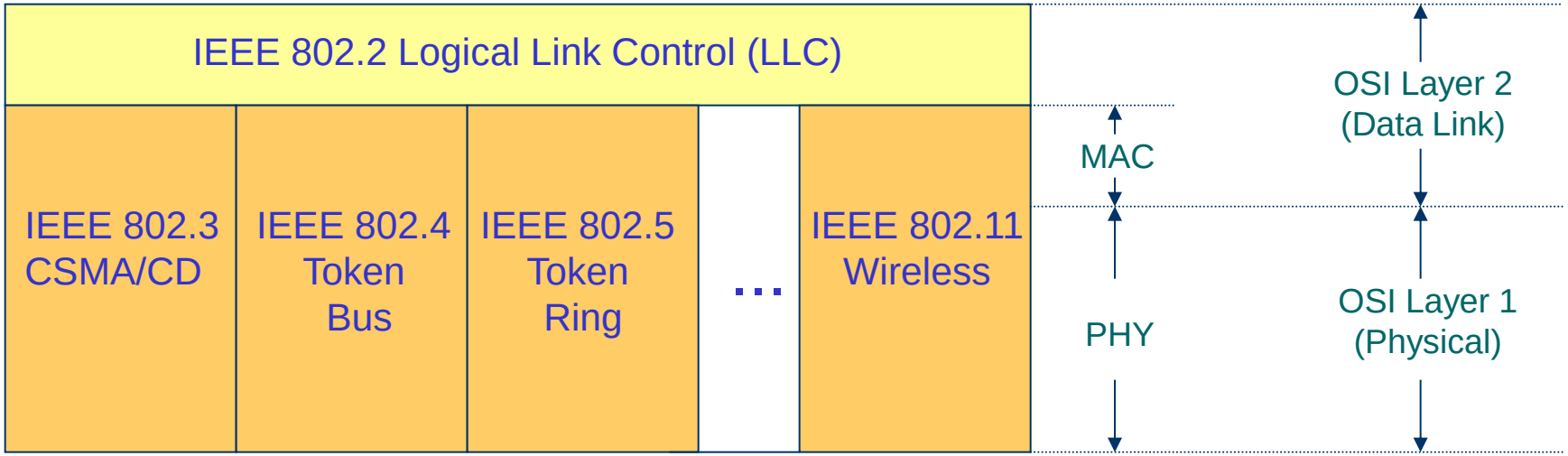
Πρωτόκολλα Πολλαπλής Πρόσβασης

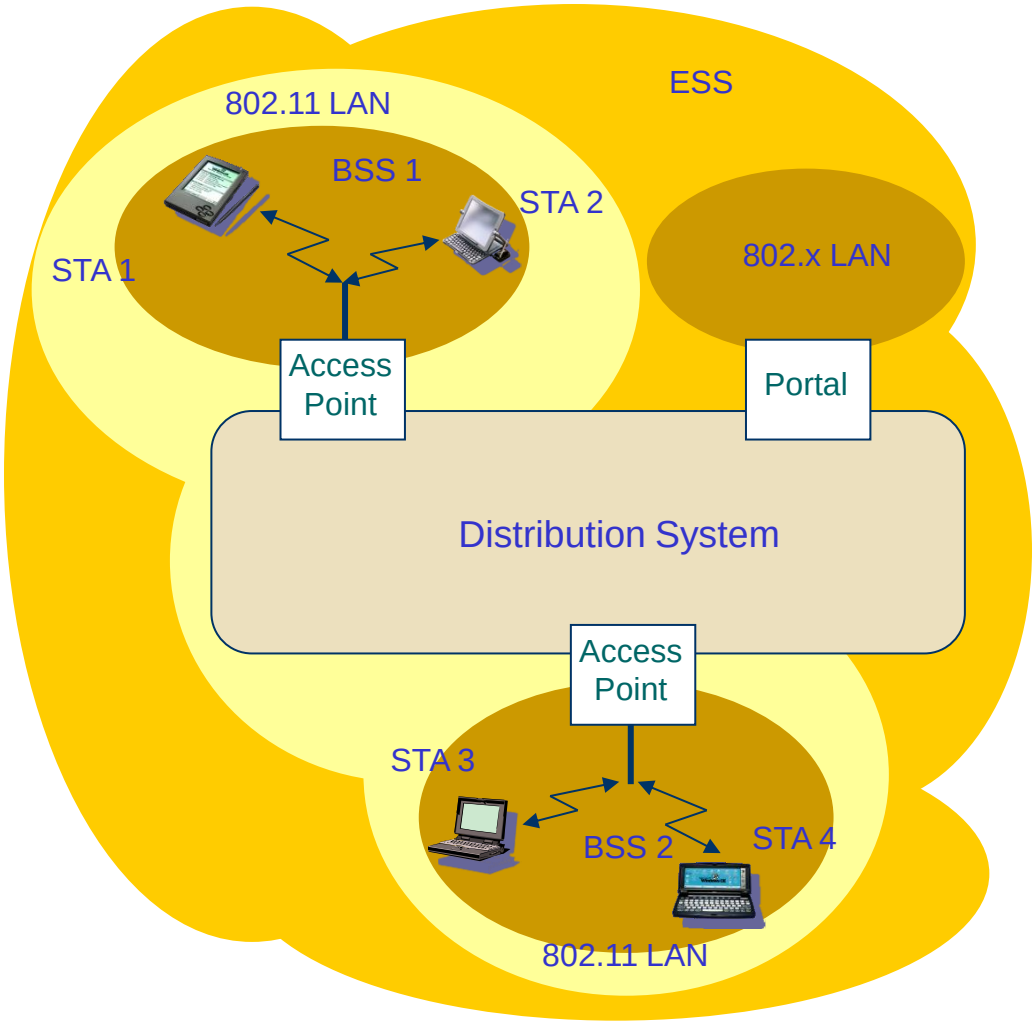
(συνέχεια)

Ασύρματα Τοπικά Δίκτυα Τύπου IEEE 802.11

Η οικογένεια προτύπων 802.x



802.11 Με Υποδομή



Station (STA) - Σταθμός
τερματικό με μηχανισμούς πρόσβασης στο ασύρματο μέσο και δυνατότητα επικοινωνίας με το Access Point

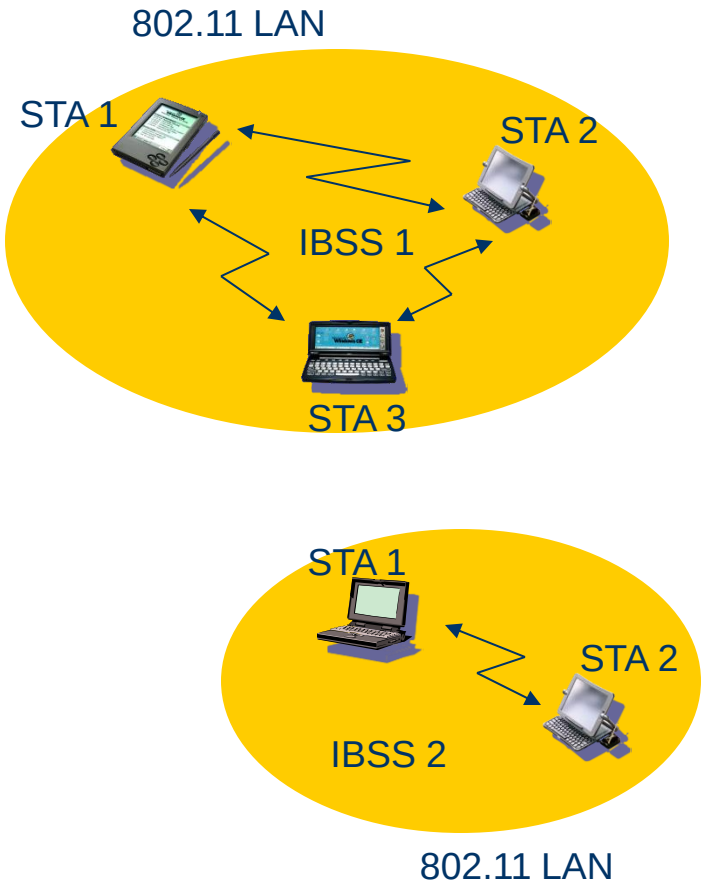
Basic Service Set (BSS)
ομάδα σταθμών που χρησιμοποιούν την ίδια ραδιο-συχνότητα

Access Point – Σημείο Πρόσβασης
σταθμός ο οποίος επικοινωνεί τόσο με το ασύρματο τοπικό δίκτυο, όσο και με το σύστημα διανομής (distribution system)

Portal
γέφυρα μεταξύ του συστήματος διανομής και εξωτερικών δικτύων

Distribution System – Σύστημα Διανομής
δίκτυο διασύνδεσης πολλών BSS σε ένα ESS (Extended Service Set)

802.11 Χωρίς Υποδομή (Ad-Hoc)



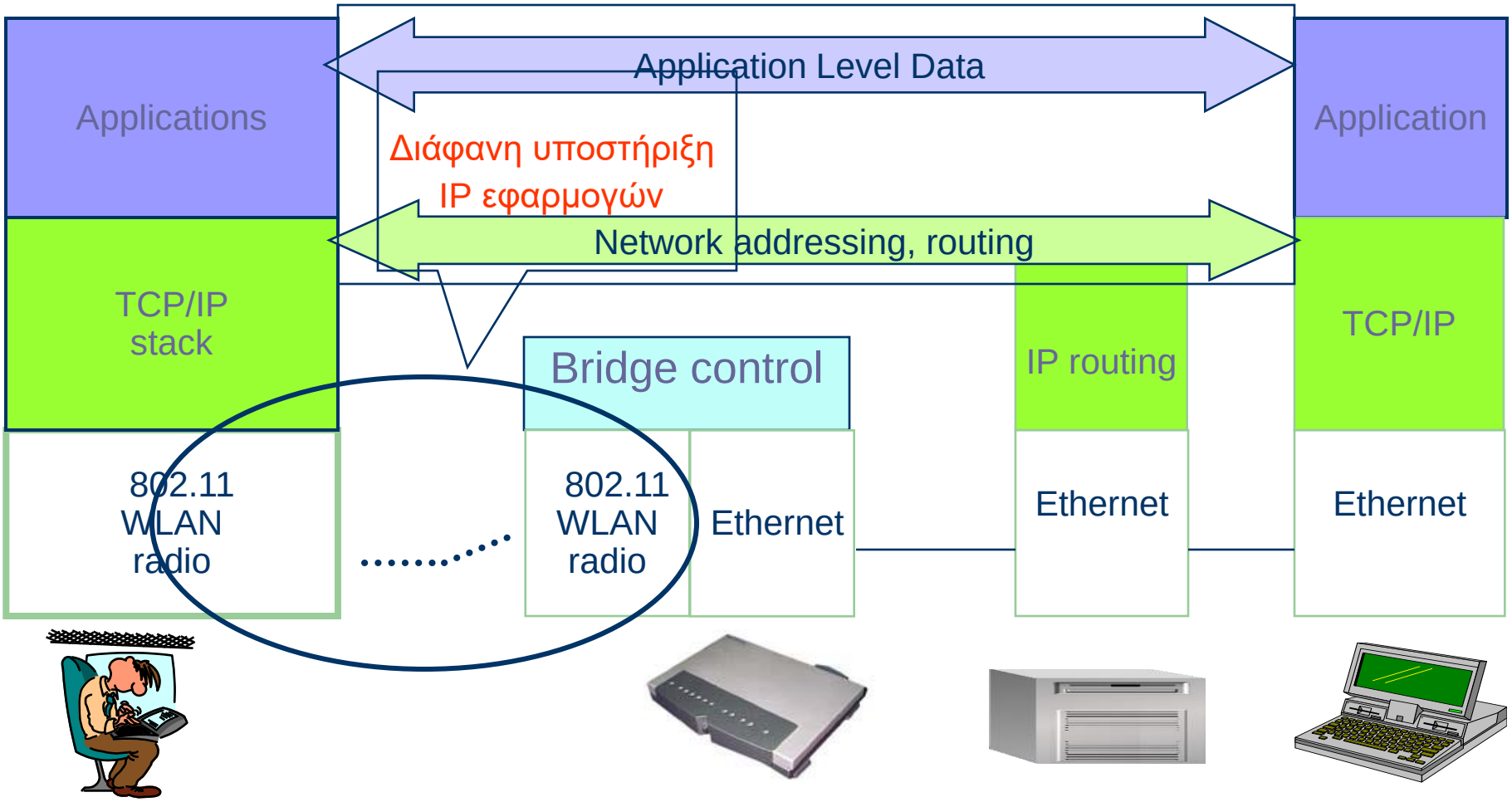
Station (STA)

τερματικό με μηχανισμούς πρόσβασης στο ασύρματο μέσο

Independent Basic Service Set (IBSS)

ομάδα σταθμών που χρησιμοποιούν την ίδια ραδιο-συχνότητα, χωρίς την παρεμβολή σημείου πρόσβασης

802.11 – Ασύρματη Επέκταση του Ethernet



Το MAC είναι υπεύθυνο για

- ✓ δέσμευση του καναλιού
- ✓ διευθυνσιοδότηση (addressing)
- ✓ δομή των πλαισίων μετάδοσης
- ✓ έλεγχο λαθών (επαναμεταδόσεις)
- ✓ fragmentation/reassembly

Τρία είδη πλαισίων:

✓management (association, synchronization, authentication)

✓control (acks, end of contention-free period)

✓user data

Μέθοδοι Πρόσβασης

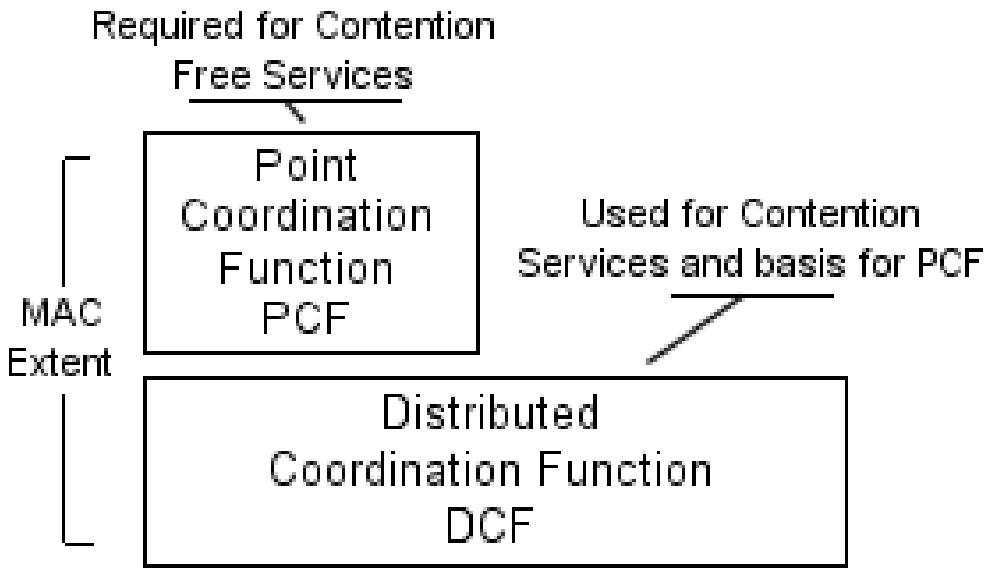
Distributed Coordination Function (DCF)

- υποχρεωτική
- η βασική μέθοδος πρόσβασης
- βασίζεται στον ανταγωνισμό για το μέσο (contention)

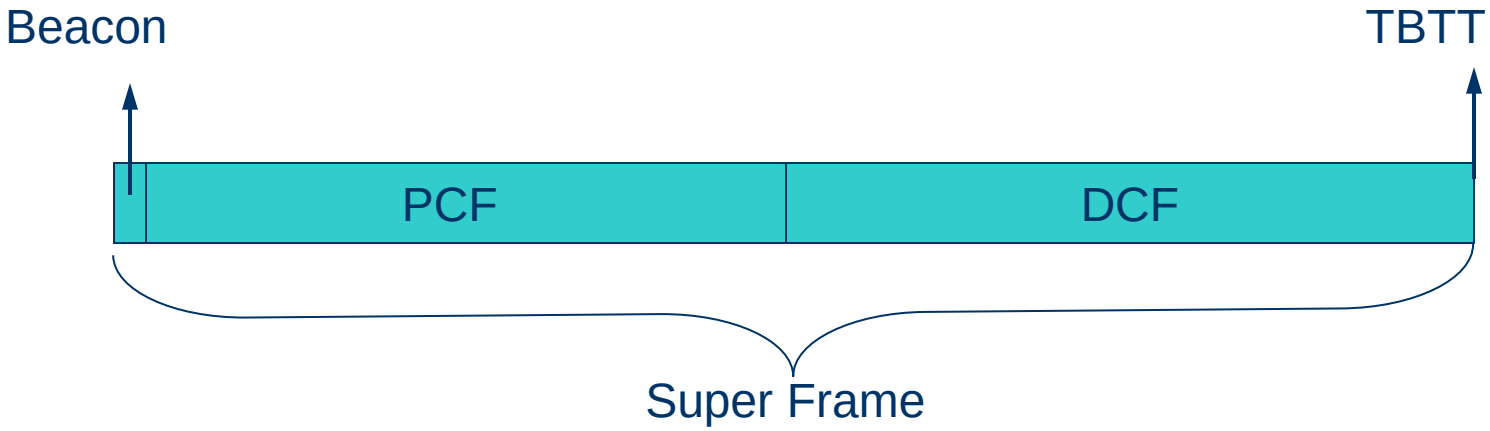
Point Coordination Function (PCF)

- προαιρετική
- χωρίς ανταγωνισμό
- μειώνει τις μεταβολές στις καθυστερήσεις μετάδοσης

-μόνο στη δομημένη διάρθρωση (infrastructure mode)



Μέθοδοι Πρόσβασης



DCF - Distributed Coordinated Function
(Contention Period - *Ad-hoc Mode*)

PCF - Point Coordinated Function
(Contention Free Period – *Infrastructure BSS*)

Beacon - Management Frame

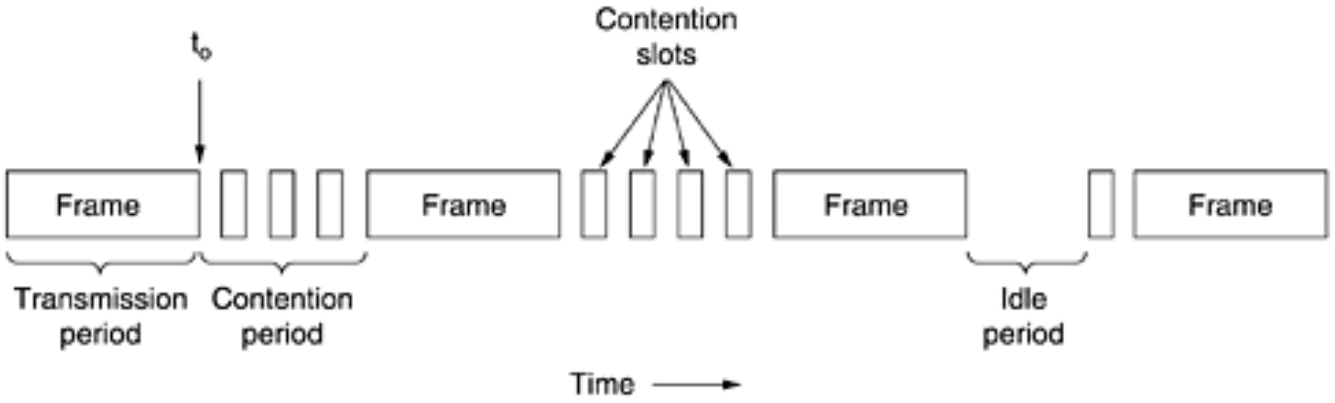
Synchronization of Local timers

Delivers protocol related parameters (e.g., version)

TBTT (Target Beacon Transition Time)

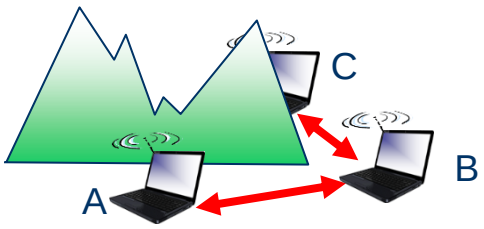
Πολλαπλή Προσπέλαση Ανίχνευσης Φέροντος Με Ανίχνευση Σύγκρουσης(CSMA/CD)

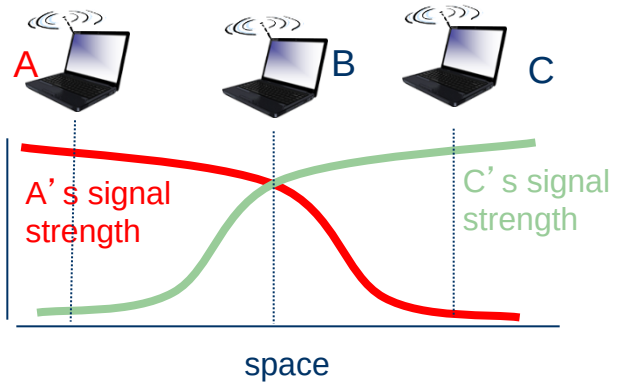
- κάθε κόμβος μπορεί να ακούσει **πριν μεταδώσει** και οι φυσικές ιδιότητες του καναλιού επιτρέπουν σε ένα κόμβο να ακούει το κανάλι **ενώ μεταδίδει**
- αμέσως μόλις ο κόμβος ανιχνεύσει την σύγκρουση:
  - εγκαταλείπει τη μετάδοση
  - περιμένει τυχαίο χρονικό διάστημα πριν ξαναπροσπαθήσει
- Χρησιμοποιείται στο Ethernet
- δύσκολο να εφαρμοστεί σε ασύρματες μεταδόσεις



IEEE 802.11: πολλαπλή πρόσβαση

- αποφυγή συγκρούσεων: >1 κόμβοι μεταδίδουν την ίδια στιγμή
- 802.11: CSMA – “αφουγκράζεται” το κανάλι πριν μεταδώσει
  - μη συγκρουστείς με εν εξελίξει μετάδοση από άλλο κόμβο
- 802.11: *χωρίς* ανίχνευση σύγκρουσης!
  - δύσκολο να λάβει (ανιχνεύσει συγκρούσεις) όταν μεταδίδει λόγω αδύναμων λαμβανόμενων σημάτων (εξασθένιση)
  - δεν μπορεί να αντιληφθεί όλες τις συγκρούσεις σε κάθε περίπτωση: κρυμμένο τερματικό, εξασθένιση
  - στόχος: *αποφυγή συγκρούσεων:* CSMA/C(ollision)A(voidance)





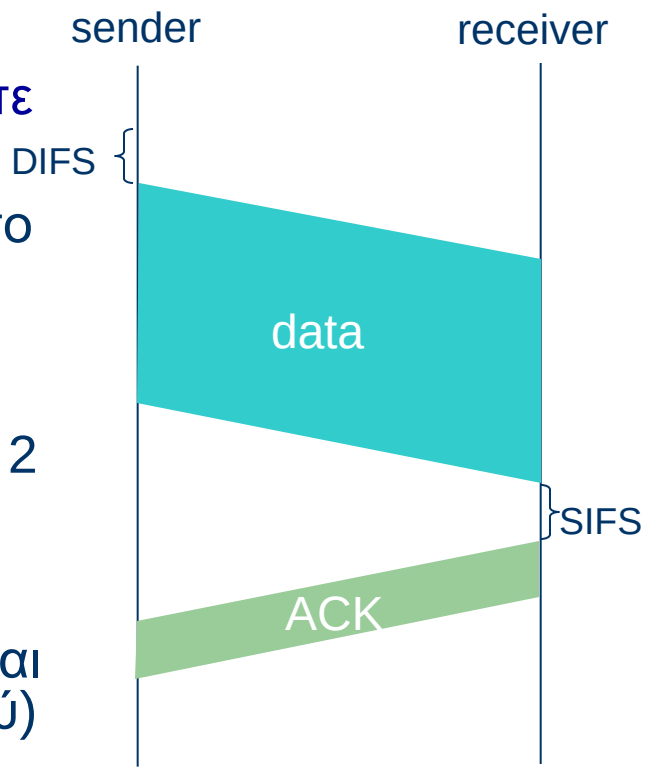
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 αποστολέας

- αν «αισθανθείς» το κανάλι αδρανές για **DIFS** τότε μετάδωσε ολόκληρο το πλαίσιο (όχι CD)
- αν «αισθανθείς» το κανάλι απασχολημένο τότε
  - ξεκίνησε τυχαίο χρόνο οπισθοχώρησης
  - χρονομετρητής μετράει αντίστροφα όταν το κανάλι είναι αδρανές
  - μετάδωσε όταν λήξει ο χρονομετρητής
  - αν δεν λάβεις ACK, αύξησε το τυχαίο διάστημα οπισθοχώρησης, επανάλαβε το 2

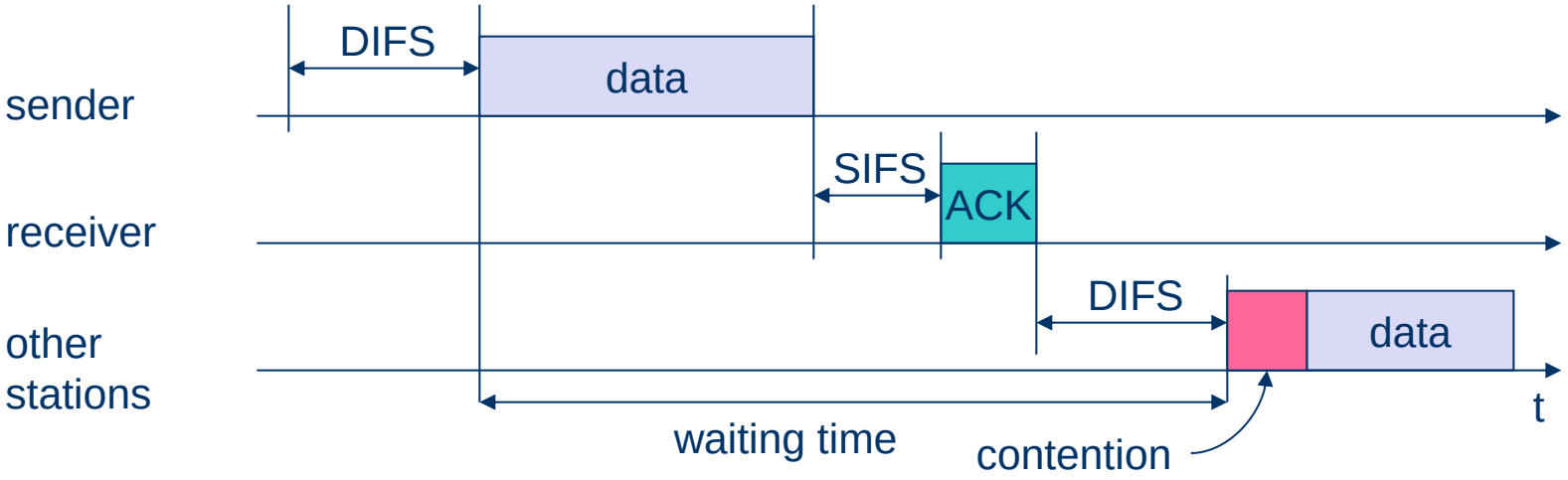
802.11 δέκτης

- αν το πλαίσιο παραληφθεί ΟΚ
  - στείλε ACK μετά από **SIFS** (ACK χρειάζεται λόγω προβλήματος κρυμμένου τερματικού)



802.11 - CSMA/CA access method

- Αποστολή πακέτων
  - Ο κόμβος πρέπει να διαπιστώσει το κανάλι αδρανές για χρόνο ίσο με DIFS πριν στείλει δεδομένα
  - Ο παραλήπτης επιβεβαιώνει (μετά από χρόνο SIFS) αν το πακέτο παρελήφθη σωστά (CRC)
  - Σε περίπτωση λάθους, επαναμέταδοση μετά από τυχαίο χρόνο



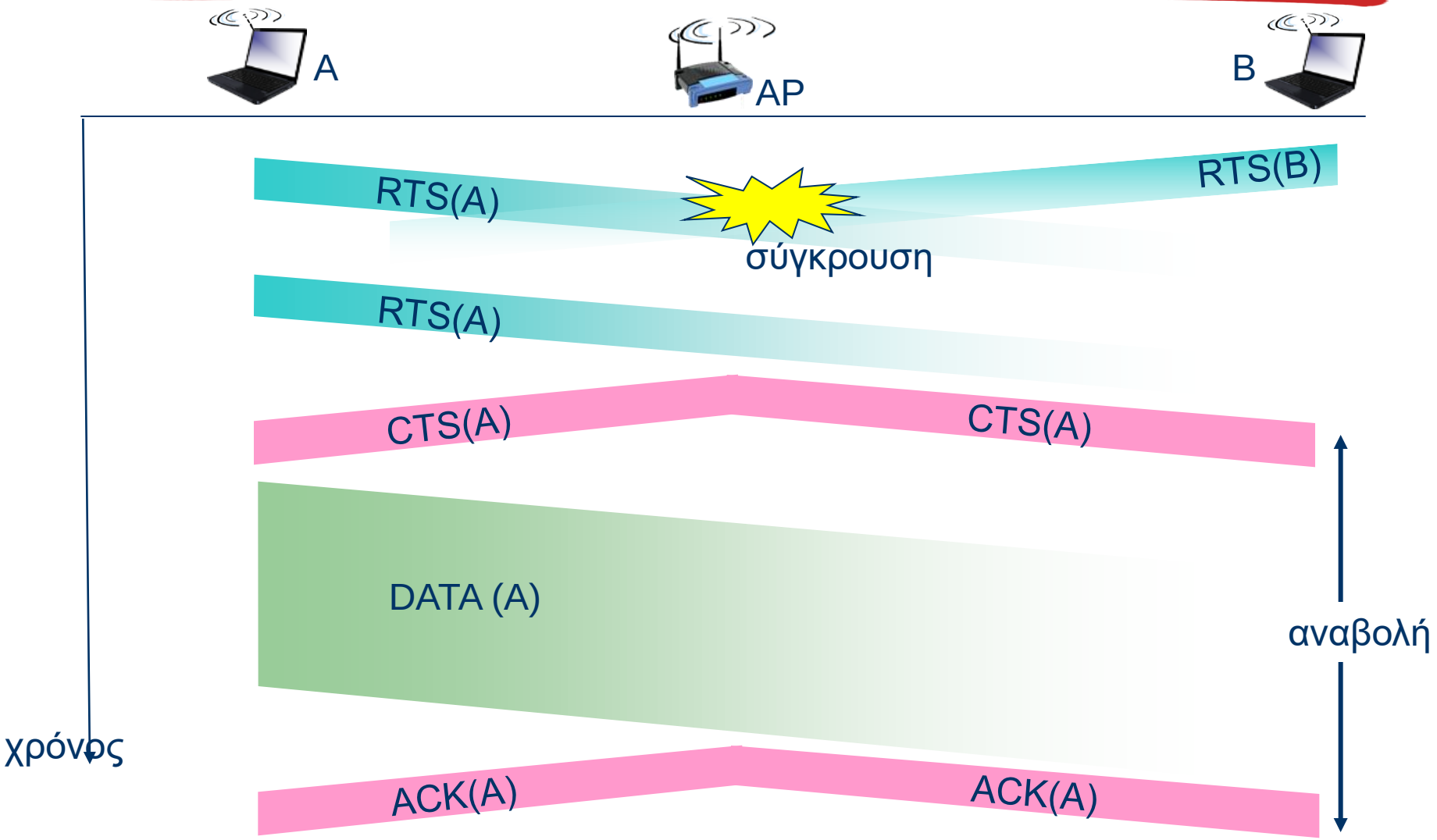
Αποφυγή συγκρούσεων (περισσότερα)

ιδέα: επίτρεψε στον αποστολέα να "κάνει κράτηση" στο κανάλι αντί για τυχαία πρόσβαση των πλαισίων δεδομένων → αποφυγή συγκρούσεων μεγάλων πλαισίων δεδομένων

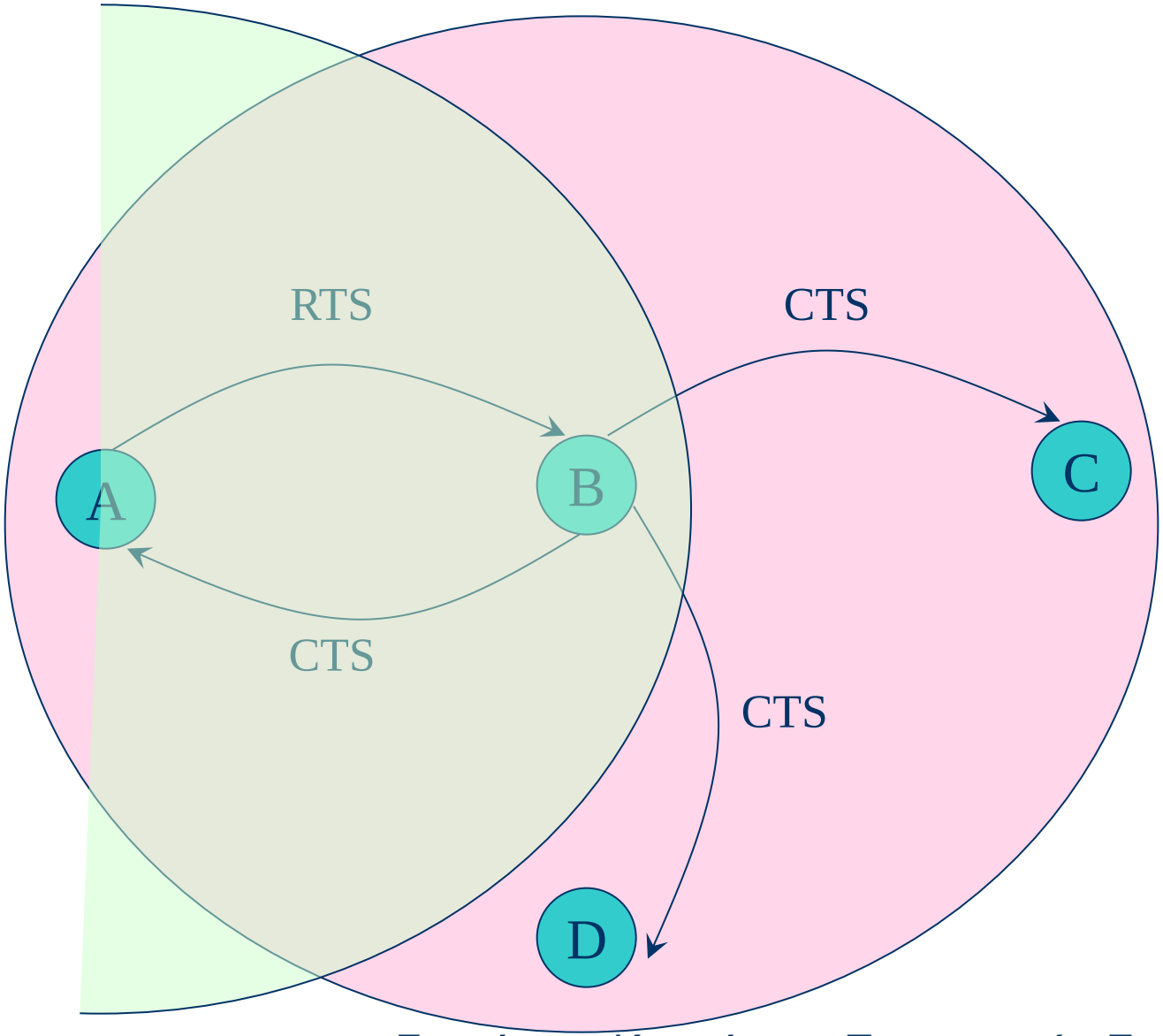
- ο αποστολέας πρώτα μεταδίδει *μικρά* πακέτα request-to-send (RTS) (αίτηση για αποστολή) στο BS (σταθμό βάσης) χρησιμοποιώντας CSMA
  - τα RTS μπορεί να συγκρουστούν μεταξύ τους (αλλά είναι μικρά)
- AP εκπέμπει clear-to-send (CTS) σε απόκριση του RTS
- το CTS (clear to send – "ελεύθερο" για αποστολή) ακούγεται από όλους τους κόμβους
  - ο αποστολέας μεταδίδει πλαίσιο δεδομένων
  - οι άλλοι σταθμοί αναβάλλουν τις μεταδόσεις

απόφυγε συγκρούσεις πλαισίων δεδομένων εντελώς, χρησιμοποιώντας μικρά πακέτα κράτησης!

Αποφυγή Συγκρούσεων: «κράτηση» καναλιού μέσω RTS-CTS



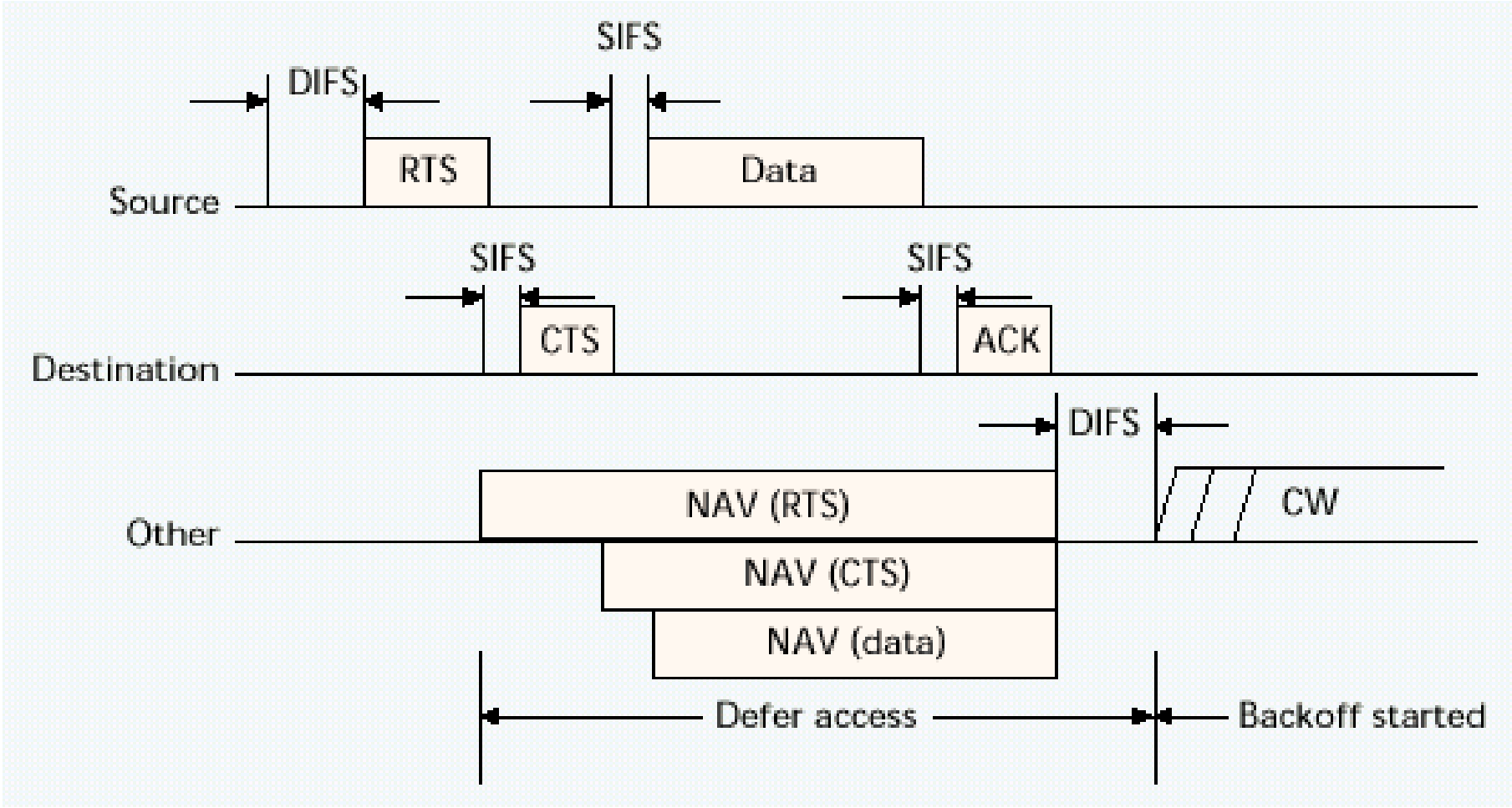
Αποφυγή σύγκρουσης στον κόμβο B



Distributed Coordination Function

- CSMA/CA based protocol
  - Listen before talk
  - Collision Avoidance αντί για Collision Detection
  - Διαφορετικό από τα CSMA/CD που χρησιμοποιούνται σε ενσύρματα

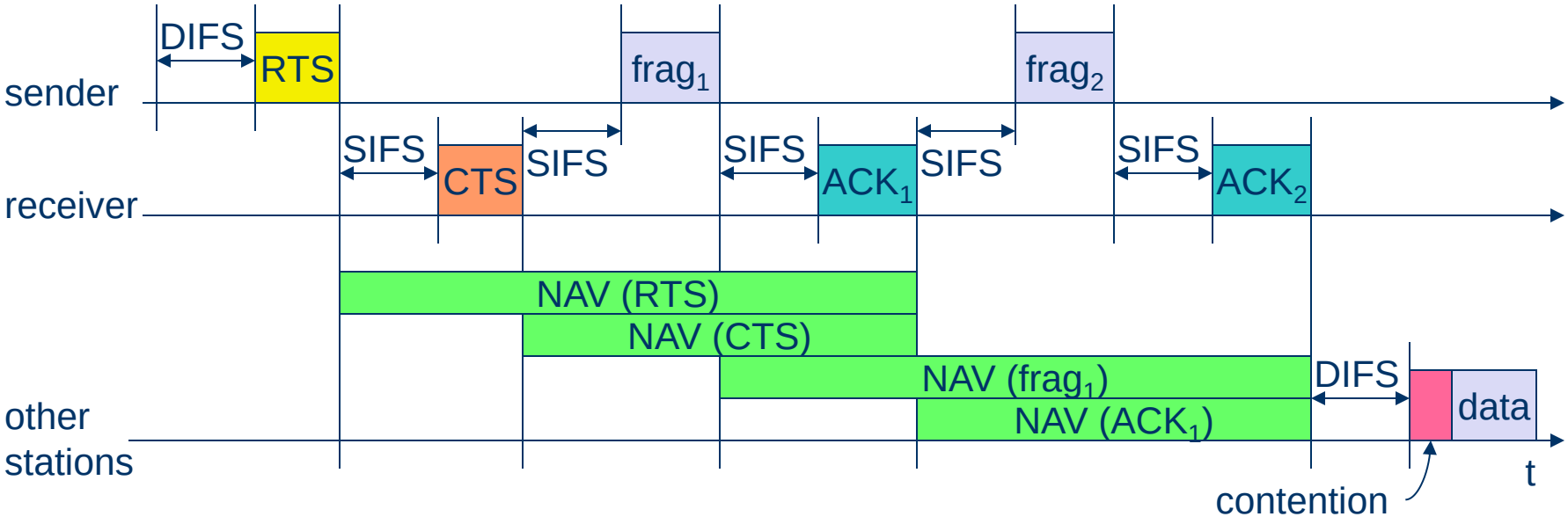
- Χρησιμοποιεί Acknowledgment για κάθε μετάδοση
- Διόρθωση λαθών μέσω επαναμεταδόσεων
- Χρησιμοποιεί 4-way handshake (μέσω μηνυμάτων RTS/CTS) για «Virtual Carrier Sensing»
- Αντιμετωπίζει το πρόβλημα του κρυμμένου τερματικού



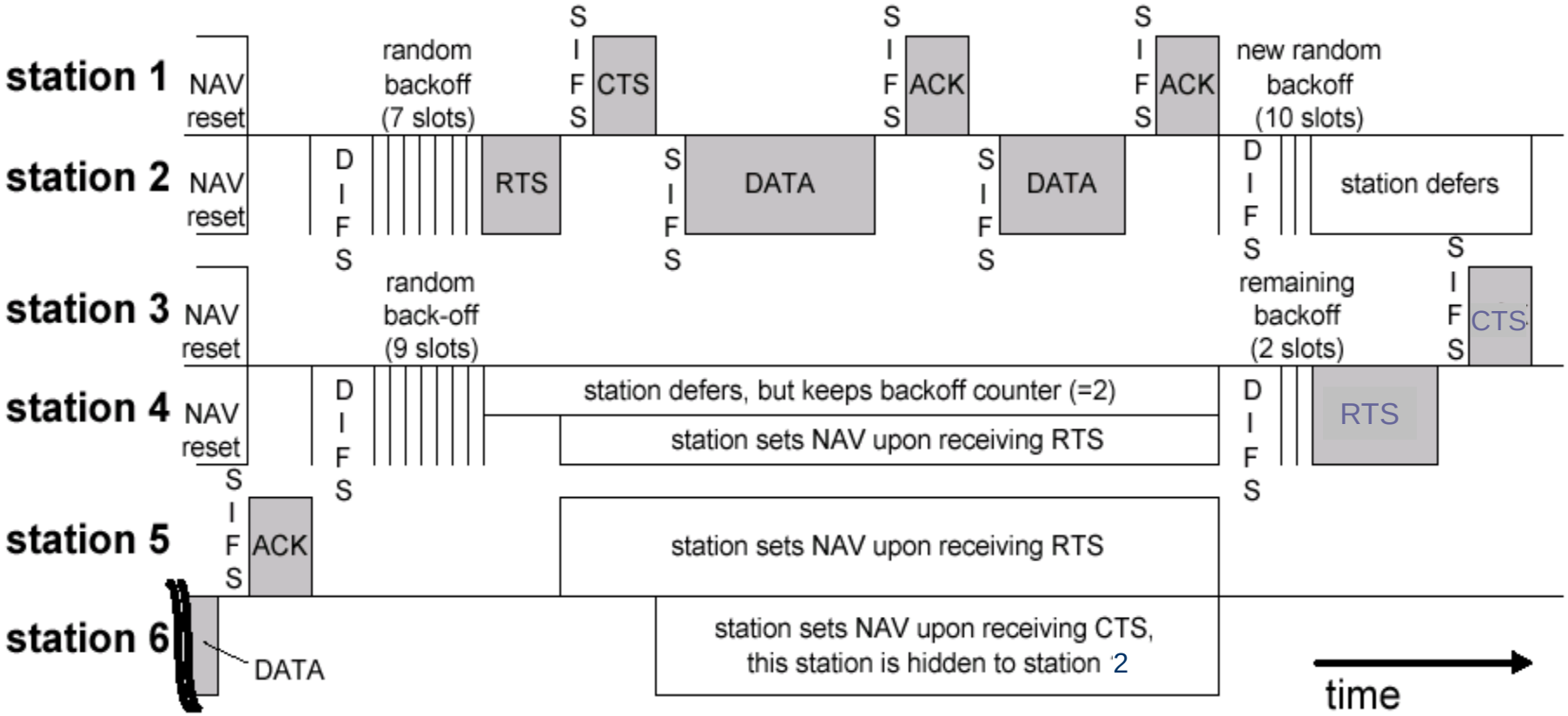
- Ισχύει πάντα SIFS<DIFS

- Πολύ σημαντική η ενημέρωση των NAVs (Network Allocation Vectors) με τη χρήση των RTS/CTS/data MPDUs για την εφαρμογή power saving μηχανισμών και την αποφυγή συγκρούσεων

Fragmentation



Παράδειγμα Μετάδοσης με DCF



Το CW διπλασιάζεται μετά από κάθε σύγκρουση

- Initial CW -> 3 (τιμές backoff 0-3)
- CW after Collision 1 → 7 (τιμές backoff 0-7)
- CW after Collision 2 → 15 (τιμές backoff 0-15)
- CW after Collision 3 → 31 (τιμές backoff 0-31)
- CW after Collision 4 → 63 (τιμές backoff 0-63)

Βασικά Μειονεκτήματα DCF

- Απρόβλεπτος αριθμός συγκρούσεων
- Απρόβλεπτες καθυστερήσεις επιτυχούς μετάδοσης
- Απρόβλεπτη ρυθμαπόδοση (throughput)
- Μη ελεγχόμενη επιλογή σταθμού προς μετάδοση

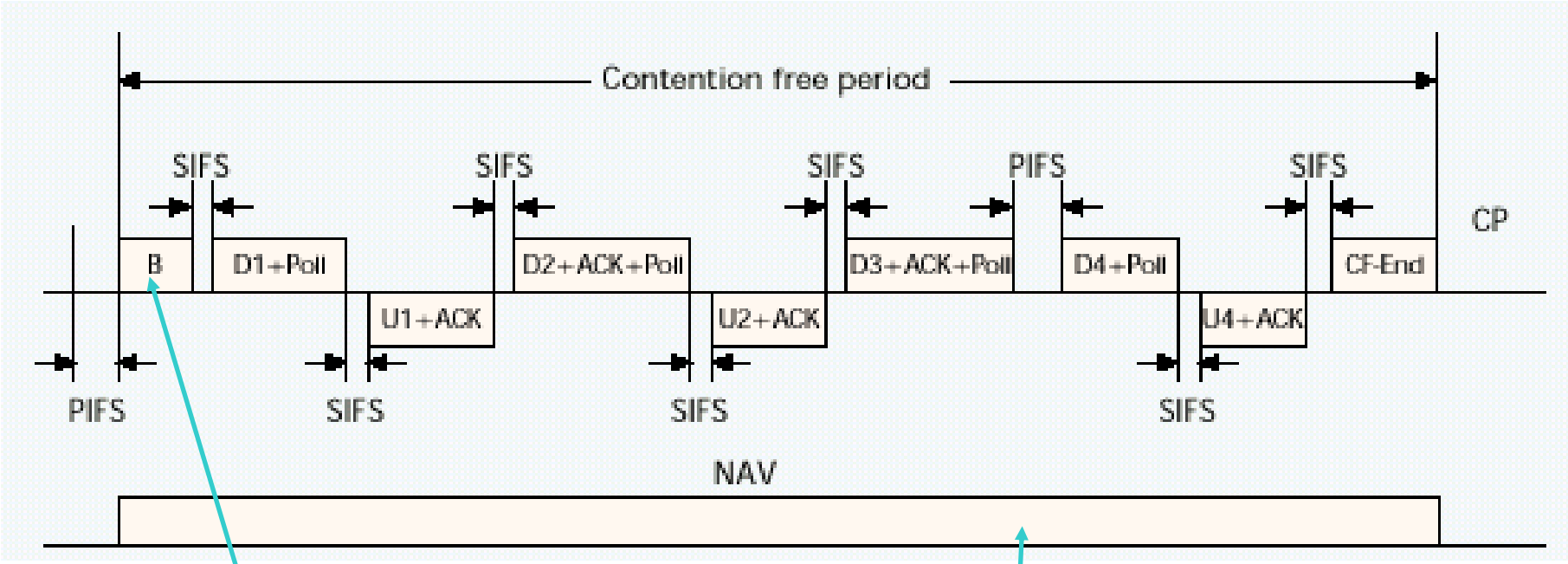
Και ένα πλεονέκτημα:

- Χαμηλή καθυστέρηση μετάδοσης και καλή απόδοση σε χαμηλό φόρτο

Point Coordination Function (I)

- ✓ Ενεργοποιείται από το AP όποτε αυτό κρίνει ότι πρέπει να περάσει σε contention-free period (π.χ. όταν διακρίνει μεγάλο αριθμό συγκρούσεων)
- ✓ Γενικά, όταν η κίνηση είναι χαμηλή συμφέρει το DCF, ενώ όταν είναι υψηλή συμφέρει το PCF
- ✓ Σε αυτή τη λειτουργία το AP ονομάζεται και Point Coordinator
- ✓ Έχει προτεραιότητα σε σχέση με την DCF γιατί ενεργοποιείται μετά από ανενεργό χρόνο PIFS<DIFS

Point Coordination Function (II)



Synchronization beacon

Variable duration of
Contention Free Period

Βασικά μειονεκτήματα του PCF

✓Τα τερματικά δεν έχουν τρόπο να μεταδώσουν τις απαιτήσεις τους στο AP

✓Το AP δεν έχει τρόπο να διακόψει μια μετάδοση σε εξέλιξη για να στείλει το synchronization beacon *

✓ Το Poll δεν καθορίζει χρόνο για τον οποίο δίνεται το κανάλι με αποτέλεσμα ένας σταθμός να μπορεί να το κρατήσει όσο έχει δεδομένα προς μετάδοση *

* Maximum packet (MPDU) allowed 4095 bytes = 32760 bits = 32,76 msec (για κανάλι 1Mbps)

Ασφάλεια στο 802.11

Όπου απαιτείται κρυπτογράφηση και πιστοποίηση 3 παράγοντες λαμβάνονται υπόψη

- οι ανάγκες του χρήστη για ασφάλεια και πόσο αυτές θα κοστίσουν

- η ευκολία στη χρήση του μηχανισμού

- οι κυβερνητικοί περιορισμοί στις μεθόδους κρυπτογράφησης, ειδικά όσον αφορά την εξαγωγή τους

Wired Equivalent Privacy (WEP) Protocol

- Σχετικά αποδοτικό, σε σχέση με το κόστος και τις ανάγκες που καλύπτει
- «Αυτο-συγχρονιζόμενο» (σταθμοί μπαίνουν και βγαίνουν εύκολα)
- Χαμηλών υπολογιστικών αναγκών
- Προαιρετικό στην υλοποίηση
- Περιλαμβάνει δύο διαδικασίες (κρυπτογράφηση και πιστοποίηση)
- Κρυπτογράφηση και πιστοποίηση γίνονται με τον ίδιο τρόπο και το ίδιο κλειδί (όποιος κλέψει το κλειδί μπορεί να κάνει τα πάντα)

Κρυπτογράφηση (Encryption)

- Υλοποιείται με ένα κρυφό κλειδί μήκους 40 bits αποθηκευμένο μόνιμα στους σταθμούς
- Το κλειδί αυτό περνά από μια γεννήτρια για να παραχθεί μια ακολουθία χαρακτήρων βασισμένη στο κρυφό κλειδί
- Η ακολουθία και τα δεδομένα τροφοδοτούν μια συνάρτηση XOR
- Το αποτέλεσμα τροφοδοτείται για μετάδοση

Παράδειγμα Κρυπτογράφησης

Έστω ότι το διαδικό 2 (00000010) είναι το κλειδί κρυπτογράφησης.
Περνάει από μια XOR με το κείμενο που θέλουμε να μεταδώσουμε.
Για το παράδειγμά μας το κείμενο είναι το "HI"

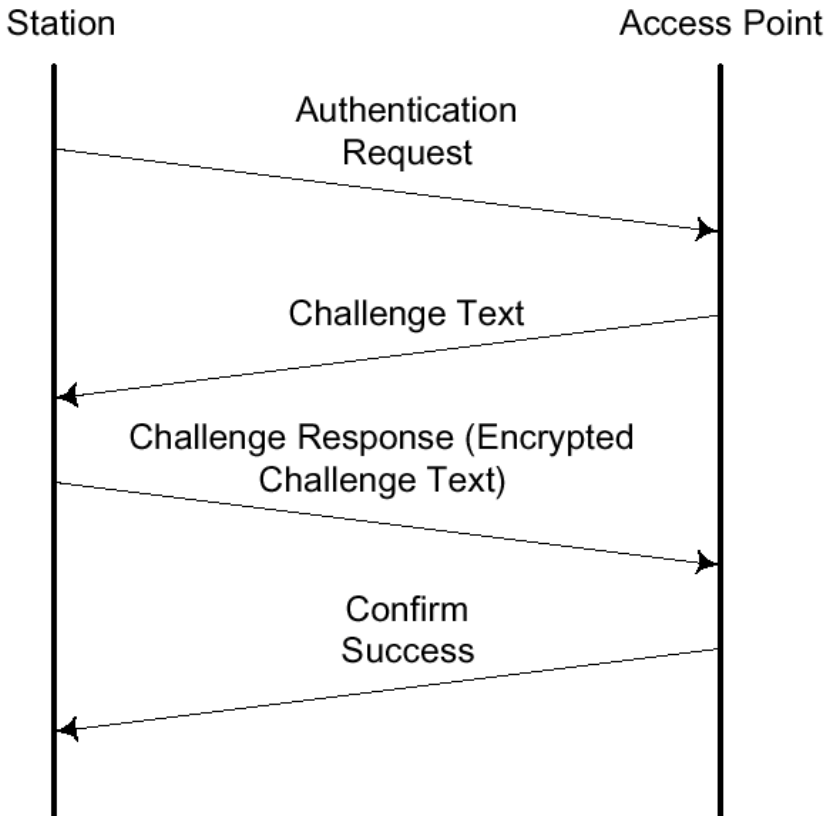
	H	I	
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
XOR	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	
	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	Κρυπτογραφημένο κείμενο

Όταν λαμβάνεται το κρυπτογραφημένο κείμενο περνά πάλι από μια XOR
Με το ίδιο κλειδί για να ανακτηθεί το αρχικό κείμενο.

	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	Κρυπτογραφημένο κείμενο
XOR	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
	H	I	

Πιστοποίηση (Authentication)

•Χρησιμοποιεί το ίδιο κρυφό κλειδί με την κρυπτογράφηση (όχι και τόσο καλό από άποψη ασφάλειας)



Shared Key Authentication

Node

Access Point

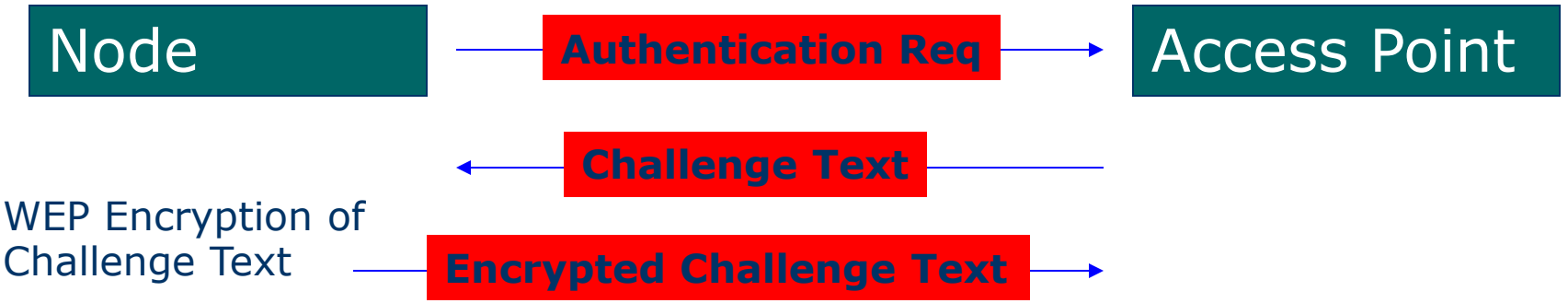
Shared Key Authentication

Shared Key Authentication

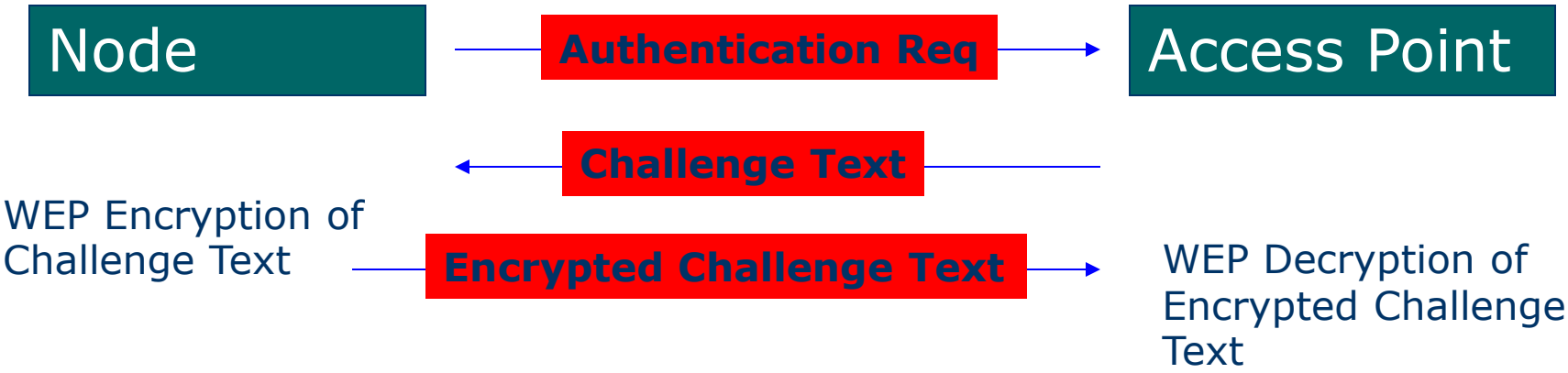
Shared Key Authentication

WEP Encryption of
Challenge Text

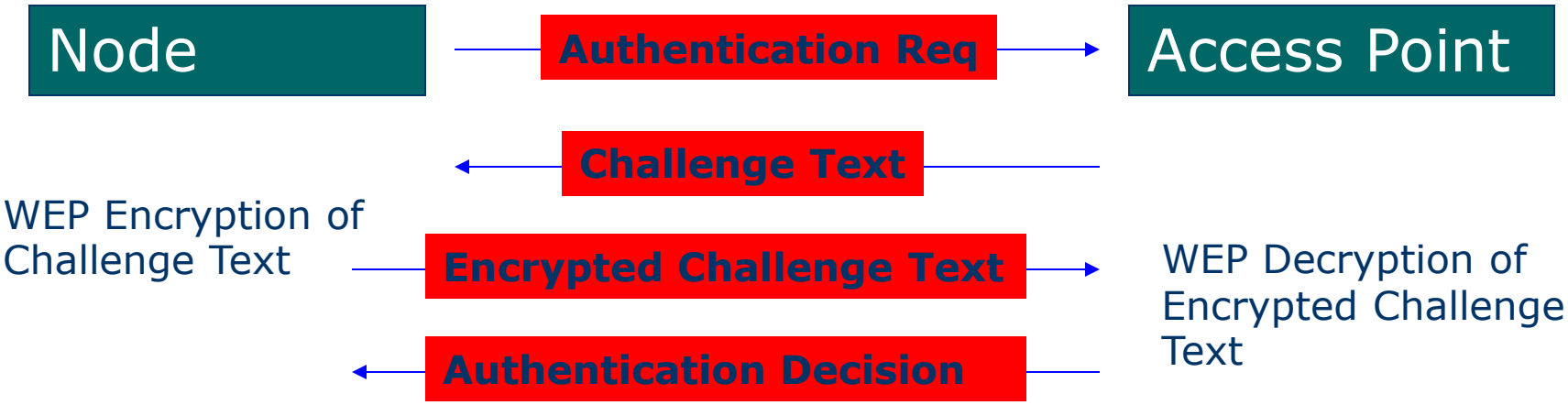
Shared Key Authentication



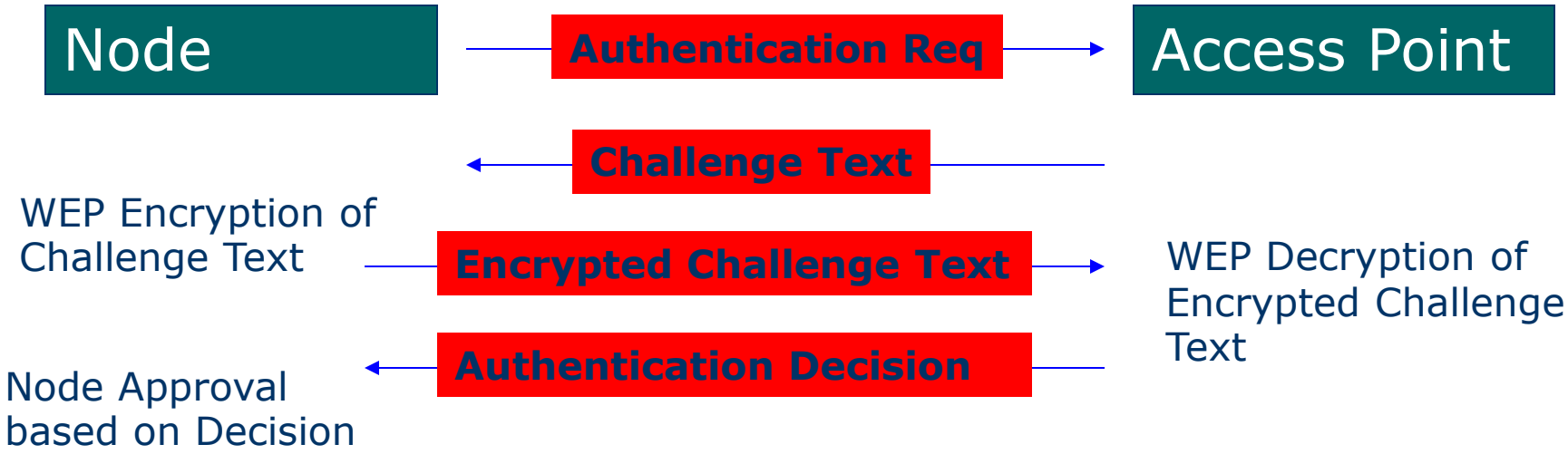
Shared Key Authentication



Shared Key Authentication



Shared Key Authentication



Κινητικότητα

A STA associated with a BSS

Poor connection quality ?

Yes

Scan the medium

Find a better connection ?

No

Yes

Reassociation request to new AP

Reassosiation response

No

Yes

STA has roamed to a new AP

Old AP is notified through DS

•Καμία ρύθμιση για τα πακέτα που θα χαθούν κατά τη διάρκεια του handover