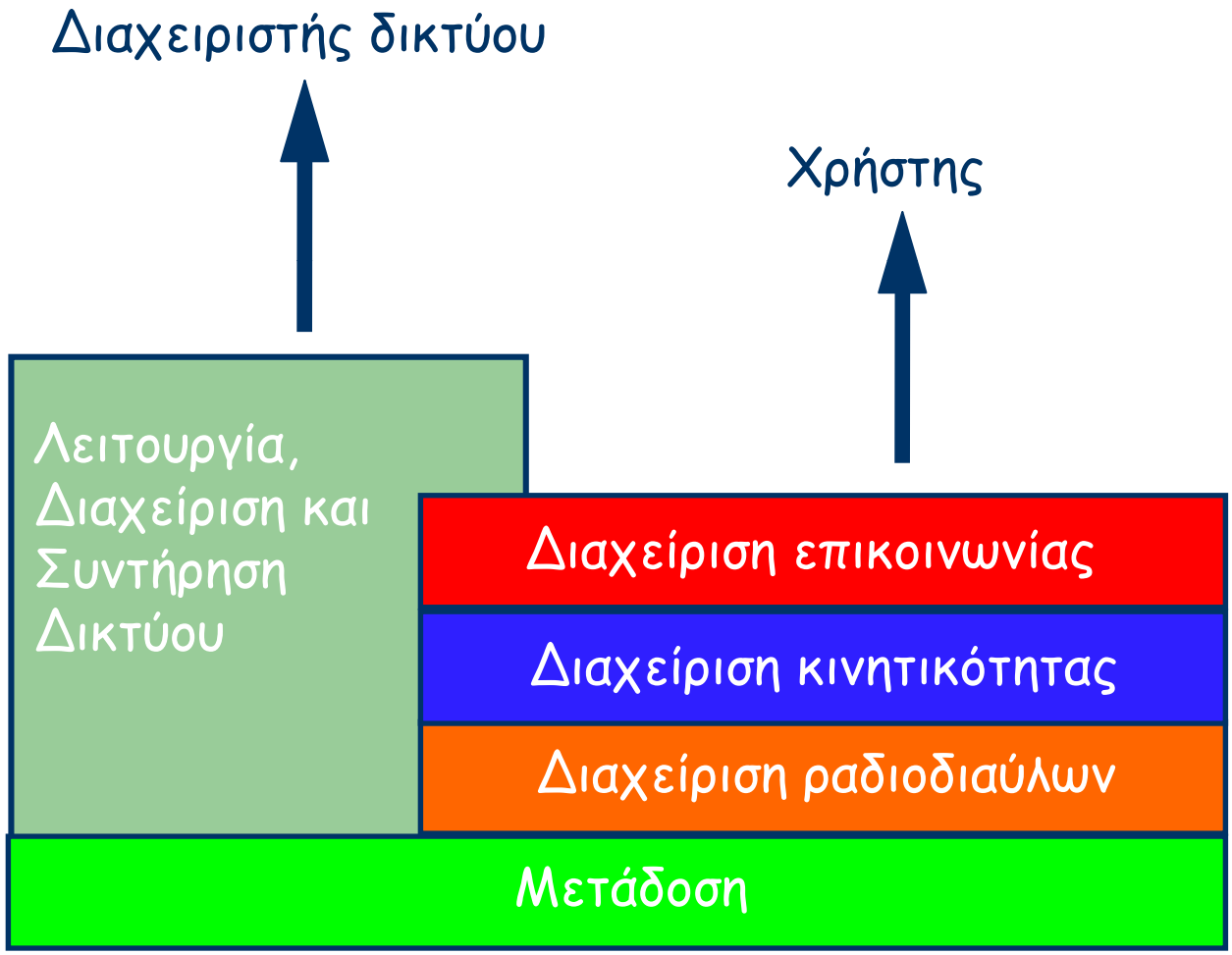
Δίκτυα Κινητών και Προσωπικών Επικοινωνιών

Διαχείριση κινητικότητας

Περίληψη

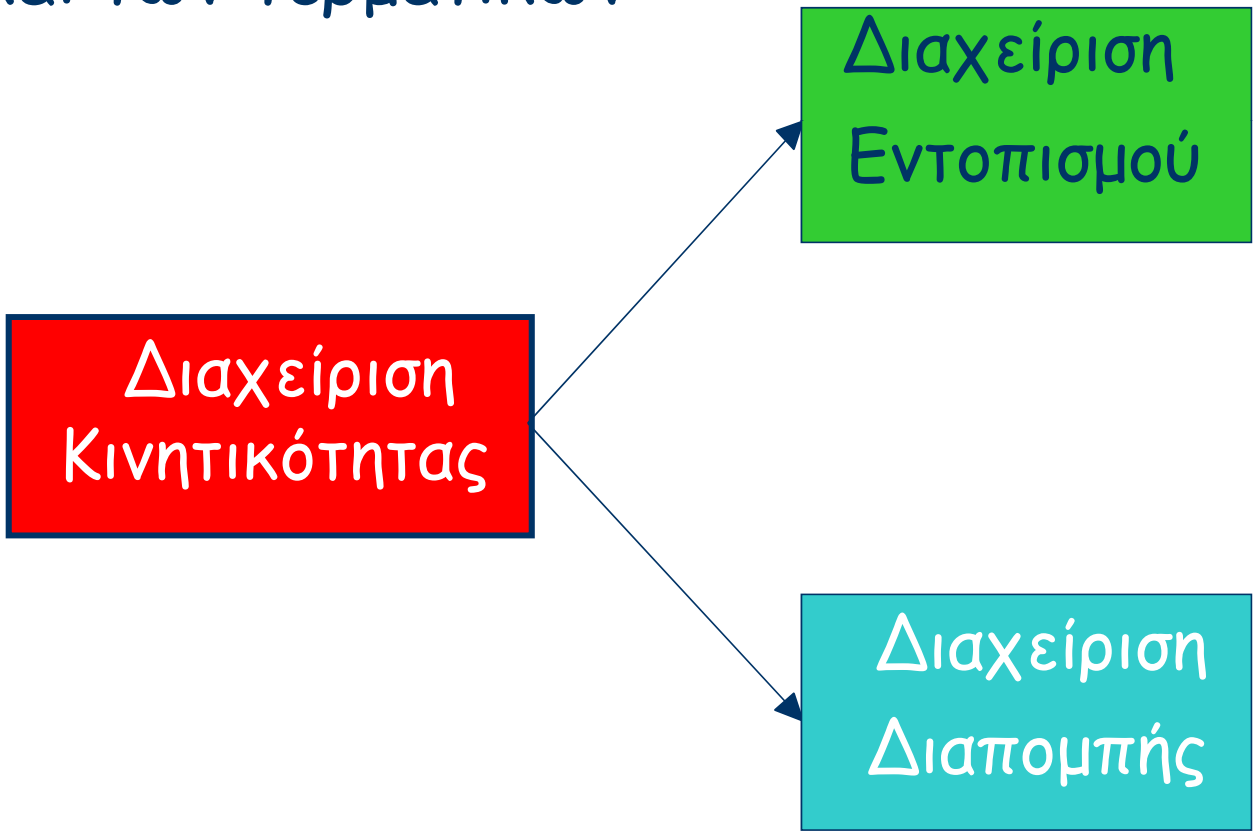
- Διαχείριση εντοπισμού
  - Ενημέρωση θέσης
  - Παράδοση κλήσης
- Ενημέρωση θέσης και εντοπισμός δεδομένων
  - Κεντρικές βάσεις δεδομένων
  - Κατανεμημένες βάσεις δεδομένων
- Ενημέρωση θέσης και Αναζήτηση
  - Δυναμικές μέθοδοι ενημέρωσης θέσης
  - Μέθοδοι αναζήτησης
- Διαχείριση εντοπισμού στο UMTS
- Διαχείριση ασφάλειας στο GSM

Μοντέλο αναφοράς



Διαχείριση κινητικότητας

Λειτουργίες και διαδικασίες που έχουν σχέση με την κίνηση των χρηστών και των τερματικών



Διαχείριση κινητικότητας

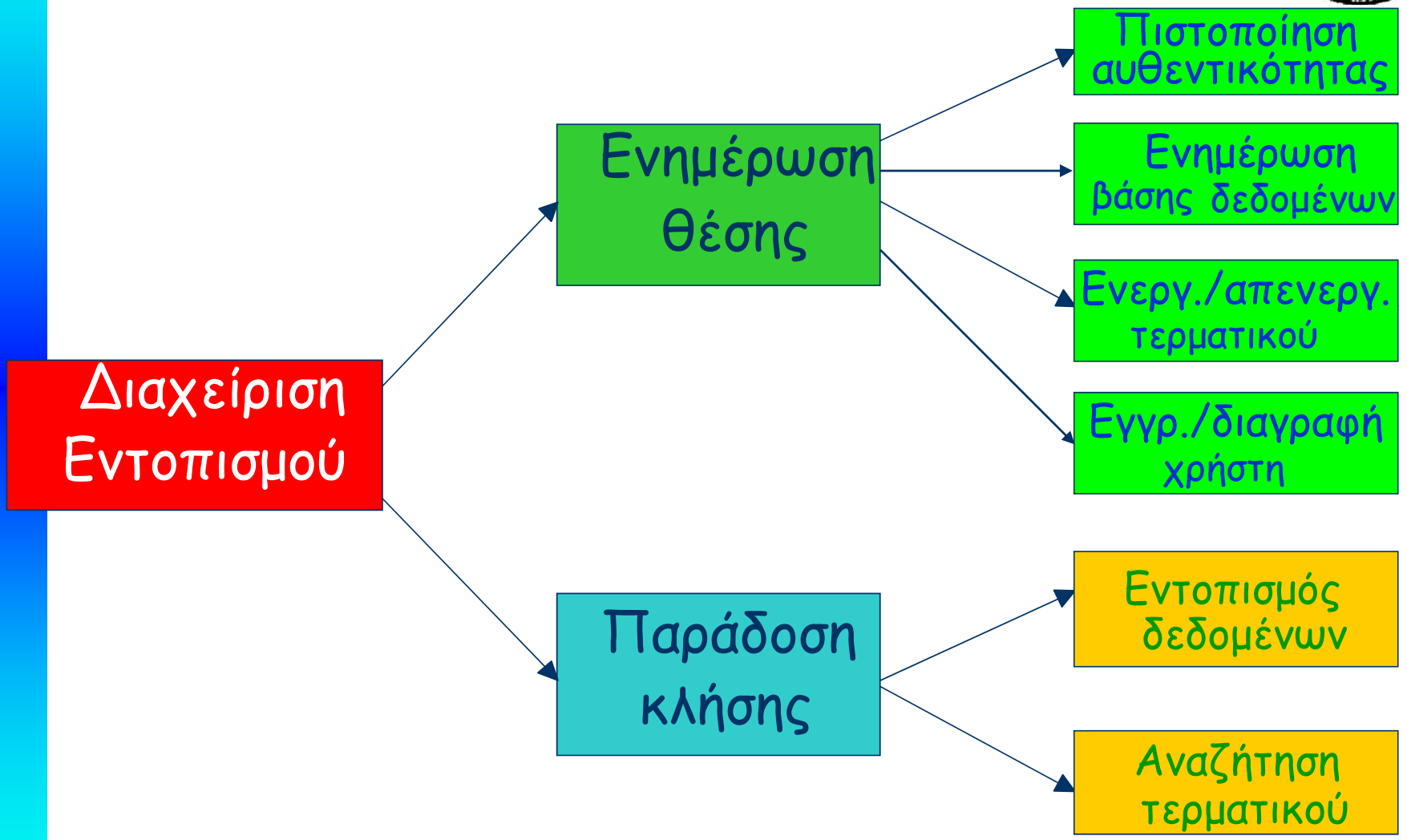
- Περιλαμβάνει το σύνολο των διαδικασιών που αφορούν:
  - την ενημέρωση του δικτύου για τη θέση και την κατάσταση των κινητών τερματικών (χρηστών)
  - τον προσδιορισμό της θέσης του καλούμενου για προώθηση της εισερχόμενης κλήσης
  - τη διαδικασία της διαπομπής

Διαχείριση εντοπισμού

Η διαχείριση εντοπισμού έχει δύο όψεις:

1) πώς ο κινούμενος χρήστης ή το κινούμενο τερματικό αντιμετωπίζει την αλλαγή περιβάλλοντος (της θέσης του)
2) πώς η υποδομή του συστήματος διαχειρίζεται τα δεδομένα που αφορούν τη θέση των τερματικών (χρηστών), ώστε να καθιστά δυνατή την εγκατάσταση κλήσεων προς κινούμενα τερματικά (χρήστες).

Διαχείριση εντοπισμού



Διαχείριση εντοπισμού

Διαδικασία ενημέρωσης θέσης

- Οι λειτουργίες που απαρτίζουν τη διαδικασία ενημέρωσης θέσης δεν σχετίζονται με τις κλήσεις.
- Έχουν ως σκοπό να ενημερώνουν το δίκτυο για:
  - τη θέση των τερματικών που βρίσκονται σε λειτουργία
  - την παρούσα κατάσταση των τερματικών
  - την κατάσταση εγγραφής των χρηστών

Διαχείριση εντοπισμού

Διαδικασία παράδοσης της κλήσης

- Οι λειτουργίες που απαρτίζουν τη διαδικασία παράδοσης της κλήσης ενεργοποιούνται μόνο όταν υπάρχει εισερχόμενη κλήση για κινητό τερματικό
  - εντοπισμός δεδομένων
  - αναζήτηση τερματικού

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

- Οι τρέχουσες τεχνικές βασίζονται σε ιεραρχική βάση δεδομένων δύο επιπέδων
- Οι πληροφορίες που αφορούν χρήστες (τερματικά) αποθηκεύονται σε δύο τύπους καταχωρητών
  - καταχωρητής θέσης οικείων (Home Location Register, HLR)
  - καταχωρητής θέσης επισκεπτών (Visitors Location Register, VLR)

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

- Η *στατική* (μόνιμη) πληροφορία του HLR είναι:
  - ο αριθμός κλήσης του κινητού συνδρομητή (*Mobile Subscriber Number, MSN)*
  - η διεθνής ταυτότητα του συνδρομητή (*International Mobile Subscriber Identity, IMSI*)
  - το κλειδί ελέγχου αυθεντικότητας
  - οι πληροφορίες για τις βασικές και συμπληρωματικές υπηρεσίες (profile)

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

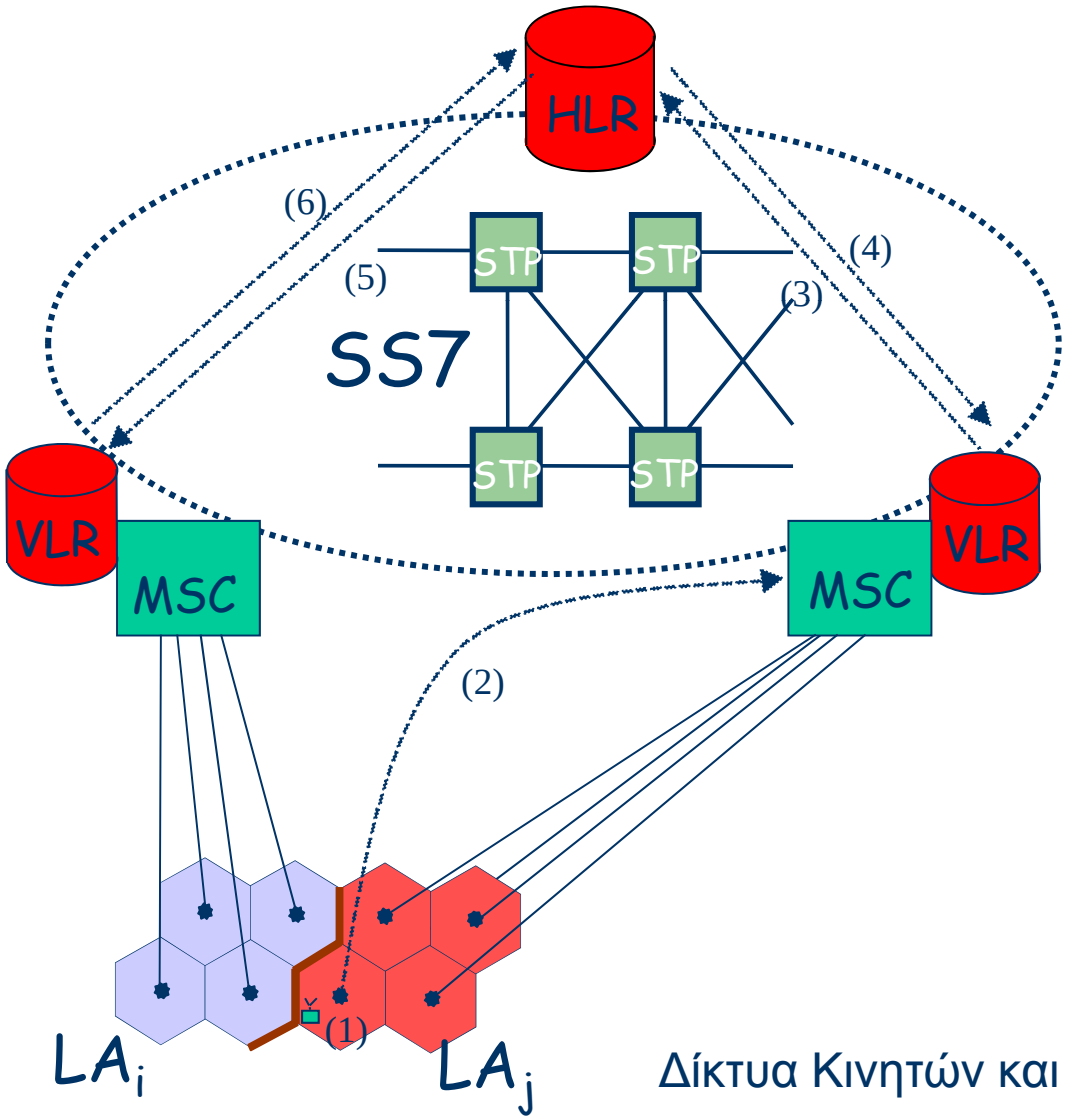
- Η *δυναμική* πληροφορία του HLR περιλαμβάνει:
  - τις παραμέτρους ελέγχου αυθεντικότητας και κρυπτογράφησης
  - τον αριθμό περιαγωγής κινητού σταθμού (*Mobile Station Roaming Number, MSRN*), ή
  - τη διεύθυνση του VLR ή αντίστοιχα την ταυτότητα της LA
  - την κατάσταση του κινητού τερματικού
  - προσωρινές πληροφορίες σχετικές με τις υπηρεσίες που χρησιμοποιεί

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

- Ο VLR περιέχει στατική και δυναμική πληροφορία ανάλογη με εκείνη του HLR
- περιέχει επιπλέον και την προσωρινή ταυτότητα κινητού συνδρομητή (*Temporary Mobile Subscriber Identity, TMSI*)

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία ενημέρωσης θέσης



Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

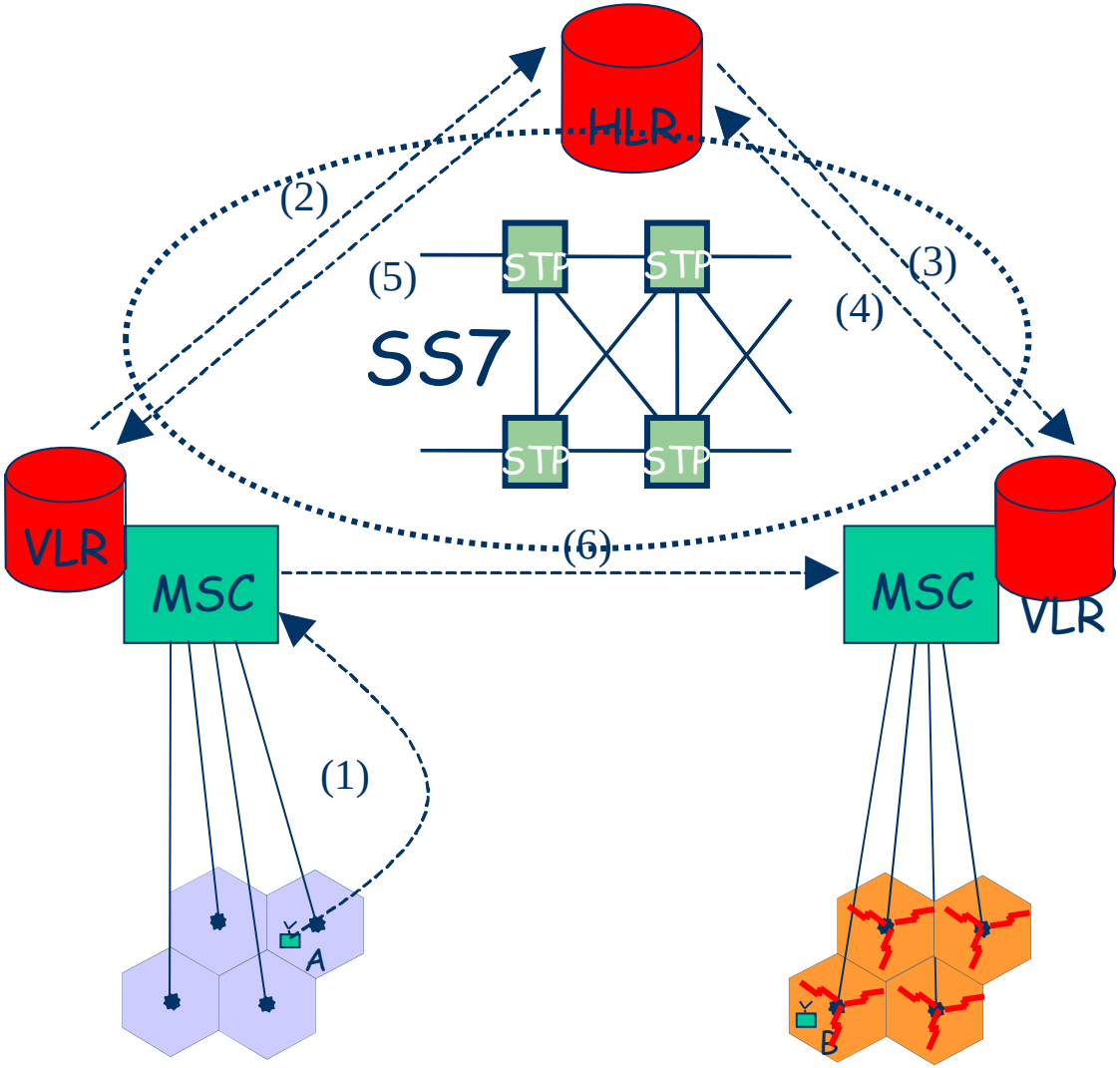
Διαδικασία παράδοσης της κλήσης

- Διακρίνουμε δύο κυρίως βήματα:

1) προσδιορισμός του VLR που εξυπηρετεί το καλούμενο κινητό τερματικό (interrogation)
2) εντοπισμός της τρέχουσας κυψέλης στην οποία περιφέρεται το καλούμενο κινητό τερματικό (paging).

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία παράδοσης της κλήσης



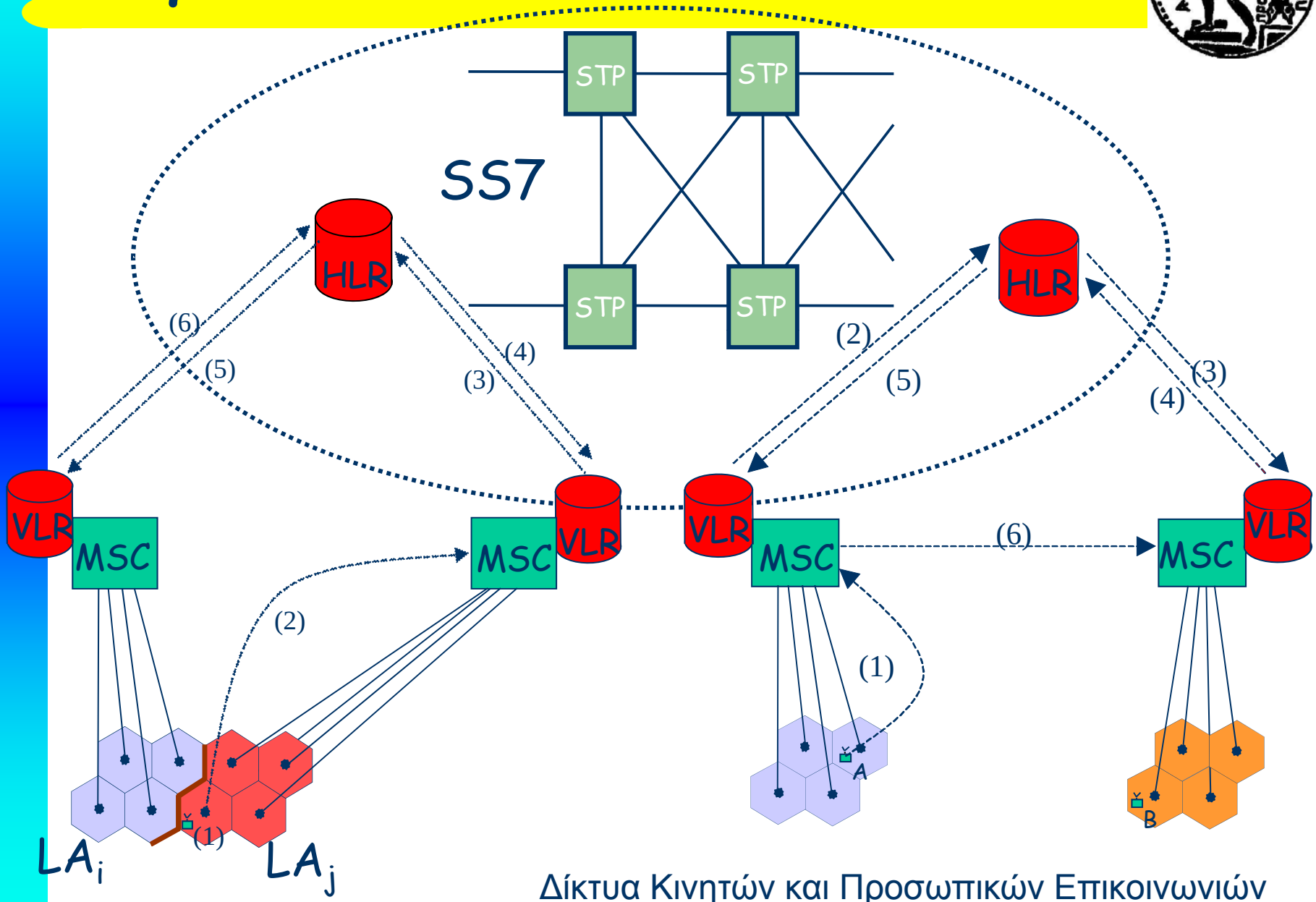
Δίκτυα Κινητών και Προσωπικών Επικοινωνιών

Διαχείριση εντοπισμού στα επίγεια δίκτυα κινητών επικοινωνιών

Διαδικασία παράδοσης της κλήσης

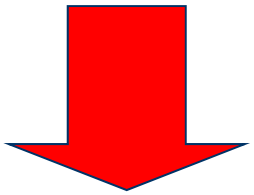
- Ο σχεδιασμός των LA (σχήμα, θέση, διάταξη) όσο και η στρατηγική αναζήτησης στην LA είναι μεγάλης σημασίας
  - καθορίζουν τις απαιτήσεις σε σηματοδοσία (διαδικασία ενημέρωσης θέσης, αναζήτηση)
  - επηρεάζουν σημαντικά τον ρυθμό προσβάσεων στη βάση δεδομένων (διαδικασία ενημέρωσης θέσης)
- Ο εντοπισμός δεδομένων και η αναζήτηση είναι συμπληρωματικές διαδικασίες.

Ενημέρωση Θέσης και εντοπισμός δεδομένων



Ενημέρωση Θέσης και εντοπισμός δεδομένων

- Οι διαδικασίες αυτές μπορεί να έχουν μεγάλο κόστος όταν το MT βρίσκεται μακριά από τον HLR
- Όσο αυξάνει ο αριθμός των χρηστών, το φορτίο σηματοδοσίας που οφείλεται στη διαδικασία εντοπισμού δεδομένων είναι υπερβολικά μεγάλο



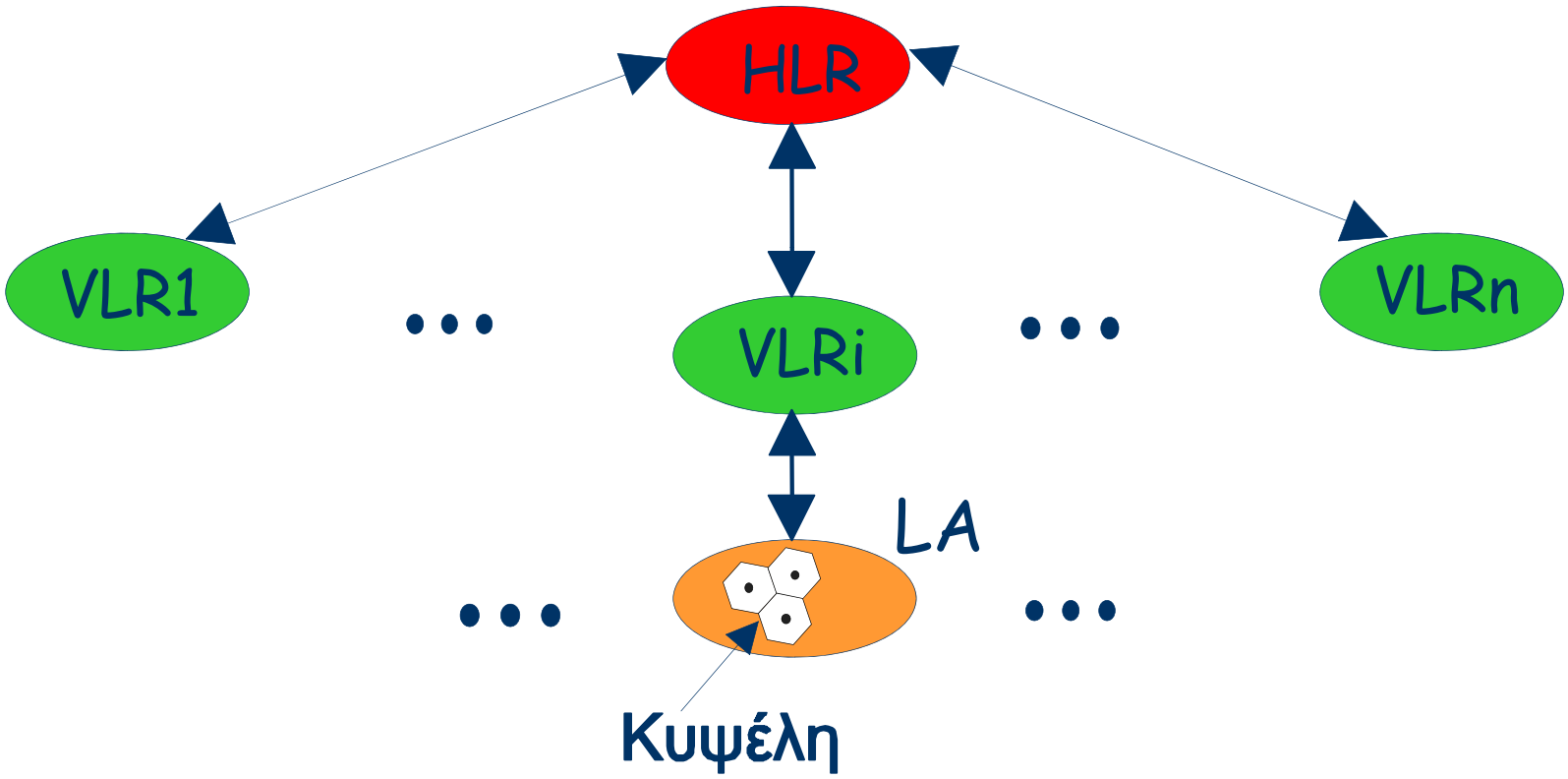
Αναζήτηση μεθόδων για τον περιορισμό του φορτίου σηματοδοσίας για τον εντοπισμό των δεδομένων

Ενημέρωση Θέσης και εντοπισμός δεδομένων

Η έρευνα στην περιοχή αυτή μπορεί γενικά να χωριστεί σε δύο κατηγορίες:

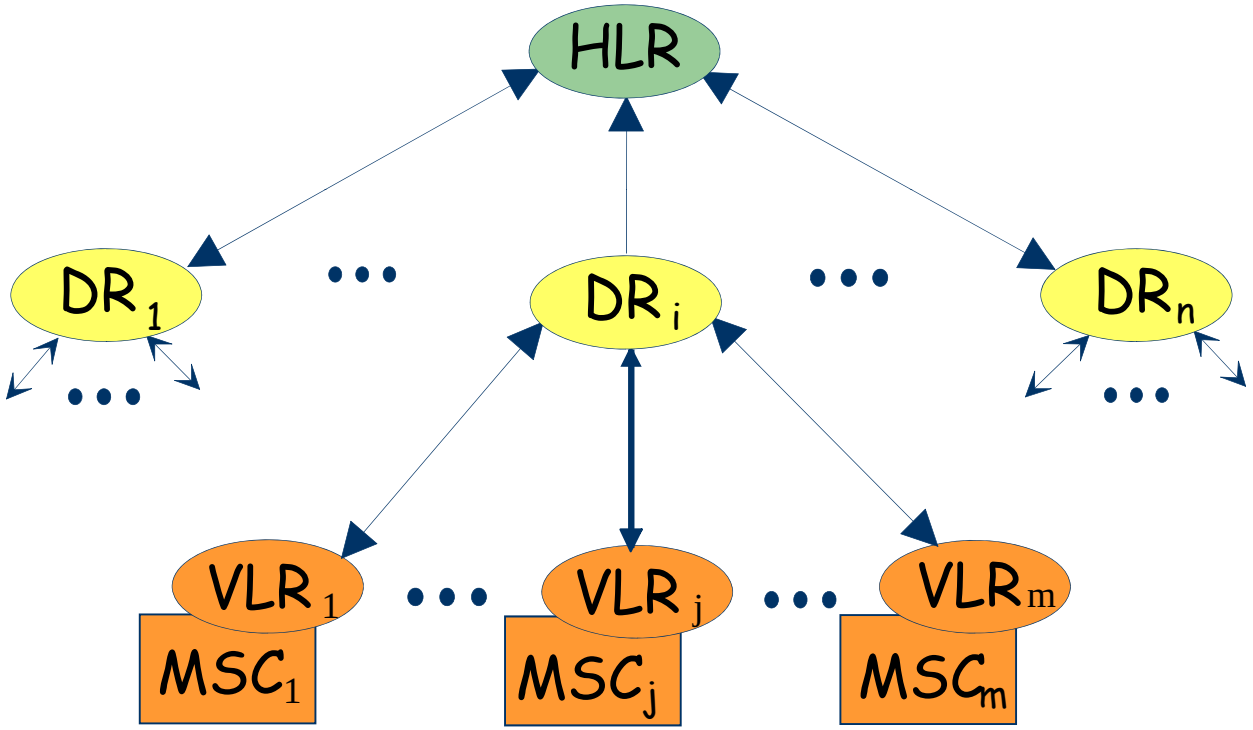
1) επεκτάσεις της στρατηγικής εντοπισμού δεδομένων που εφαρμόζεται στα συστήματα δεύτερης γενιάς
2) εντελώς νέες αρχιτεκτονικές, οι οποίες απαιτούν νέα σχήματα για τις διαδικασίες ενημέρωσης θέσης και παράδοσης κλήσης

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων



Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

Καταχωρητές καταλόγου



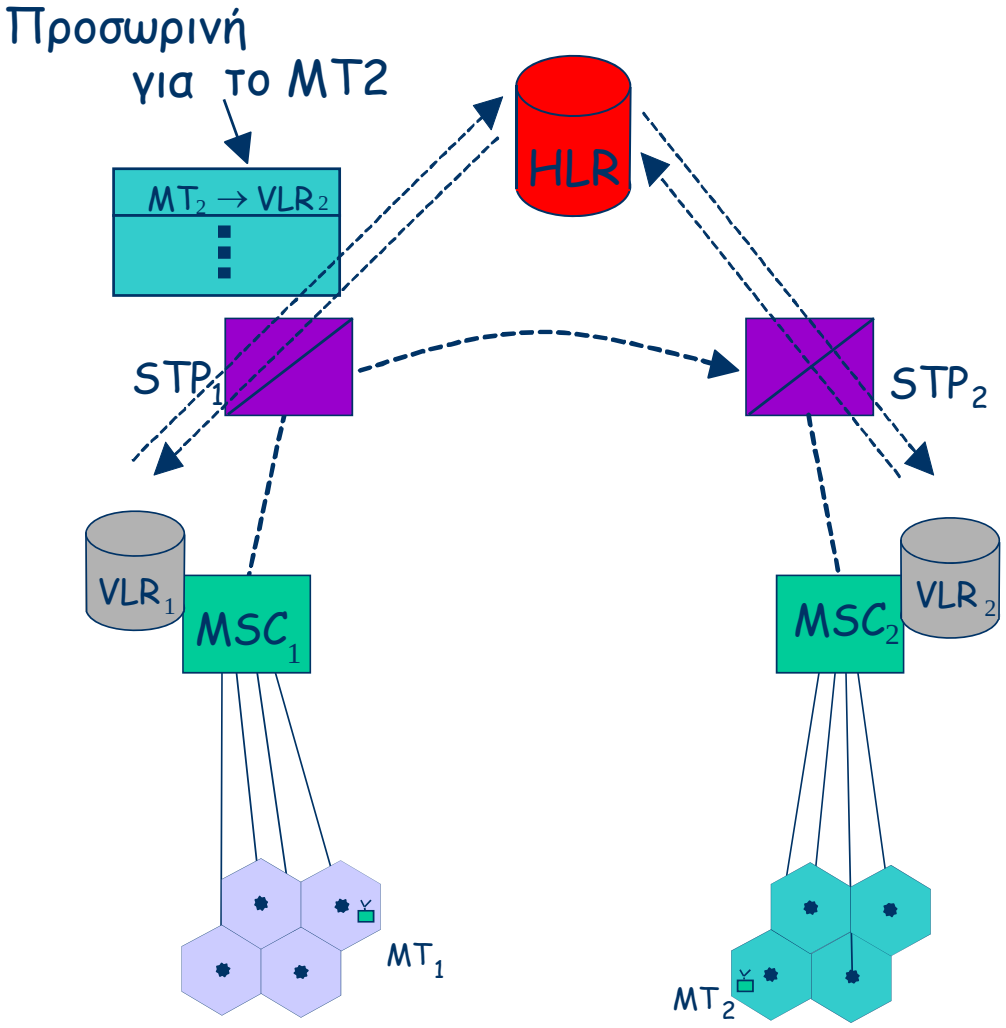
Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

- Προσθήκη νέου ιεραρχικού επιπέδου με καταχωρητές καταλόγου (DR), που ο καθένας τους καλύπτει μερικά MSC (VLR)
- Ο DR υπολογίζει και αποθηκεύει μια μορφή δείκτη θέσης για κάθε τερματικό που εξυπηρετεί
  - Τοπικός δείκτης (DR→MSC)
  - Άμεσος απόμακρος δείκτης (DR→MSC)
  - Έμμεσος απόμακρος δείκτης (DR→DR)
- Ο HLR μπορεί να τροποποιηθεί, ώστε να φυλάσσει έναν δείκτη είτε προς τον τρέχοντα DR είτε προς το τρέχον MSC

Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

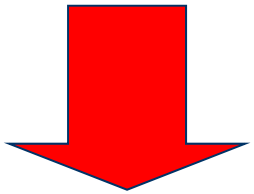
Προσωρινή αποθήκευση της θέσης του MT

- Διατήρηση προσωρινής πληροφορίας θέσης του MT στο πλησιέστερο STP
- Προσπαθούμε να αποφύγουμε την ερώτηση προς τον HLR, όποτε είναι δυνατό



Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

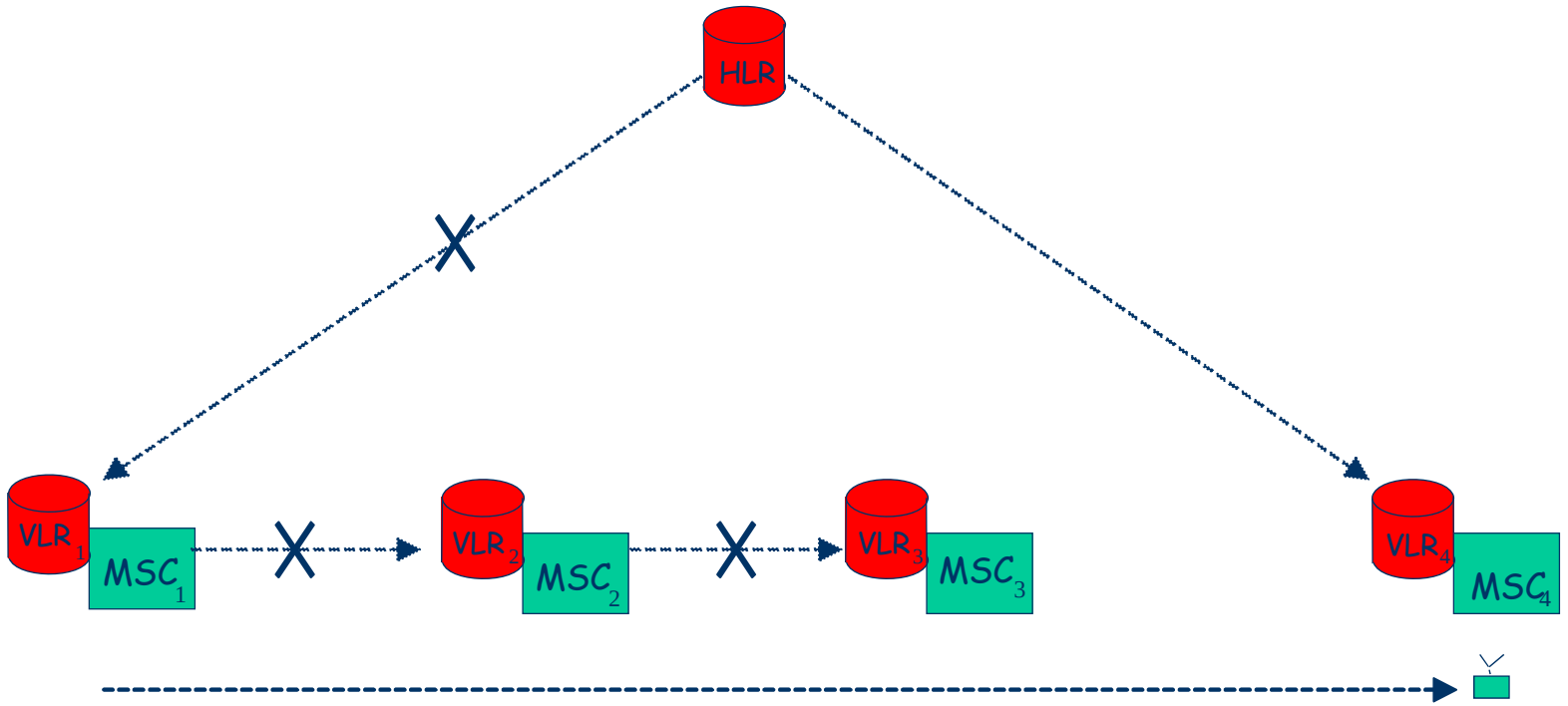
- Επανάληψη του προφίλ του χρήστη σε επιλεγμένες τοπικές βάσεις δεδομένων
- Ελέγχεται πρώτα αν υπάρχει διαθέσιμο τοπικό αντίγραφο, αν όχι ερωτάται ο HLR
- Σε μετακίνηση του MT ενημερώνονται όλα τα αντίγραφα



- Μεγαλύτερη σηματοδοσία ενημέρωσης θέσης
- Μέθοδος καθορισμού επανάληψης προφίλ

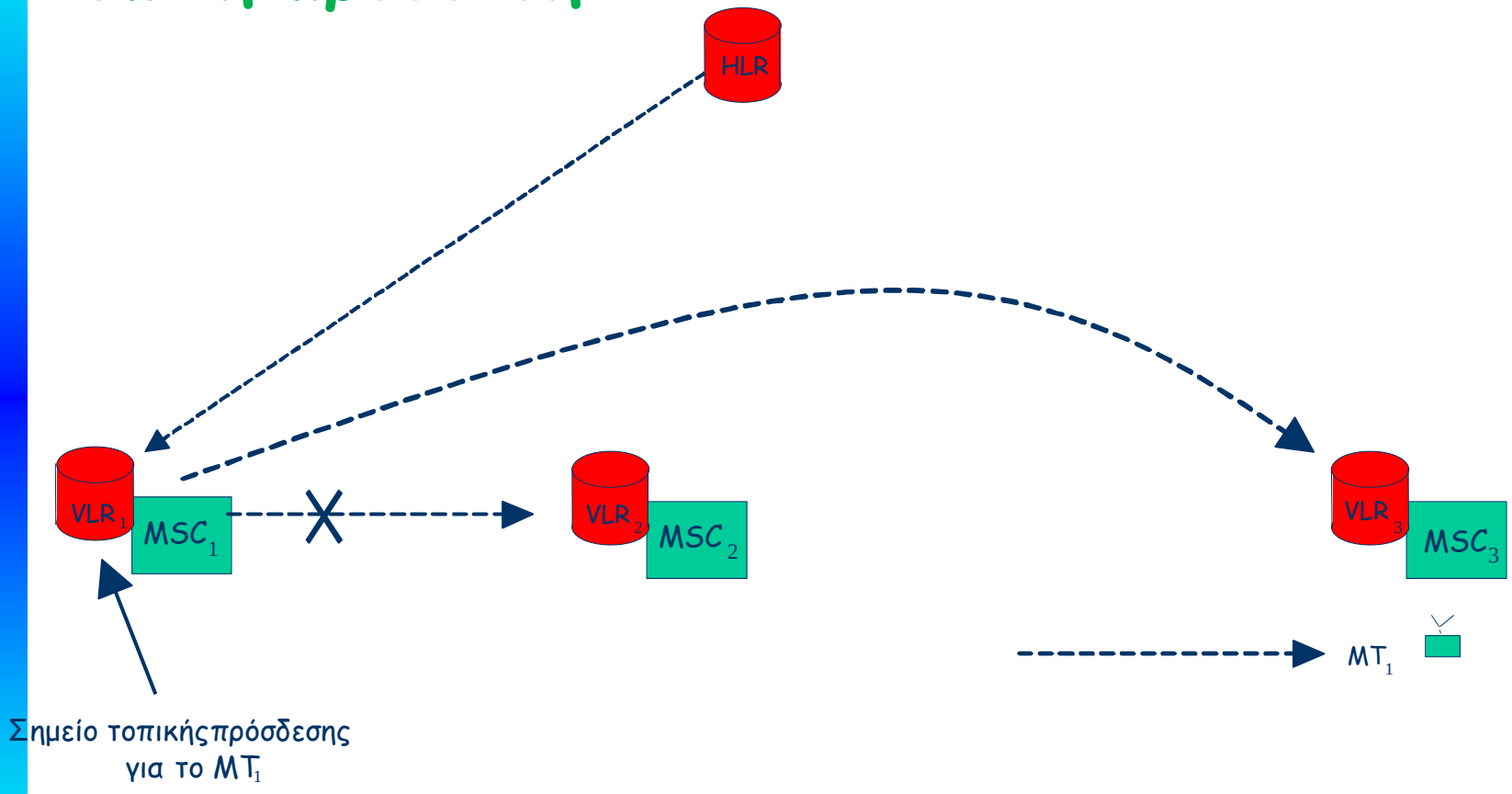
Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

Προώθηση του δείκτη για αναζήτηση δεδομένων



Αρχιτεκτονικές κεντρικών βάσεων δεδομένων

Τοπική πρόσδεση



Στατικό και δυναμικό σημείο πρόσδεσης

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

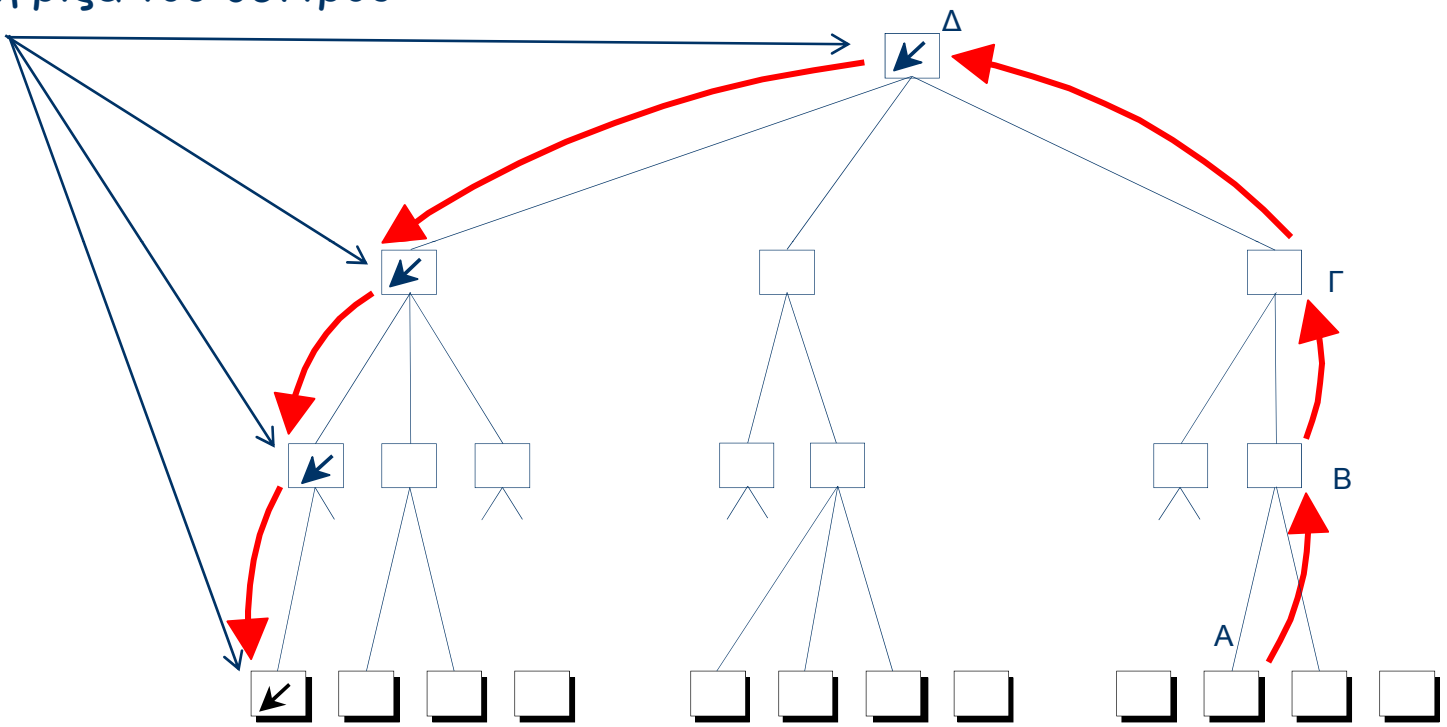
- Η κατανεμημένη βάση δεδομένων (Distributed Data Base, DDB) προσφέρει λύσεις:
  - στην ταχεία πρόσβαση στα δεδομένα
  - στον υψηλό αριθμό επικοινωνιών, με εκμετάλλευση της τοπικότητας της ζητούμενης πληροφορίας
  - στη σταδιακή απορρόφηση νέων συνδρομητών
  - στην αξιοπιστία του συστήματος και στη διαθεσιμότητα της πληροφορίας (αντίγραφα σε περισσότερους από έναν κόμβους)

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

- Τα μειονεκτήματα προέρχονται από την πολυπλοκότητα διαχείρισης των δεδομένων
  - η αναγνώριση της πληροφορίας που ακολουθεί τον χρήστη / συνδρομητή, ώστε να εξασφαλίζεται η τοπικότητα της πληροφορίας
  - η συνέπεια (consistency) της πληροφορίας
  - η διαχείριση κατανεμημένων λειτουργιών (συγχρονισμός)
  - η ασφάλεια της πληροφορίας και η προστασία του ιδιωτικού απόρρητου

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

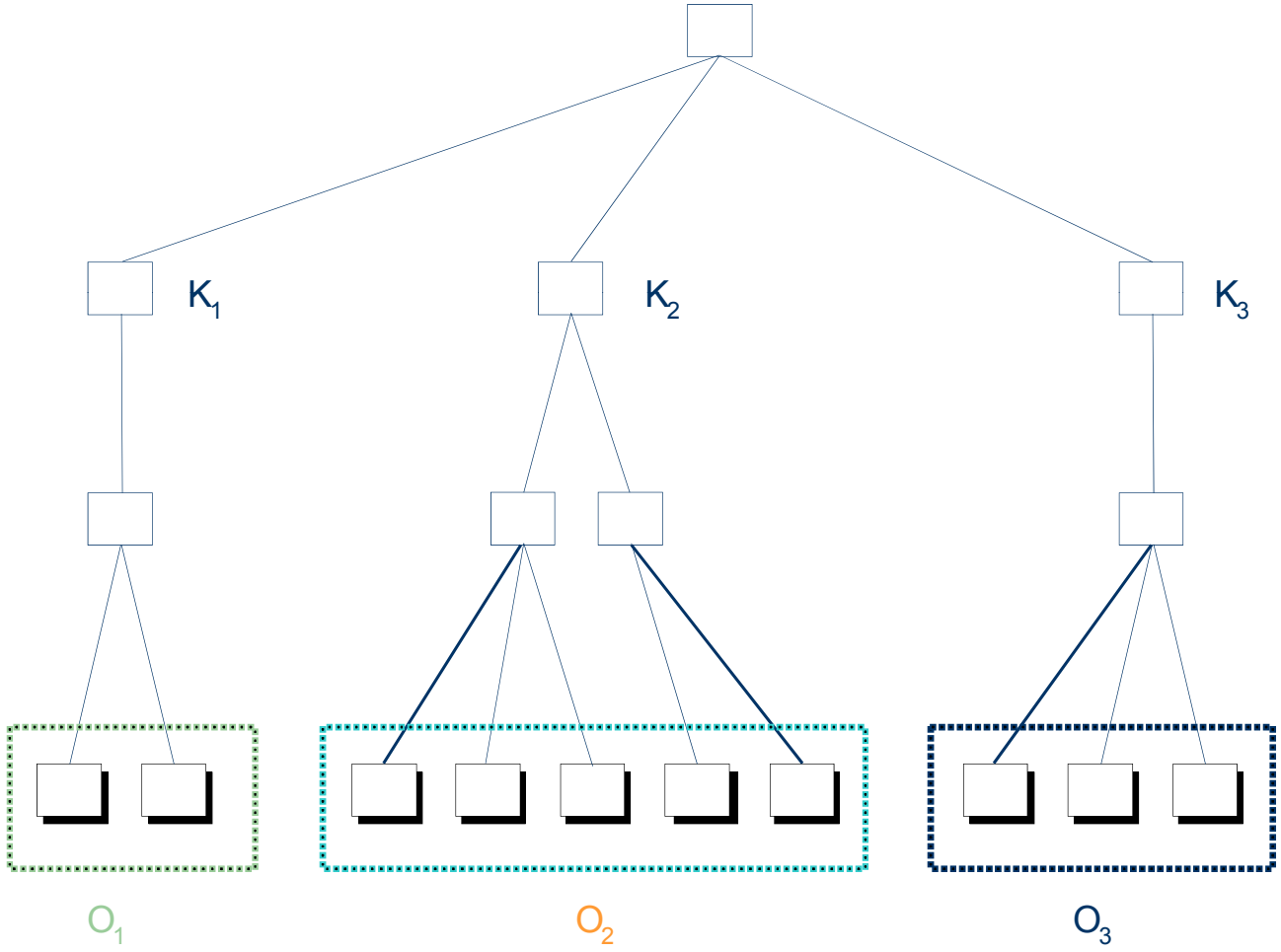
Εγγραφή σε κάθε βάση
κατά μήκος της διαδρομής
μέχρι τη ρίζα του δέντρου



LA1 LA2

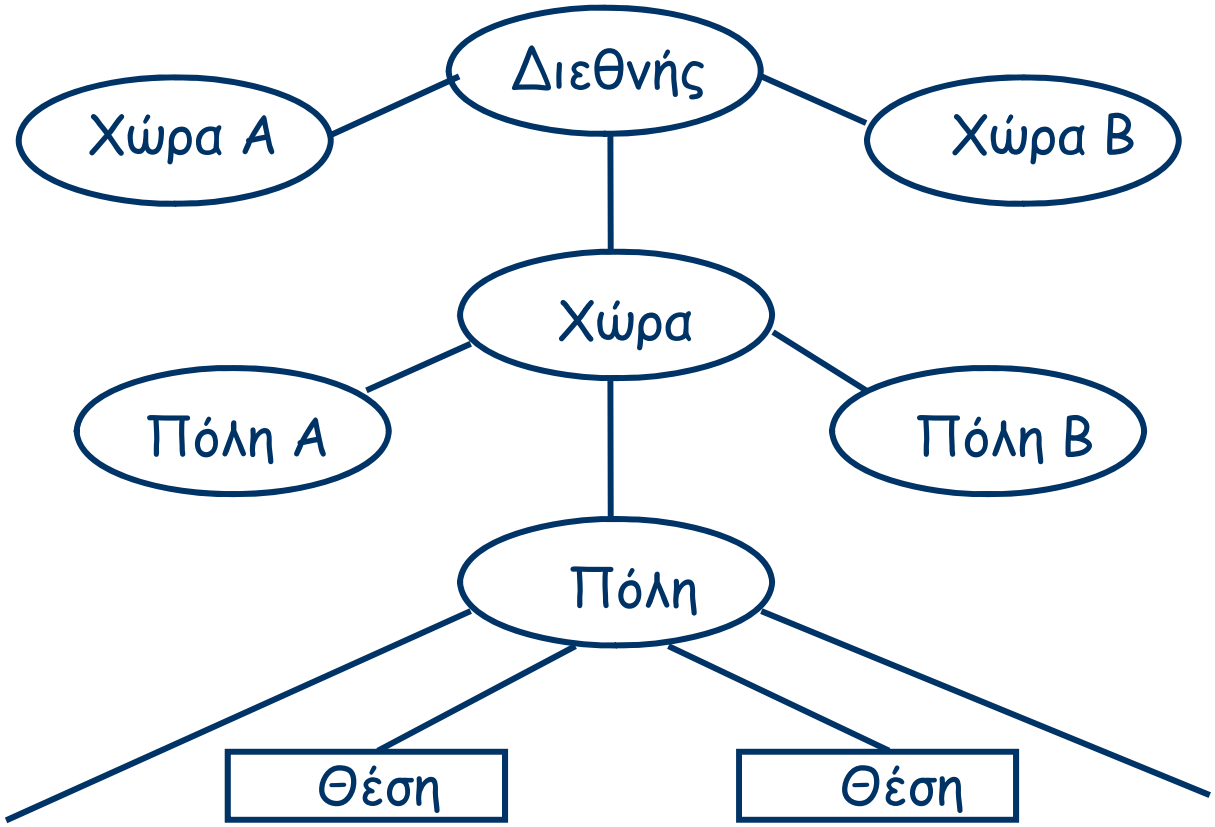
Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ομαδοποίηση



Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ιεραρχικά κατανεμημένη DB

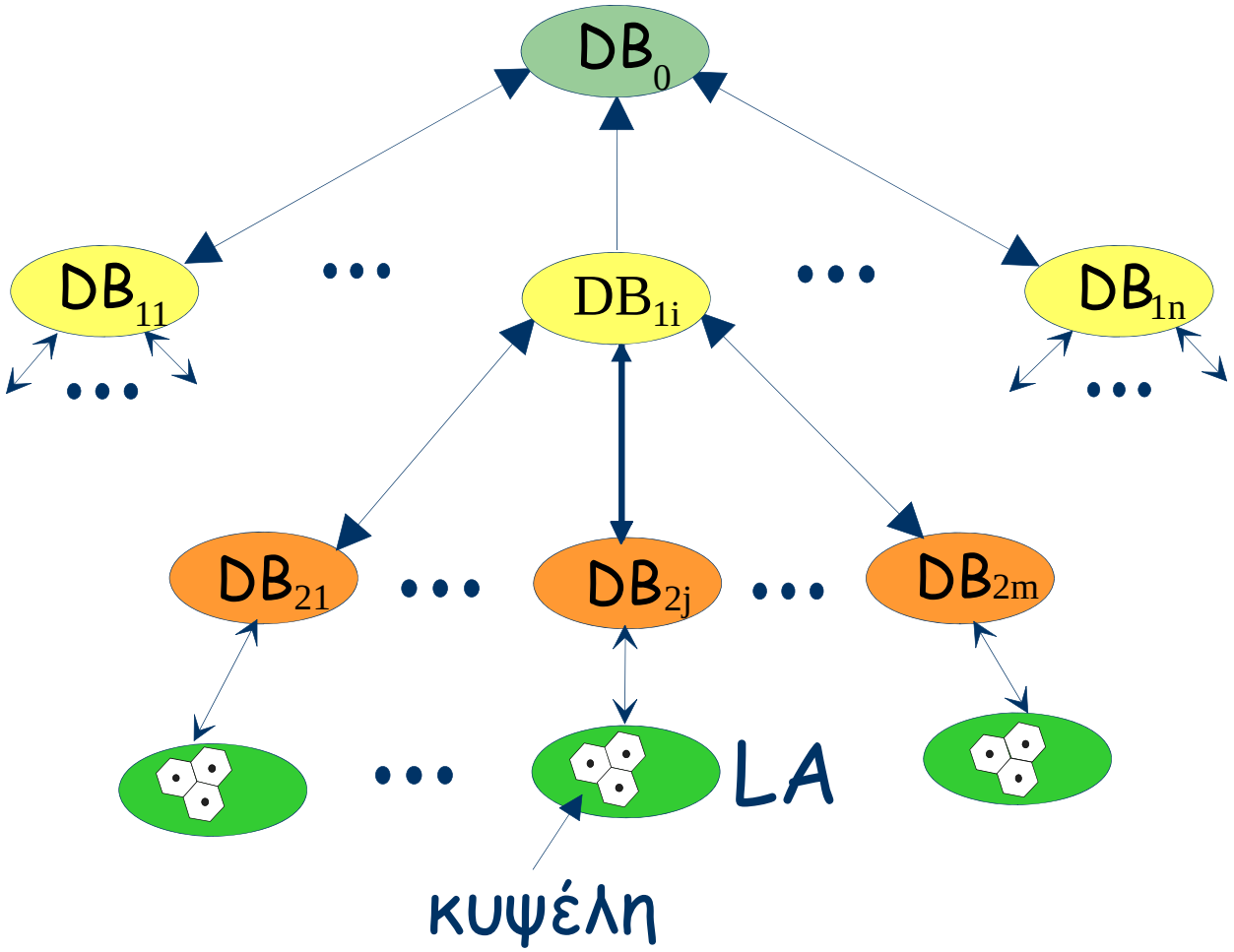


Χώρα	Πόλη	Θέση

Μορφή αριθμού

Αρχιτεκτονικές κατανεμημένων βάσεων δεδομένων

Ιεραρχική DB με τρία επίπεδα



Στρατηγικές εντοπισμού δεδομένων στην DDB

- Η υιοθέτηση μιας συγκεκριμένης στρατηγικής επηρεάζεται σημαντικά από τον τρόπο κατανομής της πληροφορίας της DDB στους κόμβους της.
- Η βασική παραδοχή είναι, ότι πληροφορία που αφορά χρήστες και τερματικά χρειάζεται σε δύο περιοχές της βάσης δεδομένων:
  - στην οικεία περιοχή (Resident Data Storage Node)
  - στην περιοχή που επισκέπτεται ο χρήστης (Visitors Data Storage Node).

Στρατηγικές εντοπισμού δεδομένων στην DDB

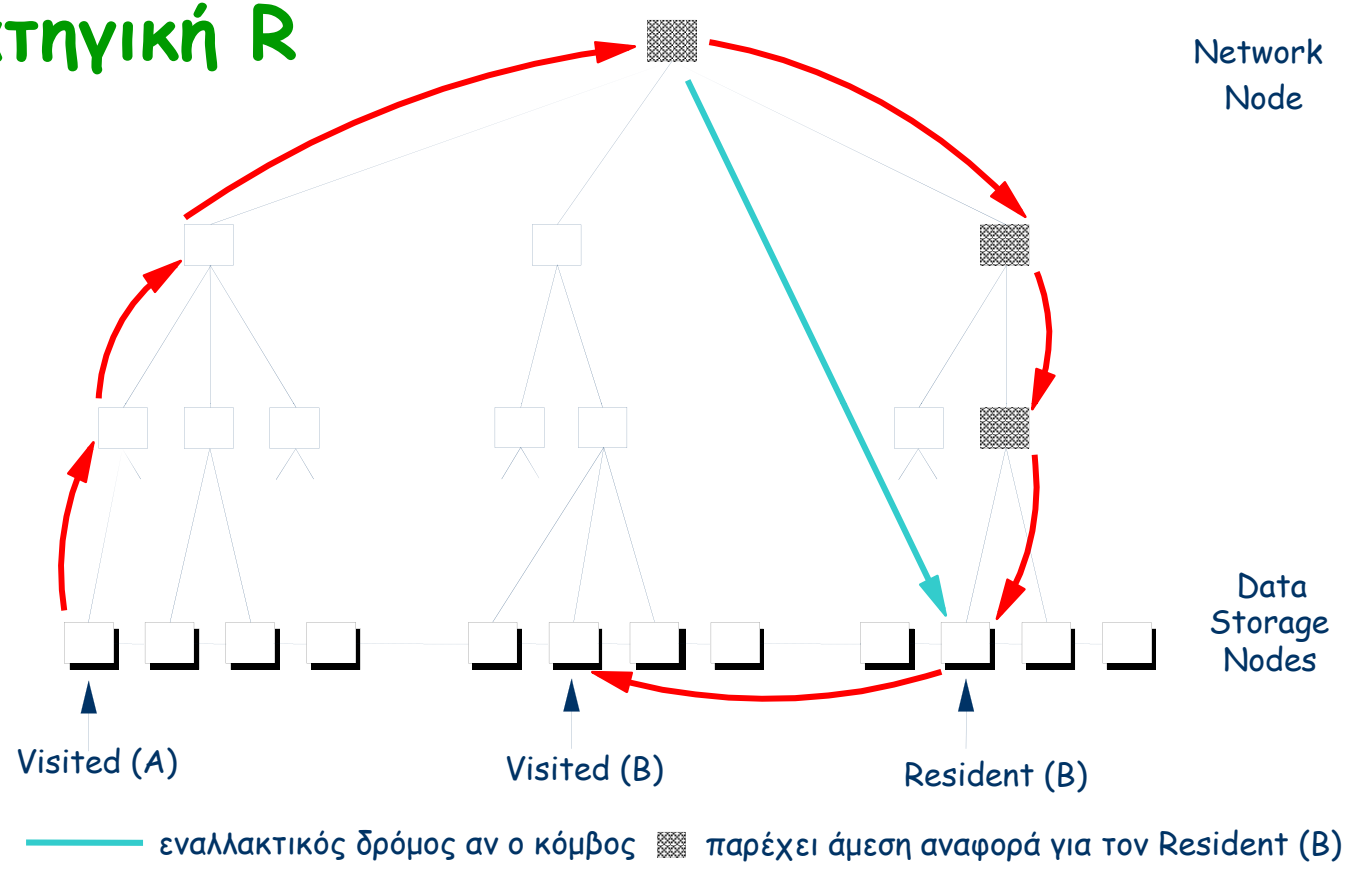
- Όσον αφορά τη συνολική επίδοση του συστήματος, η στρατηγική εντοπισμού δεδομένων επηρεάζει:
- την καθυστέρηση εντοπισμού δεδομένων (interrogation delay)
- την επίδοση της DDB
  - επηρεάζει τον αριθμό των κατανεμημένων κόμβων της DDB, που θα ερωτηθούν
  - καθορίζει τον μηχανισμό ενημέρωσης της πληροφορίας στους κατάλληλους κόμβους
  - επηρεάζει τον χώρο αποθήκευσης που χρειάζεται για τη σωστή λειτουργία της

Στρατηγικές εντοπισμού δεδομένων στην DDB

- Από την πλευρά του παρόχου δικτύου, μια αποτελεσματική στρατηγική εντοπισμού δεδομένων πρέπει να έχει τα εξής χαρακτηριστικά:
  - να ελαχιστοποιεί, όσο είναι δυνατό, τον απαιτούμενο χώρο αποθήκευσης
  - να ελαχιστοποιεί τον ρυθμό άφιξης ερωτήσεων, κατά τη διάρκεια του εντοπισμού της ζητούμενης πληροφορίας
  - να ελαχιστοποιεί τον ρυθμό άφιξης αιτήσεων που αφορούν την ενημέρωση της πληροφορίας παραπομπών

Στρατηγικές εντοπισμού δεδομένων στην DDB

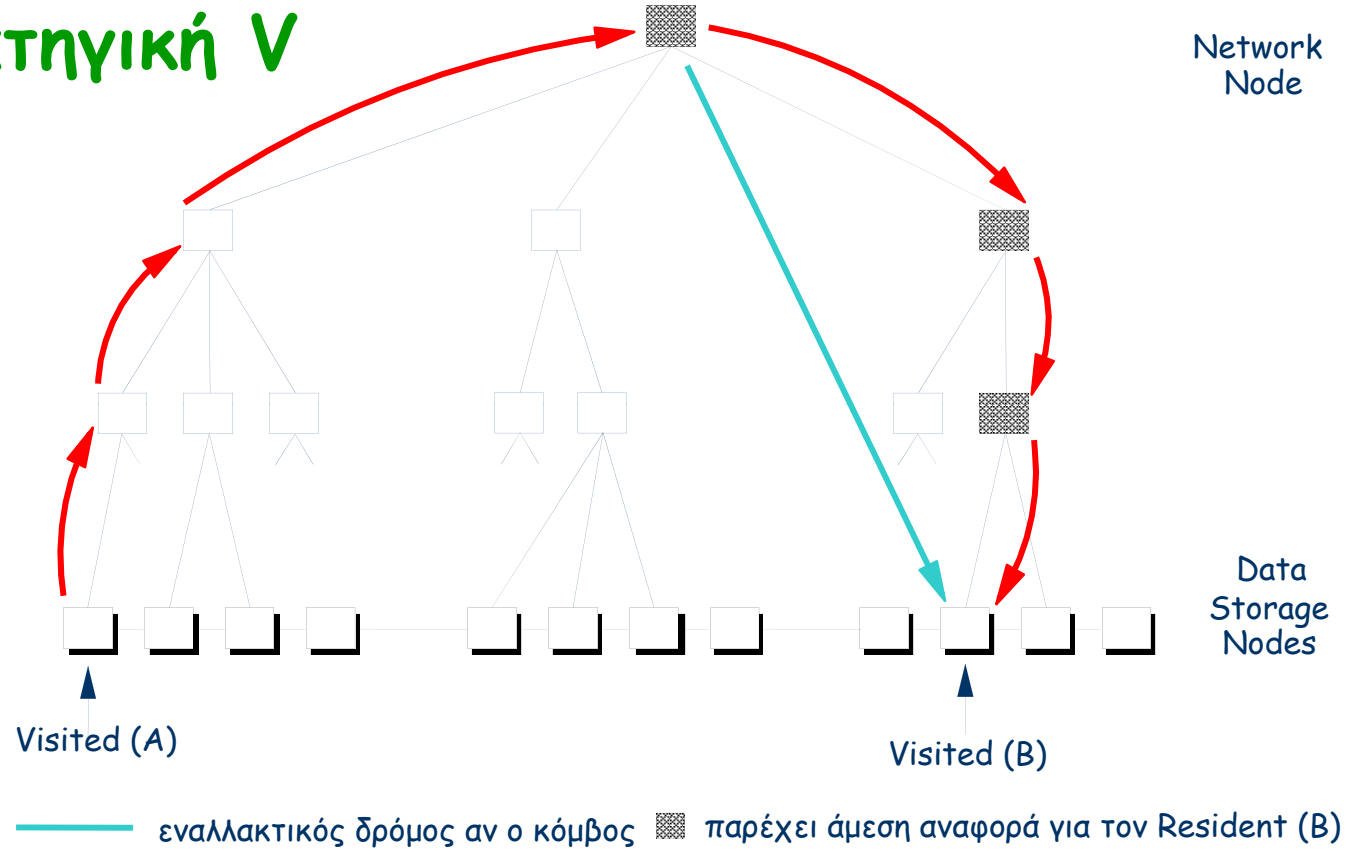
Στρατηγική R



+ απλοί κανόνες
- μεγάλοι βρόχοι
- οικείος κόμβος εκτός ⇒ οικείοι χρήστες εκτός

Στρατηγικές εντοπισμού δεδομένων στην DDB

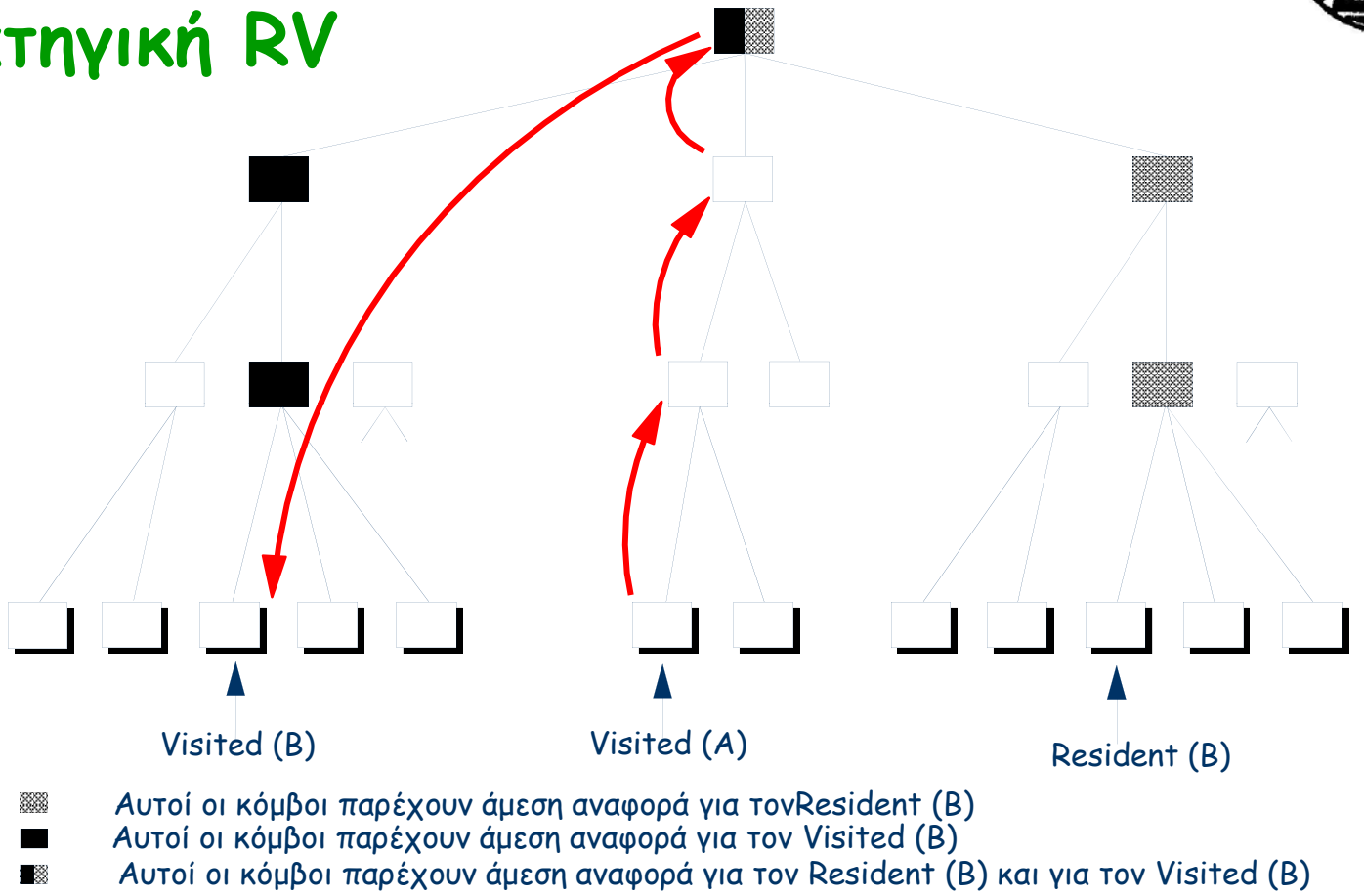
Στρατηγική V



+ υποστηρίζει τοπικότητα, όχι μεγάλοι βρόχοι
- καθυστέρηση
- αναποτελεσματική χρήση των ISN

Στρατηγικές εντοπισμού δεδομένων στην DDB

Στρατηγική RV

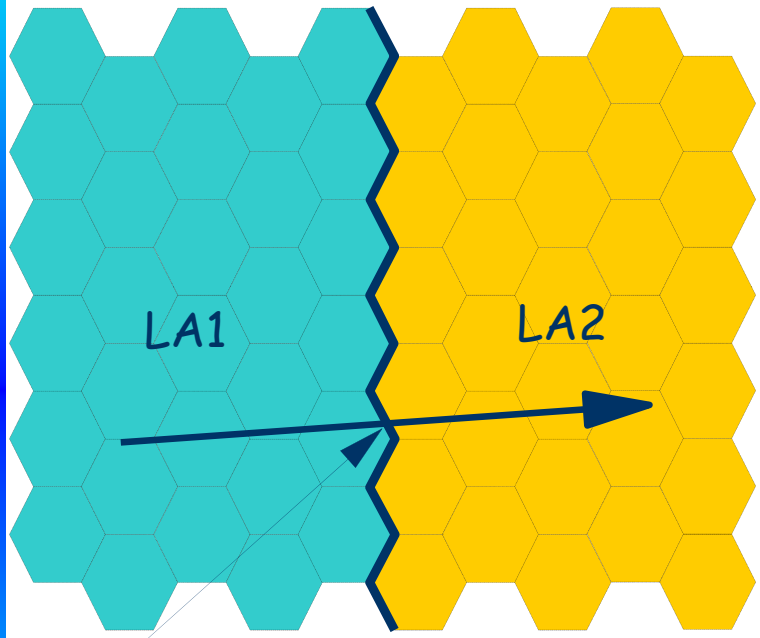


+ υποστηρίζει τοπικότητα
+ λιγότερες ανεπιτυχείς αναζητήσεις στους ISN
- μεγαλύτερος χώρος αποθήκευσης

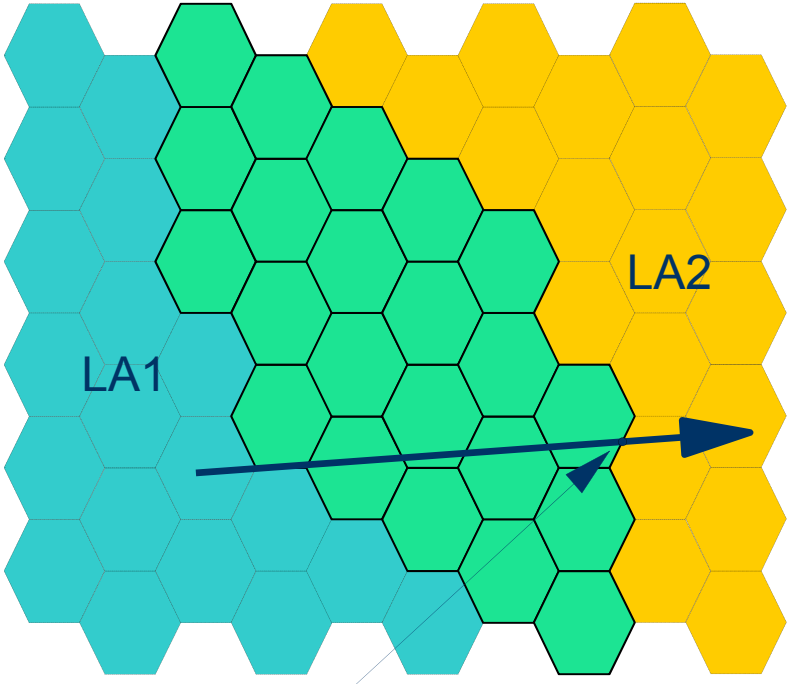
Ενημέρωση θέσης και αναζήτηση

- Υπάρχουν μερικά μειονεκτήματα όσο αφορά την επίδοση των διαδικασιών ενημέρωσης θέσης και αναζήτησης που βασίζονται στις LA
  - Υπερβολικές ενημερώσεις θέσης από MT που μετακινούνται κατά μήκος των συνόρων δύο LA
  - Η αναζήτηση ενός MT σε όλην την LA, μπορεί να έχει ως αποτέλεσμα υπερβολικό όγκο κίνησης
  - Η κινητικότητα και ο ρυθμός άφιξης των κλήσεων των MT μεταβάλλονται και δεν υπάρχει ένα μέγεθος LA, το οποίο να είναι βέλτιστο για όλους τους χρήστες

Ενημέρωση θέσης και αναζήτηση

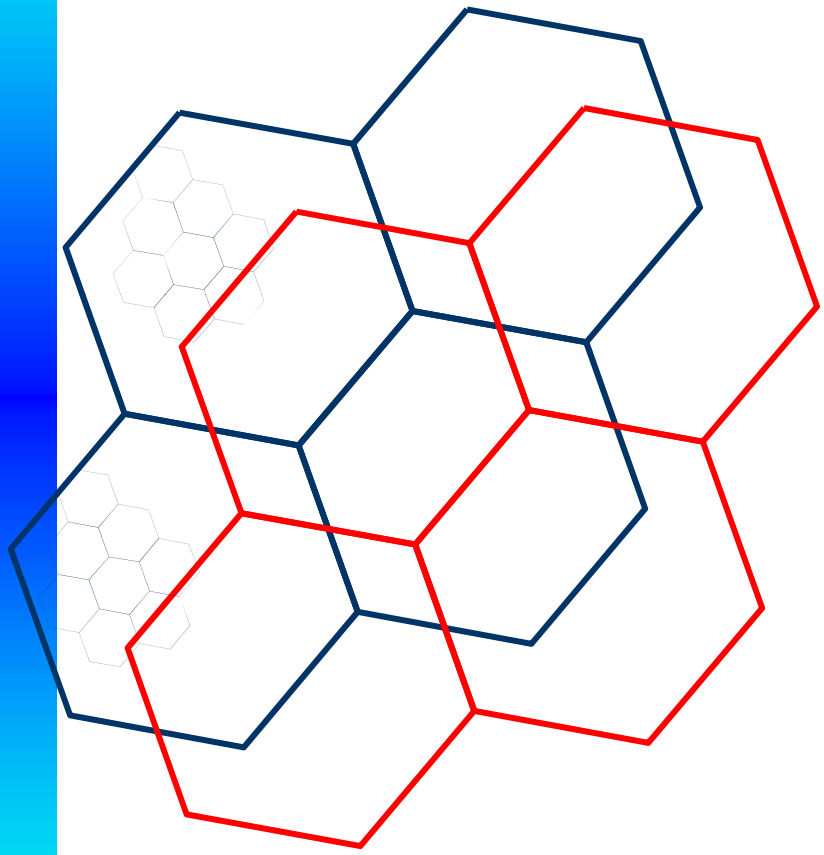


Ενημέρωση θέσης θα γίνει εδώ



Ενημέρωση θέσης θα γίνει εδώ

Ενημέρωση Θέσης και αναζήτηση



LA ομάδας 1

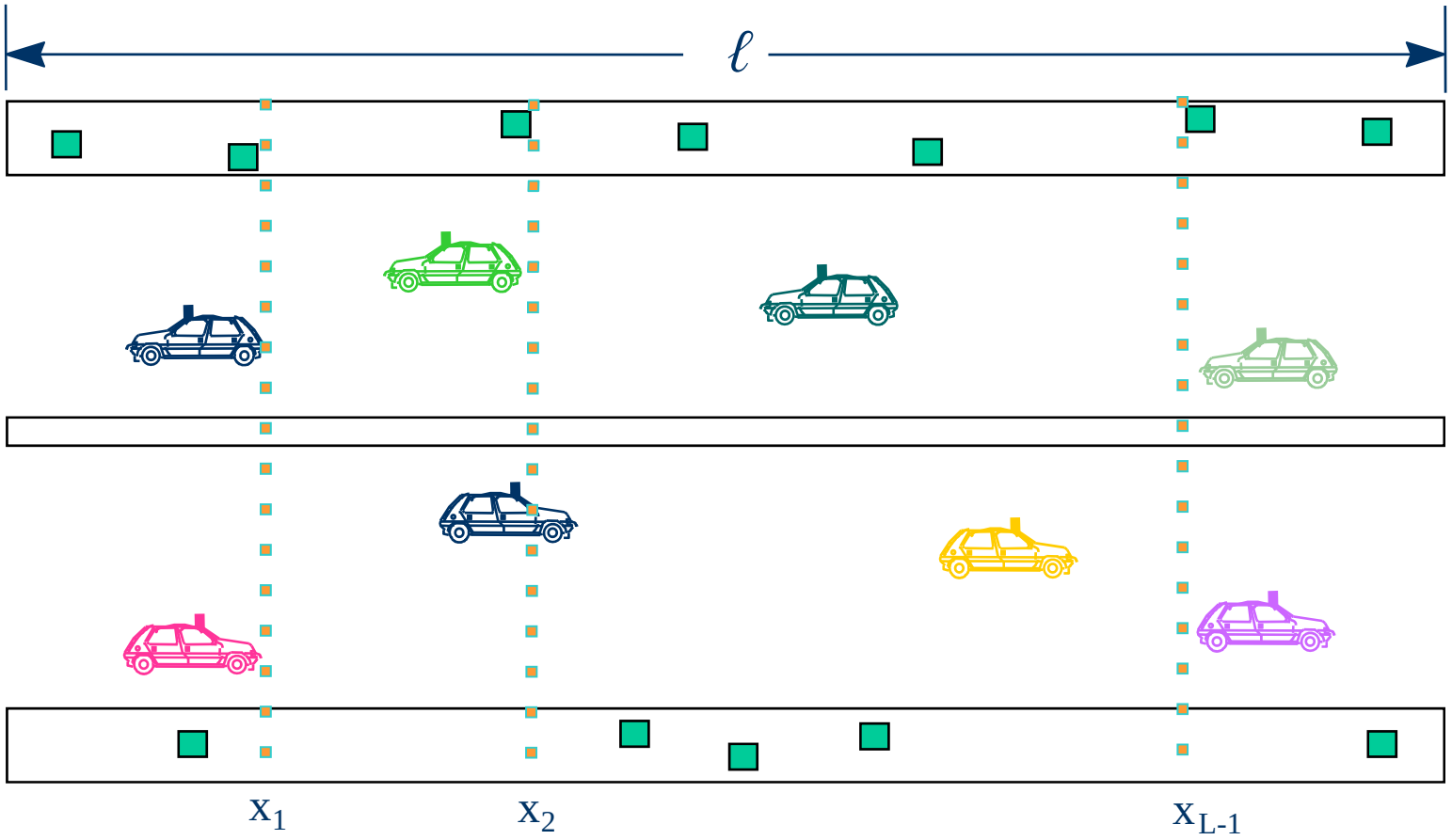
LA ομάδας 2

Ενημέρωση θέσης και αναζήτηση

- Το κόστος του συστήματος για την ενημέρωση θέσης και για την αναζήτηση εξαρτάται από δύο παράγοντες:
  1. Το φορτίο σηματοδοσίας, που προκαλείται από τις ανταλλαγές μηνυμάτων κατά τη διάρκεια των διαδικασιών ενημέρωσης θέσης και αναζήτησης.
  2. Το πλήθος διεργασιών με τη βάση δεδομένων, που πραγματοποιείται κατά την ενημέρωση θέσης και την αναζήτηση.

Ενημέρωση θέσης και αναζήτηση

Παράδειγμα 10.2



Ενημέρωση Θέσης και αναζήτηση

Κόστος αναζήτησης

$$C_{pi} = P \cdot \lambda \cdot N_i \cdot B_i$$

$$N_i = \int_{x_{i-1}}^{x_i} \rho(x)dx \qquad B_i = \int_{x_{i-1}}^{x_i} \beta(x)dx$$

$$C_p(\vec{x}) = P \cdot \lambda \cdot \sum_{i=1}^{L} N_i \cdot B_i \qquad \vec{x} = (x_1, \ldots, x_{L-1})$$

Κόστος ενημέρωσης θέσης

$$C_u(\vec{x}) = R \cdot \sum_{i=1}^{L-1} q(x_i)$$

Ενημέρωση θέσης και αναζήτηση

Βελτιστοποίηση

$$\min_{L}[\min_{\vec{x}}(P\cdot\lambda\cdot\sum_{i=1}^{L}B_i\cdot N_i + R\cdot\sum_{i=1}^{L-1}q(x_i))]$$

Εφαρμογή: $\rho(x)=\rho$, $q(x)=q$, $\beta(x)=\beta$

$$C(\vec{x}) = P\cdot\sum_{i=1}^{L}\beta\cdot\lambda\cdot\rho\cdot(x_i - x_{i-1})^2 + R\cdot(L-1)q$$

$x_i = i x_L / L = i\,\ell / L$

Ενημέρωση θέσης και αναζήτηση

Για σταθερό L

$$C(\vec{x}^*) = l^2 \cdot P \cdot \beta \cdot \lambda \cdot \rho / L + R \cdot (L-1)q$$

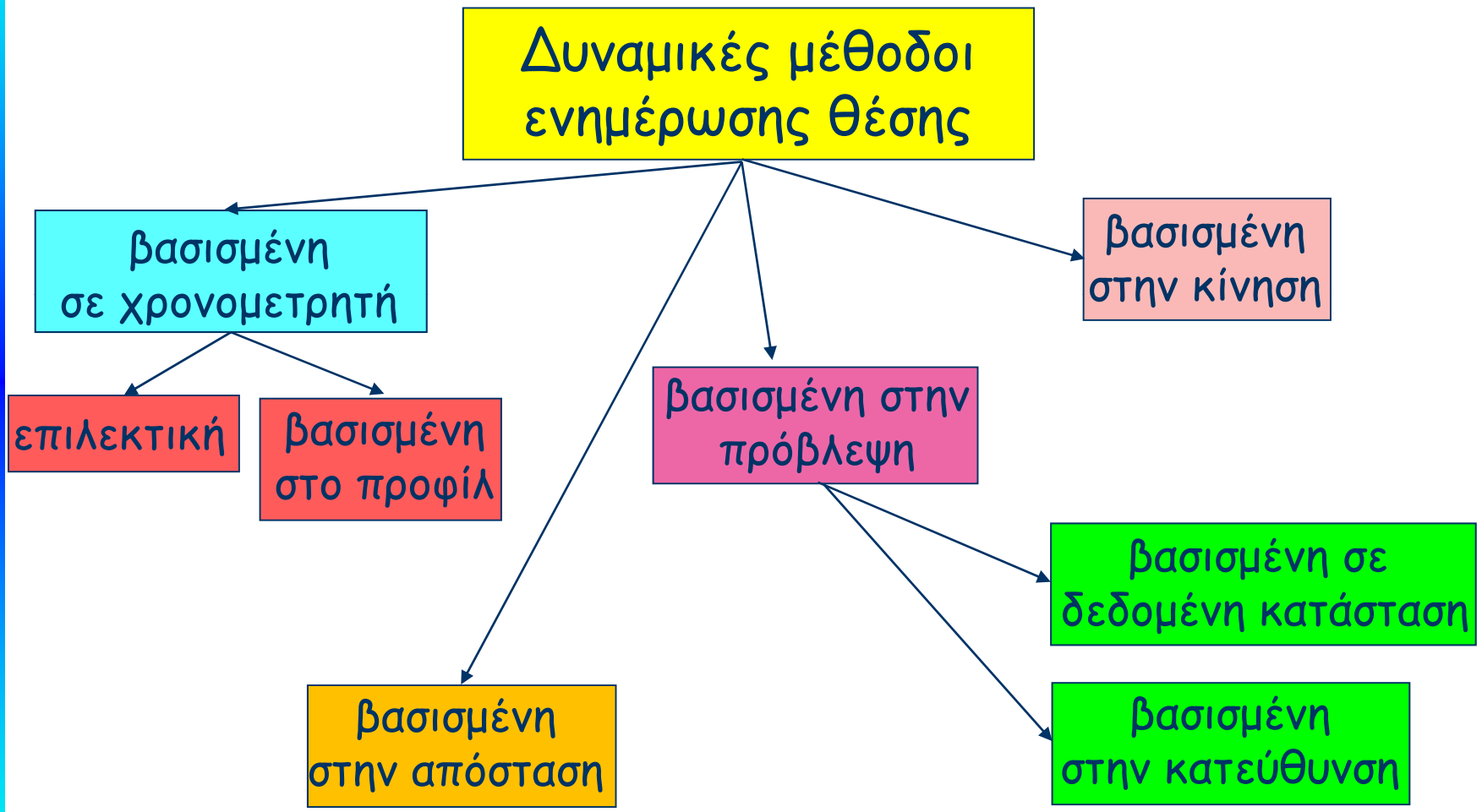
$$L = l \cdot \sqrt{\frac{P \cdot \beta \cdot \lambda \cdot \rho}{R \cdot q}}$$

$$C_{\min} = 2l\sqrt{P \cdot \beta \cdot \lambda \cdot \rho \cdot R \cdot q} - R \cdot q$$

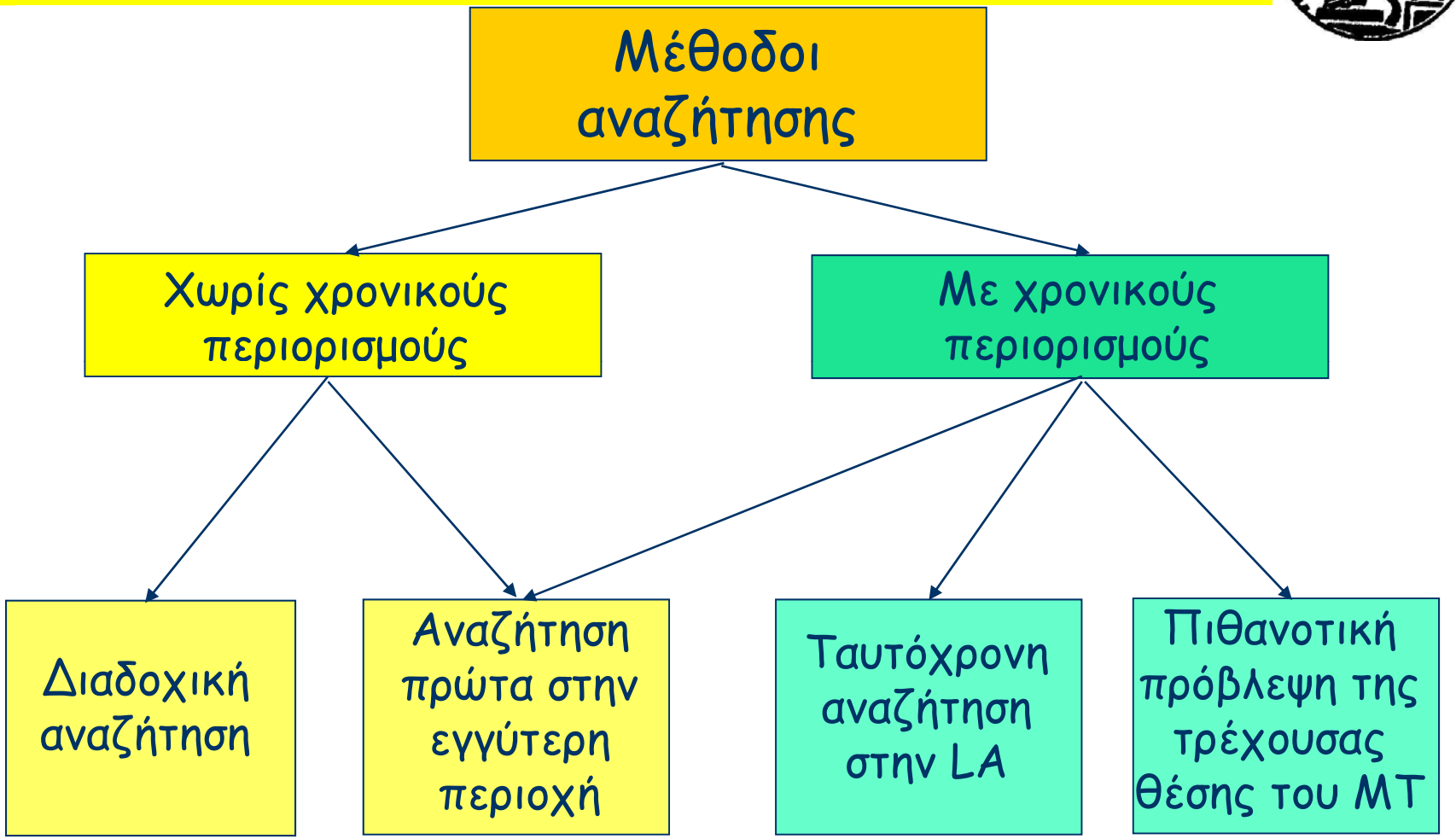
Δυναμικές μέθοδοι ενημέρωσης θέσης

- Δυναμική ρύθμιση των παραμέτρων διαχείρισης εντοπισμού των επιμέρους χρηστών, ώστε να βελτιστοποιηθεί η επίδοση του συστήματος
  - μέθοδοι που βασίζονται στον *χρόνο*
  - μέθοδοι που βασίζονται στην *κίνηση*
  - μέθοδοι που βασίζονται στην *απόσταση*
  - μέθοδοι *πρόβλεψης*

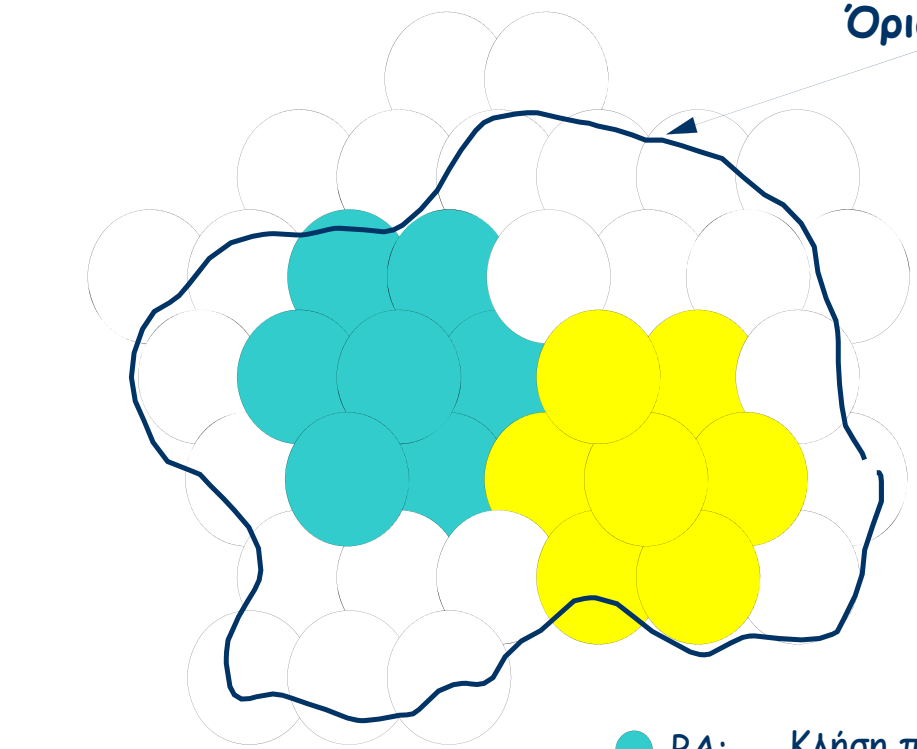
Δυναμικές μέθοδοι ενημέρωσης θέσης



Μέθοδοι αναζήτησης



Ευφυής αναζήτηση

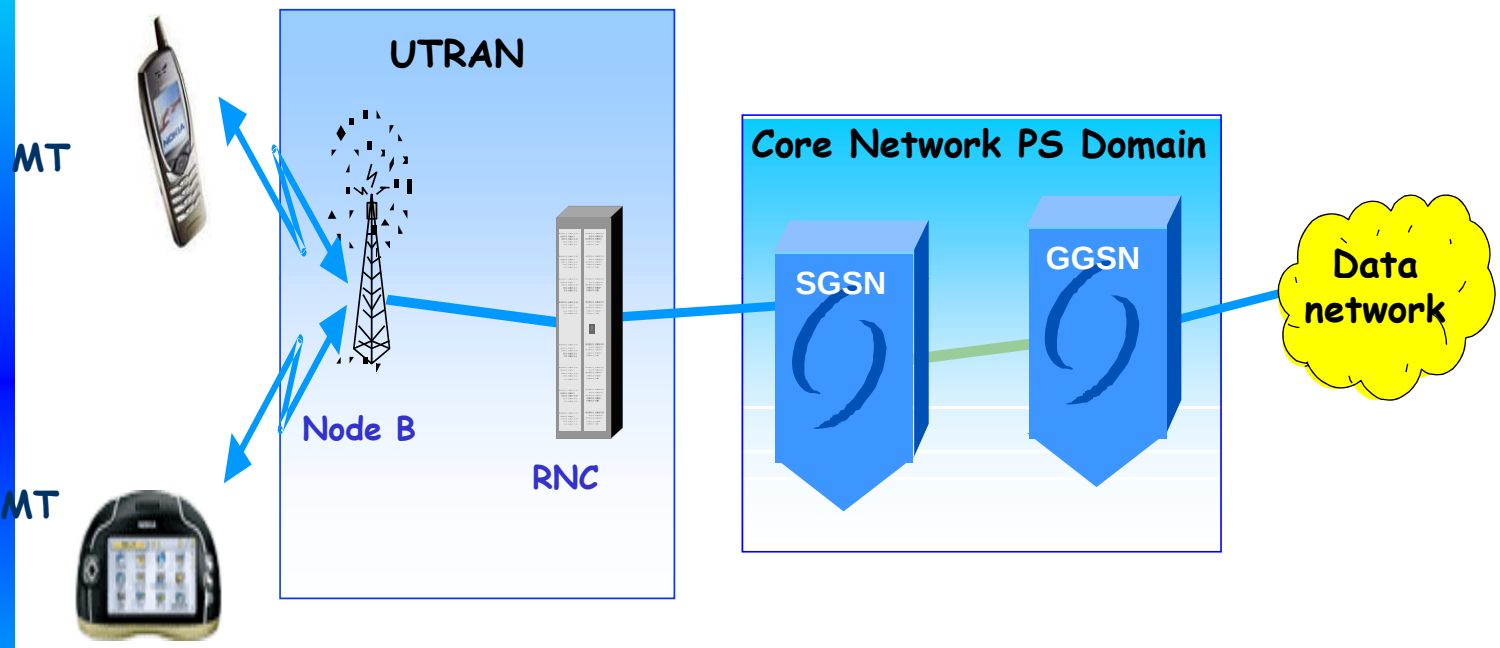


Κυψέλη

PA: Κλήση που τερματίζει στον χρήστη A

PA: Κλήση που τερματίζει στον χρήστη B

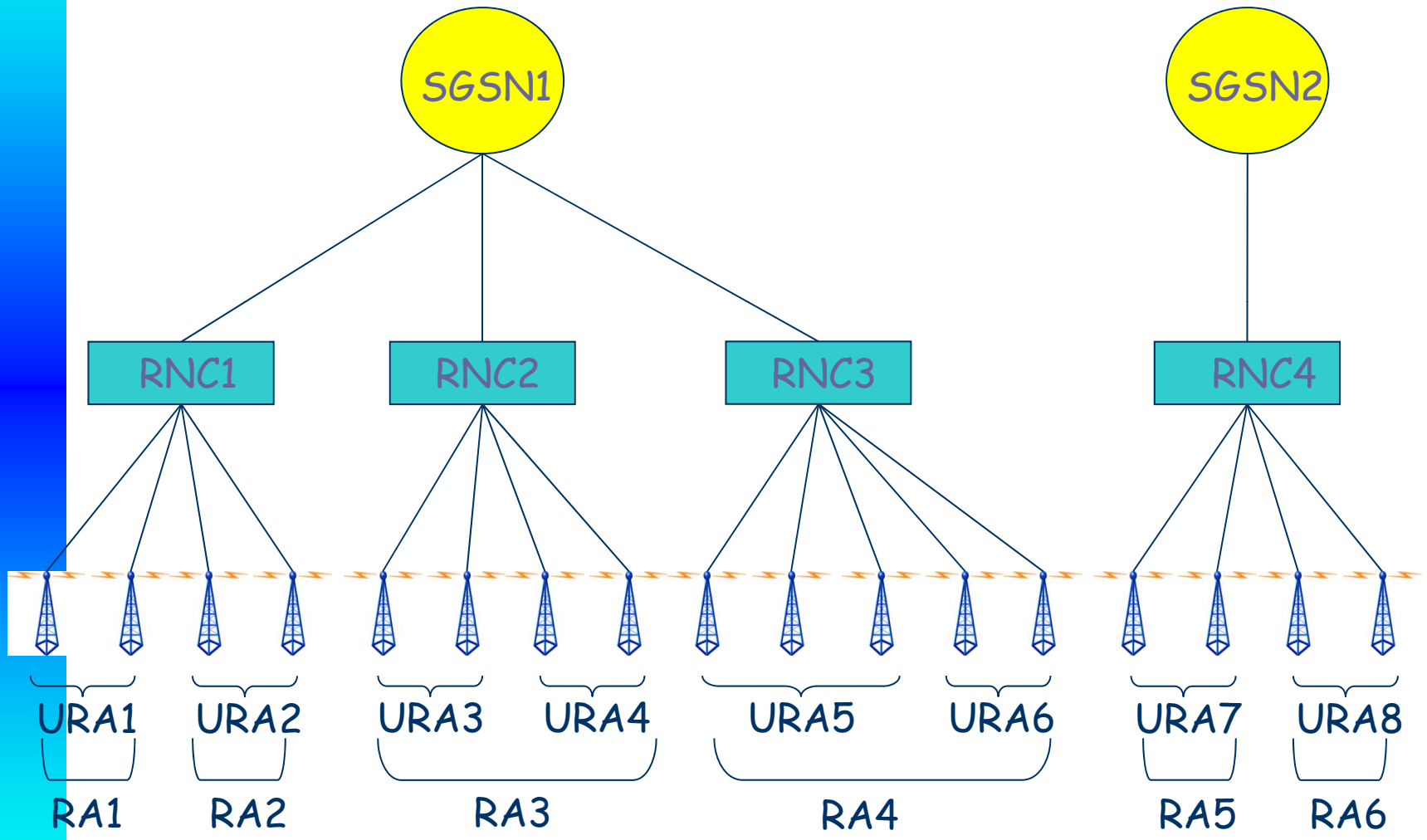
Διαχείριση εντοπισμού στο UMTS



Node B: Base station
RNC: Radio Network Controller
MT: Mobile Terminal

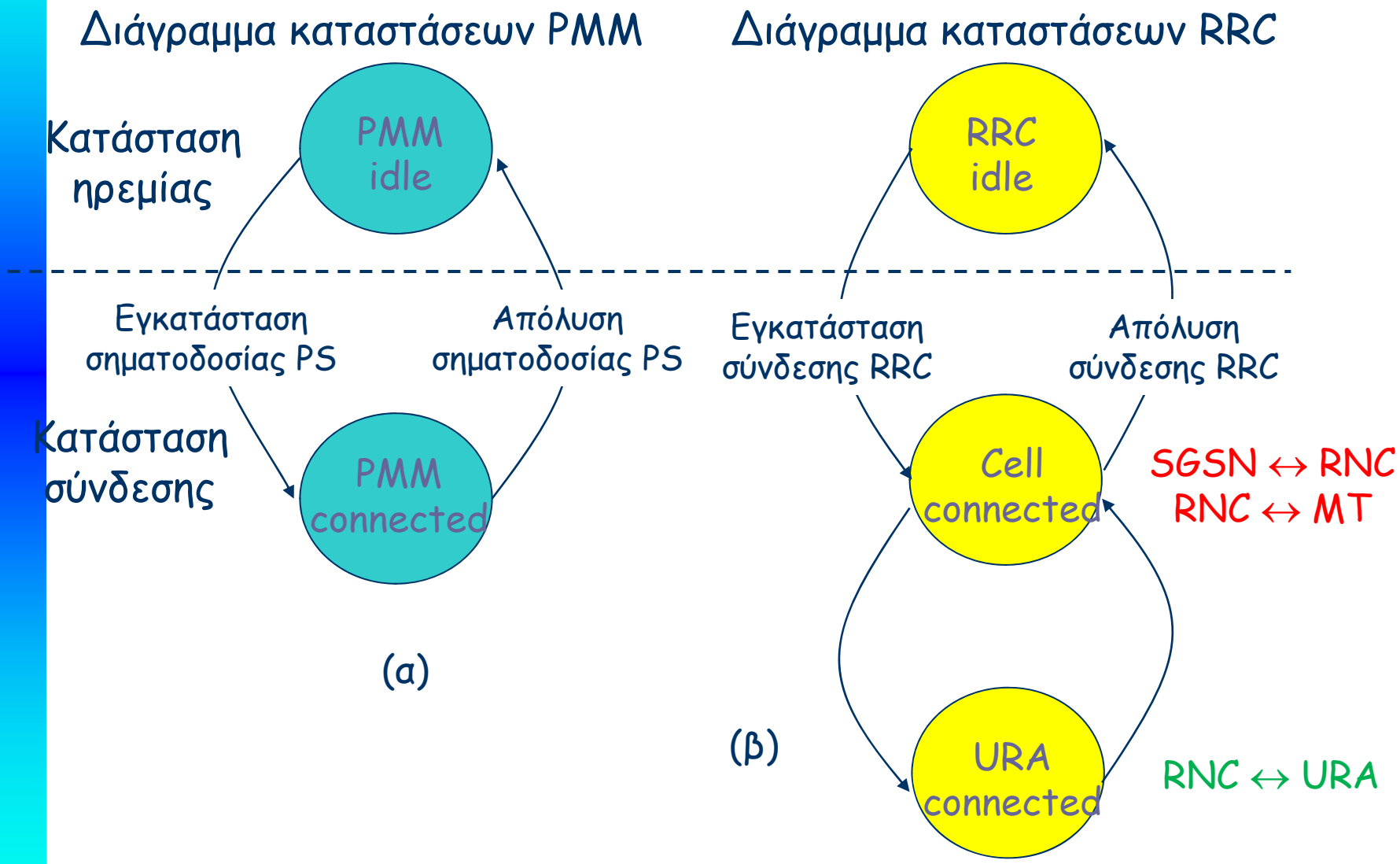
GGSN: Gateway GPRS Support Node
SGSN: Serving GPRS Support Node
UTRAN: UMTS Terrestrial Radio Access Network

Διαχείριση εντοπισμού στο UMTS



RA: Routing Area
URA: UTRAN Registration Area

Διαχείριση εντοπισμού στο UMTS



Διαχείριση ασφάλειας

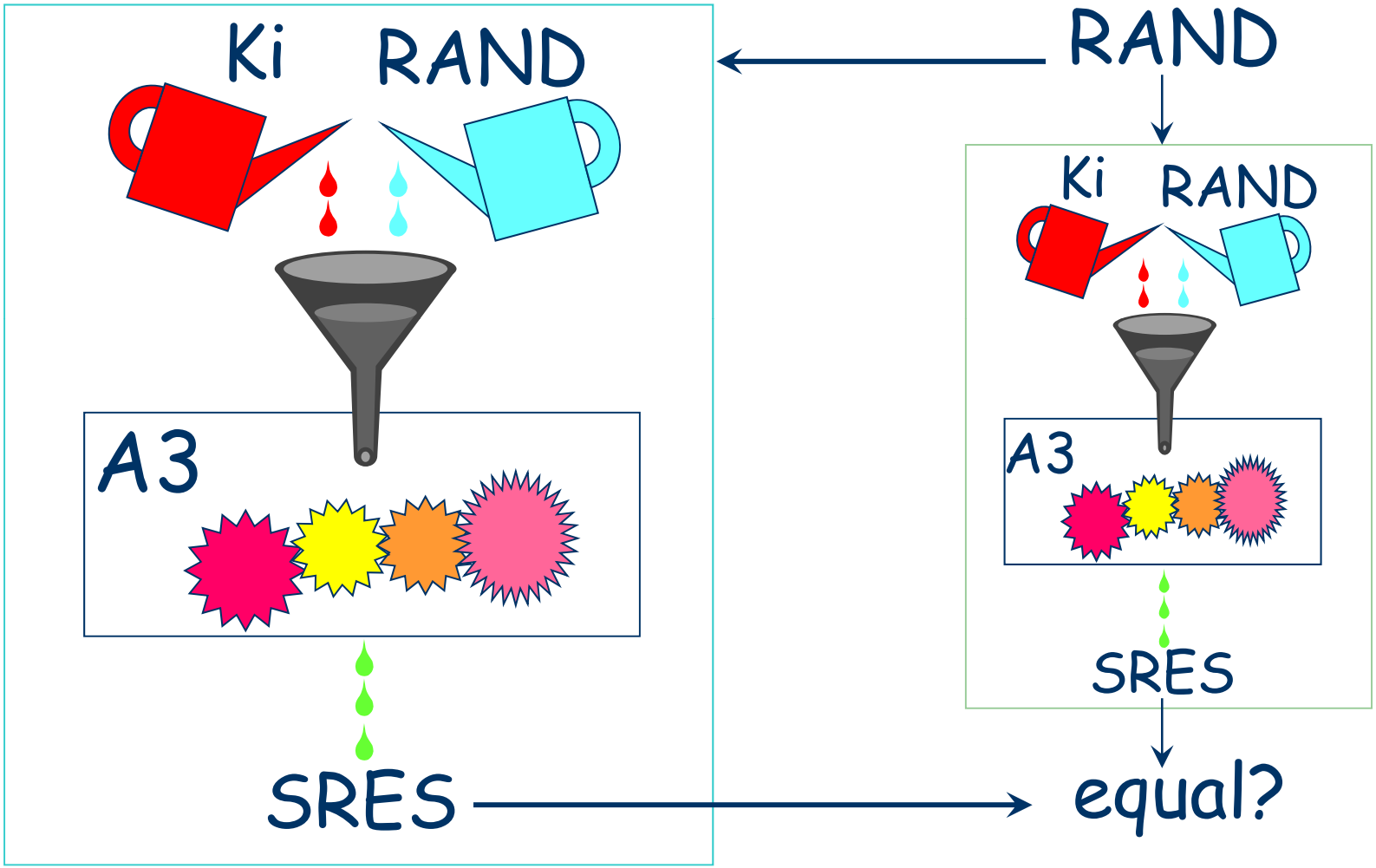
Δύο στόχοι:

- προστασία δικτύου από μη εξουσιοδοτημένη πρόσβαση
  - πιστοποίηση αυθεντικότητας
- προστασία του απορρήτου της επικοινωνίας
  - κρυπτογραφημένη μετάδοση στο ασύρματο τμήμα
  - προστασία σηματοδοσίας με τον ίδιο τρόπο
  - αντικατάσταση του IMSI με TMSI

Λειτουργίες ασφάλειας

- απλή πιστοποίηση αυθεντικότητας (χρήση PIN)
  - μικρή προστασία
  - στο GSM το PIN ελέγχεται από το SIM χωρίς να μεταδίδεται στο ασύρματο τμήμα
- μία πιο περίτεχνη τεχνική συνίσταται στο να γίνει κάποια ερώτηση, που μόνο ο σωστός χρήστης (MT με το SIM) μπορεί να απαντήσει
- υπάρχει ένας τεράστιος αριθμός ερωτήσεων και είναι απίθανο να χρησιμοποιηθεί δύο φορές η ίδια ερώτηση

Λειτουργίες ασφάλειας



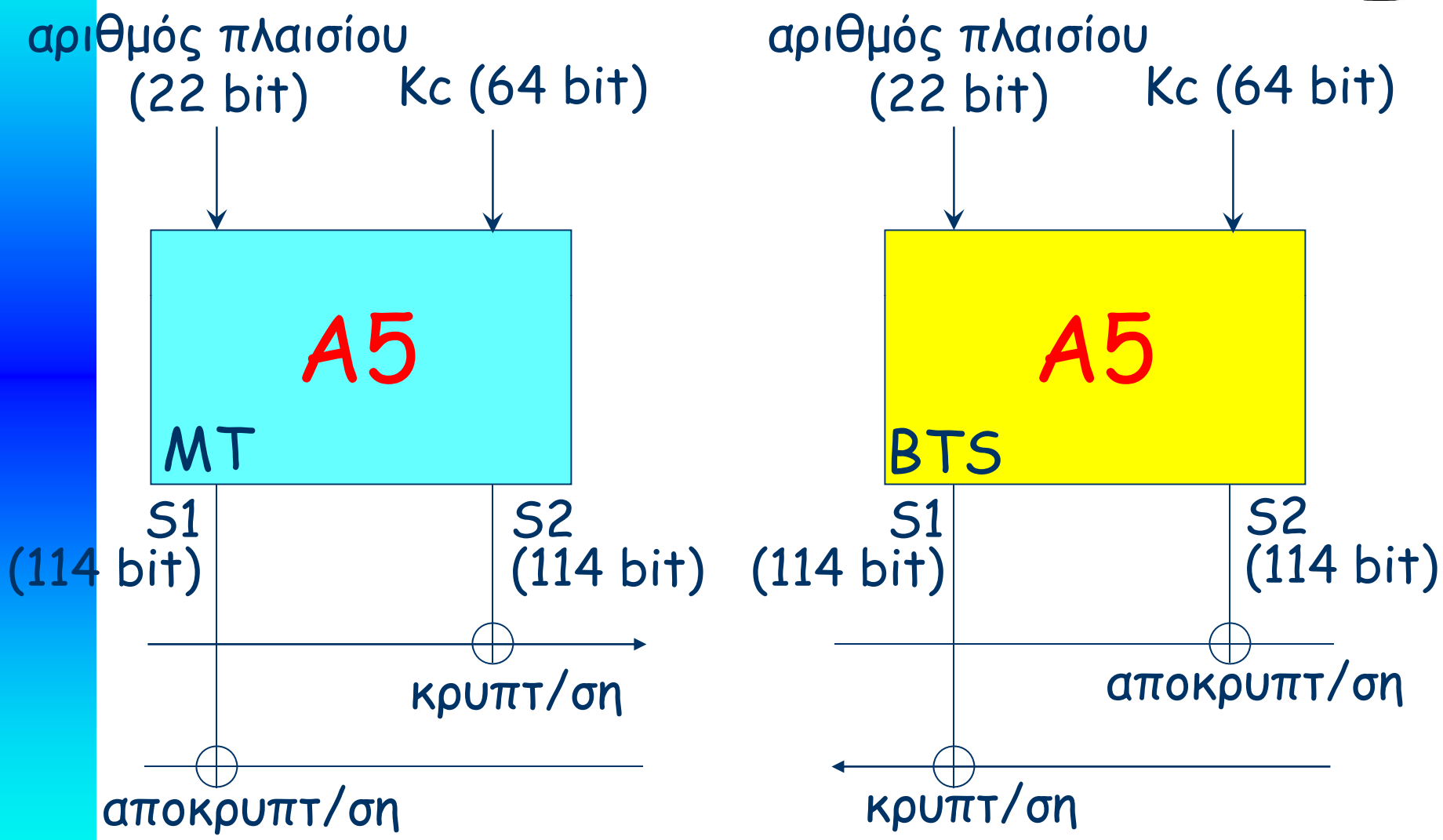
Λειτουργίες ασφάλειας

- SRES : Signed RESult
- SRES = f (Ki, RAND) : εύκολο
- Ki = g (SRES, RAND) : όσο το δυνατό πιο πολύπλοκο
- Ακόμη και αν είναι γνωστά αρκετά ζεύγη (RAND,SRES) για τον ίδιο χρήστη (δηλ. το ίδιο Ki), ο υπολογισμός πρέπει να παραμένει πολύ πολύπλοκος
- Ο μόνος περιορισμός είναι τα 128 bit του RAND και τα 32 bit του SRES. Το Ki μπορεί να έχει οποιοδήποτε μήκος (αν μεταφέρεται, περιορίζεται στα 128 bit).

Κρυπτογράφηση

- Λειτουργία exclusive OR μεταξύ:
  - 114 κωδικοποιημένων bit μιας ριπής
  - 114 bit της ακολουθίας κρυπτογράφησης που παράγεται από ειδικό αλγόριθμο, τον A5
- Η ακολουθία κρυπτογράφησης για κάθε ριπή παράγεται από τον A5 με υπολογισμό δύο εισόδων:
  - αριθμός πλαισίου
  - Kc (συμφωνείται μεταξύ MT και δικτύου)

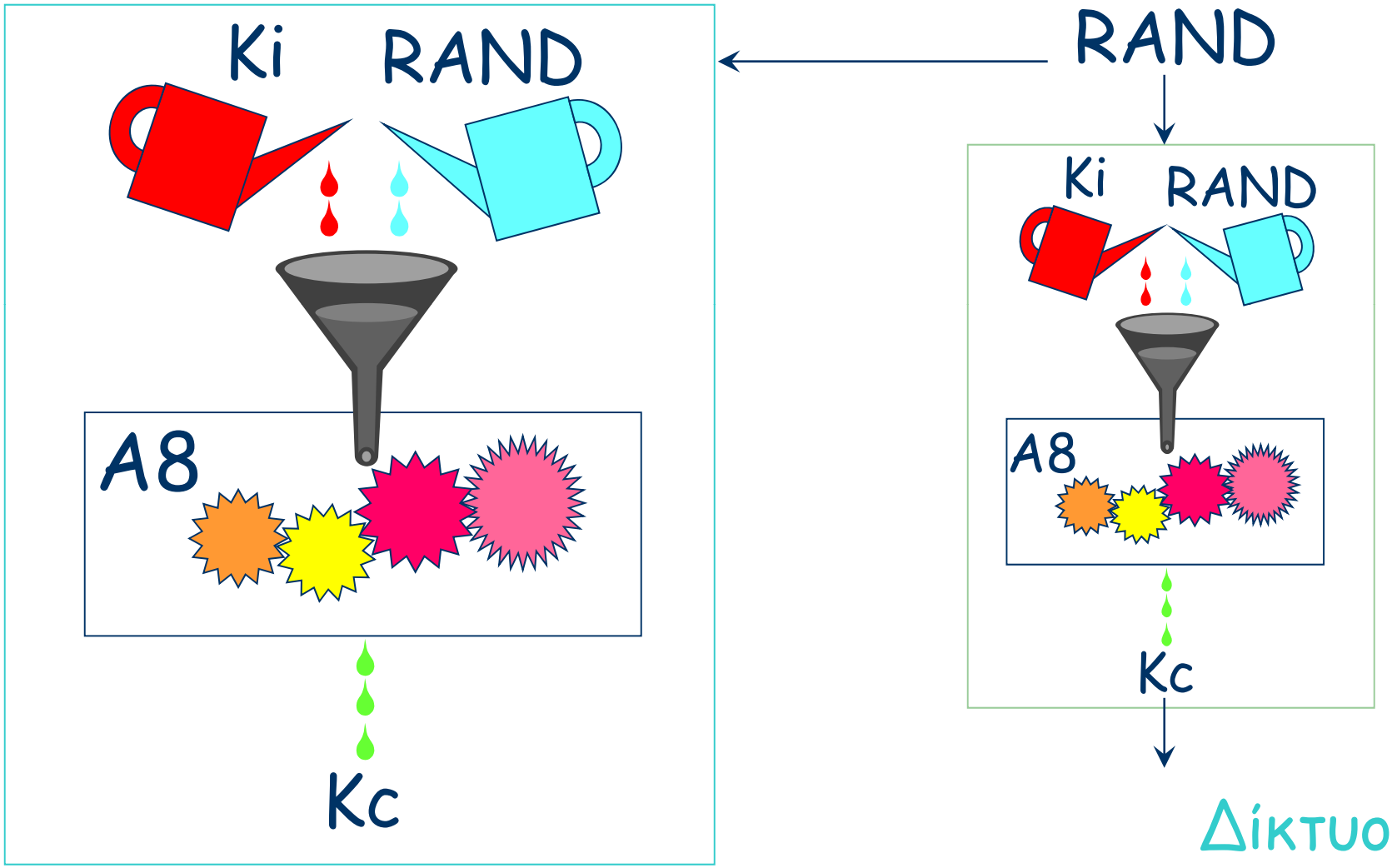
Κρυπτογράφηση



Διαχείριση κλειδιών

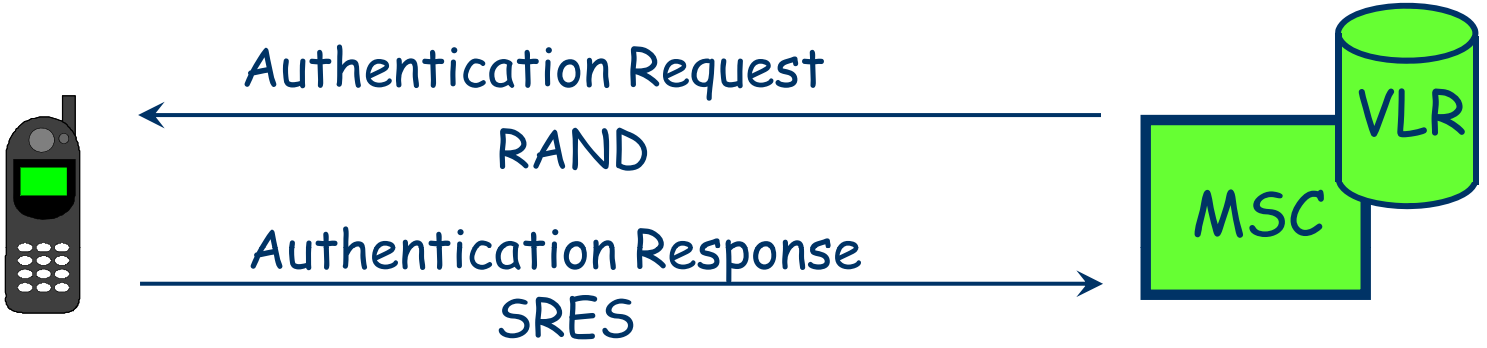
- Το Kc συμφωνείται μεταξύ MT και δικτύου πριν αρχίσει η κρυπτογράφηση
- Υπολογίζεται κατά τη διάρκεια της διαδικασίας πιστοποίησης αυθεντικότητας
- Το Kc φυλάσσεται στο SIM για να υπάρχει και μετά το switch-off. Φυλάσσεται επίσης και στο MSC/VLR.
- Αλγόριθμος A8 για τον υπολογισμό του Kc από τον RAND

Διαχείριση κλειδιών



Διαχείριση κλειδιών

Πιστοποίηση αυθεντικότητας και παραγωγή κλειδιών



Μεταφορά δεδομένων ασφαλείας