layer Convergence Protocol
PMD: Physical Medium Dependent

Λειτουργίες υποστρώματος MAC

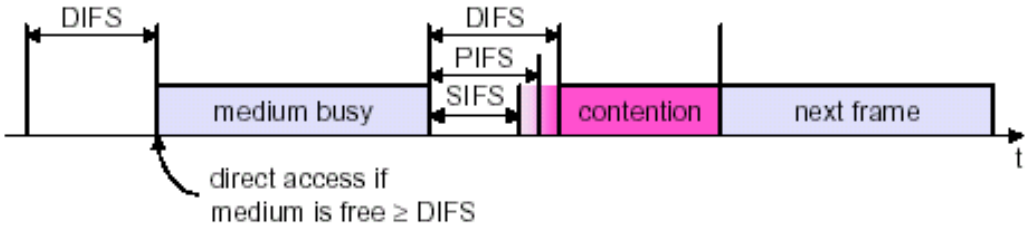
- Κάθε σταθμός και AP σε ένα 802.11 WLAN υλοποιεί τις υπηρεσίες του υποστρώματος MAC οι οποίες παρέχουν την δυνατότητα στις ομότιμες (peer) LLC οντότητες (entities) να ανταλλάσσουν MSDUs (MAC Service Data Units) μεταξύ των MAC SAPs (Service Access Points).
- Το υποστρώμα MAC παρέχει 3 κύριες λειτουργίες:
  - Πρόσβαση στο ασύρματο μέσο
  - Προσχώρηση (joining) σε ένα δίκτυο
  - Παροχή των λειτουργιών ‘authentication’ και ‘privacy’

Μέθοδοι Πρόσβασης στο Μέσο

- Οι δύο τρόποι πρόσβασης στο MAC επίπεδο που έχουν οριστεί στο πρωτόκολλο IEEE 802.11 είναι οι:
  - DCF (Distributed Coordination Function)
    - Αποτελείται από έναν μηχανισμό 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)
    - Παρέχει υπηρεσίες χωρίς ανταγωνισμό (contention) με σημειακό συντονισμό.
    - Χρησιμοποιείται για εφαρμογές πραγματικού χρόνου, όπου απαιτείται προνομιακή μεταχείριση έναντι της απλής αποστολής δεδομένων.
    - Το πρωτόκολλο αυτό στηρίζεται στην πρόσβαση στο μέσο και εκτελείται μόνο σε AP (χρήσιμο για infrastructure δίκτυα), ενώ κύριο ρόλο παίζει ένας ελεγκτής ο οποίος καλείται PC (Point Coordinator) και βρίσκεται στα APs.

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 γίνεται ξεκινώντας από αυτό με την μικρότερη διάρκεια:
  - SIFS: Short InterFrame Space
  - PIFS: PCF InterFrame Space
  - DIFS: DCF InterFrame Space
  - EIFS: Extended InterFrame Space



Χρονικά Διαστήματα Πρόσβασης

- 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.
- 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.
  - Δίνεται η δυνατότητα στον σταθμό που ήδη μεταδίδει να ολοκληρώσει τη διαδικασία μετάδοσης των πλαισίων που έχει προς μετάδοση.

Χρονικά Διαστήματα Πρόσβασης

- 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 (Contention Free Period).
  - 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

Χρονικά Διαστήματα Πρόσβασης

- 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:

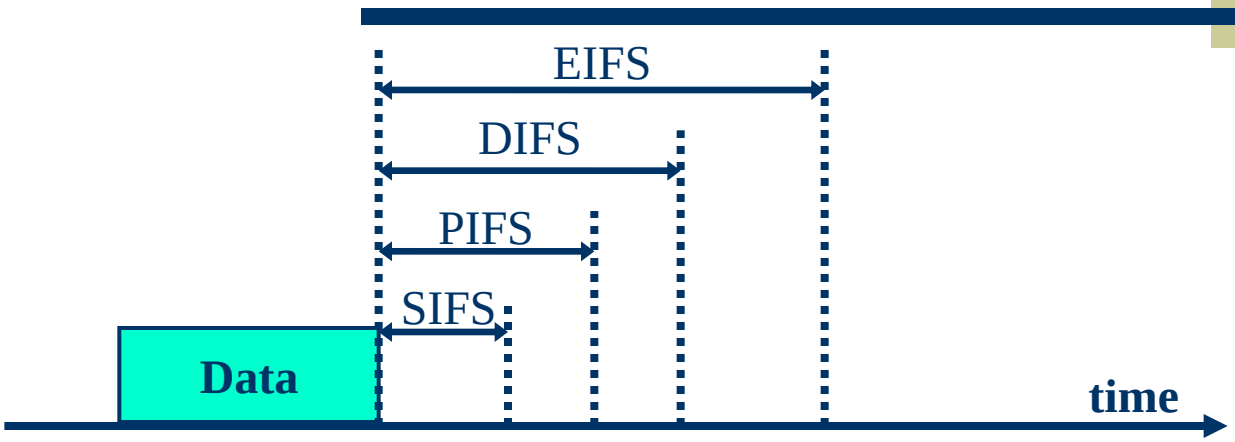
    EIFS = SIFSTime + (8 x ACKSize) + PreambleLength + PLCPHeaderLength + DIFS

Χρονικά Διαστήματα Πρόσβασης

- Φαίνονται οι τιμές που δίνονται από το Standard, ανάλογα με το φυσικό επίπεδο που χρησιμοποιείται.

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

Access Spacing



IFS	Interframe Space		
SIFS	Short IFS	Highest Priority	ACK,CTS, Poll Messages and Responses, CF-End
PIFS	PCF IFS	2nd priority	PCF Operation Mode (Beacon)
DIFS	DCF IFS	3rd priority	DCF Operation Mode (back-off, RTS)
EIFS	Extended IFS	Lowest priority	After detection of erroneous frame

Λειτουργία του DCF

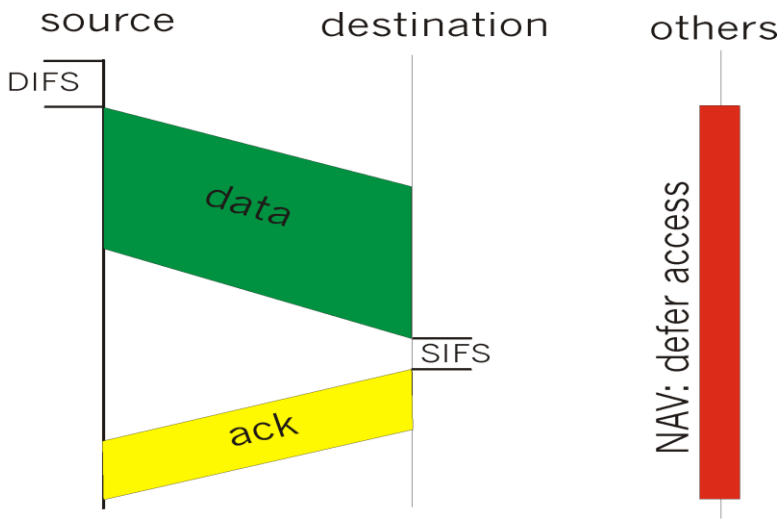
- Μηχανισμός ανίχνευσης φέροντος
- Λειτουργία του DCF με τη μέθοδο CSMA/CA
- Διαδικασία επαλήθευσης (ack) από το υποστρώμα MAC
- Διαδικασία υποχώρησης (backoff)
- Λειτουργία του DCF με τη μέθοδο RTS/CTS

Λειτουργία του DCF
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.
- 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 υποστρώμα MAC για να αποφασίσει την κατάσταση του καναλιού.

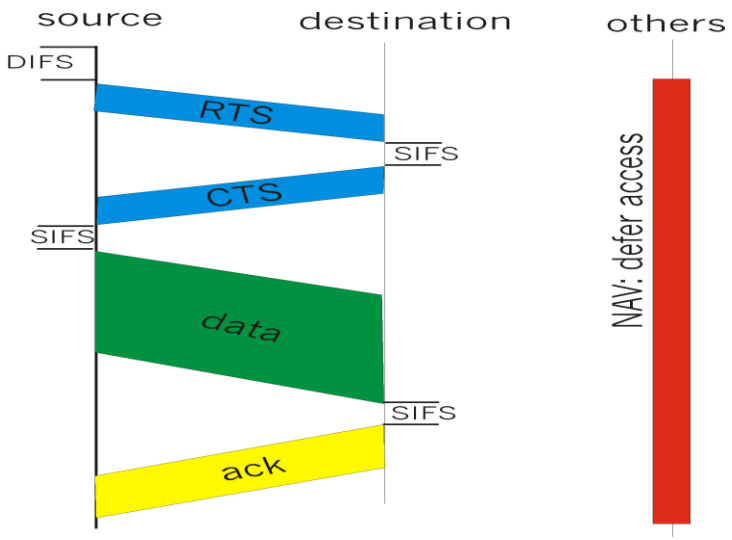
Λειτουργία του DCF Μέθοδος CSMA/CA

- CSMA
  - Έλεγχος αν ο δίαυλος είναι ελεύθερος για χρονικό διάστημα DIFS (Distributed Inter Frame Space)
  - Εκπομπή δεδομένων (Χωρίς έλεγχο συγκρούσεων)
  - Ο δέκτης στέλνει ACK μετά από χρόνο SIFS (Short Inter Frame Space)
  - Αν ο πομπός δεν λάβει ACK τότε επαναμεταδίδει.



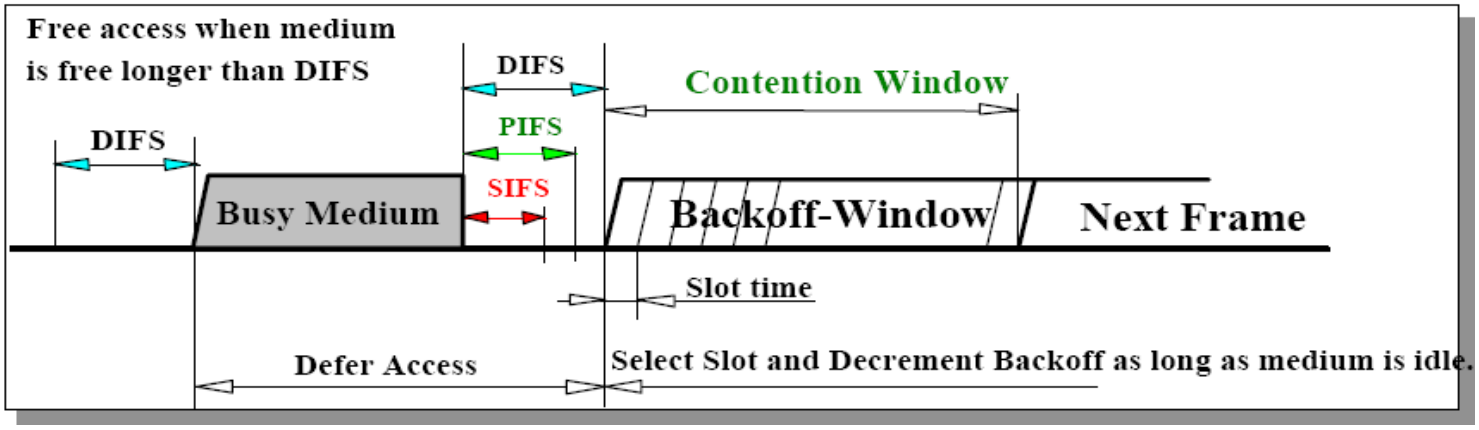
Λειτουργία του DCF Μέθοδος CSMA/CA

- CA
  - Ο πομπός στέλνει ένα RTS στο δέκτη.
  - Αν ο δέκτης εκείνη τη χρονική στιγμή δεν επικοινωνεί με άλλο STA στέλνει στον πομπό CTS.
  - Όσα STAs ακούν το CTS δεν επιτρέπεται να εκπέμψουν
  - Στη συνέχεια ο πομπός στέλνει τα πακέτα και περιμένει επιβεβαίωση



Λειτουργία του DCF Μέθοδος CSMA/CA

- Ένας σταθμός που θέλει να μεταδώσει ανιχνεύει αρχικά το μέσο για να διαπιστώσει αν ένας άλλος σταθμός μεταδίδει. Αν το μέσο είναι:
  - κατειλημμένο, αναβάλλει τη 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.



Λειτουργία του DCF Μέθοδος CSMA/CA

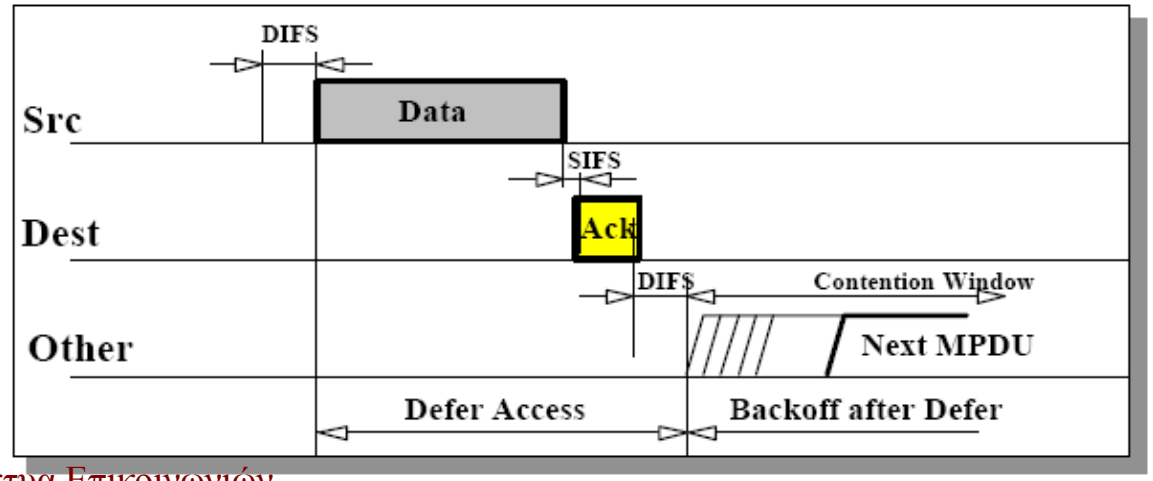
- Ο σταθμός λήψης ελέγχει το CRC του ληφθέντος πακέτου και στέλνει ένα πακέτο επαλήθευσης (ACK). Η λήψη του πακέτου επαλήθευσης δηλώνει στον πομπό ότι δεν συνέβη σύγκρουση.
- Αν ο αποστολέας δεν λάβει το πακέτο επαλήθευσης ξαναστέλνει το πακέτο μέχρι να λάβει την επαλήθευση. Η διαδικασία αυτή επαναλαμβάνεται για ένα συγκεκριμένο αριθμό επαναμεταδόσεων.
- Οι τυχόν συγκρούσεις που θα συμβούν πρέπει να ανιχνευθούν από το επίπεδο MAC ώστε η επαναμετάδοση 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.
- Οι σταθμοί που χρησιμοποιούν FH πρέπει να έχουν ολοκληρώσει την μετάδοση ενός ολόκληρου MPDU και του αντίστοιχου ACK (αν απαιτείται) πριν το όριο του ‘dwell time’.

Λειτουργία του DCF
Διαδικασία επαλήθευσης

- Θετική επαλήθευση: Ένας σταθμός πρέπει να απαντήσει με μια επαλήθευση αν το CRC του ληφθέντος πλαισίου είναι σωστό.
- 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.

Λειτουργία του DCF Διαδικασία επαλήθευσης

- Η περίοδος μεταξύ της λήξης μετάδοσης του πακέτου και αρχή του πλαισίου επαλήθευσης (ACK frame) είναι μία SIFS (Short Inter Frame Space).
- Αναβάλλει (defer) την πρόσβαση βασιζόμενο στο Carrier Sense
  - CCA από το PHY and Virtual Carrier Sense state.
- Απευθείας πρόσβαση όταν το μέσο είναι sensed free για μεγαλύτερο διάστημα από DIFS, αλλιώς αναβάλλει και οπισθοχωρεί (backoff).
- Ο δέκτης διαφορετικών πλαισίων επιστρέφει ένα ACK άμεσα όταν ο CRC διορθώνει.
  - Όταν δε λαμβάνεται κανένα ACK, τότε επανεκπέμπεται το πλαίσιο μετά από τυχαίο backoff (μέχρι το μέγιστο όριο).



Λειτουργία του DCF
Διαδικασία υποχώρησης (backoff)

- 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 (**backoff**) για έναν επιπρόσθετο χρόνο (ο οποίος χωρίζεται σε σχισμές) πριν την μετάδοση, εκτός αν ο μετρητής υποχώρησης (backoff 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.

Λειτουργία του DCF
Διαδικασία υποχώρησης (backoff)

- Αν ο σταθμός προσπαθεί να εκπέμψει και το μέσο είναι κατειλημμένο, αυξάνει το maximum *backoff time* εκθετικά.
- Backoff Timer = Random () * Slot_Time
  - Random(): ένας ψευδοτυχαίος αριθμός ομοιόμορφα κατανεμημένος στο διάστημα [0, CW], όπου CW είναι ένας ακέραιος μεταξύ CWmin and CWmax
    - newCW = oldCW * 2 + 1
  - Slot_Time: μεγάλο αρκετά για έναν σταθμό ώστε να ανιχνεύσει αν άλλος σταθμός έχει προσπελάσει στο μέσο σε αυτό το slot.
- Εκτέλεση του exponential backoff:
  - Πρώτη προσπάθεια εκπομπής στο πλαίσιο εκπομπής και το μέσο είναι κατειλημμένο (initial window [0, CWmin])
  - Για κάθε εκπομπή (υπολογίζεται newCW)
  - Μετά από μία επιτυχής εκπομπής (το παράθυρο μειώνεται σε [0, CWmin])

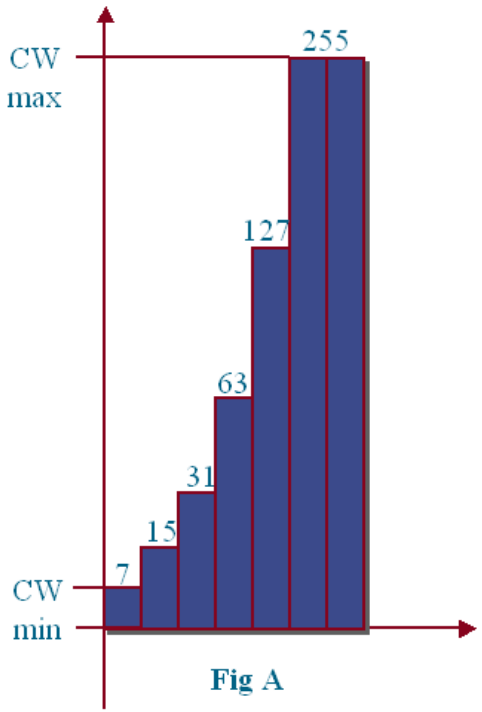
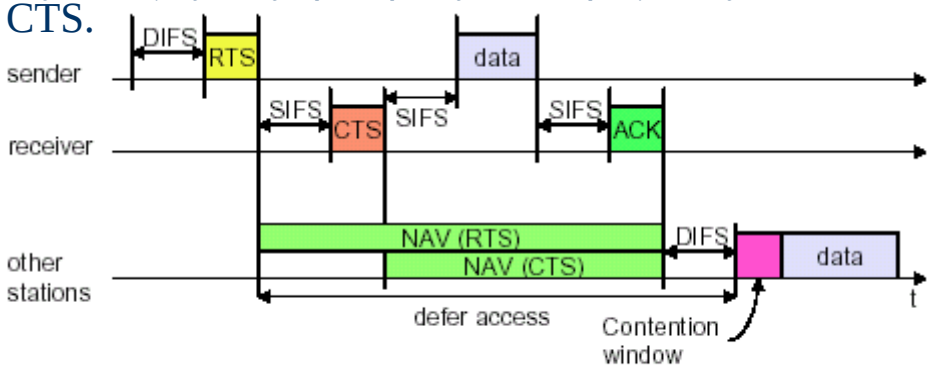


Fig A

Λειτουργία του DCF Μέθοδος RTS/CTS

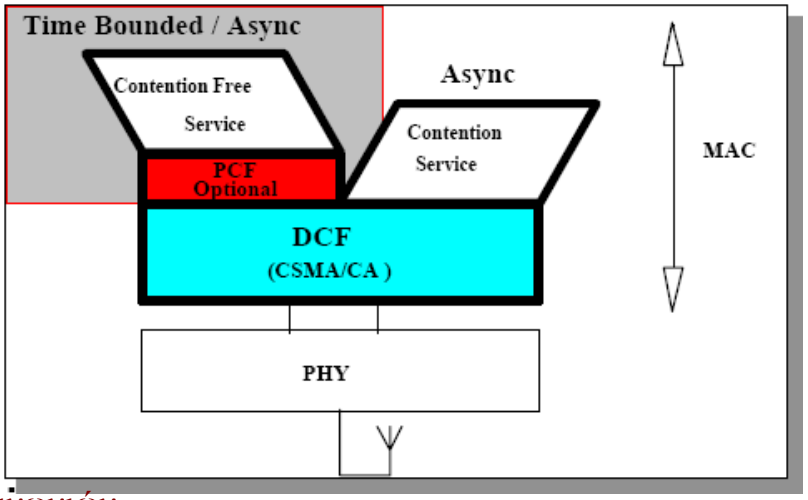
- Η διαδικασία για την αποστολή πακέτων με την συγκεκριμένη μέθοδο γίνεται με την παρακάτω σειρά:
  - Ο σταθμός που θέλει να στείλει δεδομένα στέλνει αρχικά ένα πακέτο RTS (Request To Send) με τις παραμέτρους κράτησης (reservation) του μέσου, αφού πρώτα περιμένει για ένα DIFS. Η κράτηση καθορίζει το χρονικό διάστημα που χρειάζεται για την αποστολή των δεδομένων.
  - 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.
  - Ο σταθμός αποστολής μπορεί τώρα να στείλει άμεσα τα δεδομένα τα οποία θα επιβεβαιωθούν μέσω ACK.
  - Οι άλλοι σταθμοί αποθηκεύουν τις αλλαγές στις κρατήσεις του στρώματος που διανέμονται μέσω των RTS και CTS.



NAV: Network Allocation Vector

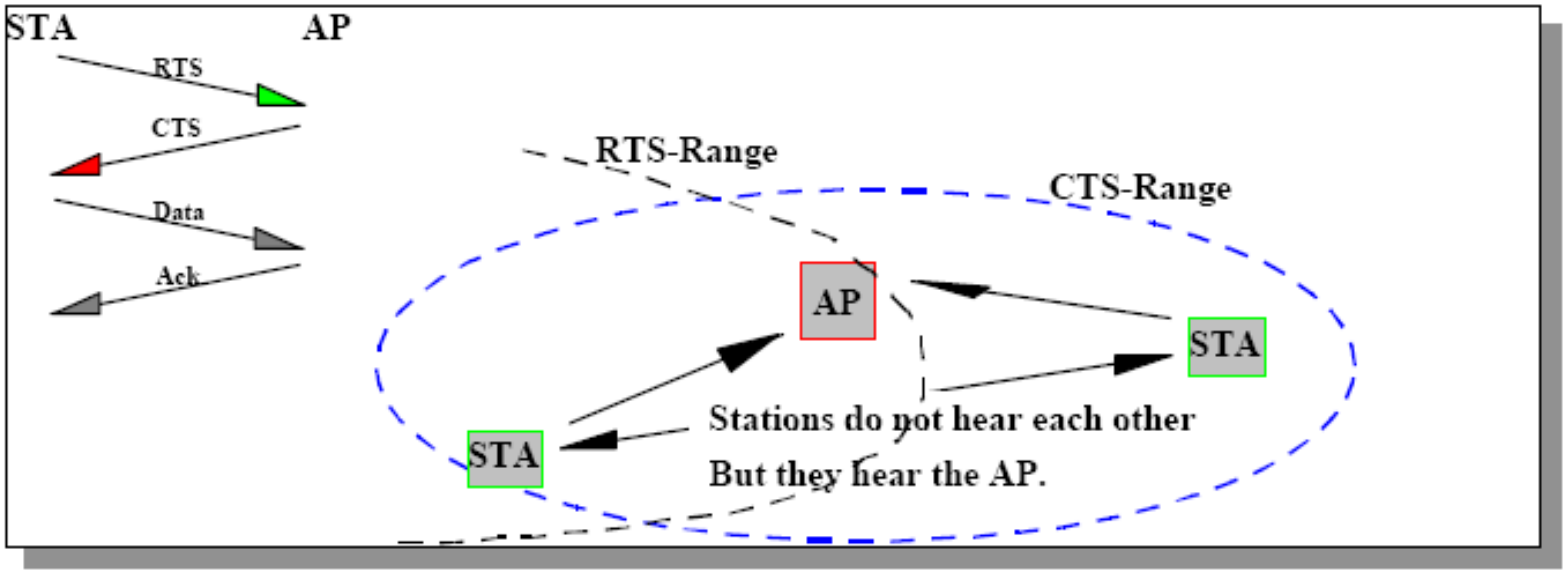
Λειτουργία του PCF

- Η υπηρεσία Contention Free χρησιμοποιεί την Point Coordination Function (PCF) σε μία βάση DCF.
  - Χαμηλές διακυμάνσεις καθυστέρησης μετάδοσης για την υποστήριξη των υπηρεσιών Time Bounded.
  - Υποστηρίζει async Data, Voice ή mixed
  - Ελεγκτής Point Coordinator στο AP
- Συνύπαρξη μεταξύ Contention και optional Contention Free



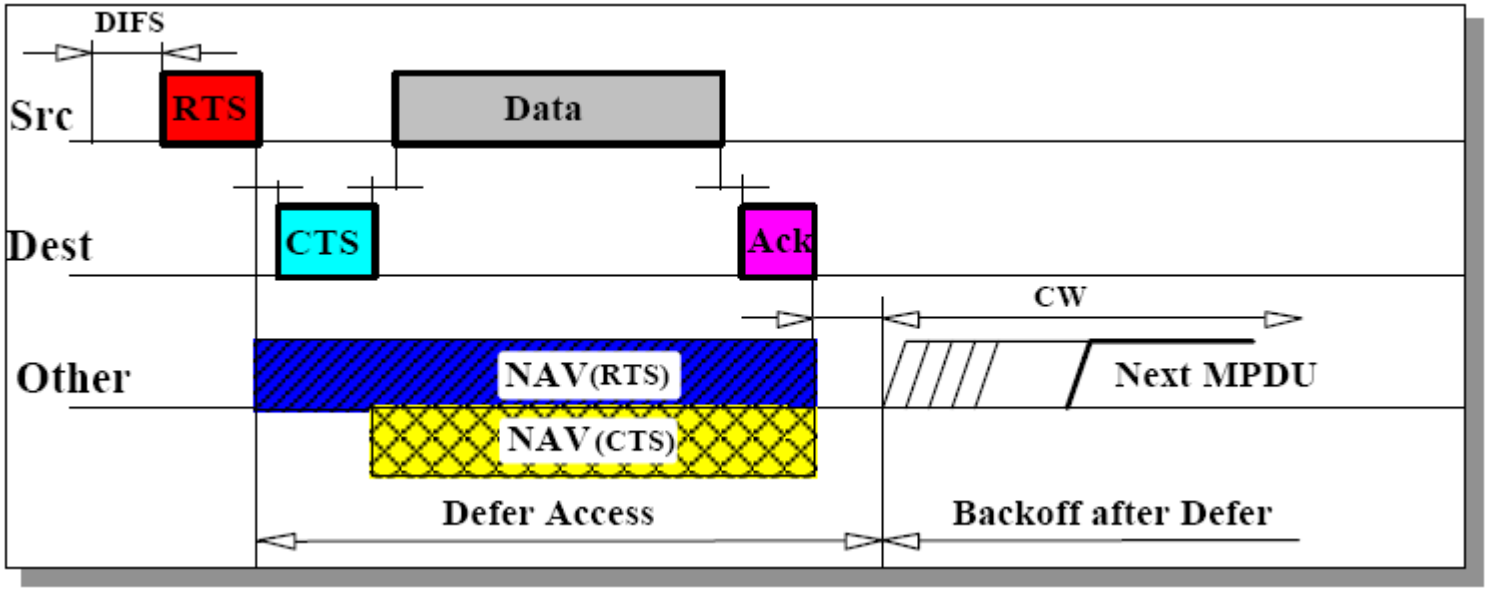
Πρόβλημα κρυμμένου κόμβου

- Διαχωρισμός της ανταλλαγής πλαισίων ελέγχου (RTS/CTS)
- Κατανέμουν τη διάρκεια (duration) μεταξύ Tx and Rx σταθμών.



Απαιτήσεις για το πρόβλημα κρυμμένου κόμβου

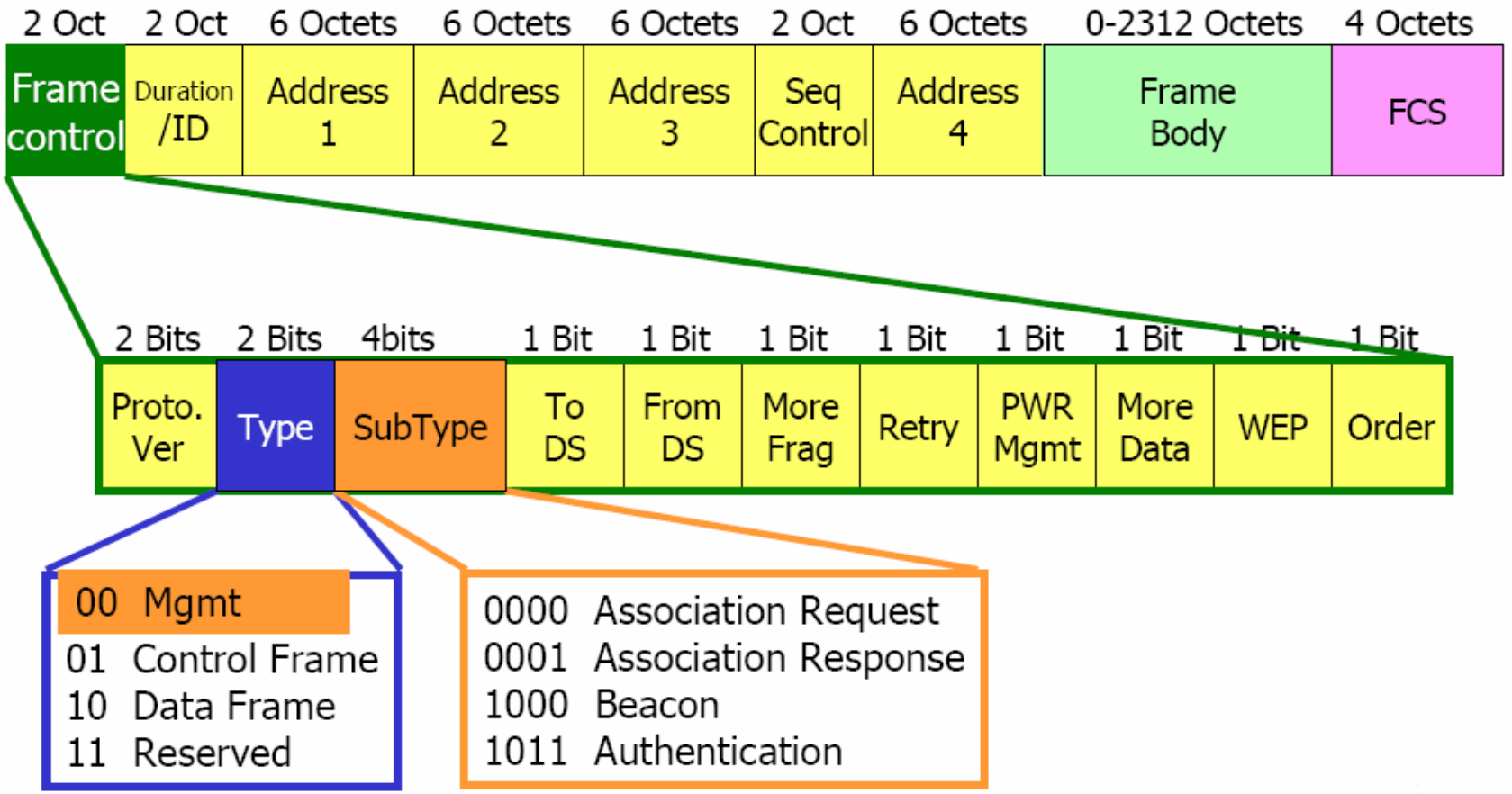
- Τα πεδία της διάρκειας (duration) των RTS and CTS πλαισίων κατανέμουν την πληροφορία του μέσου που είναι καταχωρημένη σε ένα Network Allocation Vector (NAV).
- Μεταχρονίζουν (defer) στον NAV ή στον "CCA" υποδεικνύοντας ότι το μέσο είναι απασχολημένο.
- Η χρήση των RTS / CTS είναι προαιρετική αλλά πρέπει να υλοποιηθεί.



Δομή πλαισίου MAC

- Για την μεταφορά των MSDUs μεταξύ ομότιμων LLCs, το υποστρώμα MAC χρησιμοποιεί τριών ειδών τύπους πλαισίου:
  - **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

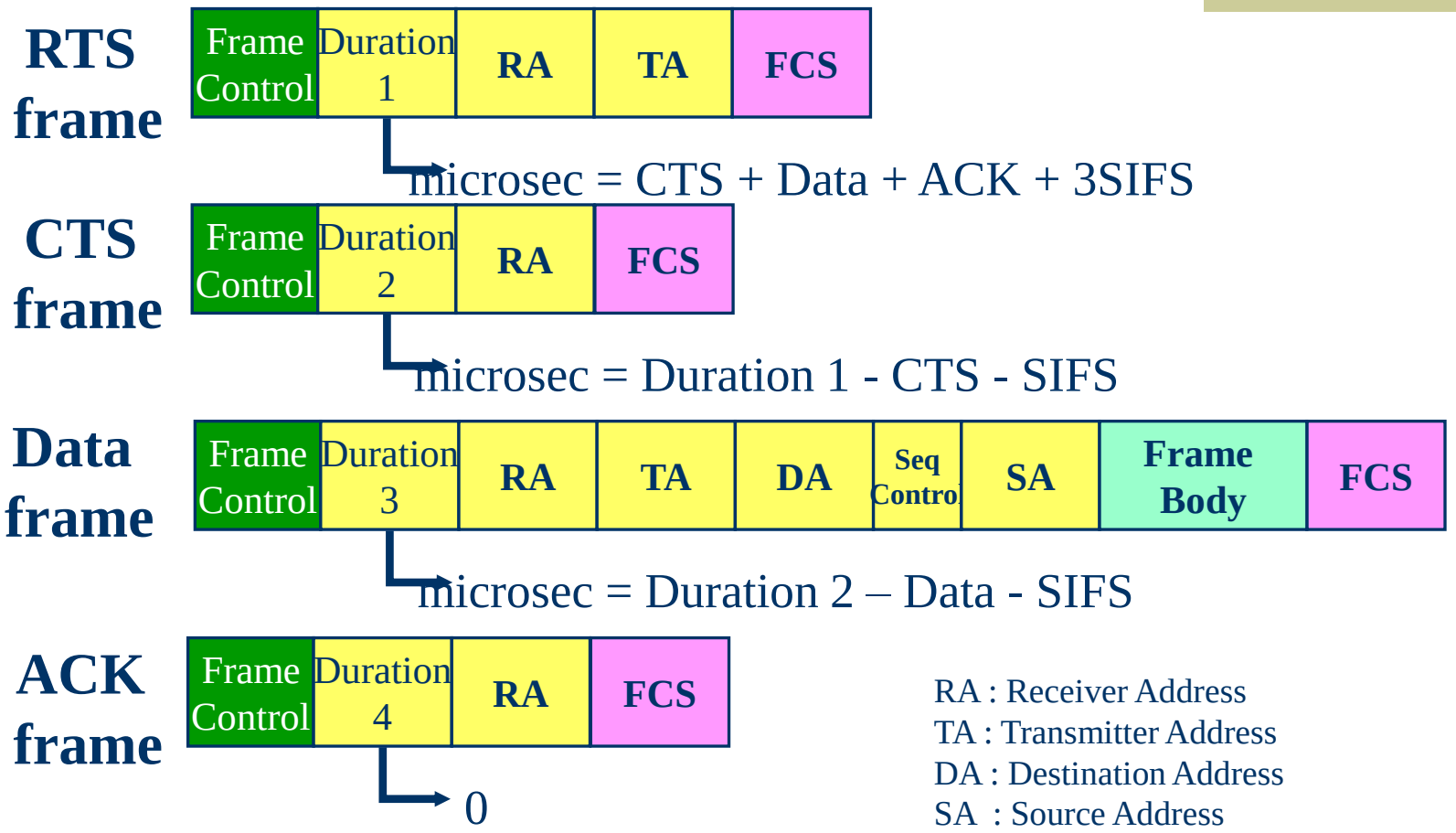
Δομή πλαισίου MAC



Δομή πλαισίου MAC

- 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.
- 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.

Δομή πλαισίου MAC



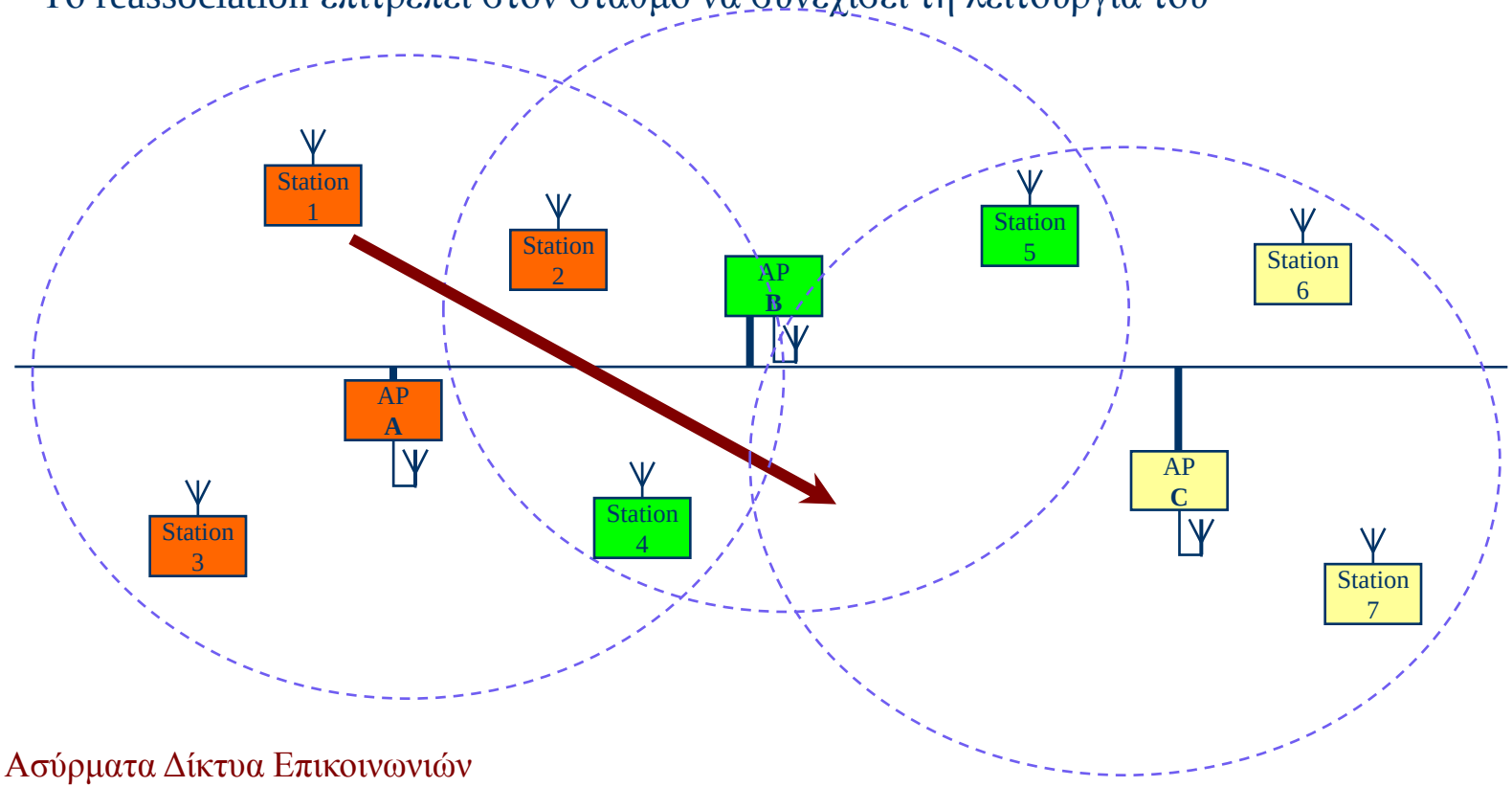
RA : Receiver Address
TA : Transmitter Address
DA : Destination Address
SA : Source Address
FCS : Frame Check sequence

Συσχέτιση και Περιαγωγή

- Το 802.11 MAC επίπεδο είναι υπεύθυνο για το πώς ένας σταθμός συσχετίζεται με ένα σημείο πρόσβασης.
- Όταν ένας τέτοιος πελάτης μπει στην εμβέλεια ενός ή περισσότερων σημείων πρόσβασης διαλέγει ένα AP για να συσχετιστεί μαζί του βασιζόμενος στην ισχύ του σήματος και τα ποσοστά λαθών στα πακέτα που παρατηρεί.
- Μόλις γίνει δεκτός από το σημείο πρόσβασης, ο πελάτης συγχρονίζεται στη ραδιοσυχνότητα του καναλιού του AP.
- Περιοδικά εξετάζει όλα τα 802.11 κανάλια για να αποφανθεί αν υπάρχει κάποιο σημείο πρόσβασης που θα του παρείχε καλύτερη απόδοση. Αν διαπιστώσει κάτι τέτοιο, επανασυσχετίζεται με το νέο AP.

Περιαγωγή

- Οι κινητοί σταθμοί μπορούν να φύγουν ...
  - από την περιοχή κάλυψης των APs τους
  - αλλά να συνδεθούν σε άλλα APs
- Το reassociation επιτρέπει στον σταθμό να συνεχίσει τη λειτουργία του



Κινητικότητα Χρηστών

- Σε ένα IP-based δίκτυο, υπάρχουν δύο ειδών κινητικότητες χρηστών:
  - roaming (περιπλάνηση) εντός του ίδιου subnet (η IP διεύθυνση ενός STA παραμένει ίδια κατά την αλλαγή AP) (Intra-Network Handover).
  - roaming μεταξύ διαφορετικών subnets (η IP διεύθυνση ενός STA μπορεί να αλλάξει κατά την αλλαγή AP) (Inter-Network Handover).
- Το υποπρότυπο IEEE 802.11f ορίζει ακριβώς τη διαδικασία του Handover.

Ποιότητα Υπηρεσίας σε WLAN

- Φυσικά όπως και στα LAN έτσι και στα WLAN η ποιότητα υπηρεσιών από άκρη σε άκρη δεν είναι εξασφαλισμένη.
- Πρόβλημα:
  - Και οι δύο μέθοδοι πρόσβασης (DCF, PCF) δεν υποστηρίζουν μηχανισμούς Diffserv και κατ' επέκταση QoS.
- Λύση:
  - Στο πρότυπο IEEE 802.11e ορίζονται δύο νέες συναρτήσεις πρόσβασης:
    - Enhanced Distributed Coordination Function (EDCF)
    - Hybrid Coordination Function (HCF)
  - Ένα BSS που υποστηρίζει το πρότυπο IEEE 802.11e ονομάζεται QoS supporting BSS

Ασφάλεια σε WLANs - Γενικά

- Είναι σαφές ότι τα ενσύρματα LAN είναι πιο ασφαλή από τα ασύρματα και αυτό οφείλεται στους παρακάτω λόγους:
  - Στα WLANs το μέσο μετάδοσης (Ασύρματο κανάλι) έχει συγκεκριμένες δυνατότητες απόδοσης και εμφανίζει σημαντικές και μεγάλες διαφορές συγκρινόμενο με το ενσύρματο κανάλι των LANs. Το γεγονός αυτό οφείλεται στη ασύρματη φύση του καναλιού και στο ότι παρουσιάζει μεγάλες μεταβολές με το πέρασμα του χρόνου.
  - Ο οποιοσδήποτε μπορεί να έχει πρόσβαση στο κανάλι μετάδοσης (Αέρας) κάτι που δεν ισχύει στα ενσύρματα δίκτυα.

Ασφάλεια σε WLANs - Αλγόριθμοι

- Οι αλγόριθμοι που χρησιμοποιούνται σήμερα είναι:
  - Shared Key Authentication
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA) (Αναπτύχθηκε από Wi-Fi οργανισμό)
  - IP SEC

Προβλήματα:

WEP: Εμφανίζει σημαντικά κενά ασφάλειας

WPA: Καλύπτει κενά του WEP, δεν καλύπτει την ανάγκη για ουσιαστική ασφάλεια στα ασύρματα τοπικά δίκτυα

IP SEC: Εφαρμόζεται τοπικά σε κάθε χρήστη και καλύπτει μόνο Point to Point συνδέσεις

Στόχος WEP / WPA

- Αυθεντικοποίηση ---- Ο κύριος στόχος του WEP ήταν η υπηρεσία αυθεντικοποίησης του client στο access point αλλά όχι αντιστρόφως. Έτσι επιτυγχάνεται η ελεγχόμενη σύνδεση με το δίκτυο το οποίο προστατεύεται.
- Εμπιστευτικότητα ---- Η εμπιστευτικότητα ήταν ο δεύτερος στόχος του WEP. Επιτεύχθηκε με την κρυπτογράφηση των δεδομένων ώστε η πρόσβαση σε αυτά να είναι αδύνατη.
- Ακεραιότητα ---- Ένας άλλος στόχος του WEP ήταν η ακεραιότητα ώστε να μην είναι δυνατό να αλλαχθούν τα περιεχόμενα του μηνύματος κατά την διάρκεια μετάδοσης χωρίς να γίνει αντιληπτό.

Ελλείψεις Ασφαλείας

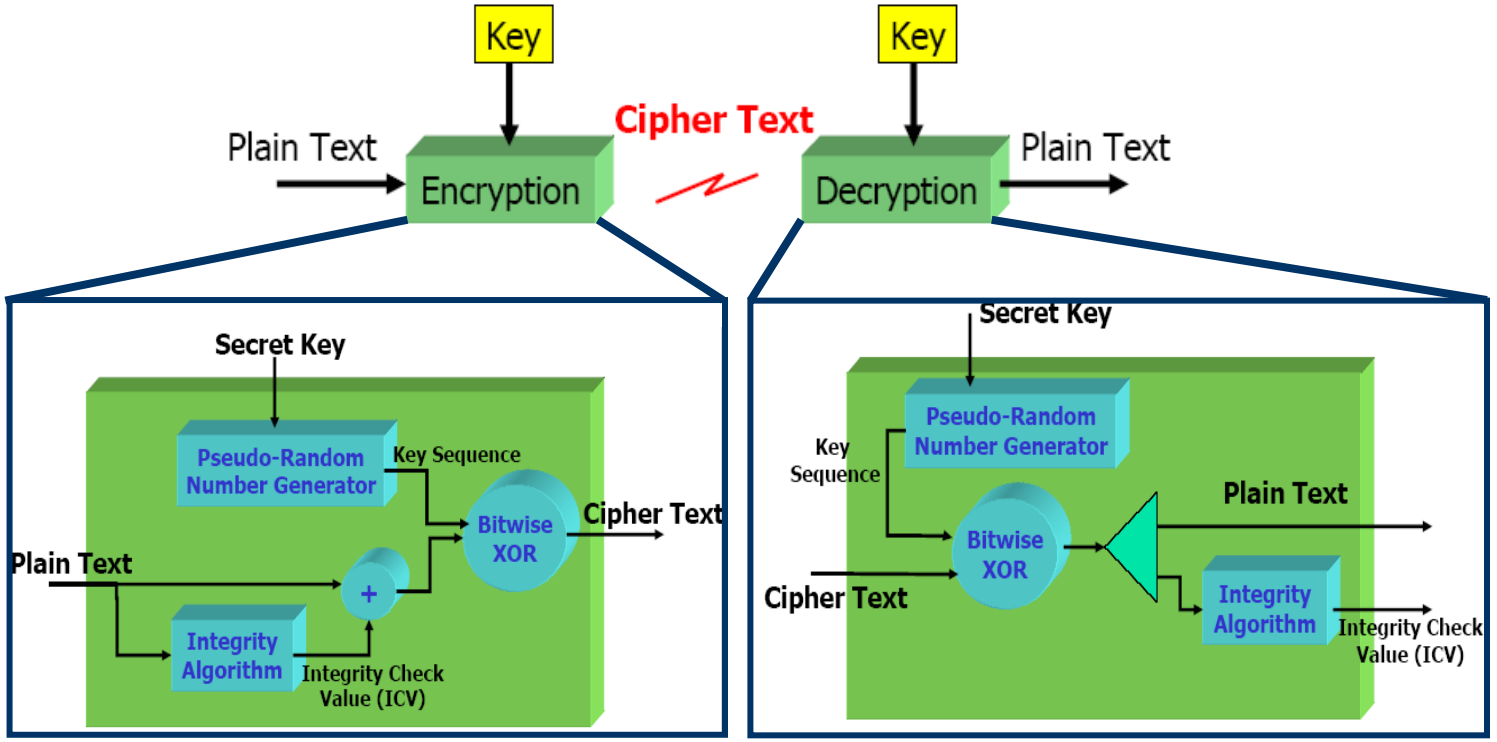
- Αυθεντικοποίηση --- Ευάλωτο σε «Man in the middle» επίθεση
- Εμπιστευτικότητα, Ακεραιότητα --- Η κρυπτογράφηση με χρήση WEP είναι επισφαλής. Η ακεραιότητα υποστηρίζεται από την χρήση ενός CRC το οποίο υπολογίζεται με χρήση του WEP.
- Έλλειψη μηχανισμού διαχείρισης κλειδιών

Αδυναμίες του WEP

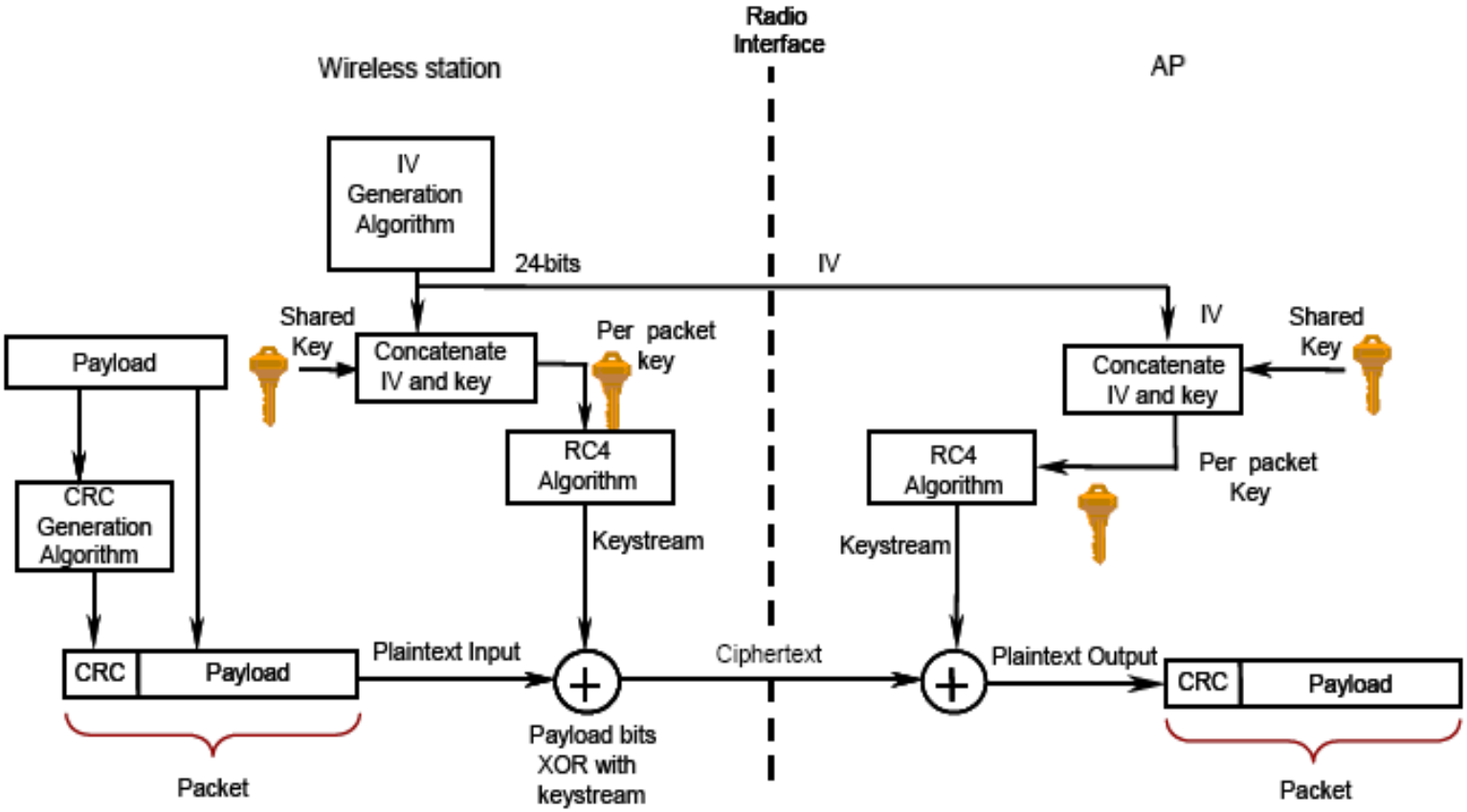
- Επισφαλής για οποιοδήποτε μήκος κλειδιού.
- Το Initialization Vector (IV) έχει μικρό μήκος των 24bit
- Το IV ταξιδεύει μαζί με το μήνυμα σε μορφή plain-text
- Ο επιτιθέμενος μπορεί να περιμένει την κρυπτογράφηση δεύτερου πακέτου με το ίδιο IV και να αποσπάσει το κύριο κλειδί

Wired Equivalent Privacy (WEP)

- Encryption Algorithm, RC4
- Per-packet encryption key = 24-bit Initialization Vector (IV) διασπάται σε ένα pre-shared key
- Το WEP επιτρέπει στο IV να επαναχρησιμοποιηθεί σε κάθε πλαίσιο
- Data και ICV κρυπτογραφούνται κάτω από το per-packet encryption key

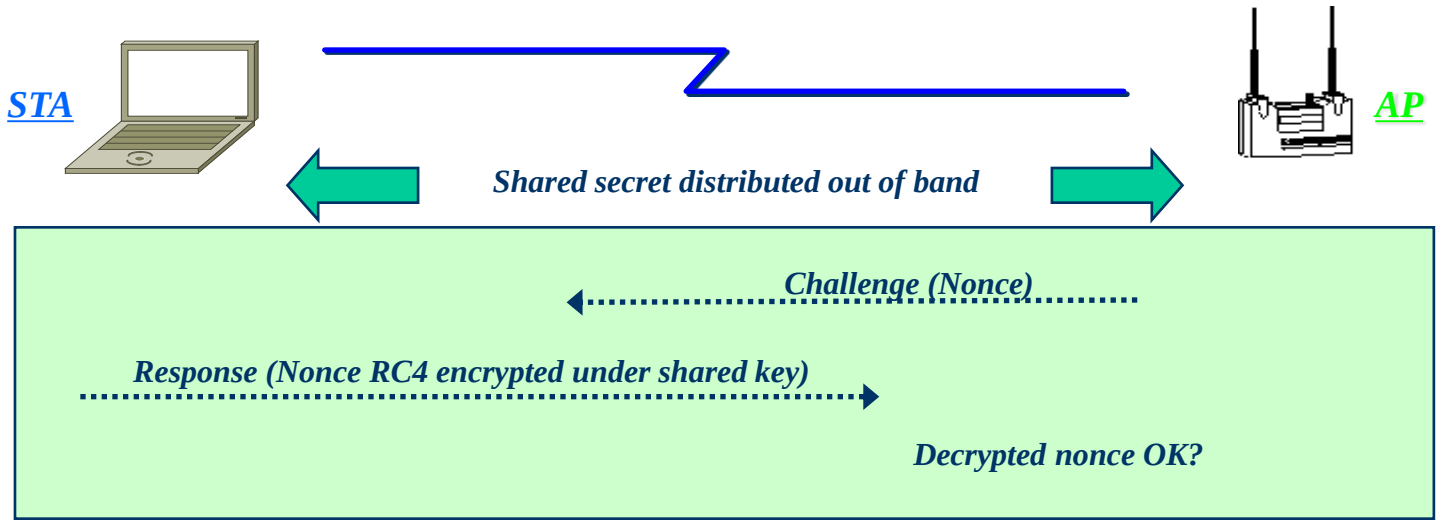


Κρυπτογράφηση μηνυμάτων με το WEP



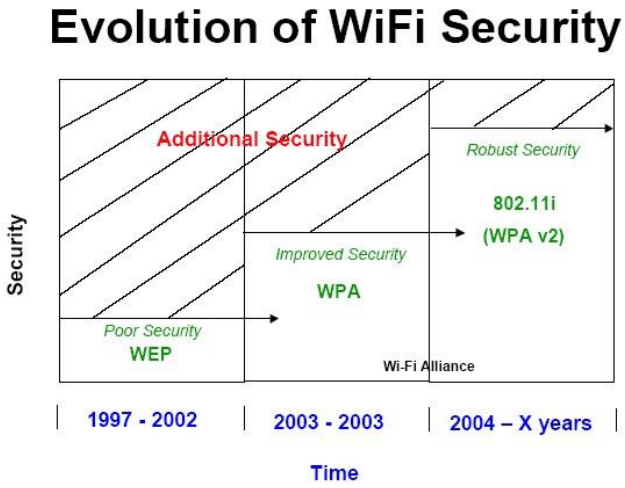
Shared Key Authentication

- Το authentication key κατανέμεται out-of-band
- Το Access Point παράγει ένα "randomly generated" challenge
- Ο σταθμός κωδικοποιεί το challenge χρησιμοποιώντας pre-shared secret



Ασφάλεια σε WLANs – Η Λύση

- Η IEEE βρίσκεται στη διαδικασία ορισμού του προτύπου IEEE 802.11i
  - Extensible Authentication Protocol (EAP)
  - Advanced Encryption Standard (AES)
  - Temporal Key Integrity Protocol (TKIP)
  - Robust Security Network (RSN)

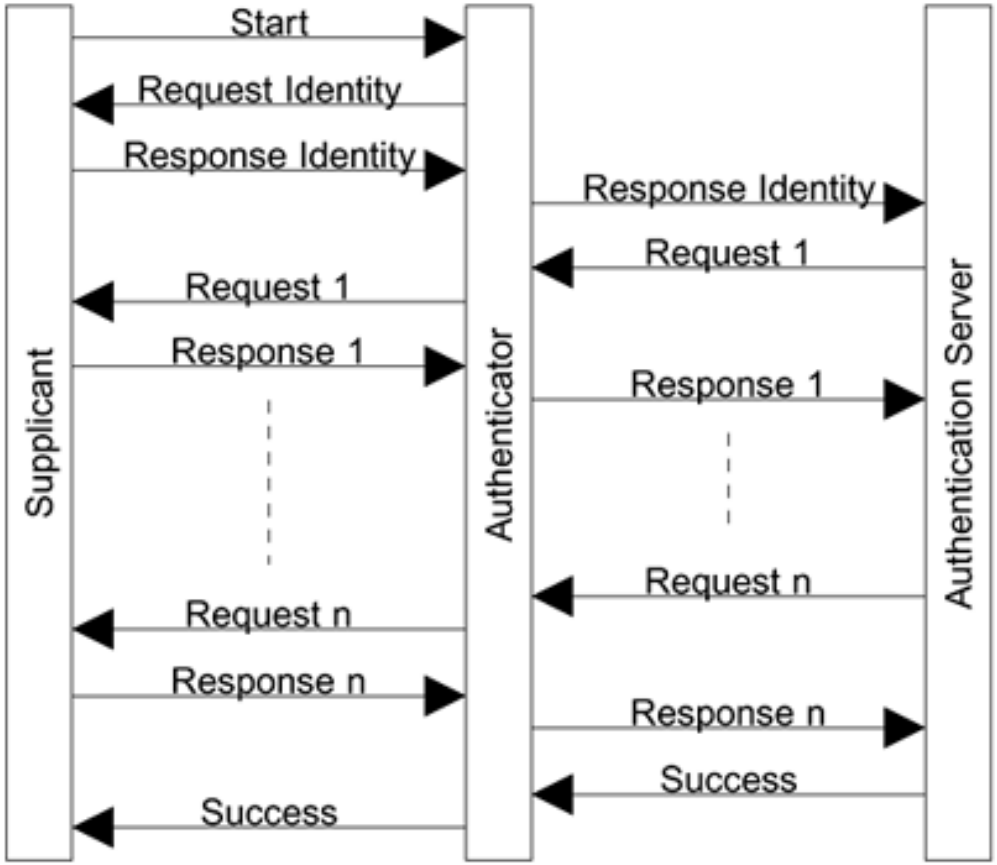


WPA: WiFi Protect Access

802.11i
Authentication enhancement

- Το IEEE 802.1X χρησιμοποιείται για port-based έλεγχο στο δίκτυο. Η επικύρωση γίνεται με την χρήση RADIUS, AEGIS. Και ενός πρωτοκόλλου βασισμένο στο EAP, όπως στο EAP-TLS

Διάδοση μηνυμάτων EAP



802.11i
Key management and establishment

- Τετραμερής χειραψία --- Μετά την ανταλλαγή τεσσάρων μηνυμάτων προκύπτουν τα κλειδιά τα οποία θα χρησιμοποιηθούν στην επικοινωνία.
- Πολυμερής χειραψία --- Δημιουργεί ένα κλειδί για χρήση προς όλη την ομάδα χρηστών. Χρησιμοποιεί τα επιμέρους κλειδιά.

802.11i
Encryption enhancement

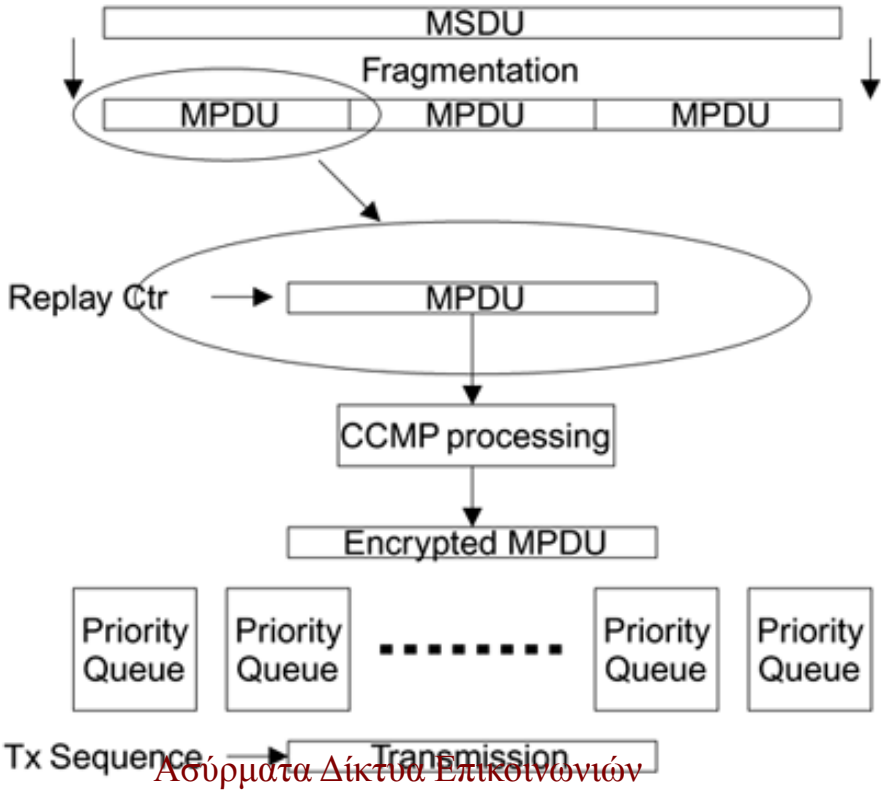
- Το TKIP δημιουργήθηκε για να καλύψει το WEP.
  - Ακεραιότητα --- Michael
  - IV από 24 σε 48bit και αποκλεισμό επισφαλών τιμών. Ταυτόχρονα με χρήση άλλου τρόπου κρυπτογράφησης.
  - TKIP sequence counter (TSC) --- Το IV χρησιμοποιείται σαν μετρητής. Αποκλείονται μηνύματα με TSC μακριά από το τελευταίο που έχει ληφθεί.

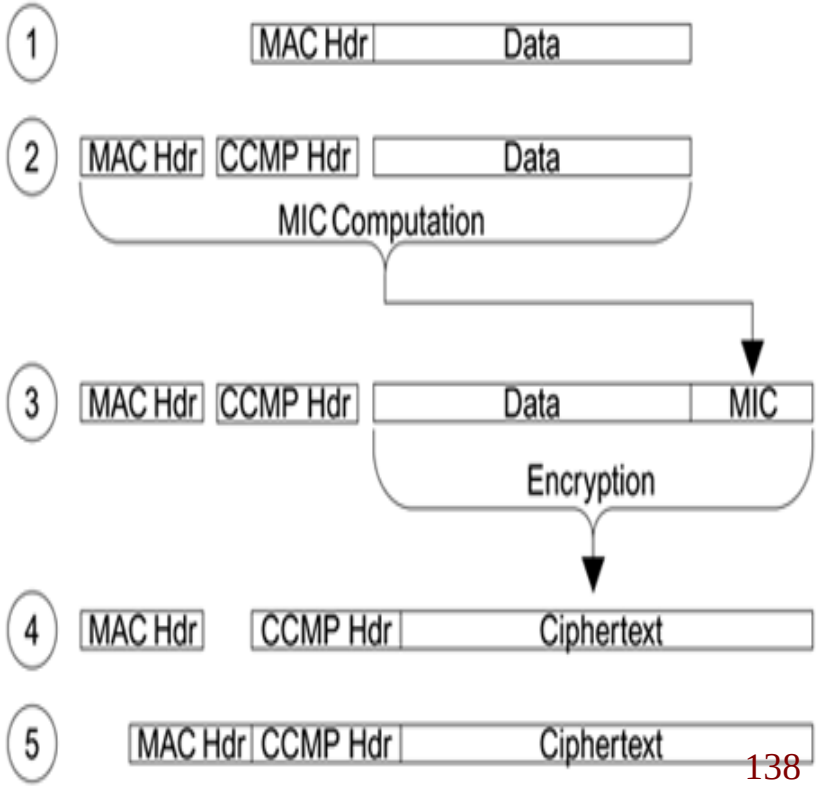
802.11i
Encryption enhancement

- AES-CCMP
  - AES --- Block cipher όπως ήταν ο RC4 για το WEP. Ο AES μπορεί να κρυπτογραφήσει με τέσσερεις διαφορετικές μεθόδους.

802.11i
Encryption enhancement

- Λειτουργία του CCMP





Πρότυπο 802.11n

- Το 802.11n είναι το πρότυπο του MAC επιπέδου για ασύρματο εξοπλισμό τύπου 802.11. Λόγω της αξιοποίησης νέων τεχνικών το 802.11n είναι ικανό να πλησιάσει ταχύτητες μετάδοσης των ~630Mbps