



# Ασύρματα Τοπικά Δίκτυα Wireless Local Area Networks (WLAN)

# Ασύρματα LAN

- ◆ Τα ασύρματα τοπικά δίκτυα επιτρέπουν σε σταθμούς εργασίας, servers, εκτυπωτές, αλλά και συσκευές όπως κινητά τηλέφωνα, PDA, τηλεοράσεις, κάμερες, DVD players, προβολείς κ.λ.π. να συνδέονται σε δίκτυο ή μεταξύ τους χωρίς την ανάγκη εγκατάστασης καλωδιακών συστημάτων

# Ασύρματα LAN

- ◆ Η σύνδεσή τους γίνεται με τη βοήθεια πομποδεκτών που βρίσκονται σε κάθε σταθμό εργασίας κ.λ.π.
- ◆ Η ευελιξία που παρέχουν έχει δώσει τεράστια ώθηση στην εξάπλωσή τους ενώ ισχυρό βοηθητικό στοιχείο είναι ότι πολλά ADSL modem/router έχουν και ασύρματους πομποδέκτες για τη διευκόλυνση της σύνδεσης στο διαδίκτυο

# Ασύρματα LAN

- ◆ Η ασύρματη επικοινωνία γίνεται με μετάδοση πακέτων σε μορφή half duplex σε ταχύτητες διασύνδεσης που πρακτικά κυμαίνονται από 1 έως 100 Mbps και έχει γίνει “defacto standard” για την ακραία ευρυζωνική διασύνδεση σε σπίτια, γραφεία ή δημόσια σημεία πρόσβασης στο διαδίκτυο (hot spots)

# Ασύρματα LAN

## Πλεονεκτήματα

- ◆ Κινητικότητα καθώς εξυπηρετούν τη σύνδεση και επικοινωνία χωρίς την ανάγκη σταθερής καλωδιακής σύνδεσης
- ◆ Ταχύτητα υλοποίησης
- ◆ Χαμηλό κόστος εγκατάστασης και λειτουργίας

# Ασύρματα LAN

## Μειονεκτήματα

- ◆ Δυσκολία κάλυψης όλων των χώρων ενός κτιρίου
- ◆ Περιορισμός στη χωρητικότητα που οφείλεται σε παρεμβολές ή στους περιορισμούς του ασύρματου εύρους ζώνης συχνοτήτων
- ◆ Ασφάλεια επικοινωνίας
- ◆ Αξιοπιστία επικοινωνίας (παρεμβολές)

# Πρότυπα

- ◆ Η ΙΕΕΕ τυποποίησε την οικογένεια 802.11 για τα ασύρματα τοπικά δίκτυα
- ◆ Το 802.11 υποδιαιρείται σε ομάδες εργασίας που παράγουν συνώνυμες τυποποιήσεις:

**802.11a** WLAN μέχρι 54 Mbps στα 5 GHz με OFDM

# Πρότυπα

**802.11b** WLAN μέχρι 11 Mbps στα 2,4 GHz με DSSS

**802.11c** Bridge procedures

**802.11d** ρυθμίσεις στο MAC για διεθνή  
περιαγωγή

**802.11e** quality of service στα a,b,g

**802.11g** WLAN μέχρι 54 Mbps στα 2,4 GHz με OFDM



# Πρότυπα

**802.11h** διαχείριση φάσματος στα 5 GHz με έλεγχο συγκρούσεων

**802.11i** θέματα ασφάλειας κρυπτογράφησης - authentication

**802.11n** WLAN μέχρι 100Mbps με πολλαπλούς πομπούς/δέκτες

**802.11p** πρόσβαση από κινούμενους σταθμούς

# Πρότυπα

**802.11r** ταχεία περιαγωγή

**802.11s** δικτύωση βρόγχου

**802.11u** διασύνδεση με μη 802 δίκτυα

**802.11v** διαχείριση ασύρματου δικτύου

**802.11w** protected management frames

**802.11z** extensions to DLS

# Πρότυπα

**802.11aa** streaming audio video

**802.11ac** για υψηλές συχνότητες >6 GHz

**802.11ad** για πολύ υψηλές συχνότητες >60 GHz

- ◆ Οι συσκευές που ακολουθούν τα πρότυπα 802.11b,g,n έχουν κοινή ονομασία Wi-Fi που προέρχεται από το Wireless Fidelity (κατά το Hi-Fi)

# Πρότυπα

- ◆ Για την εύκολη διασυνδεσιμότητα με συστήματα διαφορετικών κατασκευαστών ο οργανισμός Wi-Fi Alliance δημιουργεί διαδικασίες πιστοποίησης συμβατότητας

# Πρότυπα

- ◆ Το πρότυπο 802.11 υποστηρίζει δύο λογικές διασύνδεσης

**Ομότιμη** (ad-hoc) όπου όλοι οι σταθμοί είναι ισότιμοι στην πρόσβαση στο κοινό μέσο

Με **σημείο πρόσβασης** (infrastructure) όπου ένας κεντρικός κόμβος αναλαμβάνει τον έλεγχο πρόσβασης στο κοινό μέσο

# Στοιχεία ασύρματου LAN

- ◆ Σημείο πρόσβασης (Access Point-AP) είναι στην ουσία το ασύρματο hub όπου συνδέονται όλοι οι ασύρματοι σταθμοί και συνήθως είναι το σημείο σύνδεσης με το ενσύρματο δίκτυο
- ◆ Σταθμοί οι συσκευές που διαθέτουν ασύρματο πομποδέκτη και το κατάλληλο λογισμικό, συμβατές με το πρότυπο 802.11

# Στοιχεία ασύρματου LAN

- ◆ Δικτυακές ομάδες (Service Sets) για να υπάρχει επικοινωνία μεταξύ συσκευών πρέπει αυτές να είναι ενταγμένες κάθε φορά σε μια ασύρματη ομάδα. Σύμφωνα με το πρότυπο 802.11 οι ομάδες αυτές αναφέρονται ως WLAN Service Sets (SS) και διακρίνονται σε BSS, IBSS και ESS

# Στοιχεία ασύρματου LAN

Το **Independent BSS** (IBSS) είναι ένα σύνολο από σταθμούς που επικοινωνούν απευθείας μεταξύ τους χωρίς τη μεσολάβηση AP (ad-hoc σύνδεση)

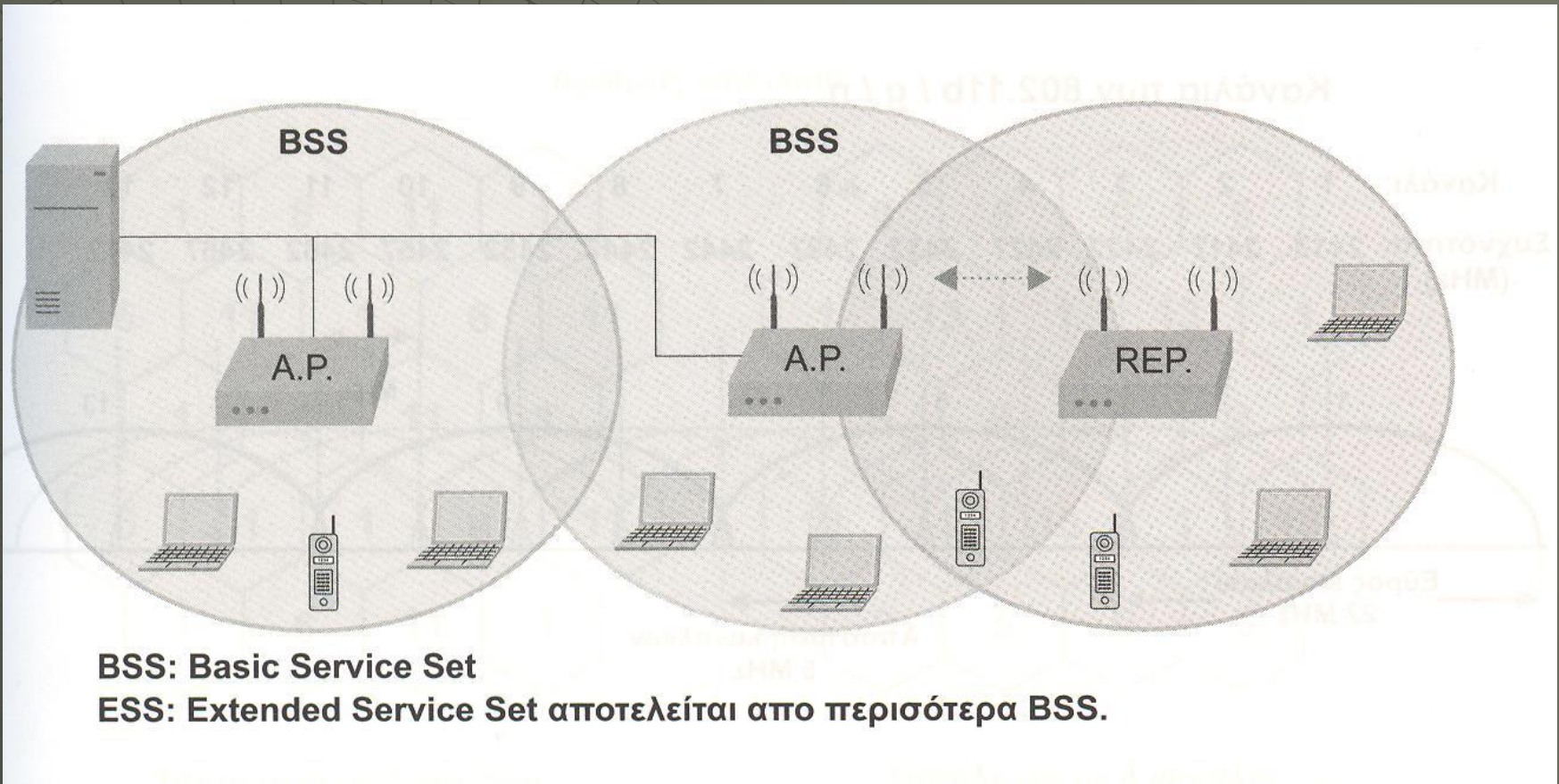
Το **Basic Service Set** (BSS) είναι ένα σύνολο από σταθμούς που επικοινωνούν με ένα AP και η λειτουργία ξεκινά από το ίδιο το AP



# Στοιχεία ασύρματου LAN

Το **Extended Service Set (ESS)** είναι ένα εκτεταμένο δίκτυο που χρησιμοποιεί περισσότερα του ενός AP. Αποτελείται από περισσότερα του ενός BSS και λειτουργεί ως ενιαίο με την ίδια ταυτότητα. Για την επέκταση ενός BSS σε ESS μπορούμε να προσθέσουμε AP με ενσύρματη σύνδεση ή ασύρματα (ως επαναλήπτες)

# Στοιχεία ασύρματου LAN



# Στοιχεία ασύρματου LAN

- ◆ Κάθε Service Set χαρακτηρίζεται από μια ταυτότητα (ID) την SSID που αποτελείται από 2-32 χαρακτήρες ενώ παράλληλα υπάρχει και η ταυτότητα του κάθε AP των 48 bit η οποία δεν είναι εμφανής και συνήθως είναι η MAC address του AP
- ◆ Σύστημα Διανομής για τη διασύνδεση των διαφόρων AP σε ένα ESS

# Στοιχεία ασύρματου LAN

- ◆ Μέσο μετάδοσης Για την ασύρματη μετάδοση μεταξύ των σταθμών ή των AP χρησιμοποιούνται οι περιοχές συχνοτήτων 2,4 και 5 GHz. Το χρησιμοποιούμενο φάσμα συχνοτήτων και ο διαχωρισμός τους σε κανάλια είναι ανάλογα με το πρότυπο που ακολουθείται. Το ίδιο συμβαίνει και για τις διαμορφώσεις

# Εύρος ζώνης - κανάλια

- ◆ Για την ασύρματη ζεύξη χρησιμοποιούνται δύο **ελεύθερες** περιοχές συχνοτήτων που δεν απαιτούν αδειοδότηση (στα 2,4 GHz και στα 5 GHz). Στην πράξη χρησιμοποιείται περισσότερο η 2,4 GHz
- ◆ Στα 802.11 b,g χρησιμοποιείται το φάσμα 2400-2483 GHz →

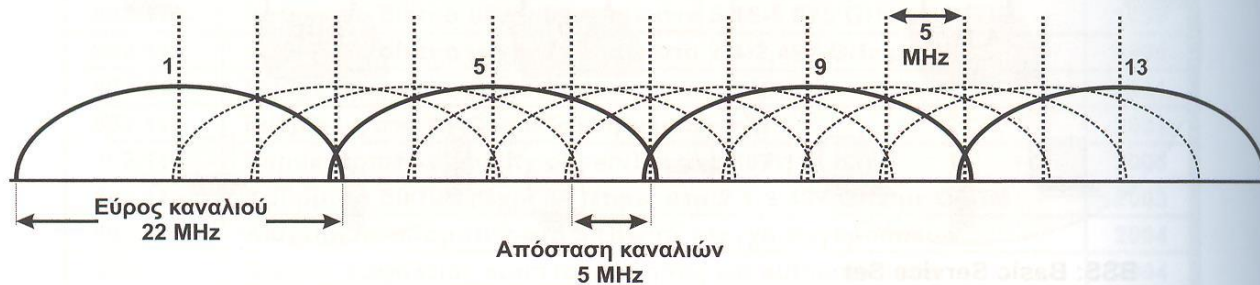
# Εύρος ζώνης - κανάλια

→ που διαιρείται σε 13 επικαλυπτόμενα κανάλια που το καθένα έχει εύρος ζώνης 22 MHz, ενώ η απόσταση μεταξύ των κεντρικών συχνοτήτων των καναλιών είναι 5 MHz. Στις ΗΠΑ χρησιμοποιούνται μόνο τα 11 κανάλια ενώ στην Ιαπωνία υπάρχει και 14<sup>ο</sup> κανάλι στο τέλος της κλίμακας

# Εύρος ζώνης - κανάλια

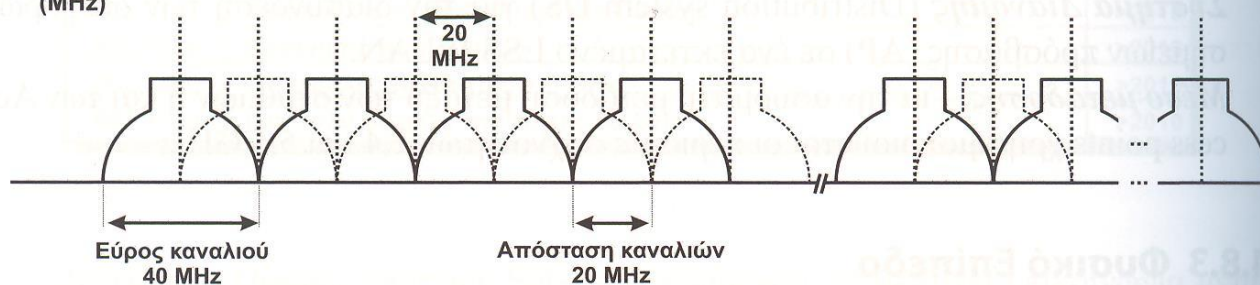
## Κανάλια των 802.11b / g / n

Κανάλι:	1	2	3	4	5	6	7	8	9	10	11	12	13
Συχνότητα: (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472



## Κανάλια των 802.11a / n

Κανάλι:	1	2	3	4	5	6	7	8	9	10	11	...	19
Κανάλι:	36	40	44	48	52	56	60	64	100	104	108	...	140
Συχνότητα: (MHz)	5180	5200	5220	5240	5260	5280	5300	5320	5500	5520	5540	...	5700



# Εύρος ζώνης - κανάλια

- ◆ Στην περιοχή των 5 GHz που διατίθεται μεγαλύτερο φάσμα η απόσταση των καναλιών είναι 20 MHz
- ◆ Έχουμε πολύ περισσότερα μη επικαλυπτόμενα κανάλια
- ◆ Όσο αυξάνεται η συχνότητα μειώνεται η εμβέλεια και έτσι σε αυτή την περιοχή έχουμε μικρότερες αποστάσεις και απαιτούνται πολλά AP



# Εύρος ζώνης - κανάλια

- ◆ Το πρότυπο 802.11 (για τη ζώνη 2,4 GHz που χρησιμοποιείται στην πράξη) προβλέπεται ότι το σήμα εκπομπής σε κάθε κανάλι πρέπει να εξασθενεί κατά 30 db σε απόσταση +11 MHz και -11MHz από την κεντρική συχνότητα ώστε να ελαχιστοποιούνται οι παρεμβολές στα γειτονικά κανάλια

# Εύρος ζώνης - κανάλια

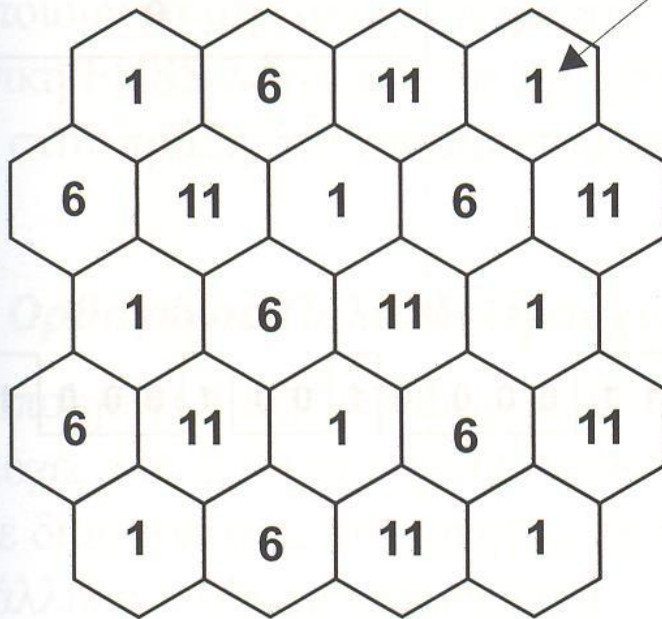
- ◆ Υπάρχουν μόνο 3 μη επικαλυπτόμενα κανάλια (1, 6, 11) ή 4 κανάλια με ελάχιστη ακραία επικάλυψη (1, 5, 9, 13)
- ◆ Χρειάζεται προσοχή κατά την εγκατάσταση των συστημάτων γιατί αν υπάρχουν άλλα AP με γειτονικά επικαλυπτόμενα κανάλια θα υπάρχουν παρεμβολές μεταξύ τους→

# Εύρος ζώνης - κανάλια

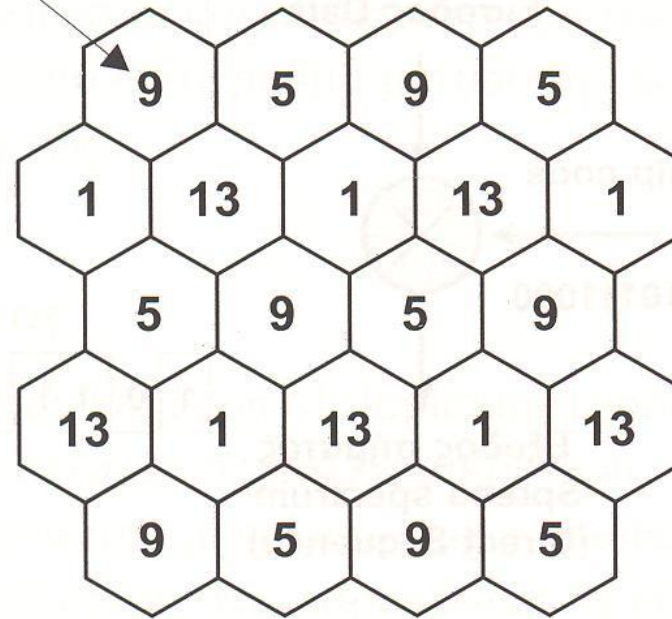
- με αποτέλεσμα την σημαντική μείωση των επιδόσεων ταχύτητας και απόστασης
- ◆ Για την βέλτιστη λειτουργία, πρέπει πρώτα να γίνεται ανίχνευση των ενεργών καναλιών στην περιοχή έτσι ώστε η προσθήκη ενός νέου AP να προγραμματίζεται σε μακρινά μη επικαλυπτόμενα κανάλια

# Εύρος ζώνης - κανάλια

Αριθμός καναλιού



Τοπολογία με 3 κανάλια



Τοπολογία με 4 κανάλια

# Διαμόρφωση

- ◆ Το πρότυπο 802.11 προσδιορίζει τρεις τεχνικές για την ασύρματη μετάδοση:

Direct Sequence Spread Spectrum  
(DSSS)

Frequency Hopping Spread Spectrum  
(FHSS)

Orthogonal Frequency Division  
Multiplexing (OFDM)

# DSSS

- ◆ Η τεχνολογία μετάδοσης ευρέος φάσματος χρησιμοποιήθηκε σε στρατιωτικές εφαρμογές για δεκαετίες λόγω των πλεονεκτημάτων της. Αντοχή σε παρεμβολές και δυσκολία υποκλοπής.
- ◆ Στην DSSS κάθε Bit κωδικοποιείται με ένα τρόπο γνωστό μόνο στον πομπό και τον δέκτη και εκπέμπεται →

# DSSS

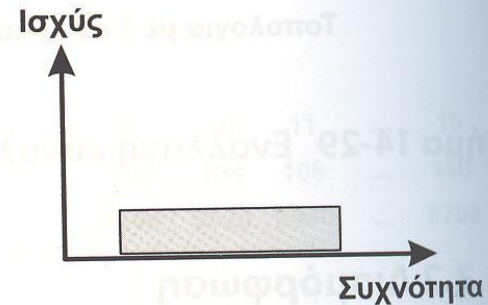
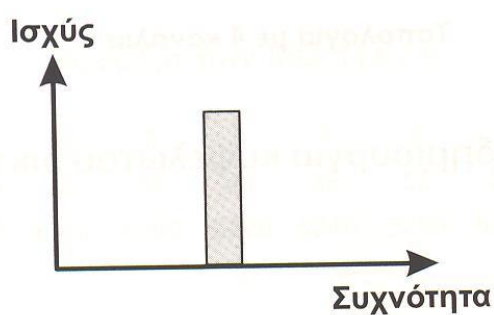
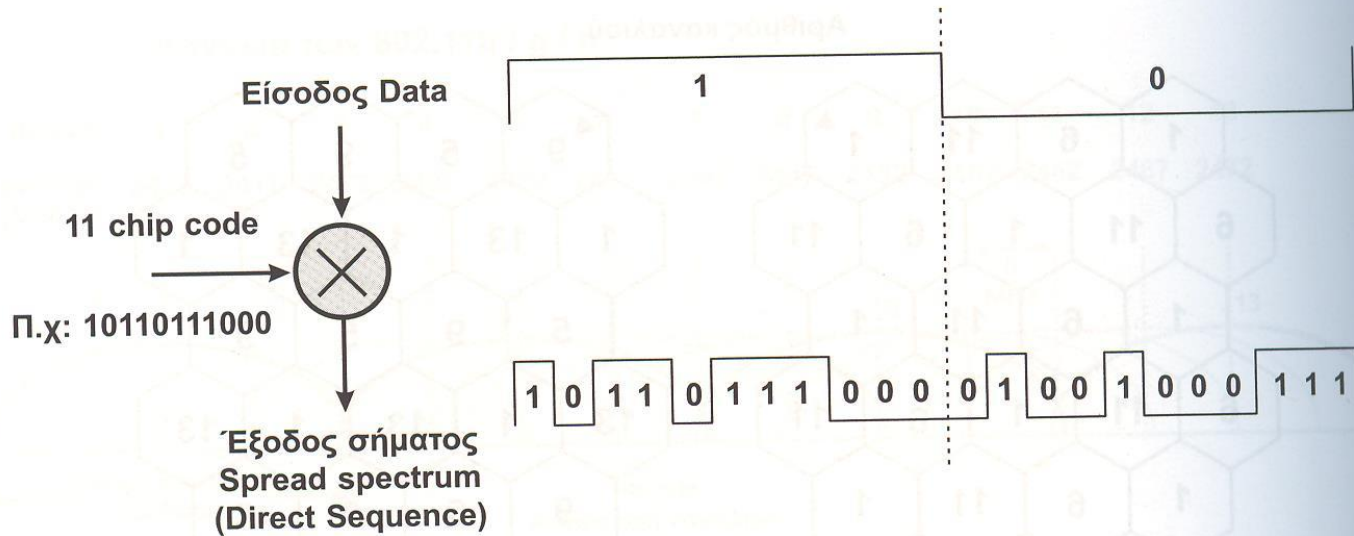
- σε όλες τις διαθέσιμες συχνότητες.  
Αν ένας υποκλοπέας αποθηκεύσει τα μεταδιδόμενα δεδομένα για να τα επεξεργαστεί, η πιθανότητα αναγνώρισης των πραγματικών δεδομένων είναι εξαιρετικά μικρή καθώς υπάρχουν χιλιάδες τρόποι κωδικοποίησης
- ◆ Για 1Mbps το DSSS χρησιμοποιεί→

# DSSS

- τεχνική διαμόρφωσης DB-PSK (differential binary PSK) ενώ για ρυθμό μετάδοσης 2-11 Mbps την DQ-PSK (differential quadrature PSK)
- ◆ Τα συστήματα DSSS κατανέμουν την ενέργεια του εκπεμπόμενου σήματος σε μεγάλο φάσμα συχνοτήτων διαμορφώνοντας το αρχικό σήμα με ένα άλλο μεγαλύτερου εύρους ζώνης



# DSSS



# DSSS

- ◆ Σύμφωνα με το 802.11 για τη διασπορά αυτή χρησιμοποιείται ένα σήμα που αποτελείται από 11 bit (chips) το οποίο πολλαπλασιάζεται με κάθε bit των προς διαμόρφωση δεδομένων
- ◆ Ο λόγος chip/bit ονομάζεται λόγος διασποράς και χαρακτηρίζει το βαθμό διασποράς στη ζώνη συχνοτήτων

# DSSS

- ◆ Το πρότυπο ορίζει λόγο 11 αλλά διάφορα προϊόντα χρησιμοποιούν και μεγαλύτερο (11-20)
- ◆ Όσο μεγαλύτερο πλήθος των chips τόσο πιο ανθεκτική σε σφάλματα είναι η μετάδοση αλλά απαιτείται μεγαλύτερο φάσμα συχνοτήτων
- ◆ Ο δέκτης κάνει την αντίστροφη διαδικασία μετατροπής των chips/bit

# DSSS

- ◆ Το ισχυρό πλεονέκτημα αυτής της διαμόρφωσης είναι ότι η διασπορά σε μεγαλύτερο φάσμα το κάνει να αντιστέκεται καλύτερα σε παρεμβολές ενώ βοηθά τον δέκτη να μπορεί να ξεχωρίσει το σήμα ακόμη και όταν είναι ασθενές ή σε θορυβώδες περιβάλλον

# FHSS

- ◆ Ο πομπός χρησιμοποιεί διαδοχικές εκπομπές σε μια σχετικά στενή περιοχή συχνοτήτων και μεταπηδά από συχνότητα σε συχνότητα μέσα στην περιοχή του καναλιού
- ◆ Οι συσκευές απαιτείται να γνωρίζουν την ακριβή ακολουθία μεταπηδήσεων αλλά και το χρόνο παραμονής του πομπού σε κάθε συχνότητα

# FHSS

- ◆ Το 802.11 προβλέπει διαίρεση του χρήσιμου φάσματος στα 2,4 GHz σε 79 κανάλια του 1 MHz. Ο μέγιστος χρόνος παραμονής σε κάθε κανάλι είναι 400msec ή 2,5 hops/sec. Προβλέπει επίσης 22 διαφορετικούς ακολουθιακούς συνδυασμούς μετάπτωσης ώστε να μην αλληλοπαρεμβάλλονται οι σταθμοί

# OFDM

- ◆ Η κωδικοποίηση OFDM διαιρεί το σήμα σε πολλά μικρότερα τα οποία εκπέμπει σε διαφορετικές συχνότητες επιτυγχάνοντας έτσι μεγαλύτερους ρυθμούς μετάδοσης, ενώ παράλληλα όλη η μετάδοση είναι ανθεκτική σε παρεμβολές. Χρησιμοποιείται στην 802.11a, 802.11g και 802.11n

# Υλοποιήσεις 802.11

- ◆ Πέραν του αρχικού προτύπου 802.11 έχουν υλοποιηθεί τα 802.11a,b,g,n
- ◆ **802.11b** λειτουργεί στη ζώνη 2,4 GHz με ρυθμούς μετάδοσης έως 11Mbps. Εμβέλεια τα 50m σε εσωτερικό χώρο στα 11 ενώ 130m στο 1 Mbps. Σε εξωτερικό χώρο με οπτική επαφή τα 200m στα 11 και έως 400m στο 1 Mbps



# Υλοποιήσεις 802.11

- ◆ **802.11a** λειτουργεί στη ζώνη 5,15-5,875 GHz που είναι λιγότερο χρησιμοποιούμενη σε σχέση με τα 2,4 με διαμόρφωση OFDM με ρυθμούς μετάδοσης 6,8,12,18,24,36,48,54 Mbps διότι χρησιμοποιεί μεγαλύτερο εύρος ζώνης συχνοτήτων (0,725GHz έναντι 0,097 GHz στη 802.11b). Για τα 54Mbps εμβέλεια 10m ενώ στα 6→

# Υλοποιήσεις 802.11

- η απόσταση φτάνει τα 70m. Στην πράξη οι κατασκευαστές έχουν εγκαταλείψει τη βασική 802.11 καθώς και την 802.11a
- ◆ Το 2003 Εγκρίθηκε το 802.11g που λειτουργεί στα 2,4 GHz αλλά με OFDM που επιτρέπει ρυθμούς μετάδοσης έως 54 Mbps όπως η 802.11a για μεγαλύτερες αποστάσεις

# Υλοποιήσεις 802.11

- ◆ Σε εσωτερικούς χώρους φθάνει τα 25m στα 54 Mbps ενώ στα 6 η απόσταση αγγίζει τα 90m. Σε εξωτερικούς χώρους στα 54 μπορεί να φτάσει τα 75m ενώ στα 6 καλύπτει μέχρι 400m
- ◆ Η τελευταία και πιο εξελιγμένη τυποποίηση 802.11n έχει τα ίδια βασικά στοιχεία όπως η 802.11g

# Υλοποιήσεις 802.11

- ◆ Με την προσθήκη της τεχνικής MIMO (multiple input, multiple output) συνδυάζονται πολλαπλά σήματα που εκπέμπονται ταυτόχρονα μέσω διαφορετικών καναλιών επιτυγχάνοντας έτσι ρυθμό μετάδοσης μέχρι 144 Mbps. Απαιτεί όμως περισσότερες κεραιές στον πομποδέκτη. Η τυποποίηση αυτή →

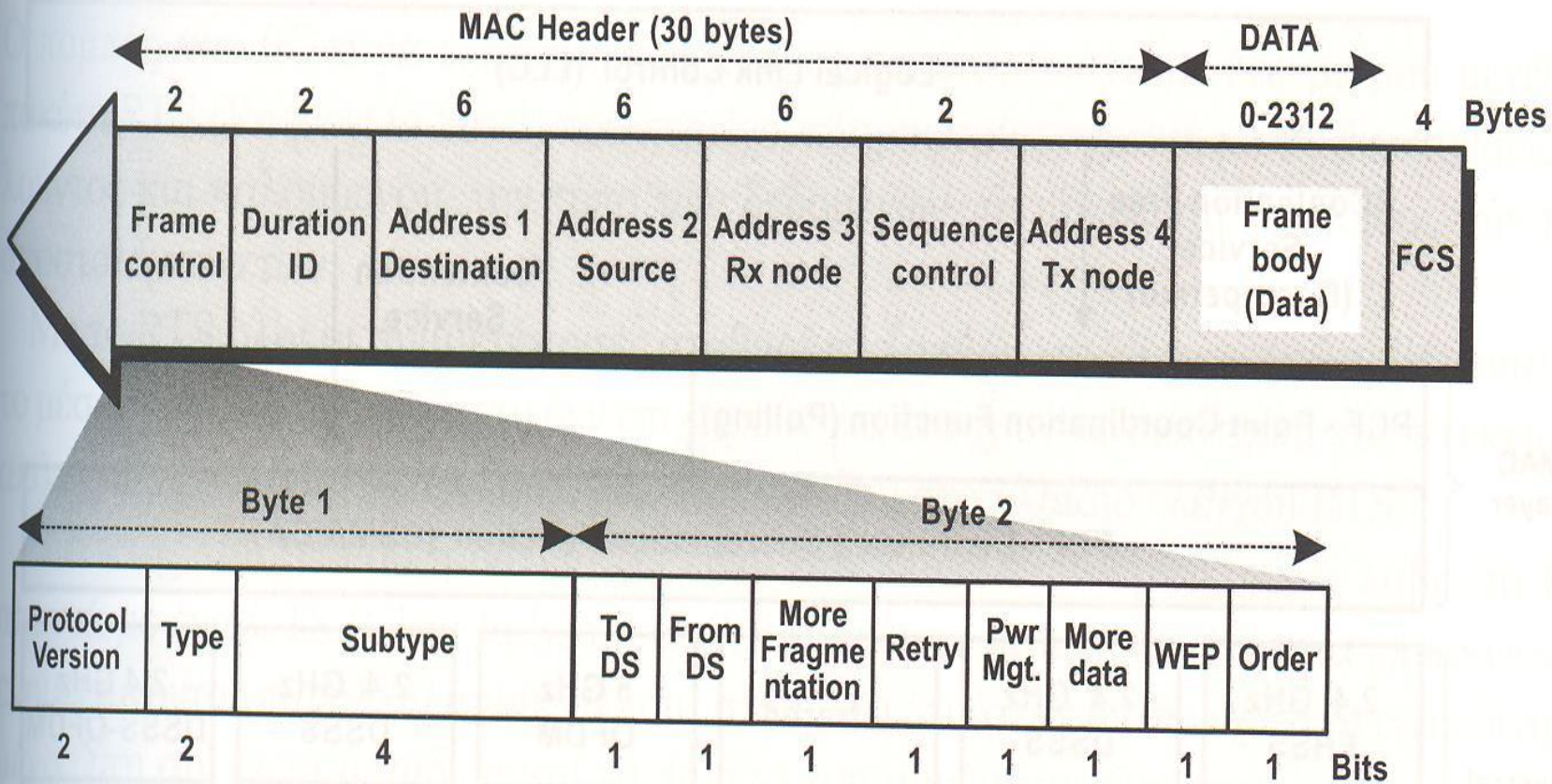
# Υλοποιήσεις 802.11

- φτιάχτηκε για να λειτουργεί και στα 2,4 GHz αλλά και στα 5 GHz
- ◆ Γενικά η ζώνη των 2,4 πλεονεκτεί έναντι των 5 καθώς οι χαμηλότερες συχνότητες εμφανίζουν μεγαλύτερη εμβέλεια και διεισδυτικότητα σε χώρους κτιρίων. Είναι όμως σε χρήση και από συσκευές όπως φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα κ.λ.π.

# Δομή πλαισίου 802.11

- ◆ Το πλαίσιο μοιάζει με αυτό του Ethernet αλλά με την προσθήκη ορισμένων χαρακτηριστικών ελέγχου, διαχείρισης και αποκατάστασης σφαλμάτων που είναι αναγκαία για το ασύρματο περιβάλλον

# Δομή πλαισίου 802.11



# Δομή πλαισίου 802.11

**Frame Control** με μήκος 2 byte προσδιορίζει το είδος των δεδομένων στο πλαίσιο και την ταχύτητα λειτουργίας της ασύρματης ζεύξης. Τα δύο πρώτα bit προσδιορίζουν το πρότυπο που χρησιμοποιείται

**Duration ID** παίρνει 3 τιμές, για τη διάρκεια, την περίοδο contention free και το PS-Poll



# Δομή πλαισίου 802.11

Το **1<sup>ο</sup> πεδίο** διεύθυνσης αναφέρεται στην διεύθυνση του παραλήπτη

Το **2<sup>ο</sup> πεδίο** αναφέρεται σε αυτήν του αποστολέα

Το **3<sup>ο</sup> πεδίο** χρησιμοποιείται για φιλτράρισμα διευθύνσεων από το δέκτη. Όταν το 1<sup>ο</sup> bit είναι 0 προσδιορίζει μια συγκεκριμένη διεύθυνση ενώ όταν είναι 1 αναφέρεται σε ομάδα διευθύνσεων

# Δομή πλαισίου 802.11

- ◆ Αν όλα τα bit της διεύθυνση του παραλήπτη είναι 1 τότε το μήνυμα απευθύνεται σε όλους τους σταθμούς που είναι συνδεδεμένοι ασύρματα με το συγκεκριμένο AP

**Sequence Control** είναι ο αριθμός ακολουθίας για την επανασύνδεση τμηματοποιημένων μηνυμάτων και έχει μήκος 2 byte

# Δομή πλαισίου 802.11

**FCS** χρησιμοποιείται για την ακεραιότητα της πληροφορίας του μηνύματος. Ο πομπός το υπολογίζει και το τοποθετεί στο τέλος. Ο δέκτης πρέπει να το επανυπολογίσει και πρέπει να βρει το ίδιο αλλιώς θεωρεί ότι υπήρξε σφάλμα κατά τη μετάδοση

# Προσπέλαση στο 802.11

- ◆ Στα ασύρματα LAN επειδή δεν μπορεί να γίνεται ταυτόχρονα λήψη από τον δέκτη και ανίχνευση σύγκρουσης, η τεχνική CSMA/CD δεν είναι κατάλληλη. Η τεχνική CSMA/CA (Collision Avoidance) δεν επιχειρεί να ανιχνεύσει την σύγκρουση αλλά να την αποφύγει ενώ ζητά και επιβεβαίωση ορθής λήψης από το δέκτη

# Προσπέλαση στο 802.11

- ◆ Η επικοινωνία είναι **half duplex** οπότε σε ένα διαθέσιμο κανάλι όταν ένας εκπέμπει οι άλλοι ακούν και μπορούν να εκπέμψουν μόνο όταν το κανάλι ελευθερωθεί
- ◆ Με την CSMA/CA μια συσκευή που θέλει να εκπέμψει ανιχνεύει συνεχώς την κίνηση στο κανάλι μέχρι να το βρει ελεύθερο

# Προσπέλαση στο 802.11

- ◆ Αναμένει για ένα χρονικό διάστημα (διαφορετικό για την καθεμία) που καθορίζεται από μια ψευδοτυχαία γεννήτρια επιλογής καθυστέρησης και αμέσως μετά από αυτό το διάστημα εκπέμπει. Έτσι αποφεύγεται η σύγκρουση όταν πολλοί σταθμοί θέλουν να εκπέμψουν μόλις απελευθερωθεί το κανάλι

# Προσπέλαση στο 802.11

- ◆ Πέραν του μηχανισμού της ψευδοτυχαίας καθυστέρησης (contention window) υπάρχει ένας πρόσθετος χρόνος που οφείλει μια συσκευή να περιμένει που ονομάζεται απόσταση πλαισίων (Interframe Spacing-IFS). Αυτός ο χρόνος εξαρτάται από τον τύπο του πλαισίου και το είδος της διαμόρφωσης

# Προσπέλαση στο 802.11

- ◆ Τα πλαίσια ελέγχου έχουμε μικρότερο IFS (10μsec) σε σχέση με αυτά των δεδομένων (50 μsec). Η διαφοροποίηση αυτή δίνει προτεραιότητα στα πλαίσια ελέγχου. Οι καθυστερήσεις IFS χωρίζονται σε:
  - ◆ SIFS (Short IFS) για πλαίσια ελέγχου
  - ◆ DIFS (Distributed IFS) για πλαίσια δεδομένων



# Προσπέλαση στο 802.11

- ◆ EIFS (Extended IFS) για τις περιπτώσεις επανεκπομπής πλαισίων που συμβαίνουν μετά από σφάλμα στη μετάδοση
- ◆ Η CSMA/CA έχει δύο τεχνικές προσπέλασης. Η Distributed Coordination Function (DCF) είναι αυτή που περιγράφηκε μέχρι τώρα και η Point Coordination Function (PCF)

# Προσπέλαση στο 802.11

- ◆ Στην PCF το AP αναλαμβάνει τη ρύθμιση της πρόσβασης βάσει διαδικασίας polling που καθορίζει την διαδοχική πρόσβαση όλων των σταθμών. Το IFS εδώ ονομάζεται PIFS (Point IFS) και είναι (25-30 μsec) μικρότερο από DIFS και μεγαλύτερο από SIFS

# Προσπέλαση στο 802.11

- ◆ Το πρότυπο 802.11 προβλέπει επίσης εκτός της βασικής διαδικασίας προσπέλασης (που αναλύθηκε έως τώρα) και μια δεύτερη που ονομάζεται RTS/CTS. Ο πομπός που θέλει να εκπέμψει στέλνει ένα μικρό πλαίσιο Request To Send (RTS) που περιέχει πληροφορίες σχετικά με τις διευθύνσεις, τον τύπο δεδομένων κ.α.

# Προσπέλαση στο 802.11

- ◆ Όλοι οι σταθμοί αντιλαμβάνονται ότι το μέσο είναι δεσμευμένο και δεν επιχειρούν για ένα χρονικό διάστημα που το εκτιμούν από τις πληροφορίες του πλαισίου RTS. Ο δέκτης του οποίου η διεύθυνση είναι στο πεδίο του παραλήπτη, απαντά με ένα Clear To Send (CTS) επιβεβαιώνοντας την επικοινωνία και ενημερώνοντας ότι →

# Προσπέλαση στο 802.11

→ το μέσο συνεχίζει να είναι δεσμευμένο. Στη συνέχεια μεταδίδονται τα πλαίσια του μηνύματος με ενδιάμεση επιβεβαίωση ορθής λήψης ACKnowledge από τον δέκτη. Αν ο πομπός δεν λάβει το CTS ή κάποιο ACK τότε η διαδικασία επαναλαμβάνεται

# Προσπέλαση στο 802.11

- ◆ Με την CSMA/CA έχουμε πραγματική εκμετάλλευση του ρυθμού μετάδοσης όχι πάνω από το μισό της ονομαστικής (π.χ. στα 54Mbps του φυσικού επιπέδου η επιτεύξιμη ταχύτητα δεν υπερβαίνει τα 27 Mbps στο υποεπίπεδο LLC)

# Διαδικασία σύνδεσης

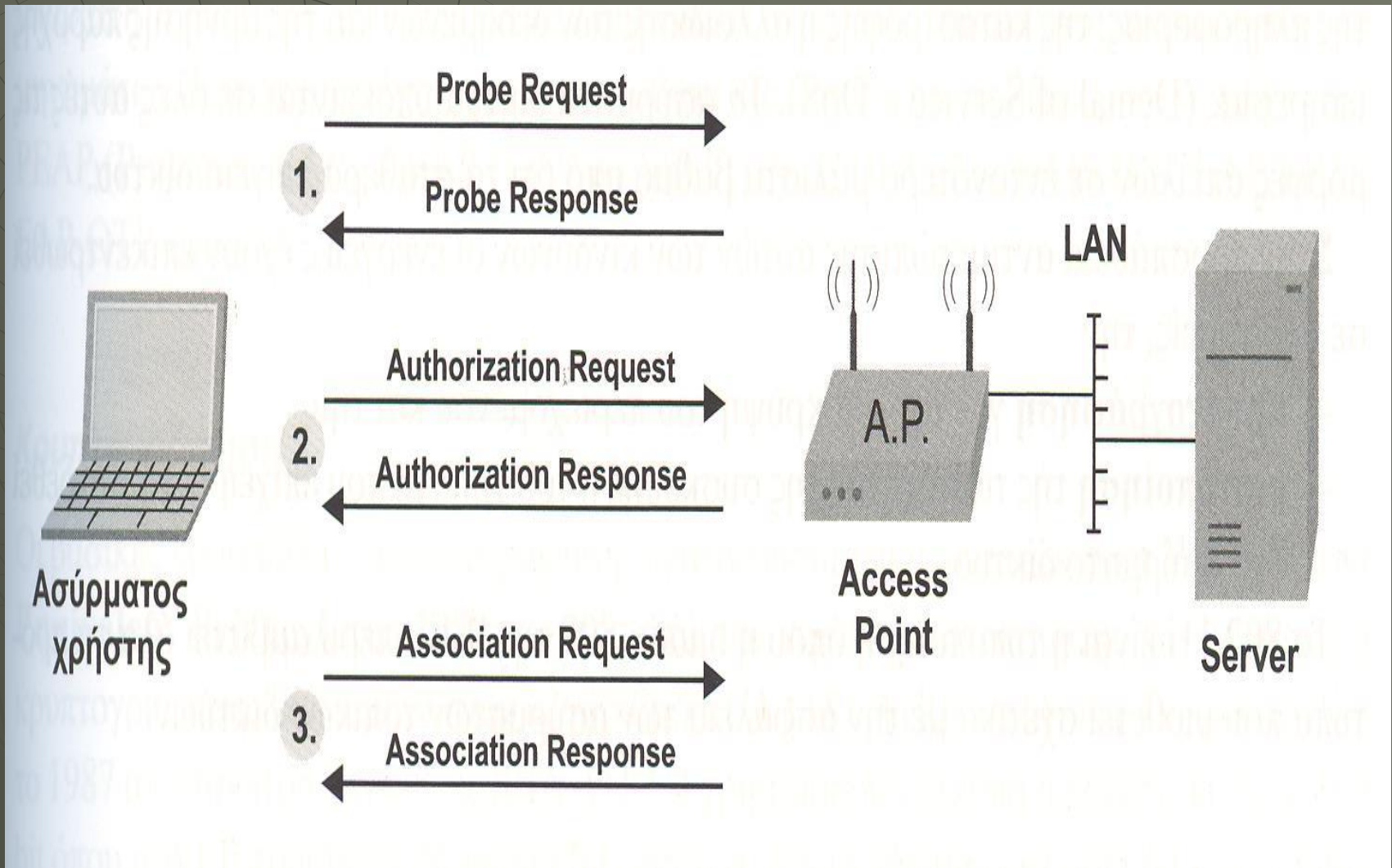
- ◆ Για να συνδεθεί ένας σταθμός σε ένα BSS υπάρχουν δύο εναλλακτικές. Η Active Scanning και η Passive Scanning
- ◆ Στην Active ο σταθμός που επιχειρεί να ενταχθεί στέλνει ένα μήνυμα Probe Request στο οποίο τα υπάρχοντα AP οφείλουν να απαντήσουν με ένα Probe Response

# Διαδικασία σύνδεσης

- ◆ Έτσι δηλώνουν την παρουσία τους και το SSID τους. Το Probe request στέλνεται διαδοχικά σε όλα τα κανάλια για την εύρεση τυχόν AP.
- ◆ Στην Passive ο σταθμός παρακολουθεί διαδοχικά τα υπάρχοντα κανάλια ανιχνεύοντας την ύπαρξη μηνυμάτων (beacons) τα οποία στέλνονται από το AP



# Διαδικασία σύνδεσης



# Διαδικασία σύνδεσης

- ◆ Η τυπική διαδικασία αποτελείται από 3 φάσεις. Φάση Ανίχνευσης AP, Φάση Πιστοποίησης (του σταθμού με χρήση μηνυμάτων authentication request και authentication response) και η Φάση Σύνδεσης (με ανταλλαγή μηνυμάτων association request και response).

# Διαδικασία σύνδεσης

- ◆ Η τελευταία φάση είναι απαραίτητη όταν ένας πιστοποιημένος σταθμός μετακινείται μεταξύ διαφορετικών AP σε ένα εκτεταμένο ESS έτσι ώστε το δίκτυο να γνωρίζει μέσω ποιου AP επικοινωνεί μαζί του
- ◆ Η μετακίνηση μεταξύ ασύρματων δικτύων ή σε διαφορετικές περιοχές εκπομπής ενός δικτύου = Περιαγωγή

# Διαδικασία σύνδεσης

- ◆ Όταν ένας σταθμός μετακινείται από την εμβέλεια ενός BSS σε ένα άλλο διακρίνουμε δύο τύπους περιαγωγής (Roaming). Την απρόσκοπτη και την περιαγωγή με επανασύνδεση
- ◆ Σε ESS προσφέρεται η πρώτη χωρίς την ανάγκη των 2 πρώτων φάσεων της σύνδεσης αλλά μόνο του Association

# Διαδικασία σύνδεσης

- ◆ Αν η μετακίνηση γίνεται μεταξύ διαφορετικών ESS τότε γίνεται περιαγωγή με επανασύνδεση που πρακτικά σημαίνει τη διακοπή των εφαρμογών ανωτέρων επιπέδων

# Ασφάλεια

- ◆ Το θέμα της ασφάλειας είναι το σοβαρότερο που αντιμετωπίζουν τα ασύρματα τοπικά δίκτυα. Ένα πλήθος προτύπων βρίσκονται σε εξέλιξη (802.11i, EAP, WPA, WPA2 κ.α.)
- ◆ Οι παραβιάσεις εμφανίζονται με τη μορφή υποκλοπής ή αποκάλυψης, της καταστροφής ή αλλοίωσης δεδομένων και της άρνησης παροχής υπηρεσίας

# Ασφάλεια

- ◆ Τα ασύρματα δίκτυα υπόκεινται σε όλες αυτές τις μορφές των απειλών και σε εντονότερο βαθμό από ότι τα σταθερά επίγεια δίκτυα
- ◆ Δύο τομείς υπάρχουν για την αντιμετώπιση τέτοιων κινδύνων:
  - ◆ **Πιστοποίηση**
  - ◆ **Κρυπτογράφηση**

# Ασφάλεια

- ◆ Το πρότυπο 802.11i περιλαμβάνει όλα τα πρότυπα σχετικά με την ασφάλεια των WLAN

## **Πιστοποίηση Ταυτότητας**

Αρχικά ο μηχανισμός πιστοποίησης βασίστηκε στην έννοια ενός κοινού κωδικού που είναι γνωστός μόνο στα εξουσιοδοτημένα μέλη ενός ασύρματου τοπικού δικτύου



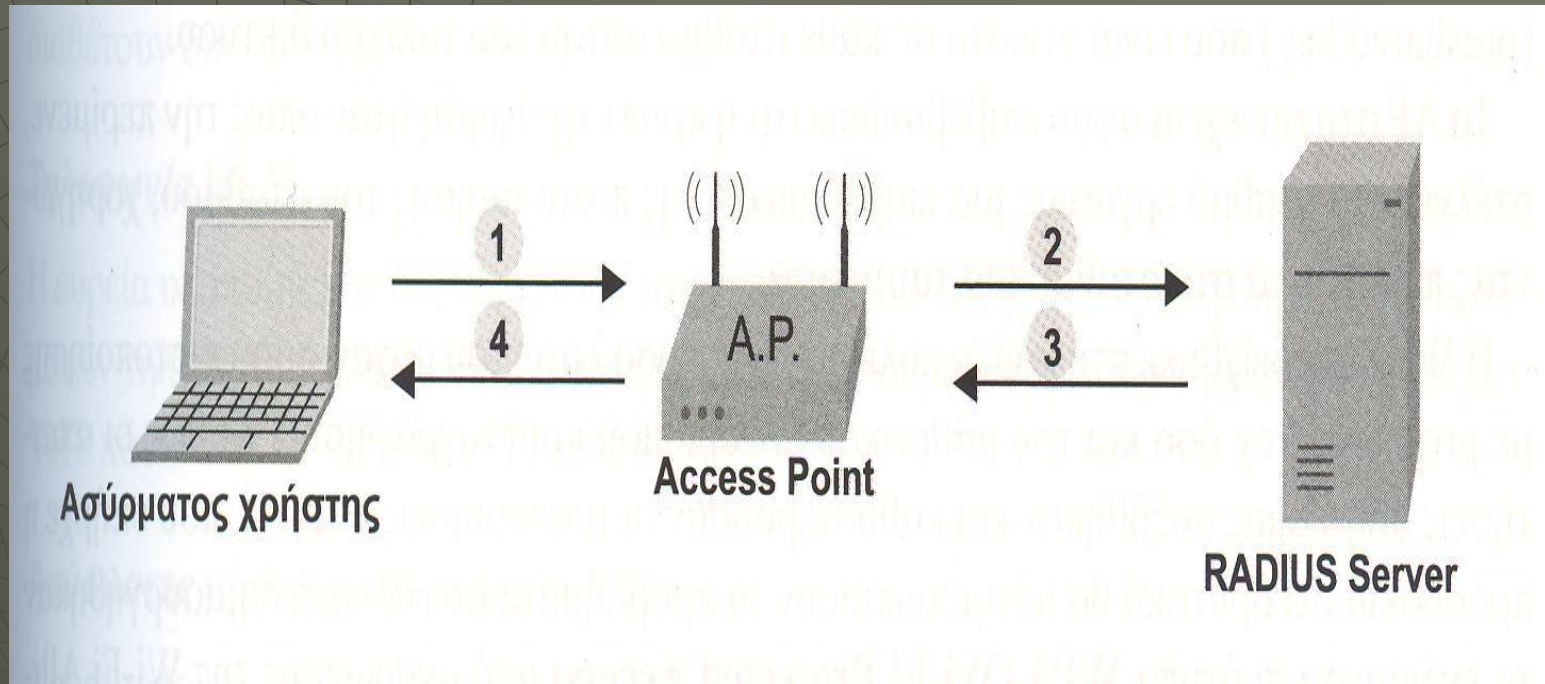
# Ασφάλεια

- ◆ Ο μηχανισμός αποδείχθηκε ανασφαλής και η ΙΕΕΕ προχώρησε στη βελτίωση της διαδικασίας με το πρότυπο 802.1X που υιοθετεί ένα τριμερές μοντέλο. Σε αυτό υπάρχουν ο αιτών, ο εξυπηρετητής πιστοποίησης που δίνει την άδεια και ο παρέχων την πρόσβαση

# Ασφάλεια

- ◆ Στο 802.1X ο αιτών πρέπει να έχει μια ταυτότητα και κάποια διαπιστευτήρια (πχ. Password, ψηφιακό πιστοποιητικό) που να πιστοποιούν την ιδιότητά του ενώ από την άλλη το δίκτυο να έχει τα κριτήρια για την αποδοχή ή την απόρριψή του. Έτσι η αίτηση πρόσβασης γίνεται μόνο στο AP

# Ασφάλεια



# Ασφάλεια

- ◆ Ο authentication server συνήθως είναι Remote Authentication Dial In User Service (RADIUS) που αναλαμβάνει να χορηγήσει την άδεια πρόσβασης
- ◆ Στην πράξη χρησιμοποιείται το Extensible Authentication Protocol (EAP) που περιγράφει τα απαραίτητα διακινούμενα μηνύματα

# Ασφάλεια

- ◆ Το EAP είναι κομμάτι του 802.1X και είναι ένα γενικότερο σύνολο μηνυμάτων διαπραγμάτευσης για πιστοποίηση και συναντάται σε διάφορες μορφές (PEAP, LEAP, EAP-TLS, EAP-TTLS, EAP-MD5 κ.λ.π.)

## **Κρυπτογράφηση**

Οι βασικές προσπάθειες κρυπτογράφησης έγιναν με το WEP

# Ασφάλεια

- ◆ Το πρότυπο Wired Equivalent Privacy (WEP) διαθέτει εκτός από μηχανισμό πιστοποίησης και μηχανισμό κρυπτογράφησης βασισμένο στον αλγόριθμο RC4. Σχεδιάστηκε το 1987 από έναν από τους δημιουργούς του RSA. Ο RC4 χρησιμοποιεί κλειδιά 40 ή 104 bit και το WEP προσθέτει άλλα 24 ενισχύοντας την ανθεκτικότητα

# Ασφάλεια

- ◆ Σήμερα θεωρείται ανεπαρκής και εγκαταλείπεται.
- ◆ Η βελτίωσή του σε Wi-Fi Protected Access (WPA) στηρίχθηκε στο πρωτόκολλο TKIP που επιτρέπει συχνό μετασχηματισμό των κλειδιών κρυπτογράφησης. Ο WPA δημιουργήθηκε από τους ανθρώπους της Wi-Fi Alliance και της 802.11i

# Ασφάλεια

- ◆ Διατήρησε τον αλγόριθμο RC4 για λόγους συμβατότητας με το WEP
- ◆ Περαιτέρω εξέλιξη ήρθε με τον WPA2 βασισμένο στον AES. Χρησιμοποιεί κλειδιά μήκους 128, 192, ή και 256 bits. Δημιουργήθηκε από το NIST το 2001. Για την πιστοποίηση χρησιμοποιεί την τριμερή επικοινωνία της 802.1X αλλά αντικατέστησε →



# Ασφάλεια

- τον RC4 με τον Advanced Encryption Standard (AES). Για λόγους συμβατότητας είναι δυνατή και η εναλλακτική χρήση TKIP. Το 802.11w ασχολείται με τα θέματα ασφάλειας όχι μόνο των data αλλά και των δεδομένων διαχείρισης
- ◆ Ενίσχυση της ασφάλειας είναι η μη αποκάλυψη του SSID

# Ασφάλεια

- ◆ Όταν το AP διαθέτει την δυνατότητα προγραμματισμού, καλό είναι να γίνεται φιλτράρισμα των MAC διευθύνσεων των συσκευών που επιθυμούμε να συνδέονται στο AP

# Πρακτικές εφαρμογές

- ◆ **Hot spot** σε δημόσιους χώρους, εμπορικά κέντρα κ.α. με τεχνολογία Wi-Fi
- ◆ **ADSL ασύρματη πρόσβαση** στα σπίτια ή μικρές εταιρίες όταν το ADSL modem-router έχει ασύρματη Wi-Fi δυνατότητα (λειτουργία ως AP)
- ◆ Τηλεφωνία μέσω Wi-Fi με αντίστοιχες συσκευές που έχουν τη δυνατότητα →

# Πρακτικές εφαρμογές

- να μεταφέρονται οι τηλεφωνικές κλήσεις VoIP πάνω από το ασύρματο Wi-Fi
- ◆ **Ασύρματες γέφυρες** που χρησιμοποιούνται για την διασύνδεση τοπικών δικτύων που βρίσκονται σε γειτονικά κτίρια ή σε μικρές αποστάσεις. Με χρήση κατευθυντήριων κεραιών μπορούμε→

# Πρακτικές εφαρμογές

→ να καλύψουμε μεγαλύτερες αποστάσεις στη σύνδεση μεταξύ των γεφυρών ενοποιώντας τα δίκτυα που συνδέονται με αυτές τις γέφυρες