ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
Τμημα Μηχ. Η/Υ & Πληροφορικης

Δίκτυα IEEE 802.11

ΜΥΕ006: ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Ευάγγελος Παπαπέτρου

Διάρθρωση μαθήματος

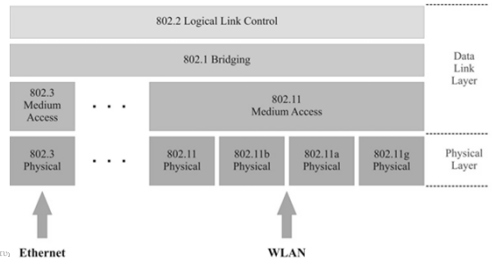
- Δομή προτύπου – Αρχιτεκτονική δικτύων IEEE 802.11
- Προδιαγραφή φυσικού μέσου
- Μηχανισμός πρόσβασης
  - Distributed Coordination Function
  - Point Coordination Function
- Διαχείριση Κινητικότητας
  - μεταγωγή και είδη μεταγωγής
- Ποιότητα Υπηρεσιών
  - το πρότυπο IEEE 802.11e
- Ασφάλεια
  - πιστοποίηση και κρυπτογράφηση, WEP
- Πλαισίωση
  - δομή και είδη πλαισίων, πλαίσια διαχείρισης, ελέγχου, δεδομένων

Δομή προτύπου (1/2)

- Φυσικό επίπεδο
  - λειτουργίες:
    - κωδικοποίηση / αποκωδικοποίηση σήματος, δημιουργία / αφαίρεση προοιμίου για συγχρονισμό, προδιαγραφή του φυσικού μέσου
  - διαφορετικές τεχνολογίες υποστηρίζονται στο φυσικό επίπεδο:
    - infrared, διευρυμένου φάσματος (DSSS, FHSS), OFDM
- Υποεπίπεδο ελέγχου λογικής σύνδεσης (LLC)
  - διεπαφή προς ανώτερα επίπεδα
  - διασύνδεση με πρωτόκολλα της ομάδας 802.x
  - έλεγχος ροής και σφαλμάτων

Δομή προτύπου (2/2)

- Υποεπίπεδο ελέγχου πρόσβασης μέσου (MAC)
  - δημιουργία πλαισίου (διεύθυνση και επίμετρο για έλεγχο σφαλμάτων)
  - αναγνώριση διεύθυνσης και έλεγχος σφαλμάτων κατά τη λήψη
  - μηχανισμός πρόσβασης



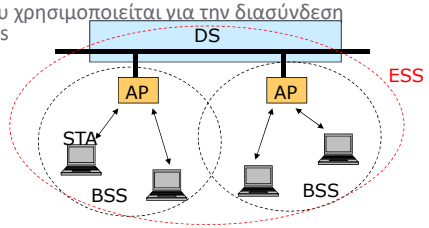
Αρχιτεκτονική δικτύων

Αρχιτεκτονική δικτύων

- Το IEEE 802.11 προδιαγράφει δύο αρχιτεκτονικές
  - δομημένη αρχιτεκτονική – Infrastructure mode
  - αδόμητα δίκτυα – ad hoc mode
- Infrastructure mode
  - ύπαρξη ενός κεντρικού σταθμού (σημείο πρόσβασης)
  - ένα τερματικό επικοινωνεί μέσω του κέντρικού σταθμού με άλλα τερματικά ή με το ενσύρματο δίκτυο
- Ad Hoc mode
  - δεν υπάρχει σημείο πρόσβασης
  - άμεση επικοινωνία μεταξύ δύο τερματικών που βρίσκονται το ένα στην εμβέλεια του άλλου

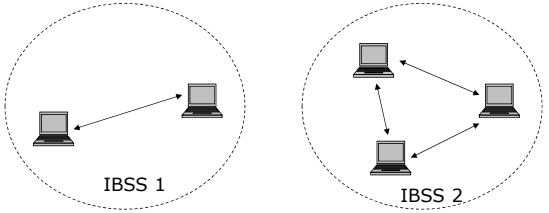
Infrastructure Mode

- Τερματικό: STA – Station
  - μπορεί να μεταδόσει μέσω του σημείου πρόσβασης
- BSS – Basic Service Set
  - ομάδα τερματικών που χρησιμοποιούν την *ίδια συχνότητα*
- ESS – Extended Service Set
  - σύνολο από BSSs που μπορούν να επικοινωνήσουν μεταξύ τους
- DS – Distribution System
  - δίκτυο κορμού που χρησιμοποιείται για την διασύνδεση διαφορετικών BSSs



Ad Hoc Mode

- STA – Station
  - τερματικό που έχει τη δυνατότητα πρόσβασης στο κοινό μέσο χωρίς τη μεσολάβηση κάποιου σημείου πρόσβασης
- IBSS – Independent Basic Service Set
  - ομάδα τερματικών που χρησιμοποιούν την ίδια συχνότητα



Διακίνηση πληροφορίας

- Πλέον της διακίνησης πληροφορίας εντός ενός BSS (ή IBSS) το IEEE 802.11 προδιαγράφει και άλλες υπηρεσίες
- Distribution Service
  - μεταφορά ενός πλαισίου MAC από ένα σταθμό σε ένα BSS σε σταθμό σε άλλο BSS
- Integration Service
  - μεταφορά δεδομένων από ένα σταθμό τοπικού δικτύου IEEE 802.11 σε σταθμό άλλου τοπικού δικτύου τεχνολογίας IEEE 802.x

Φυσικό μέσο

Προδιαγραφή φυσικού μέσου (1/2)

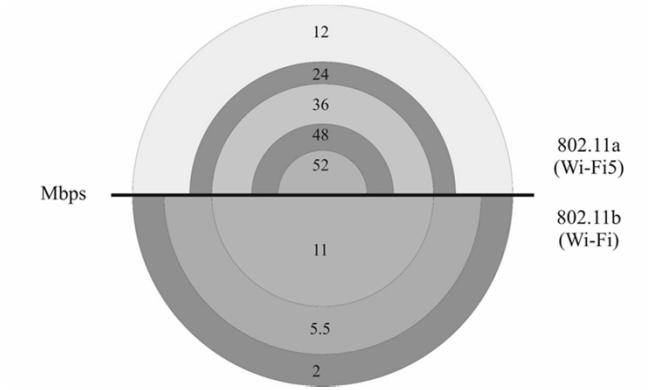
- Συχνότητες λειτουργίας και ρυθμοί μετάδοσης
  - Δίκτυα DSSS: λειτουργία στα 2.4GHz (ISM band), ρυθμός μετάδοσης δεδομένων από 1-2 Mbps
  - Δίκτυα FHSS: λειτουργία στα 2.4GHz (ISM band), ρυθμός μετάδοσης δεδομένων από 1-2 Mbps
  - Infrared: μήκος κύματος 850-950 nm, ρυθμός μετάδοσης δεδομένων από 1-2Mbps

Spectrum	2.4 GHz		
Max Physical Rate	2 Mbps		
Max Rate Layer 3	1.2 Mbps		
Medium Access Control	CSMA/CA		
Fixed Network Support	802 Family	**FH**	**DS**
	Spectrum	2.4 GHz	2.4 GHz
	Sub-carrier	1 MHz wide	11 sub-channels each of 11MHz
	Physical Rate	1 and 2 Mbps	1 and 2Mbps
	Other	Hop over 79 channels	11 chip sequence

Προδιαγραφή φυσικού μέσου (2/2)

- IEEE 802.11b
  - τεχνική διαμόρφωσης: CCK (Complementary Code Keying)
  - ρυθμοί μετάδοσης 2, 5.5 και 11Mbps
- IEEE 802.11a
  - λειτουργία στην περιοχή 5GHz
  - ρυθμοί μετάδοσης 6,9,12,18,24,36,48 και 54 Mbps
  - χρησιμοποιεί την τεχνική OFDM (Orthogonal Frequency Division Multiplexing)
  - τα φέροντα διαμορφώνονται χρησιμοποιώντας μια από τις τεχνικές BPSK, QPSK, 16-QAM και 64-QAM

Ρυθμοί μετάδοσης IEEE 802.11a και IEEE 802.11b



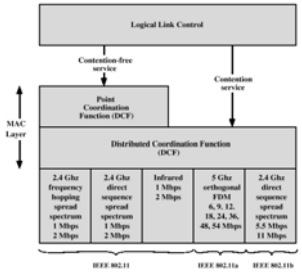
Μηχανισμός Πρόσβασης

Εισαγωγή

- Ο μηχανισμός πρόσβασης έπρεπε να έχει τα παρακάτω χαρακτηριστικά
  - μηχανισμός με κατανεμημένη λειτουργία
    - ο μηχανισμός CSMA/CD (Ethernet) ήταν ένας καλός αρχικός υποψήφιος
  - χαμηλός ρυθμός συγκρούσεων
    - ιδιαίτερη μέριμνα ώστε να μην ελαττώνεται ο ρυθμός μετάδοσης με την αύξηση της κίνησης
  - να παρέχει λύση σε προβλήματα που σχετίζονται με τη φύση της ασύρματης μετάδοσης
    - πρόβλημα του κρυμμένου τερματικού
  - να υποστηρίζει τη χρήση διαφορετικών τεχνολογιών στο φυσικό επίπεδο

Αρχιτεκτονική μηχανισμού πρόσβασης

- Ο μηχανισμός πρόσβασης αποτελείται από δύο επιμέρους διεργασίες
  - Distributed Coordination Function (DCF) – βασικός μηχανισμός
  - Point Coordination Function (PCF) – προαιρετικός μηχανισμός



Distributed Coordination Function (1/2)

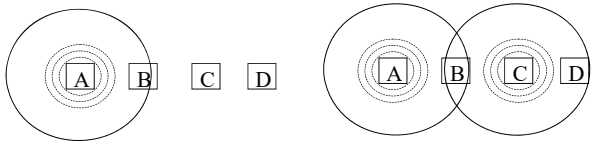
- Βασικός μηχανισμός πρόσβασης
  - χρησιμοποιείται πάντα (υποχρεωτική η χρήση του)
- Στηρίζεται στον αλγόριθμο CSMA/CA
  - πολλαπλή πρόσβαση με ακρόαση φέροντος
  - η ακρόαση φέροντος γίνεται από το φυσικό επίπεδο
    - ο μηχανισμός καλείται Clear Channel Assignment (CCA)
  - ο μηχανισμός CD (collision detection) δεν είναι εφικτός λόγω του φαινομένου του κρυμμένου τερματικού
- Βασική ιδέα: αντικατάσταση του μηχανισμού CD με έναν μηχανισμό αποφυγής συγκρούσεων (CA - Collision Avoidance)
  - η αποφυγή συγκρούσεων επιτυγχάνεται με το μηχανισμό RTS/CTS

Distributed Coordination Function (2/2)

- Ο μηχανισμός RTS/CTS είναι προεραιτικός ανάλογα με:
  - το είδος των δεδομένων
    - π.χ. σε δεδομένα φωνής φωνής δεν χρησιμοποιείται ο μηχανισμός RTS/CTS
  - το είδος της μετάδοσης
- Συγκεκριμένα για τη μετάδοση μπορούν να χρησιμοποιηθούν
  - μηχανισμός CSMA/CA με επιβεβαιώσεις
  - μηχανισμός CSMA με επιβεβαιώσεις
  - μηχανισμός CSMA χωρίς επιβεβαιώσεις
    - για δεδομένα ευρείας εκπομπής (broadcast)

Πρόβλημα κρυμμένου τερματικού

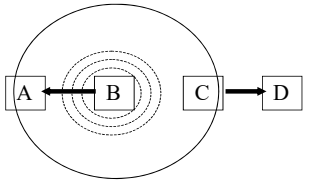
- Προκαλείται από τη φύση της ασύρματης μετάδοσης
- Φαινόμενο:
  - σύγκρουση πακέτων από δύο τερματικά (A και C) που δεν βρίσκονται το ένα στην εμβέλεια του άλλου
  - η σύγκρουση γίνεται αντιληπτή μόνο στο τερματικό B και όχι στα A και C



- Είναι ο λόγος για τον οποίο ο μηχανισμός CSMA/CD δεν μπορεί να εφαρμοστεί

Πρόβλημα αποκαλλυμένου τερματικού

- Πρόβλημα αντίστροφο από αυτό του κρυμμένου τερματικού
- Φαινόμενο:
  - η εκπομπή του B προς τον A γίνεται αντιληπτή από τον C
  - ο C ακυρώνει την προγραμματισμένη εκπομπή προς τον D
  - το φυσικό μέσο δεν αξιοποιείται πλήρως



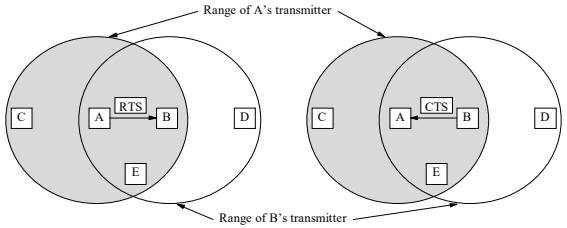
- Μειώνει την απόδοση ενός μηχανισμού CSMA

Μηχανισμός RTS/CTS (1/2)

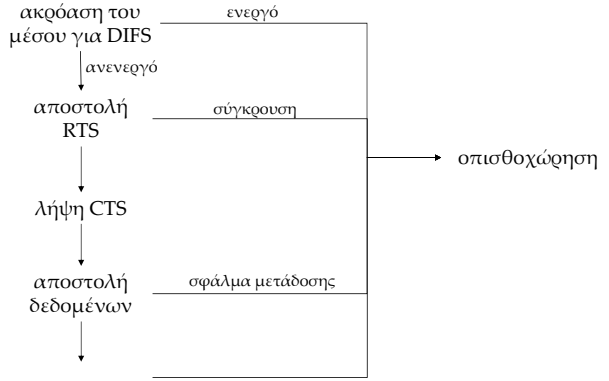
- Κάθε τερματικό που επιθυμεί να αποστείλει δεδομένα
  - εκδηλώνει την πρόθεσή του με την αποστολή ενός μικρού πλαισίου RTS (Request To Send) προς τον παραλήπτη
- Αν ο παραλήπτης μπορεί να ανταποκριθεί απαντά με ένα πλαίσιο CTS (Clear To Send)
  - αν δεν εμπλέκεται σε άλλη μετάδοση, δεν γίνεται σύγκρουση πλαισίων RTS, δεν έχει ακούσει άλλο μήνυμα CTS
- Όλα τα τερματικά που λαμβάνουν το πλαίσιο CTS αναβάλλουν πιθανές προγραμματισμένες εκπομπές
- Τα μηνύματα RTS και CTS μεταφέρουν τη διάρκεια της μετάδοσης ώστε αυτή να γίνει γνωστή στα υπόλοιπα τερματικά

Μηχανισμός RTS/CTS (2/2)

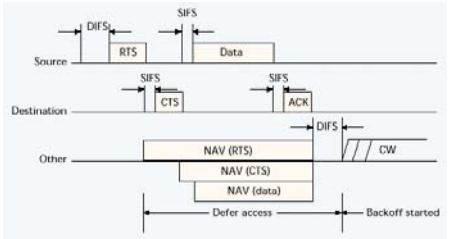
- Υπάρχει πιθανότητα σύγκρουσης μεταξύ διαφορετικών πακέτων RTS
  - η πιθανότητα αυτή είναι μικρή λόγω της διάρκειας του πλαισίου
- Μετά την αποστολή του πλαισίου CTS δεν υπάρχει πιθανότητα σύγκρουσης στα πλαίσια δεδομένων



Αλγόριθμος CSMA/CA (1/2)

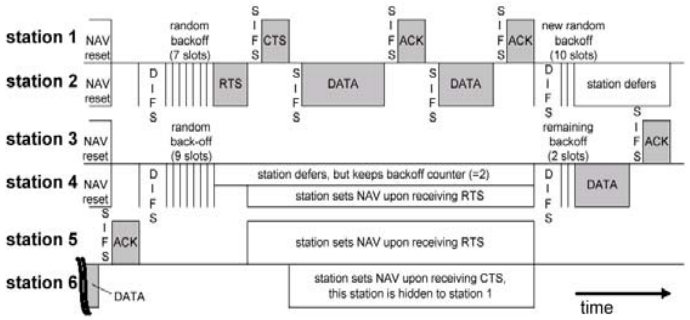


Αλγόριθμος CSMA/CA (2/2)



- Κάθε τερματικό διαθέτει ένα μετρητή (NAV) που χρησιμοποιεί για να υπολογίσει το χρόνο επόμενης ακρόασης του μέσου
  - η διαδικασία είναι σημαντική για εξοικονόμηση ενέργειας
  - στο μεσοδιάστημα τα τερματικά εισέρχονται σε κατάσταση αναμονής (sleep)

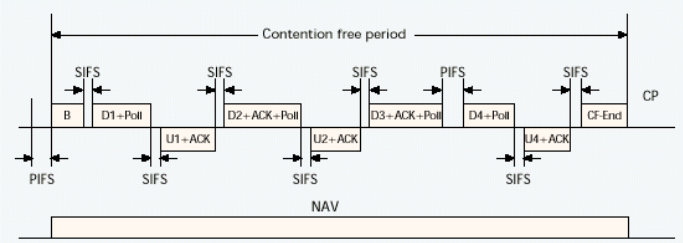
Παράδειγμα ανταγωνισμού με DCF



Point Coordination Function (1/3)

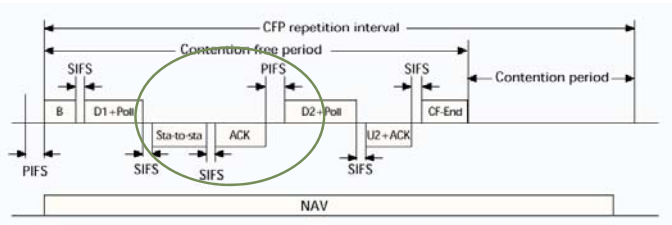
- Χρησιμοποιείται *προαιρετικά* μόνο σε δομημένο δίκτυο (infrastructure mode)
  - υπεύθυνο για τη λειτουργία του αλγόριθμου είναι το σημείο πρόσβασης (AP)
    - στην περίπτωση αυτή καλείται Point Coordinator
- Προσφέρει πρόσβαση στο μέσο χωρίς ανταγωνισμό (contention free)
  - χρησιμοποιείται για μετάδοση σύγχρονων δεδομένων
  - μειώνει τις μεταβολές στο χρόνο πρόσβασης ενός τερματικού στο μέσο
- Ο μηχανισμός εκκινείται αυτόματα από τον AP
  - π.χ. για να επιλύσει πολλαπλές συγκρούσεις
- Έχει προτεραιότητα ως προς την DCF
  - ο μηχανισμός εκκινεί μετά από ανενεργό χρόνο PIFS<DIFS

Point Coordination Function (2/3)



- Ο AP δίνει κυκλικά το δικαίωμα εκπομπής σε όλα τα τερματικά (polling)
- Χρησιμοποιούνται μια σειρά από μηνύματα ελέγχου
  - πλαίσιο συγχρονισμού (synchronization Beacon - B), πλαίσιο απόδοσης δικαιώματος εκπομπής (Poll), πλαίσιο επιβεβαίωσης (ACK), πλαίσιο λήξης περιόδου (CF-End)

Point Coordination Function (3/3)



- Ένα τερματικό μπορεί να εκπέμψει απ' ευθείας προς κάποιο άλλο
  - το τερματικό που λαμβάνει τα δεδομένα επιστέφει μια επιβεβαίωση (όπως στην περίπτωση της DCF)
  - το AP αναμένει για PIFS και συνεχίζει τη διαδικασία

Inter Frame Space – IFS (1/2)

- Χρονικά διαστήματα (IFS) διαφορετικού μεγέθους χρησιμοποιούνται για το διαχωρισμό των πλαισίων
  - διαφορετικά διαστήματα χρησιμοποιούνται ανάλογα με την κατάσταση στην οποία βίσκεται ο αλγόριθμος
  - υπάρχουν τρία διαφορετικά διαστήματα: SIFS, PIFS, DIFS
- Short IFS (SIFS)
  - το μικρότερο διάστημα IFS
  - χρησιμοποιείται σε περιπτώσεις όπου απαιτείται άμεση απάντηση σε ένα πλαίσιο
  - περιπτώσεις χρήσης:
    - επιβεβαιώσεις (ACKs), Clear To Send (CTS), απάντηση σε ένα μήνυμα Poll

Inter Frame Space – IFS (2/2)

- Point Coordination Function IFS (PIFS)
  - μέσης διάρκειας διάστημα IFS
  - χρησιμοποιείται:
    - από τον κεντρικό κόμβο που ασκεί τον έλεγχο στο μηχανισμό PCF
    - για να ληφθεί προτεραιότητα σε σχέση με την απλή τηλεπικοινωνιακή κίνηση
- Distributed Coordination Function IFS (DIFS)
  - το μεγαλύτερης διάρκειας διάστημα IFS
  - χρησιμοποιείται ως η ελάχιστη καθυστέρηση για ασύγχρονα πλαίσια που συναγωνίζονται για το κοινό μέσο

Ποιότητα Υπηρεσιών

Ποιότητα Επικοινωνίας στο IEEE 802.11 (1/2)

- Ποιότητα επικοινωνίας: *επικοινωνία με χαρακτηριστικά σύμφωνα με τις απαιτήσεις του χρήστη*
  - η ποιότητα επικοινωνίας χαρακτηρίζεται από υποκειμενικότητα (τις απαιτήσεις του χρήστη)
- Τα δίκτυα ορίζουν *επίπεδα ποιότητας υπηρεσίας*
  - οι χρήστες προσαρμόζουν τις απαιτήσεις τους στις προσφερόμενες υπηρεσίες
- Τυπικές παράμετροι ποιότητας επικοινωνίας
  - μέση καθυστέρηση από άκρο σε άκρο (mean end-to-end delay)
  - μέση μεταβολή της καθυστέρησης (mean delay jitter)
  - μέσο ποσοστό επιτυχούς παράδοσης πακέτων (delivery ratio)

Ποιότητα Επικοινωνίας στο IEEE 802.11 (2/2)

- Οι παράμετροι ποιότητας επικοινωνίας εξαρτώνται από:
  - το είδος των εφαρμογών που εξυπηρετούνται από το δίκτυο
  - το επίπεδο στο οποίο εφαρμόζεται η τεχνική
- Πρότυπο IEEE 802.11: η ποιότητα υπηρεσιών προσφέρεται μέσω του μηχανισμού πρόσβασης στο κοινό μέσο (MAC)
  - ο μηχανισμός είναι γνωστός με το όνομα IEEE 802.11e

IEEE 802.11e (1/4)

- Το πρότυπο IEEE 802.11 δεν παρέχει ποιότητα επικοινωνίας
  - ο μηχανισμός DCF δεν παρέχει εγγυήσεις για την *καθυστέρηση* και το *ρυθμό μετάδοσης δεδομένων*
  - μηχανισμός PCF: η καθυστέρηση μεταξύ δύο διαδοχικών εκπομπών ενός τερματικού δεν είναι χρονικά φραγμένη
- Ο νέος μηχανισμός έχει ως στόχους να:
  - εγγυηθεί μια ανώτατη καθυστέρηση μετάδοσης
  - να εγγυηθεί έναν *ελάχιστο ρυθμό μετάδοσης*
  - να αξιοποιήσει αποδοτικά το κοινό μέσο

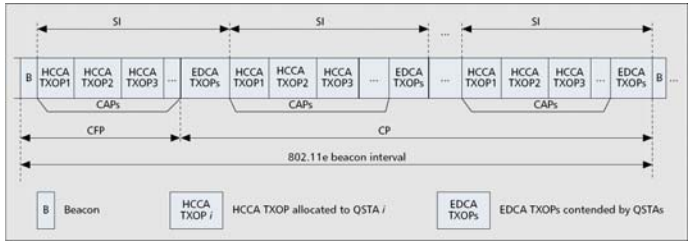
IEEE 802.11e (2/4)

- Ο μηχανισμός που υλοποιείται στο IEEE 802.11e καλείται Hybrid Coordinator Function (HCF)
- Ο HCF αποτελείται από δύο επιμέρους μηχανισμούς
  - EDCA (Enhanced Distributed Channel Access)
  - HCCA (HCF-controlled channel access)
- Ο HCF ορίζει
  - την έννοια του Traffic Stream (TS)
    - προσδιορίζει μια ροή δεδομένων και σχετίζεται με μια εφαρμογή
    - οι υπηρεσίες μετάδοσης προσφέρονται σε κάθε TS ξεχωριστά
    - κάθε κόμβος μπορεί να μεταδίδει πολλά TSs
  - την έννοια του Traffic Class (TC)
    - προσδιορίζει την προτεραιότητα κάθε TS

IEEE 802.11e (3/4)

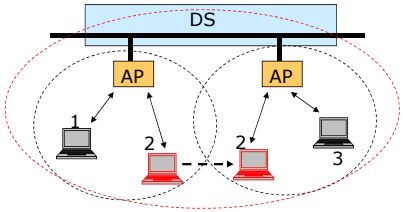
- EDCA
  - παραλλαγή του μηχανισμού DCF
  - κάθε κόμβος ανταγωνίζεται με βάση ένα χρονικό διάστημα ανάλογο της προτεραιότητας των δεδομένων
    - μεγαλύτερη προτεραιότητα = μεγαλύτερη πιθανότητα να κερδίσει το δικαίωμα εκπομπής
  - σε κάθε κόμβο ανατίθεται ένας μέγιστος χρόνος εκπομπής (TXOP) ανάλογος με την προτεραιότητα
- HCCA
  - αποτελεί βελτίωση της PCF
  - υλοποιείται σε έναν κεντρικό κόμβο (QAP)
  - ανατίθεται *περιοδικά* από τον QAP ένα πεπερασμένο χρονικό διάστημα για μετάδοση (TXOP)
  - ο χρόνος TXOP ανατίθεται σε κάθε TS

IEEE 802.11e (4/4)



Διαχείριση κινητικότητας

Κινητικότητα σταθμών και αρχιτεκτονική



- Κάθε σταθμός πρέπει να συνδεθεί με κάποιο BSS (ή IBSS)
  - για λόγους συγχρονισμού και συμμετοχής στο μηχανισμό MAC
  - για διαπραγμάτευση των παραμέτρων λειτουργίας
  - για λόγους ασφάλειας
- Ένας κινητός σταθμός μπορεί να αλλάξει BSS (ή IBSS)
  - το φαινόμενο αυτό ονομάζεται μεταγωγή (handover)

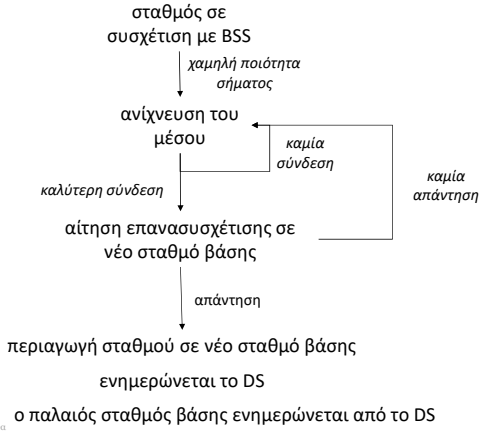
Υπηρεσίες σύνδεσης σε BSS (1/2)

- Για τη σύνδεση ενός τερματικού σε ένα BSS ορίζονται τρεις υπηρεσίες
  - συσχέτιση (assosiation)
  - επανασυσχέτιση (reassosiation)
  - αποσυσχέτιση (disassosiation)
- Συσχέτιση (Association)
  - καλείται η διαδικασία ένταξης ενός τερματικού σε ένα BSS
  - γνωστοποίηση της ταυτότητας του τερματικού και διαπραγμάτευση των παραμέτρων λειτουργίας
    - π.χ. παράμετροι λειτουργίας του φυσικού επιπέδου, όνομα BSS, κα
  - ο σταθμός βάσης (αν υπάρχει) μπορεί να αποδεχθεί ή να απορρίψει ένα σταθμό
  - δύο τρόποι συσχέτισης
    - παθητικός (αναμονή Beacon από AP)
    - ενεργητικός (αποστολή μηνύματος Probe προς τον AP)

Υπηρεσίες σύνδεσης σε BSS (2/2)

- Επανασυσχέτιση (Reassociation)
  - διαδικασία μεταφοράς της συσχέτισης σε άλλο BSS (στο ίδιο DS)
- Αποσυσχέτιση (Disassociation)
  - διαδικασία τερματισμού σύζευξης
  - μπορεί να εκκινήσει από το τερματικό ή από το AP

Διαδικασίας μεταγωγής

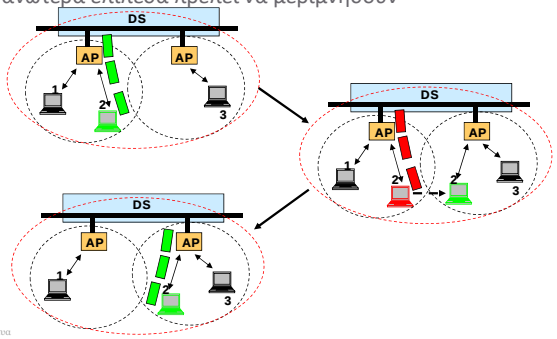


Είδη μεταγωγής

- Δύο διαφορετικά είδη μεταγωγής μπορούν να υπάρξουν
  - μεταγωγή BSS
  - μεταγωγή ESS
- Μεταγωγή BSS
  - το τερματικό μεταβαίνει από ένα BSS σε ένα άλλο που όμως ανήκει στο ίδιο ESS
- Μεταγωγή ESS
  - το τερματικό μεταβαίνει από ένα BSS ενός ESS σε άλλο BSS διαφορετικού ESS

Προβλήματα κατά τη μεταγωγή

- Δεν υπάρχει πρόβλεψη για ορθή παράδοση δεδομένων κατά τη διάρκεια μιας μεταγωγής
  - τα ανώτερα επίπεδα πρέπει να μεριμνήσουν



Inter Access Point Protocol (IAPP)

- Το πρωτόκολλο IAPP περιγράφεται στο πρότυπο IEEE 802.11f
  - στόχος: επικοινωνία των AP για την αποδοτική μεταγωγή τερματικών
- Περιλαμβάνει μια σειρά από ενέργειες μεταξύ των Aps
  - η διαδικασία εκκινεί μετά από ένα μήνυμα Reassociation Request
- Ο μηχανισμός υλοποιείται σε ανώτερα επίπεδα
- Θεωρητικά μπορεί να χρησιμοποιηθεί και για άλλα ασύρματα δίκτυα

Ασφάλεια

Ασφάλεια

- Οι ασύρματες επικοινωνίες μπορούν εύκολα να υποκλαπούν
- Για την ασφάλεια της επικοινωνίας υπάρχει η ανάγκη
  - πιστοποίησης των σταθμών
  - κρυπτογράφησης των δεδομένων
- Κάθε σταθμός μπορεί να στείλει δεδομένα μετά την πιστοποίησή του
- Η πιστοποίηση ενός σταθμού πραγματοποιείται μετά τη συσχέτισή του

Υπηρεσίες ασφάλειας και πιστοποίησης

- Πιστοποίηση ταυτότητας (Authentication)
  - γνωστοποιεί την ταυτότητα ενός κόμβου στους άλλους κόμβους (ή στον AP) και αποθηκεύει σχετικές πληροφορίες σε αυτούς
  - προβλέπεται αντίστροφος μηχανισμός όταν κάποιο τερματικό αποχωρεί από το δίκτυο
- Ακύρωση πιστοποίησης ταυτότητας (Deauthentication)
  - μετά την ακύρωση της πιστοποίησης δεν είναι δυνατό ο κόμβος να μετέχει στο δίκτυο
- Κρυπτογράφηση (Encryption)
  - αποτρέπει την ανάγνωση των δεδομένων από μη εξουσιοδοτημένα τερματικά

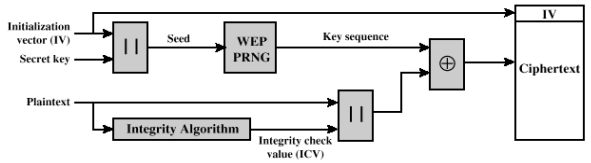
Wired Equivalent Privacy (WEP) Protocol

- Πρωτόκολλο για ασφάλεια που χρησιμοποιείται:
  - πιστοποίηση
  - κρυπτογράφηση
- Η υλοποίησή του είναι προαιρετική
- Συμβατό με αφίξεις και αποχωρήσεις κόμβων
- Σχετικά χαμηλή ασφάλεια
  - δεν χρησιμοποιείται από το 2004 και μετά
- Μικρό κόστος υλοποίησης
  - χαμηλές υπολογιστικές ανάγκες

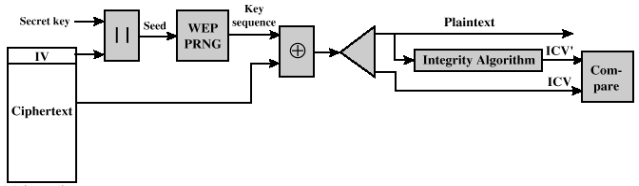
Κρυπτογράφηση (1/2)

- Υλοποιείται με βάση ένα κρυφό κλειδί
  - το μήκος του κλειδιού είναι 40 bits
  - το κλειδί είναι μόνιμα αποθηκευμένο στους σταθμούς
- Το κλειδί συνδυάζεται με μια γεννήτρια για την παραγωγή μιας ακολουθίας από bit
- Η παραγόμενη ακολουθία και τα δεδομένα συνδυάζονται με την πράξη XOR
- Το αποτέλεσμα XOR αποτελούν το πλαίσιο που μεταδίδεται στο κανάλι

Κρυπτογράφηση (2/2)



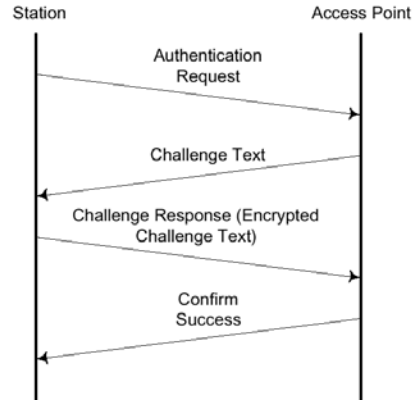
(a) Encryption



Πιστοποίηση (1/2)

- Σκοπό έχει να επιβεβαιώσει ότι το κρυφό κλειδί είναι γνωστό στο σταθμό
  - χρησιμοποιεί το ίδιο κρυφό κλειδί με την κρυπτογράφηση γεγονός που μειώνει την προσφερόμενη ασφάλεια
- Αποτελείται από τέσσερις φάσεις
  - με το τέλος της διαδικασίας επιβεβαιώνεται η επιτυχία ή αποτυχία της διαδικασίας
- Η ταυτότητα του σταθμού βάσης δεν πιστοποιείται
  - αποτελεί μειονέκτημα του πρωτοκόλλου που πρόκειται να διορθωθεί

Πιστοποίηση (2/2)



Πλαισίωση

Πλαισίωση (1/2)

- Η δομή ενός πλαισίου συμφωνεί με τη βασική δομή που προδιαγράφεται σε όλα τα δίκτυα 802.x
  - διεύθυνση παραλήπτη και αποστολέα (48 bit η κάθε μία)
  - ύπαρξη κώδικα για τον έλεγχο σφαλμάτων (CRC)
  - υπάρχουν όλα τα πεδία της δομής πλαισίων που χρησιμοποιούνται στα δίκτυα 802.x
- Η προσήλωση στον τρόπο πλαισίωσης είναι επιλογή της IEEE
  - εξυπηρετεί τη συμβατότητα με τα δίκτυα 802.x

Πλαισίωση (2/2)

- Το IEEE 802.11 προσδιορίζει την δική του πλαισίωση
  - η νέα δομή πλαισίου είναι διευρυμένη καθώς πρέπει να υποστηριχθούν νέες υπηρεσίες
- Υπάρχουν τρεις μεγάλες κατηγορίες πλαισίων
  - διαχείρισης (management) - association, synchronization, authentication
  - ελέγχου (control) - ACKs, end of Contention Free Period
  - δεδομένων (data)
- Κάθε κατηγορία πλαισίων ορίζει μια σειρά από *τύπους πλαισίων*

Τύποι πλαισίων (1/4)

Type Value b3 b2	Type Description	Subtype Value b7 b6 b5 b4	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Poll
10	Data	0011	Data + CF-Ack + CF-Poll
10	Data	0100	Null Function (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Τύποι πλαισίων (2/4)

- Τύποι πλαισίων διαχείρισης (Management)
  - τα πλαίσια διαχείρισης υποστηρίζουν τις υπηρεσίες (εκτός μεταφοράς δεδομένων) που προσφέρουν τα δίκτυα 802.11
    - π.χ. συσχέτιση με AP, πιστοποίηση, κλπ
  - οι σημαντικότεροι τύποι πλαισίων ελέγχου είναι:
    - αίτηση συσχέτισης (Association Request)
    - απάντηση συσχέτισης (Association Reply)
    - αίτηση επανασυσχέτισης (Reassociation Request)
    - απάντηση επανασυσχέτισης (Reassociation Reply)
    - αποσυσχέτιση (Disassociation)
    - πιστοποίηση (Authentication)
    - ακύρωση πιστοποίησης (Reassociation Reply)

Τύποι πλαισίων (3/4)

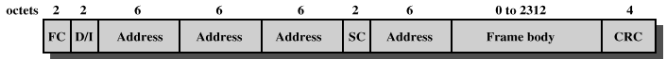
- Τύποι πλαισίων ελέγχου (Control)
  - τα πλαίσια ελέγχου χρησιμοποιούνται για την υλοποίηση του μηχανισμού πρόσβασης
  - οι τύποι πλαισίων ελέγχου είναι:
    - power save – poll (PS-Poll)
    - request To Send (RTS)
    - clear To Send (CTS)
    - επιβεβαίωση (ACK)
    - contention free end (CF-end)
    - CF-end + CF-ack

Τύποι πλαισίων (4/4)

- Τύποι πλαισίων Δεδομένων
  - Είδη πλαισίων που μεταφέρουν δεδομένα
    - δεδομένα
    - δεδομένα + CF-Ack
    - δεδομένα + CF-Poll
    - δεδομένα + CF-Ack + CF-Poll
  - Άλλα είδη πλαισίων (δε μεταφέρουν δεδομένα)
    - Null function
    - CF-Ack
    - CF-Poll
    - CF-Ack + CF-Poll

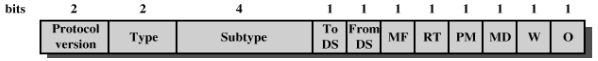
Γενική δομή πλαισίου

- Το IEEE 802.11 ορίζει την παρακάτω δομή πλαισίου



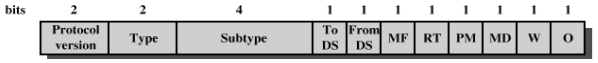
  - Frame Control (FC) - 2 bytes :
    - καθορίζει τον τύπο πλαισίου και υποστηρίζει μηχανισμού όπως ο κατακερματισμός και η ασφάλεια

- Το πεδίο έλεγχου (FC) έχει τη δομή



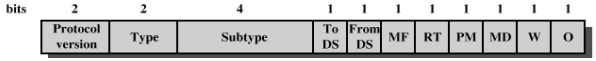
Δομή πεδίου ελέγχου (1/3)

- Protocol version (2 bits)
  - για μελλοντική διάκριση μεταξύ διαφορετικών εκδόσεων – τιμή 0
- Τα πεδία Type και Subtype προσδιορίζουν τον τύπο του πλαισίου
  - το πεδίο Type (2 bit) προσδιορίζει την κατηγορία στην οποί ανήκει το πλαίσιο, π.χ. δεδομένα, management, κλπ
  - το πεδίο Subtype (4 bit): καθορίζει το συγκεκριμένο τύπο πλαισίου στην κατηγορία που περιγράφει το πεδίο Type



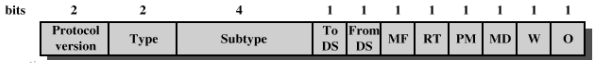
Δομή πεδίου ελέγχου (2/3)

- To DS (1 bit)
  - 1 αν το πλαίσιο πρέπει να προωθηθεί από το AP στο DS
- From DS (1 bit)
  - 1 αν το πλαίσιο προέρχεται από το DS
- More fragments
  - 1 αν άλλα θραύσματα του ίδιου πλαισίου ακολουθούν
- Retry (1 bit)
  - 1 αν πρόκειται για επανεκπομπή προηγούμενου θραύσματος ενός πλαισίου



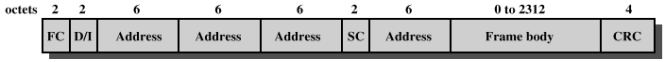
Δομή πεδίου ελέγχου (3/3)

- Power management (1 bit)
  - χρησιμοποιείται για να δηλώσει την κατάσταση του κόμβου (Power save, Active) μετά το τέλος της εκπομπής
- More data (1 Bit)
  - προσδιορίζει ότι το τερματικό έχει επιπλέον πλαίσια προς αποστολή
  - χρησιμοποιείται για το μηχανισμό περιόδευσης (Polling) ή για τη διαχείριση ισχύος
- WEP (1 bit)
  - 1 αν το πρωτόκολλο WEP χρησιμοποιείται
- Order (1 bit)
  - 1 αν κάποιο πλαίσιο δεδομένων στάλθηκε χρησιμοποιώντας την υπηρεσία αυστηρής διάταξης
  - χρήσιμη υπηρεσία όταν δεν είναι επιθυμητή η αλλαγή σειράς πλαισίων unicast



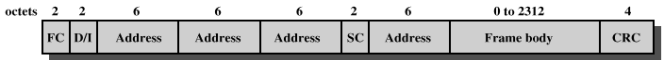
Δομή πλαισίου (1/3)

- Duration / Connection ID (DI) - 2 bytes
  - δύο ερμηνείες ανάλογα με τον τύπο του πλαισίου
    - περιέχει τη διάρκεια για τον υπολογισμό των δεικτών NAVs (Network Allocation Vectors)
    - στην περίπτωση PS-Poll πλαισίου περιέχει την ταυτότητα συσχέτισης του τερματικού
- Sequence Control (SC) – 2 bytes
  - αρίθμηση και ανασύνθεση πλαισίων και θραυσμάτων
  - περιέχει δύο τμήματα: Fragment Number και Sequence Number



Δομή πλαισίου (2/3)

- Δεδομένα :
  - δεν μπορούν να έχουν μέγεθος μεγαλύτερο από MSDU (Maximum Service Data Unit)
    - η επιλογή του MSDU σχετίζεται με θέματα απόδοσης και ισότητας των κόμβων
  - αν ένα πακέτο έχι μεγαλύτερο μέγεθος από MSDU τότε χρησιμοποιείται κατακερματισμός
  - IEEE 802.11 MSDU = 2312 bytes
- Frame Check Sequence - 32 bits
  - περιλαμβάνει κώδικα CRC για την ανίχνευση και διόρθωση σφαλμάτων

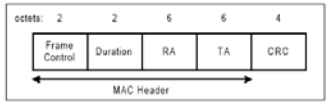


Δομή πλαισίου (3/3)

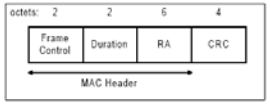
- Πεδία διευθύνσεων - 48 bits
  - υπάρχουν τέσσερις διευθύνσεις που χρησιμοποιούνται ανάλογα με τις τιμές των πεδίων ToDS και FromDS
- Address 1:
  - είναι η διεύθυνση του κόμβου αποστολέα του πακέτου
- Address 2:
  - Είναι η διεύθυνση του κόμβου παραλήπτη πακέτου
- Address 3:
  - περιέχει τη διεύθυνση του εκπέμποντως σταθμού
- Address 4:
  - περιέχει τη διεύθυνση του λαμβάνοντος σταθμού

Παραδείγματα πλαισίων

- Πλαίσιο RTS



- Πλαίσιο CTS



- Πλαίσιο επιβεβαίωσης