

# Εργαστήριο μαθήματος

- Μέρος του βαθμού (30%) θα προκύψει από μία ατομική εργασία
- Η εργασία θα πρέπει να είναι υπό μορφή παρουσίασης διάρκειας 15 λεπτών (διαφάνειες και βίντεο).
- Επιλογή από λίστα θεμάτων ή και πρόταση από το φοιτητή.
- Το πλήθος των διαφανειών αφήνεται στην κρίση κάθε φοιτητή, αρκεί η διάρκεια της παρουσίασης να μην υπερβαίνει το διαθέσιμο 15λεπτο.
- Όλες οι εργασίες θα πρέπει να υποβληθούν μέσω του eclass έως τέλος Ιανουαρίου.

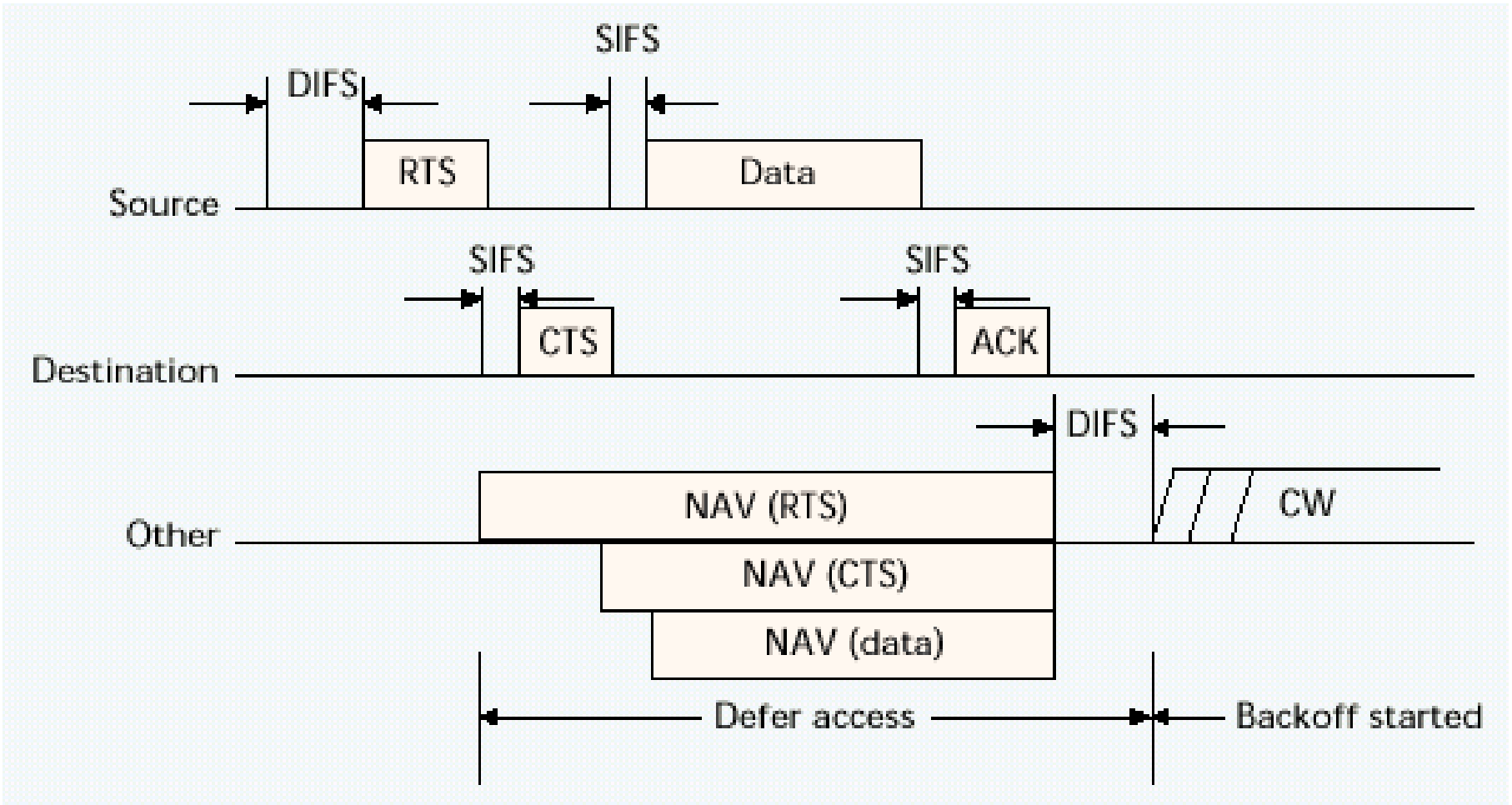
1. Κατηγοριοποίηση ασύρματων δικτύων βάσει της περιοχής κάλυψης (Body Area Network, Personal Area Network, Local Area Network, κτλ.): τύποι δικτύων, προκλήσεις στην υλοποίησή τους και τεχνολογίες
2. Μέθοδοι Πολλαπλής Πρόσβασης (Multiple Access) σε ασύρματα δίκτυα, με έμφαση σε δίκτυα 5<sup>ης</sup> γενιάς
3. Μέθοδοι συμπίεσης για αποστολή δεδομένων πάνω από ασύρματα δίκτυα
4. Αλγόριθμοι εντοπισμού θέσης σε ασύρματα κινητά δίκτυα
5. Ενεργητικές επιθέσεις σε ασύρματα δίκτυα: η περίπτωση της εκούσιας παρεμβολής (jamming) και μέθοδοι αντιμετώπισής της
6. Παθητικές επιθέσεις σε ασύρματα δίκτυα: η περίπτωση της λαθρακρόασης (eavesdropping) και μέθοδοι αντιμετώπισής της
7. Ποιότητα υπηρεσίας (Quality of Service (QoS)) και ποιότητας εμπειρίας (Quality of Experience (QoE)) σε δίκτυα 5<sup>ης</sup> γενιάς
8. Δίκτυα IEEE 802.11 (Wi-Fi): μία επισκόπηση στην 6<sup>η</sup> γενιά Wi-Fi (Wi-Fi 6) και στην 7<sup>η</sup> γενιά (Wi-Fi 7)
9. Ο ρόλος των δορυφορικών επικοινωνιών στα δίκτυα 5<sup>ης</sup> και 6<sup>ης</sup> γενιάς
10. Διαδίκτυο των Πραγμάτων (Internet of Things (IoT)) σε μη αδειοδοτημένες μπάντες συχνοτήτων: τεχνολογίες και εφαρμογές

11. Επικοινωνίες Εγγύς Πεδίου (Near Field Communication (NFC)): τι είναι, ποιες οι τεχνολογίες και ποιες οι προκλήσεις;
12. Επισκόπηση των επικοινωνιών Οχήματος-προς-Όλα (Vehicle-to-Everything (V2X))
13. Προκλήσεις στην υλοποίηση επικοινωνιών Μη-επανδρωμένων Εναέριων Οχημάτων (Unattended Aerial Vehicle (UAV)) πάνω από κυψελωτά δίκτυα
14. Προκλήσεις στην υλοποίηση εφαρμογών Επαυξημένης Πραγματικότητας (Augmented Reality (AR)), Εικονικής Πραγματικότητας (Virtual Reality (VR)) και Μικτής Πραγματικότητας (Mixed Reality (MR)) πάνω από δίκτυα 5<sup>ης</sup> γενιάς
15. Μορφοποίηση ακτινών (Beamforming): τι είναι και ποια πλεονεκτήματα προσφέρει;
16. Υποστήριξη ασύρματων δικτύων από υπηρεσίες Υπολογιστικής Νέφους (Cloud Computing)
17. Αναρρυθμιζόμενες Ευφυείς Επιφάνειες (Reconfigurable Intelligent Surfaces (RIS)): τι είναι, πώς υλοποιούνται και ποια πλεονεκτήματα προσφέρουν;
18. Χρήση ασύρματων επικοινωνιών στη Βιομηχανία 4.0 (Industry 4.0) και πέρα από αυτή (Βιομηχανία 5.0 (Industry 5.0))
19. Ψηφιακοί Δίδυμοι (Digital Twins (DTs)): τι είναι, πώς υλοποιούνται και τι ρόλο θα διαδραματίσουν τα δίκτυα 5<sup>ης</sup> και 6<sup>ης</sup> γενιάς στην πραγματοποίησή τους;
20. Διανομή Κβαντικών Κλειδιών (Quantum Key Distribution (QKD)): τι είναι και ποια η εφαρμογή της στα δίκτυα 5<sup>ης</sup> και 6<sup>ης</sup> γενιάς;

# The IEEE 802.11 family of standards



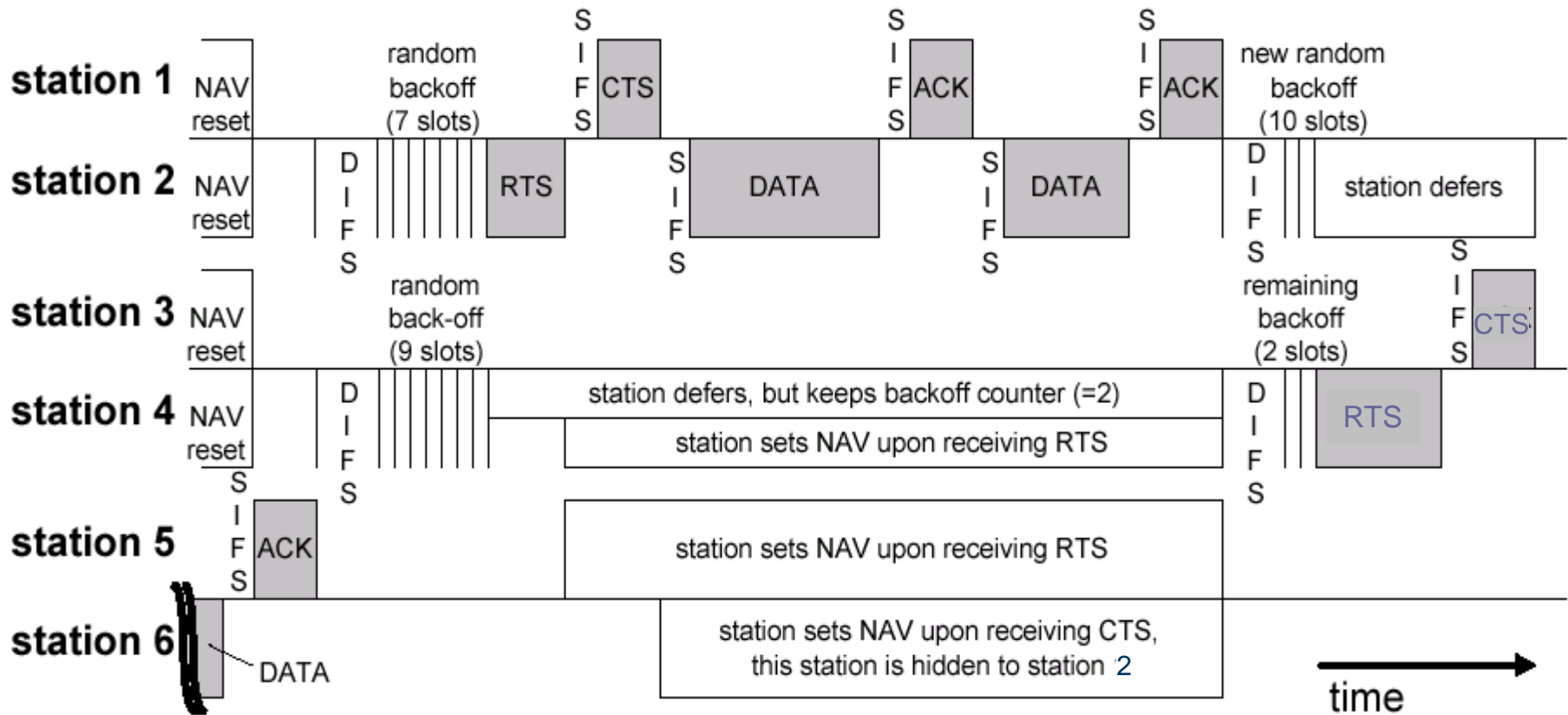
**continued**



➤ 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

# 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:

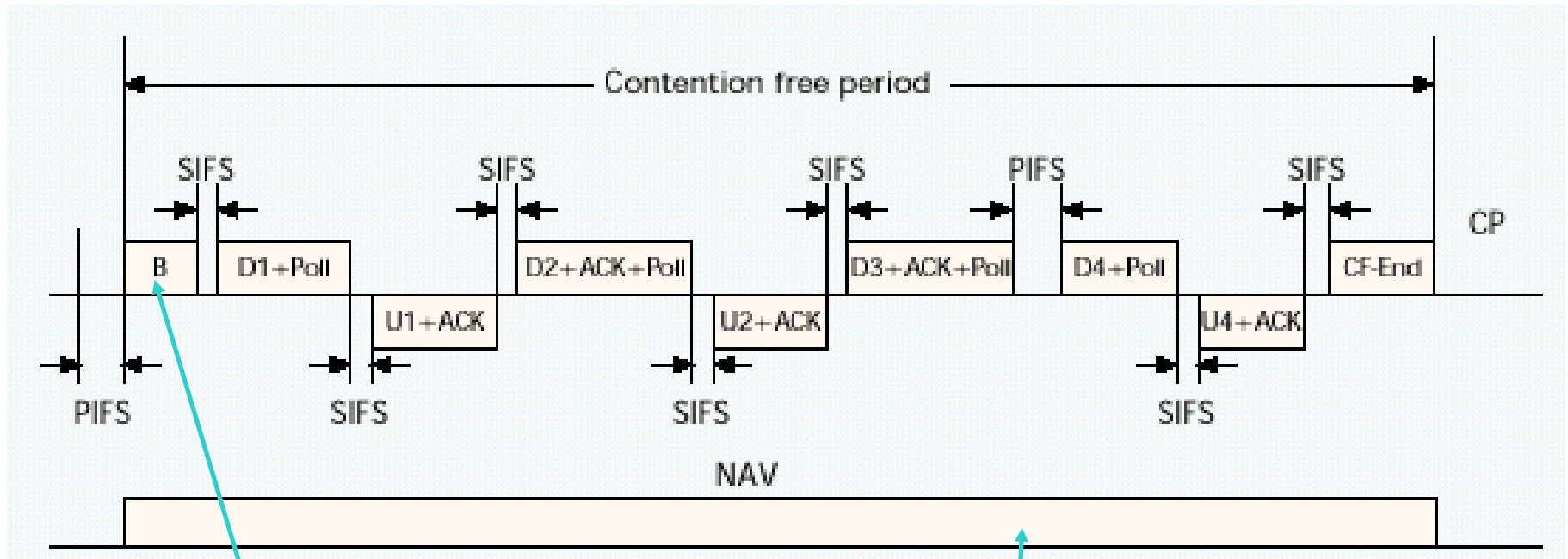
- Χαμηλή καθυστέρηση μετάδοσης και καλή απόδοση σε χαμηλό φόρτο

# 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)

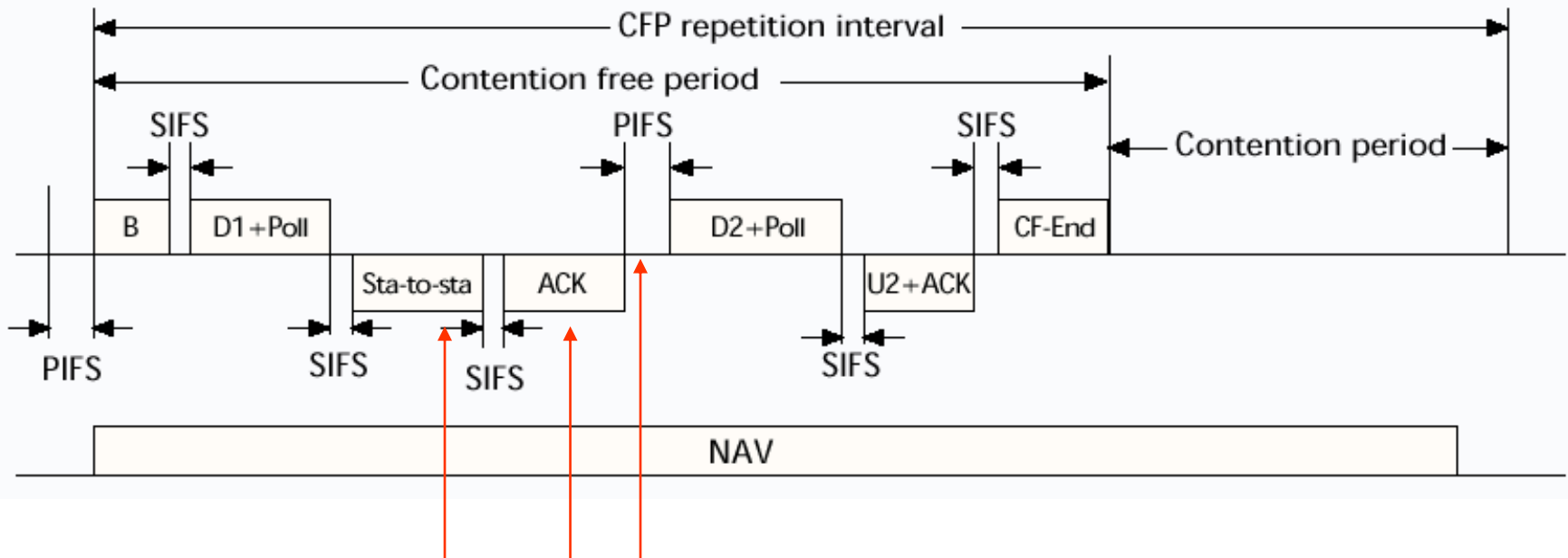


Synchronization beacon

Variable duration of  
Contention Free Period

# Point Coordination Function (III)

If a Station wants to transmit to another station during a CFP (contention-free period)



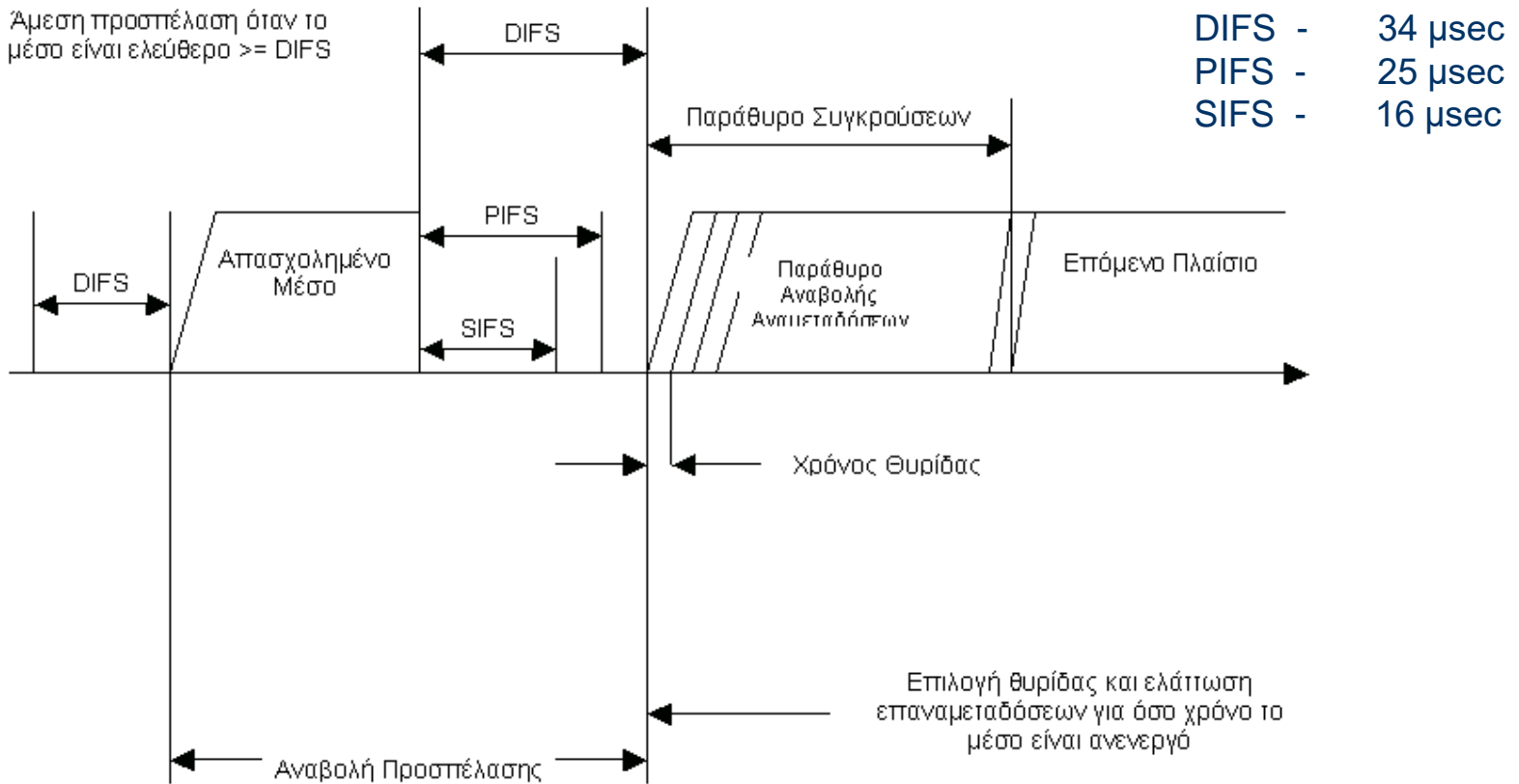
- ◆ When it is time to transmit, a STA chooses to transmit to another STA in the same BSS
- ◆ When the other STA receives data, replies with DCF Ack to the first STA
- ◆ AP waits for time equal to PIFS before continuing to the next STA (why?)

# Βασικά μειονεκτήματα του PCF, όσον αφορά το QoS

- ✓ 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)

# Inter-Frame Spaces



- Inter frame spacing required for MAC protocol traffic
  - SIFS = Short interframe space
  - PIFS = PCF interframe space
  - DIFS = DCF interframe space
- Back-off timer expressed in terms of number of time slots

# 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

# 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-συγχρονηζόμενο» (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”

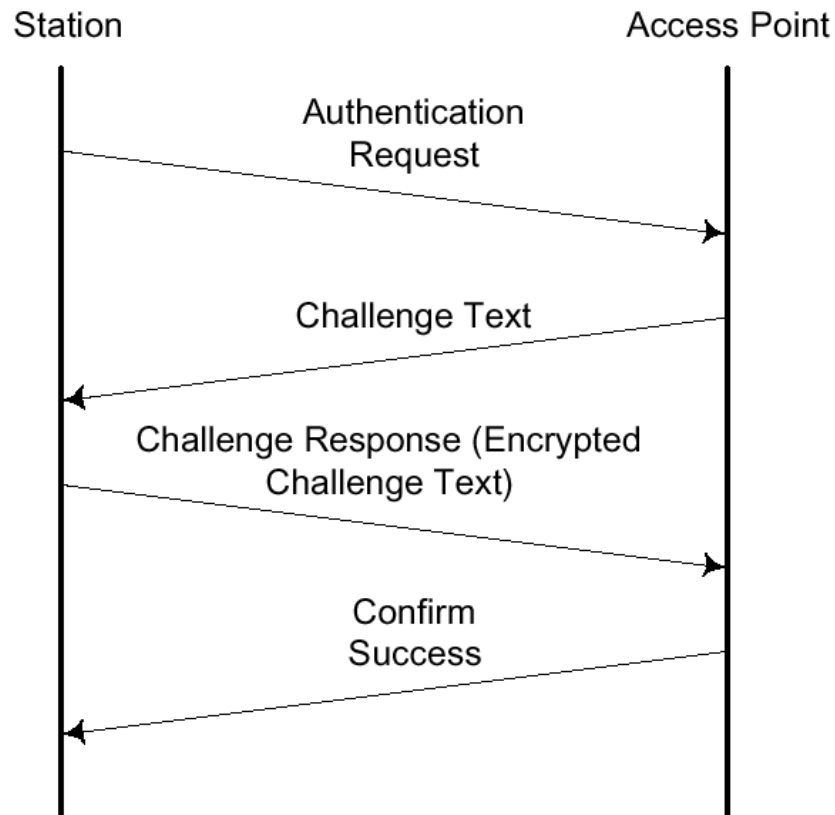
	<b>H</b>	<b>I</b>	
	0 1 0 0 1 0 0 0	0 1 0 0 1 0 0 1	
<b>XOR</b>	0 0 0 0 0 0 1 0	0 0 0 0 0 0 1 0	
	0 1 0 0 1 0 1 0	0 1 0 0 1 0 1 1	<b>Κρυπτογραφημένο κείμενο</b>

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

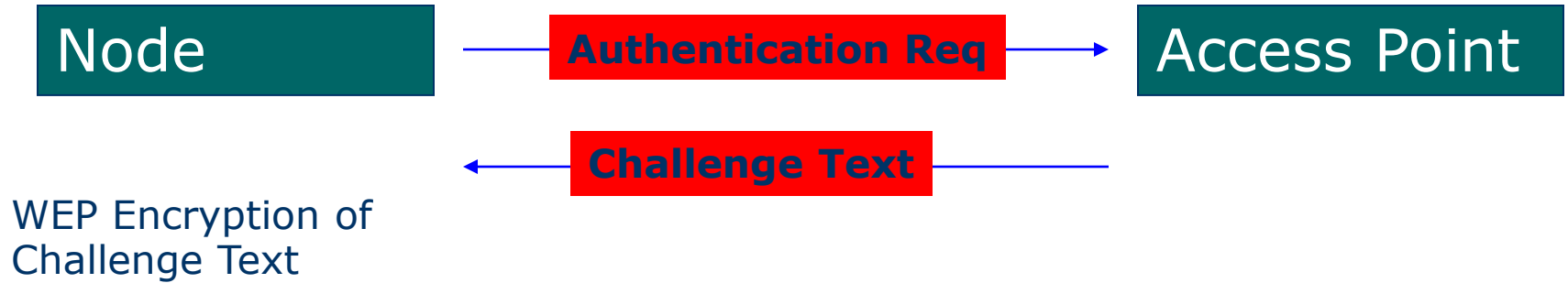
# Shared Key Authentication



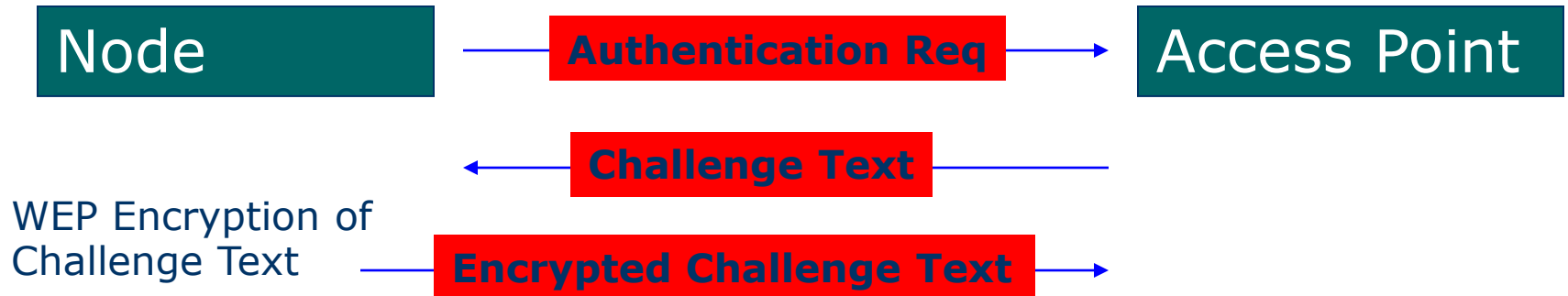
# Shared Key Authentication



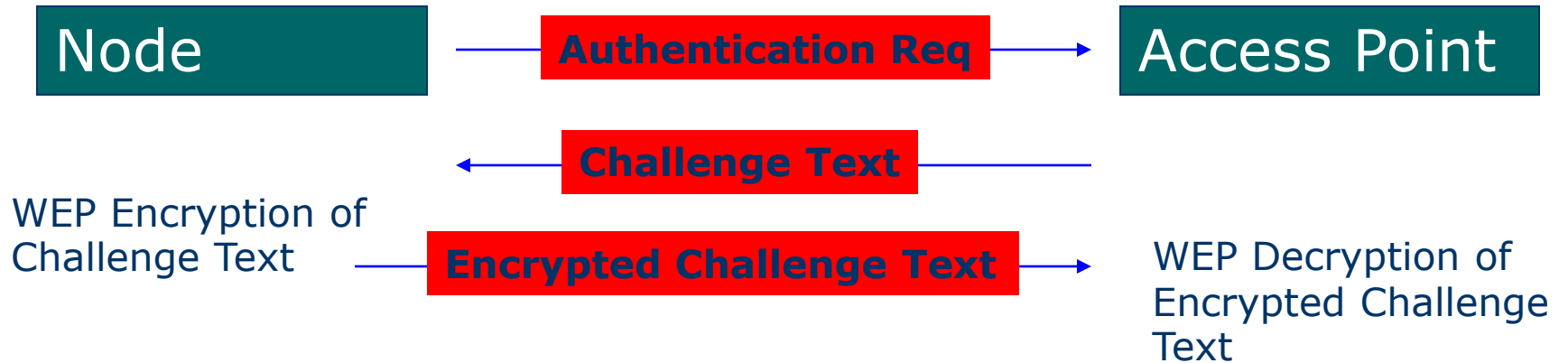
# Shared Key Authentication



# Shared Key Authentication

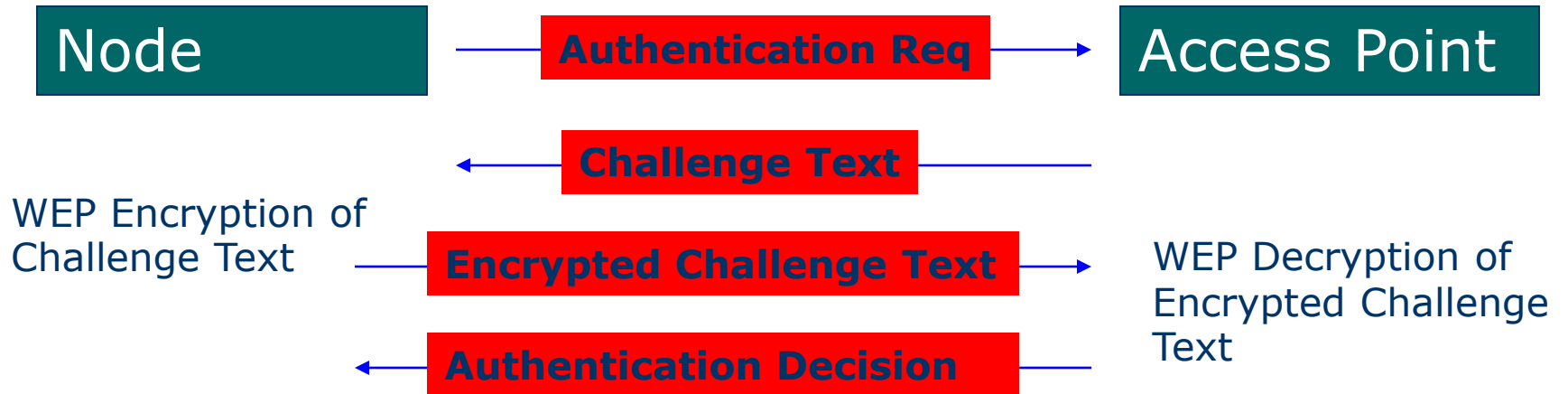


# Shared Key Authentication

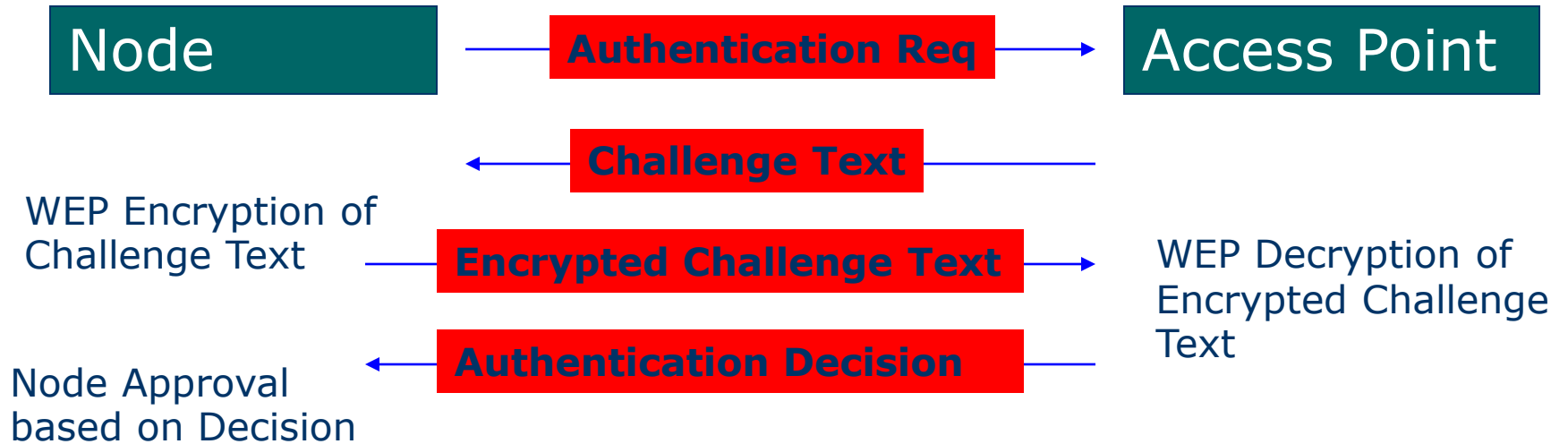




# Shared Key Authentication



# Shared Key Authentication



# WEP's vulnerabilities

- Short and static key : Actual key space is 40 bits or 104 bits.
- No easy way to exchange and distribute keys. Key change involves manually changing the key on each AP and terminal.
- Simple ASCII key strings are used as keys. Easy to crack by hackers.
- Authentication and encryption with the same key
- WEP replaced in 2004 with WiFi Protected Access (WPA) and WPA2

# Κινητικότητα

A STA associated with a BSS

Poor connection quality ?

↓ Yes

Scan the medium

Find a better connection ?

↓ Yes

Reassociation request to new AP

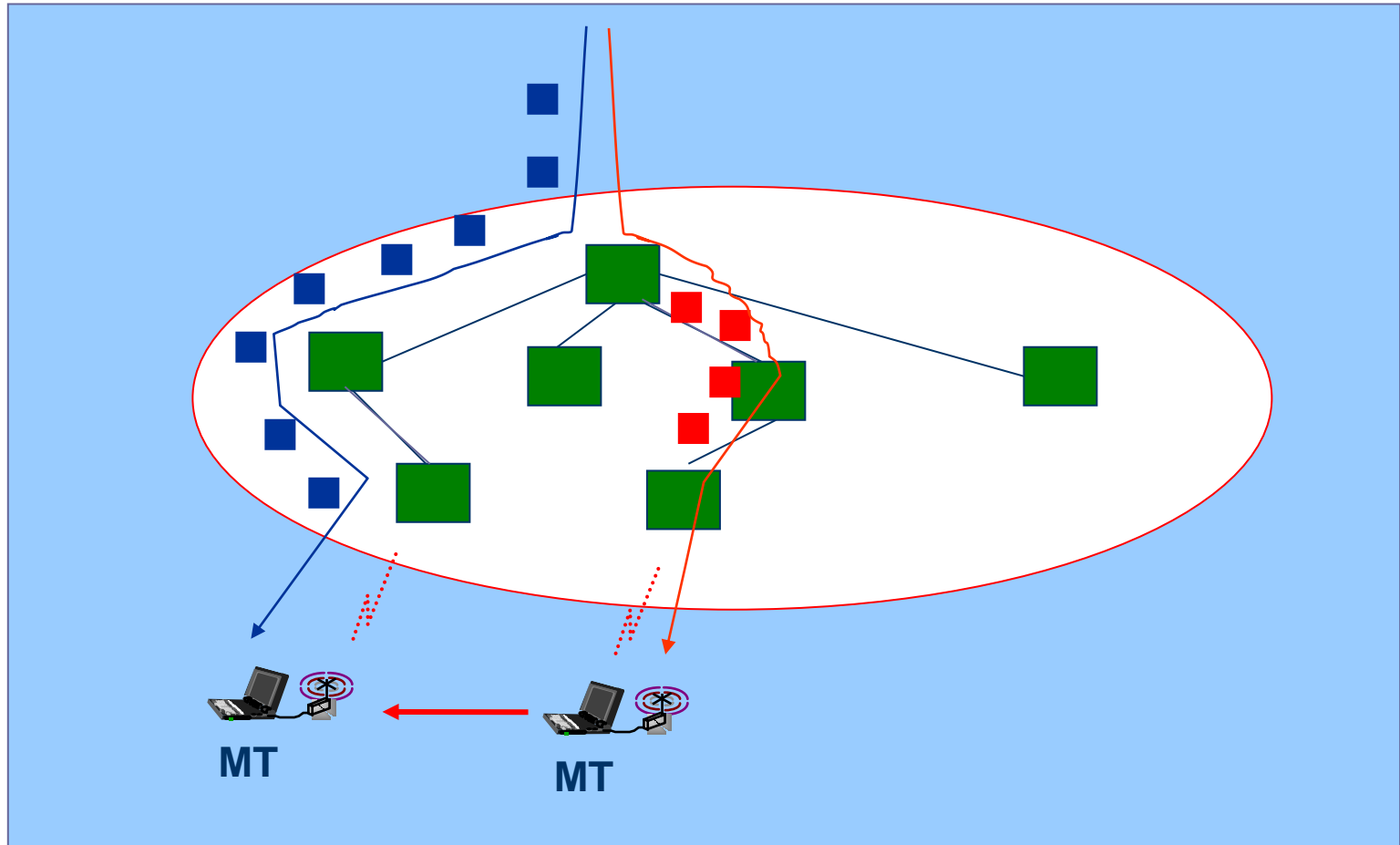
Reassociation response

↓ Yes

STA has roamed to a new AP  
Old AP is notified through DS



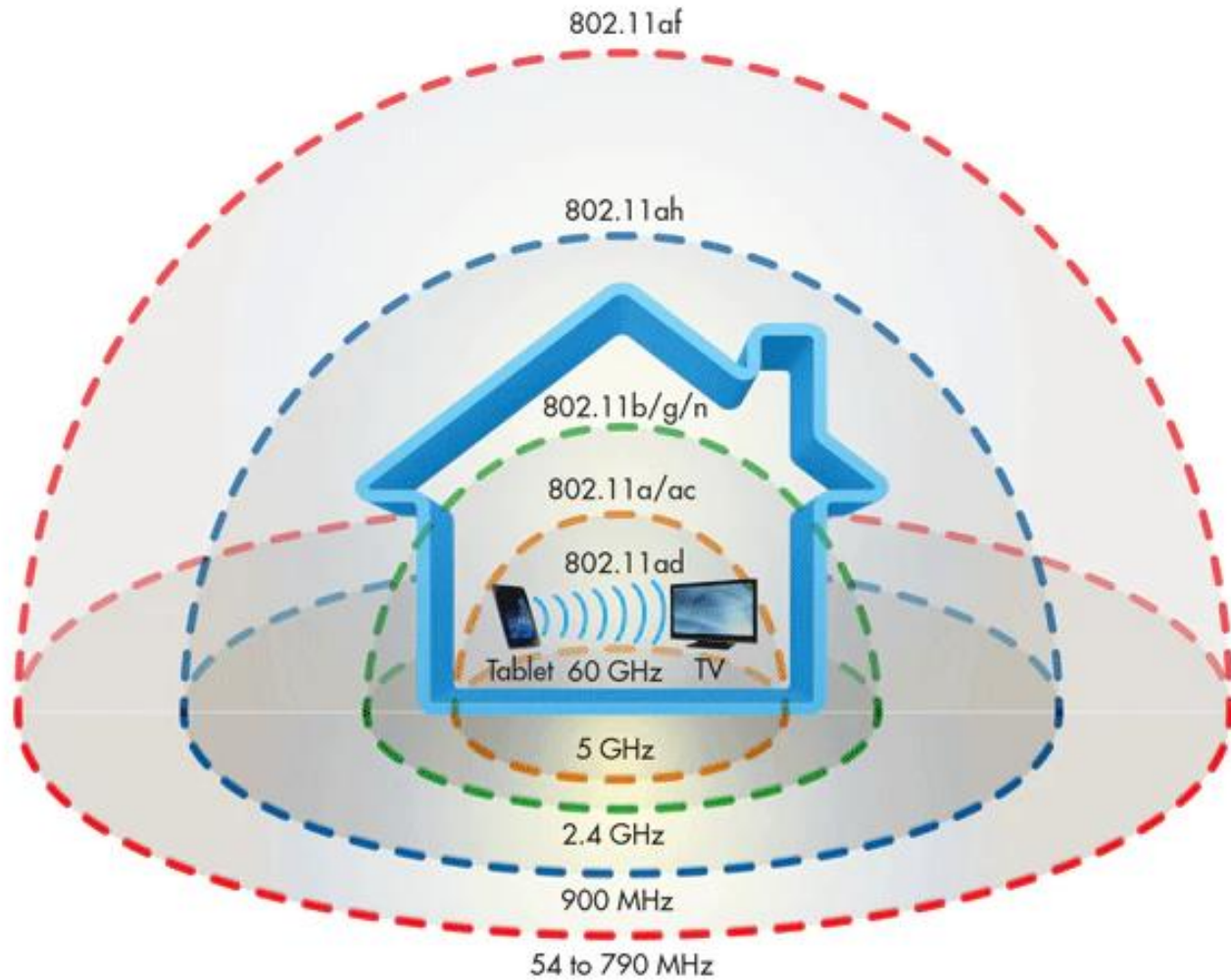
**Καμία ρύθμιση για τα πακέτα που θα χαθούν κατά τη διάρκεια του handover**



# The 802.11 family

Standard	Frequency Band	Bandwidth	Modulation Scheme	Channel Arch.	Maximum Data Rate	Range	Max Transmit Power
802.11	2.4 GHz	20 MHz	BPSK to 256-QAM	DSSS, FHSS	2 Mbps	20 m	100 mW
b	2.4 GHz	21 MHz	BPSK to 256-QAM	CCK, DSSS	11 Mbps	35 m	100 mW
a	5 GHz	22 MHz	BPSK to 256-QAM	OFDM	54 Mbps	35 m	100 mW
g	2.4 GHz	23 MHz	BPSK to 256-QAM	DSSS, OFDM	54 Mbps	70 m	100 mW
n	2.4 GHz, 5 GHz	24 MHz and 40 MHz	BPSK to 256-QAM	OFDM	600 Mbps	70 m	100 mW
ac	5 GHz	20, 40, 80, 80+80=160 MHz	BPSK to 256-QAM	OFDM	6.93 Gbps	35 m	160 mW
ad	60 GHz	2.16 GHz	BPSK to 64-QAM	SC, OFDM	6.76 Gbps	10 m	10 mW
af	54-790 MHz	6, 7, and 8 MHz	BPSK to 256-QAM	SC, OFDM	26.7 Mbps	>1km ?	100 mW
ah	900 MHz	1, 2, 4, 8, and 16 MHz	BPSK to 256-QAM	SC, OFDM	40 Mbps	1 km	100 mW

# The 802.11 family



## Wi-Fi generations

	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7 (expected)
<b>Launch date</b>	2007	2013	2019	2021	2024
<b>IEEE standard</b>	802.11n	802.11ac	802.11ax		802.11be
<b>Max data rate</b>	1.2 Gbps	3.5 Gbps	9.6 Gbps		46 Gbps
<b>Bands</b>	2.4 GHz and 5 GHz	5 GHz	2.4 GHz and 5 GHz	6 GHz	1–7.25 GHz (including 2.4 GHz, 5 GHz, 6 GHz bands)
<b>Security</b>	WPA 2	WPA 2	WPA 3		WPA3
<b>Channel size</b>	20, 40 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz	Up to 320 MHz
<b>Modulation</b>	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDMA		4096-QAM OFDMA (with extensions)
<b>MIMO</b>	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 UL/DL MU-MIMO		16x16 MU-MIMO

Source: IEEE, Intel Corporation, Wi-Fi Alliance

	x 11.5		x 1.3		x 4.8	
	<b>Wi-Fi 4</b>	<b>Wi-Fi 5</b>	<b>Wi-Fi 6/6E</b>	<b>Wi-Fi 7</b>		
<b>Standard</b>	802.11n	802.11ac	802.11ax	802.11be		
<b>Max Speed with 1 Spatial Stream</b>	150 Mbps	866.7 Mbps	1.2 Gbps	2.9 Gbps		
<b>Max Speed with 2 Spatial Streams</b>	300 Mbps	1.73 Gbps	2.5 Gbps	5.8 Gbps		
<b>Max Speed with Max # Spatial Streams</b>	600 Mbps	6.92 Gbps	9.6 Gbps	46.4 Gbps		



**IEEE 802.11e**  
**Εξασφάλιση Ποιότητας**  
**Υπηρεσίας στα Ασύρματα**  
**Τοπικά Δίκτυα**

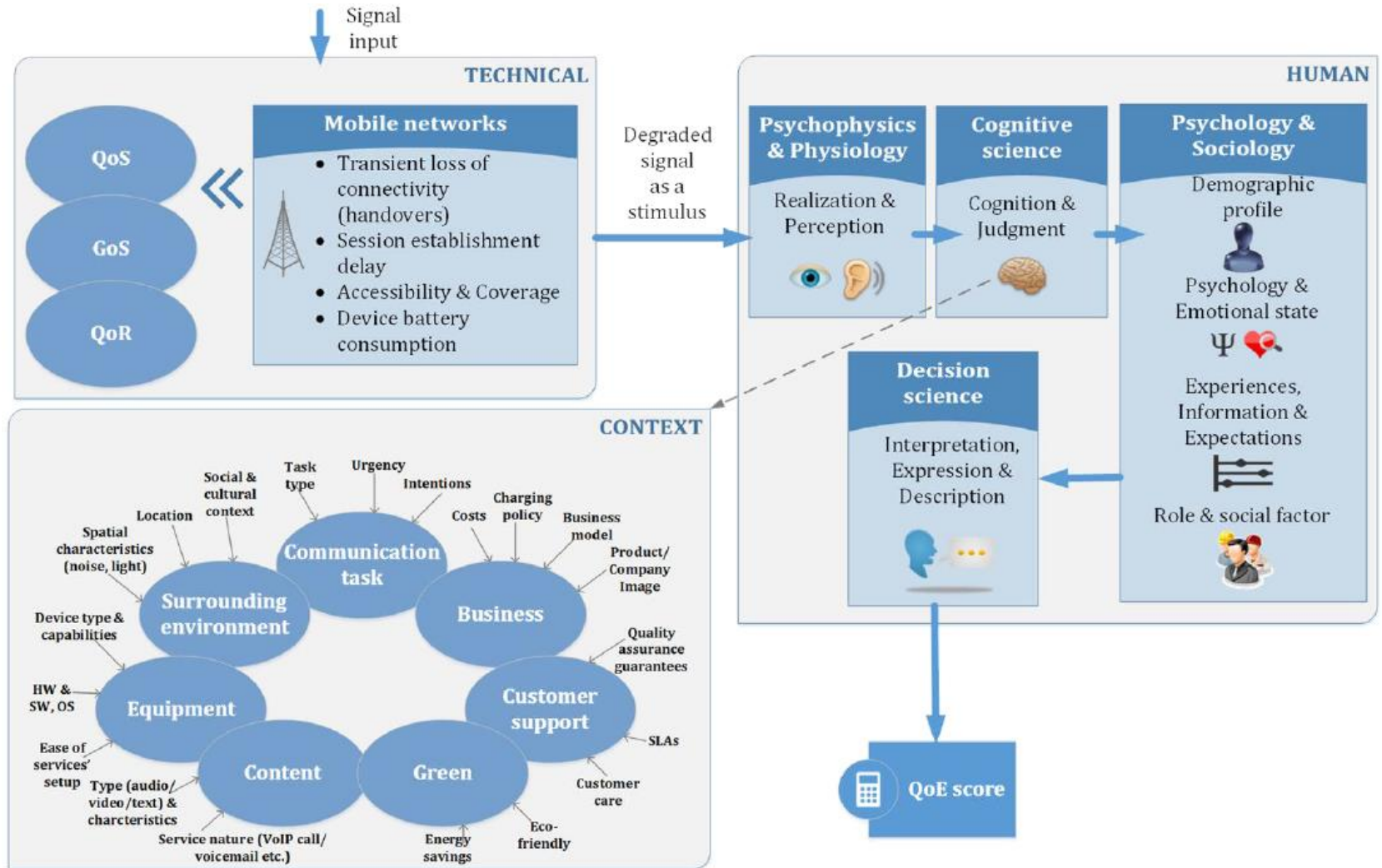
# Τι σημαίνει εξασφάλιση ποιότητας υπηρεσίας

- Ποιότητα Υπηρεσίας (Quality of Service – QoS): Η «αποδοτική» μετάδοση πληροφορίας που έχει σαν αποτέλεσμα την «ικανοποιητική» λειτουργία μιας δικτυακής εφαρμογής έτσι όπως την αντιλαμβάνεται ο χρήστης
- Τι σημαίνει «ικανοποιητική» λειτουργία; Είναι συχνά υποκειμενική και εξαρτάται από τις προτιμήσεις του χρήστη, αλλά και τις συγκεκριμένες ανάγκες του
- Τι σημαίνει «αποδοτική» μετάδοση; Είναι η μετάδοση της κίνησης που ικανοποιεί συγκεκριμένα χαρακτηριστικά (παραμέτρους ποιότητας υπηρεσίας), τα οποία εξάγονται με βάση την «ικανοποιητική» λειτουργία της δικτυακής εφαρμογής
- Τυπικές παράμετροι ποιότητας υπηρεσίας:
  - μέση καθυστέρηση από άκρο σε άκρο (mean delay),
  - μέγιστη καθυστέρηση από άκρο σε άκρο (maximum delay)
  - μέγιστη επιτρεπτή διαφορά στην καθυστέρηση (delay jitter)
  - μέσος ρυθμός απώλειας πακέτων (mean packet error rate)

# Τι σημαίνει εξασφάλιση ποιότητας υπηρεσίας

- Ανάλογα με το είδος της κίνησης και τις ανάγκες ή προτιμήσεις του χρήστη προκύπτουν οι συγκεκριμένες παράμετροι ποιότητας υπηρεσίας (QoS parameters)
- Οι εφαρμογές **πραγματικού χρόνου** (φωνή, βίντεο) έχουν απαίτηση για **μικρή μέση και μέγιστη καθυστέρηση** (100-200msec end-to-end), αλλά έχουν κάποια **ανοχή σε απώλειες πακέτων** (π.χ.,  $10^{-3}$ )
- Οι εφαρμογές **μη πραγματικού χρόνου** (email, file transfer) έχουν απαίτηση για **απολύτως σωστά δεδομένα** (ρυθμός απώλειας πακέτων ουσιαστικά μηδέν), αλλά έχουν **μεγάλη ανοχή στην καθυστέρηση** (π.χ., αρκετά δευτερόλεπτα).
- Οι τιμές των παραμέτρων «διαμοιράζονται» από τα ανώτερα επίπεδα σε τιμές ανά ζεύξη (link)
- Στόχος κάθε πρωτοκόλλου στο επίπεδο-2 (Data-Link) είναι να εξασφαλίζει τις τιμές των παραμέτρων αυτών για τη ζεύξη που αυτό ελέγχει.
- Άρα και το MAC πρωτόκολλο του 802.11 θα πρέπει να εξασφαλίζει τις τιμές των παραμέτρων ποιότητας υπηρεσίας στη ραδιο-επαφή, οι οποίες έχουν προκύψει από τα ανώτερα επίπεδα

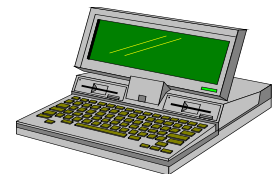
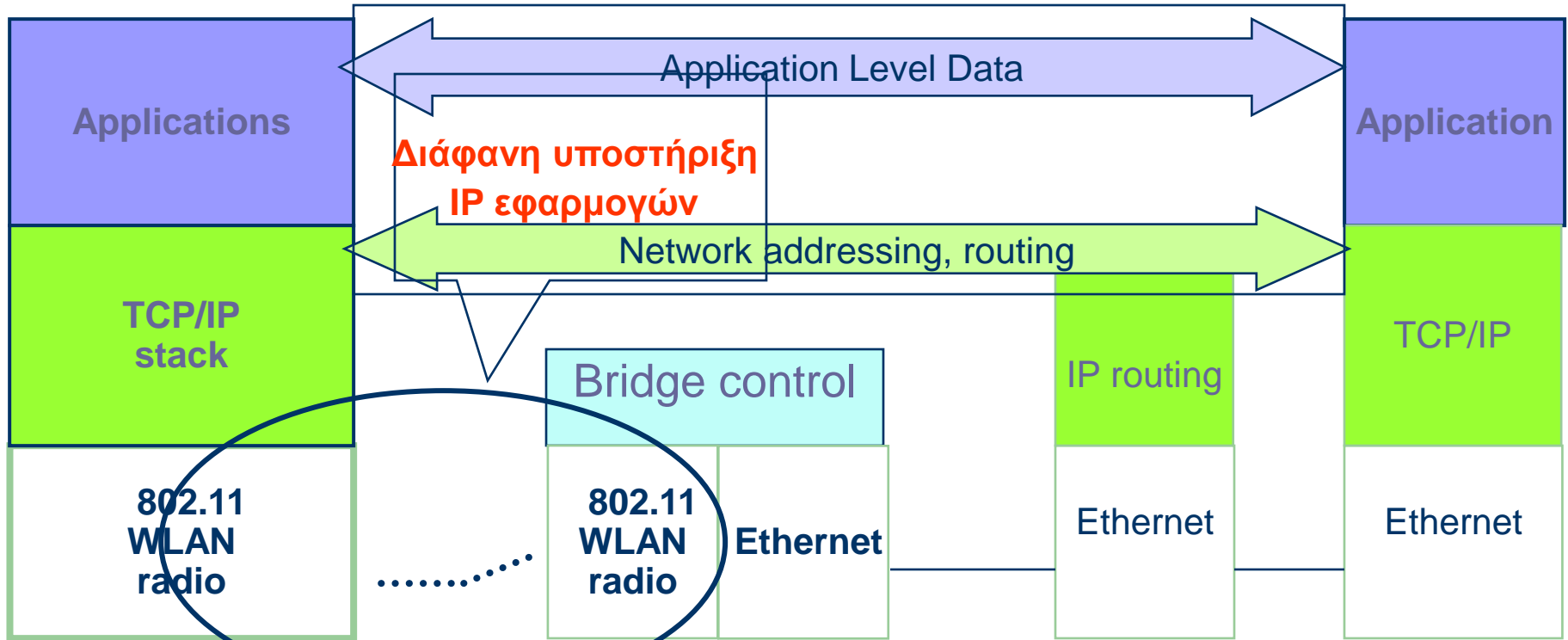
# Ποιότητα εμπειρίας - QoE



# Ποιότητα εμπειρίας - QoE

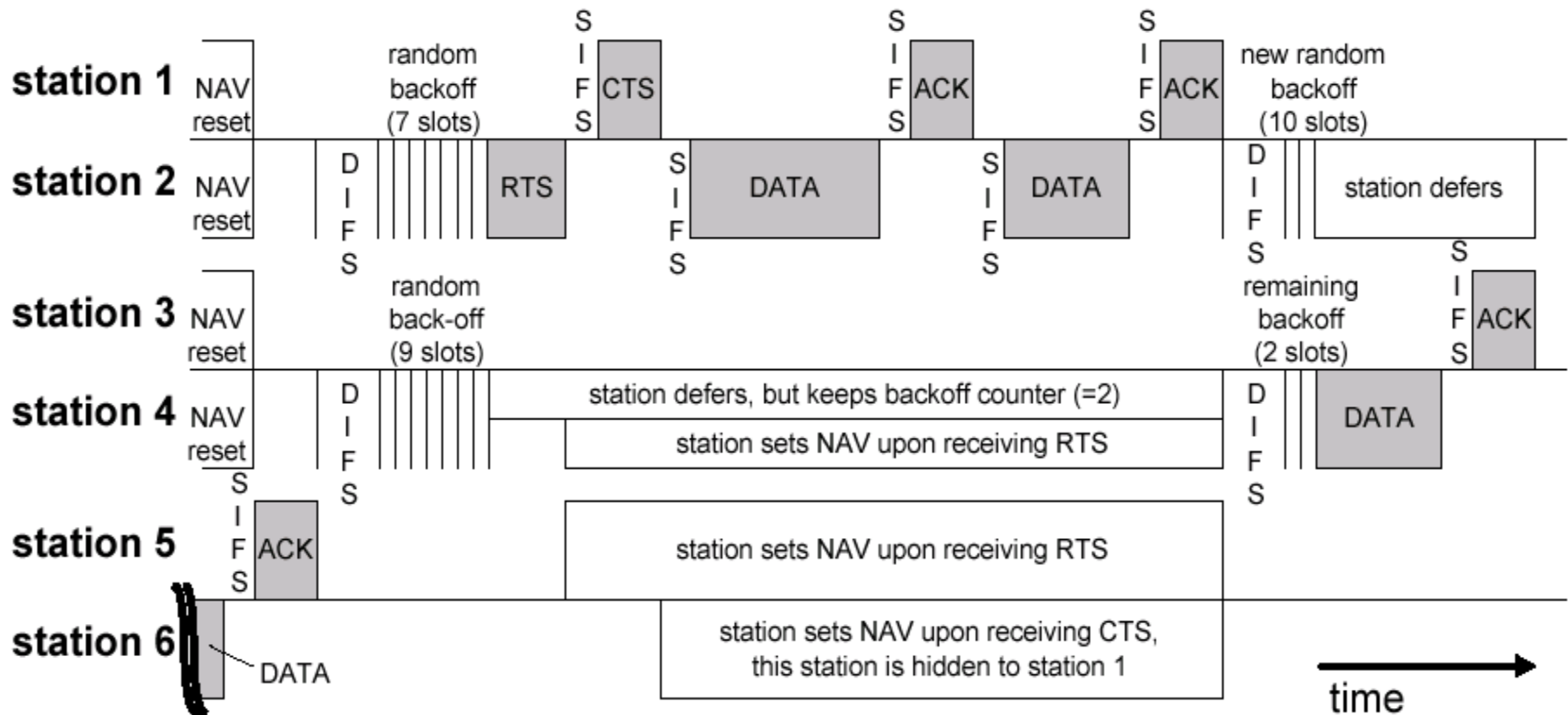
Aspect	Quality Influence Factors	
<b>Mobile networks</b>	Vertical and horizontal handovers Battery consumption Session establishment delay	Accessibility Coverage
<b>Service</b>	Call setup success ratio Blocking probability Call setup time	Call cut-off ratio Availability & Reliability
<b>Transport / Network</b>	Round trip / one-way delay Jitter Packet loss ratio Delay burstiness distribution	Loss burstiness distribution Bottleneck bandwidth Congestion period
<b>Physical</b>	SNR / SIR / SINR Bit rate BLER Outage probability Packet / Symbol / Bit Error Probability Outage capacity	Ergodic capacity / rate Throughput Diversity order / coding gain Area spectral efficiency Energy efficiency

# Εξασφάλιση Ποιότητας Υπηρεσίας σε κάθε ζεύξη



# Περιορισμοί του 802.11 σε QoS

- Το DCF βασίζεται στον ανταγωνισμό και γι' αυτό το λόγο δεν παρέχει διαφοροποίηση της κίνησης και εγγυημένες καθυστερήσεις ή απώλειες πακέτων.





# Περιορισμοί του 802.11 σε QoS

- Στο PCF δεν υπάρχει γνώση των απαιτήσεων των τερματικών ώστε το κανάλι να δίνεται στα πιο επείγοντα.
- Στο PCF είναι άγνωστη η περίοδος μετάδοσης ενός τερματικού στο οποίο δίνεται η άδεια μετάδοσης (polling).

