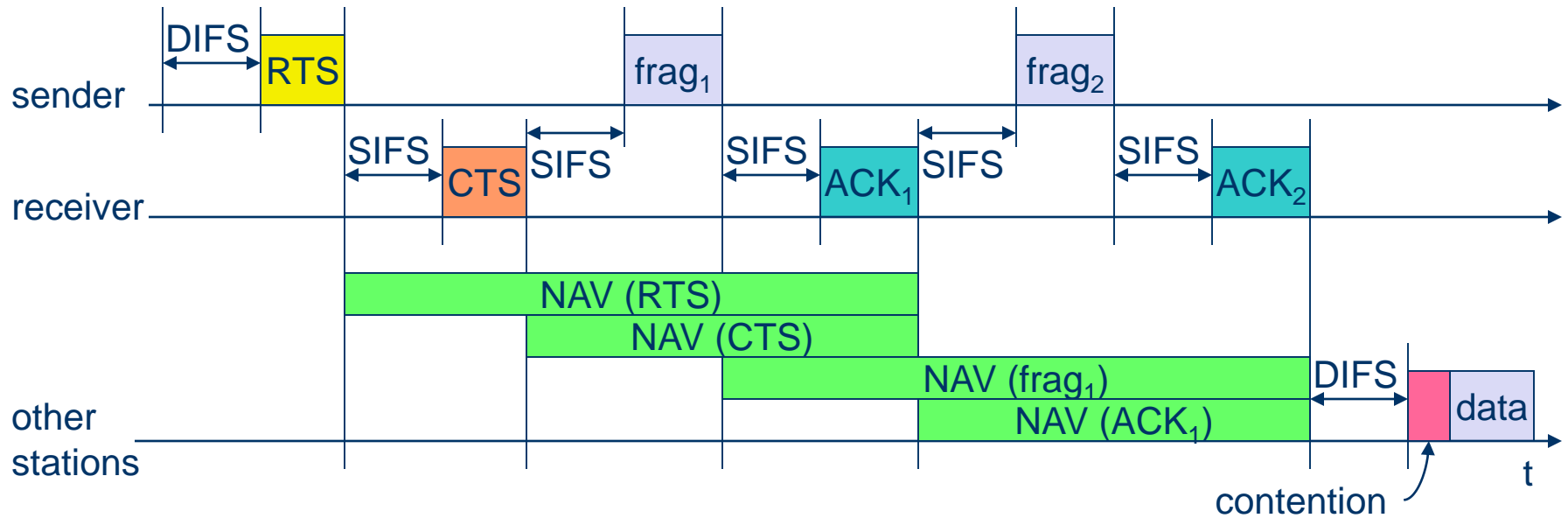


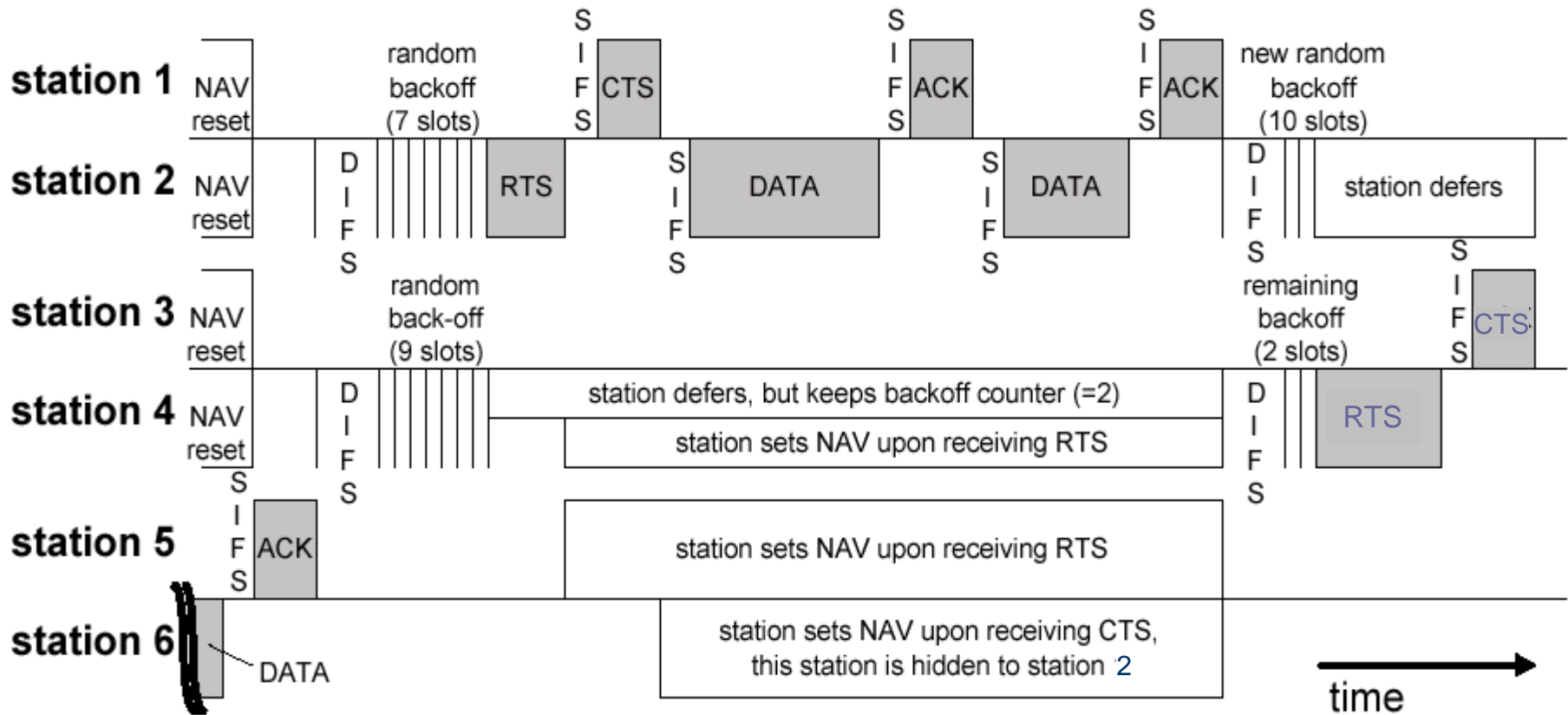
# Ασύρματα Τοπικά Δίκτυα Τύπου IEEE 802.11

## Συνέχεια

# 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

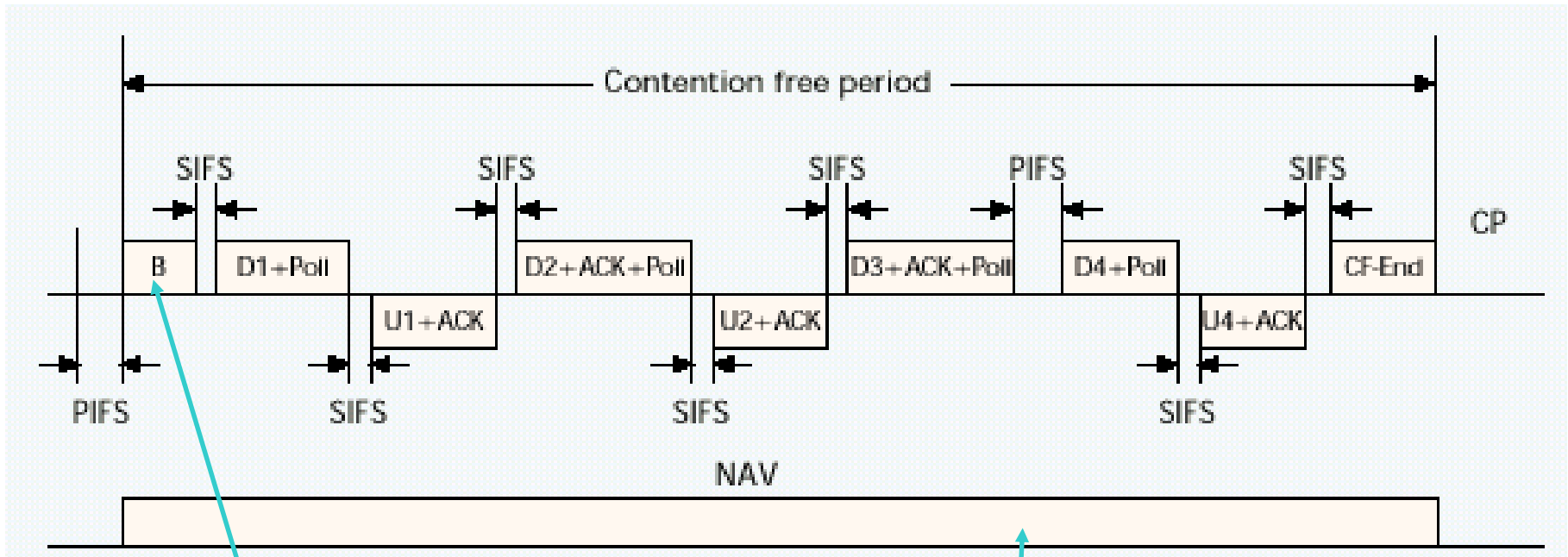
Και ένα πλεονέκτημα:

- 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”

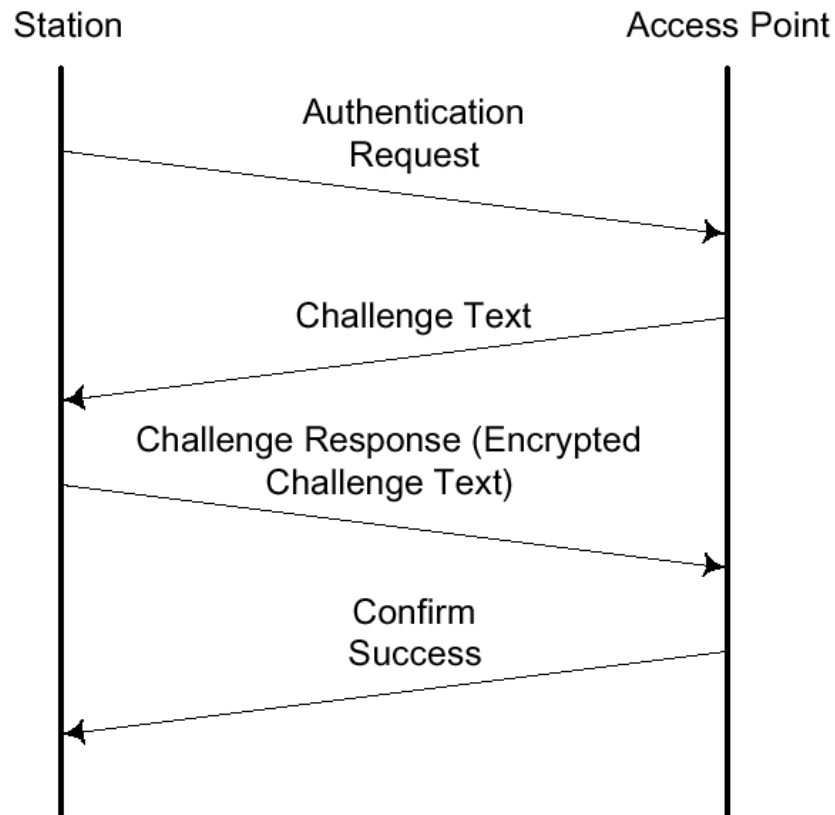
	<b>H</b>	<b>I</b>	
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
<b>XOR</b>	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	
	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	<b>Κρυπτογραφημένο κείμενο</b>

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	<b>Κρυπτογραφημένο κείμενο</b>
<b>XOR</b>	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	
	<b>H</b>	<b>I</b>	

# Πιστοποίηση (Authentication)

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



# Shared Key Authentication

Node

Access Point

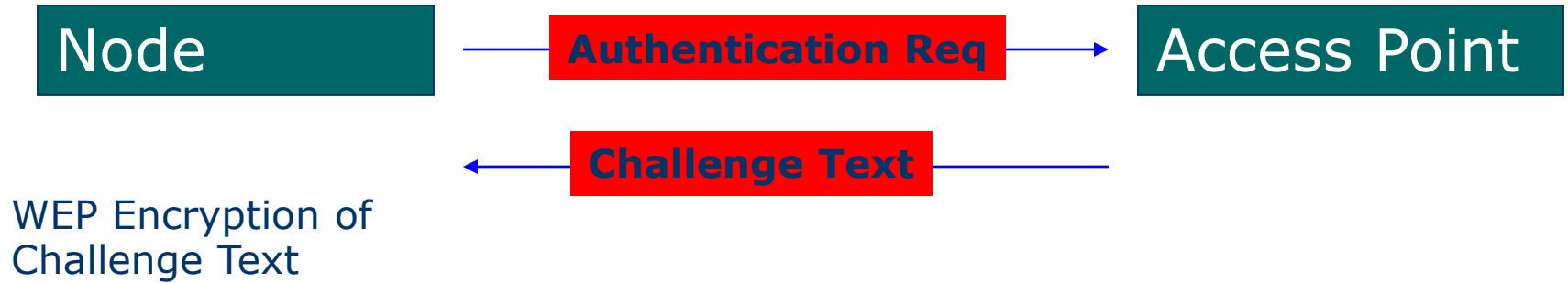
# Shared Key Authentication



# Shared Key Authentication

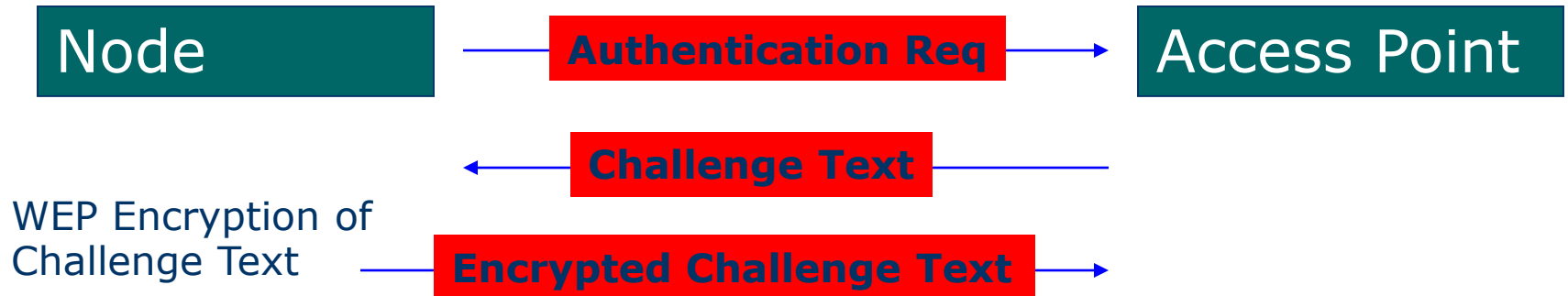


# Shared Key Authentication

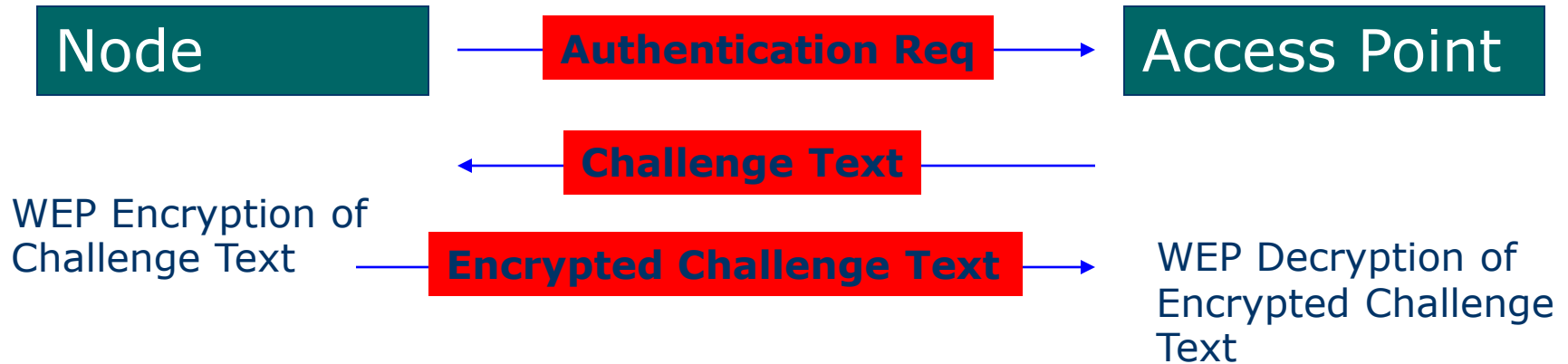




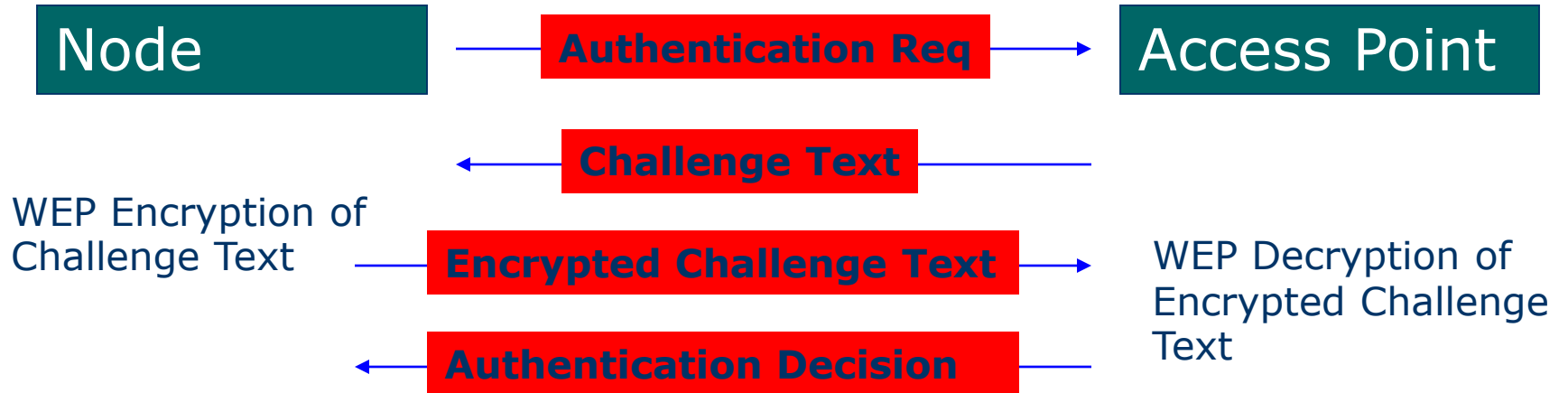
# Shared Key Authentication



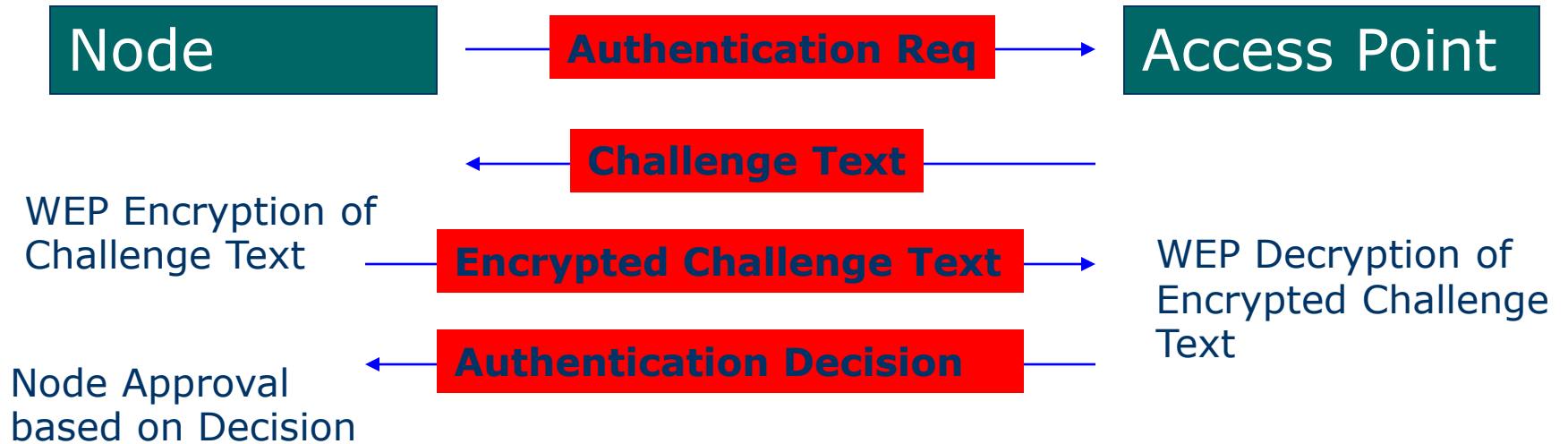
# Shared Key Authentication



# Shared Key Authentication



# Shared Key Authentication



# Κινητικότητα

A STA associated with a BSS

Poor connection quality ?

↓ Yes

Scan the medium

Find a better connection ?

↓ Yes

Reassociation request to new AP

Reassociation response

↓ 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

