ΑΣΦΑΛΕΙΑ BLUETOOTH

ΠΑΠΑΔΟΠΟΥΛΟΥ ΧΑΡΙΚΛΕΙΑ

ΙΣΤΟΡΙΑ BLUETOOTH

Το Bluetooth είναι η νέα αναδυόμενη τεχνολογία για την ασύρματη επικοινωνία. Αναπτύχθηκε από μια ομάδα αποκαλούμενη Special Interest Group Bluetooth (SIG), η οποία ιδρύθηκε τον Φεβρουάριο του 1998 από τις:

- Ericsson
- IBM
- Intel
- Nokia και
- Toshiba

ΓΙΑΤΙ ΧΡΗΣΙΜΟΠΟΙΟΥΜΕ BLUETOOTH;

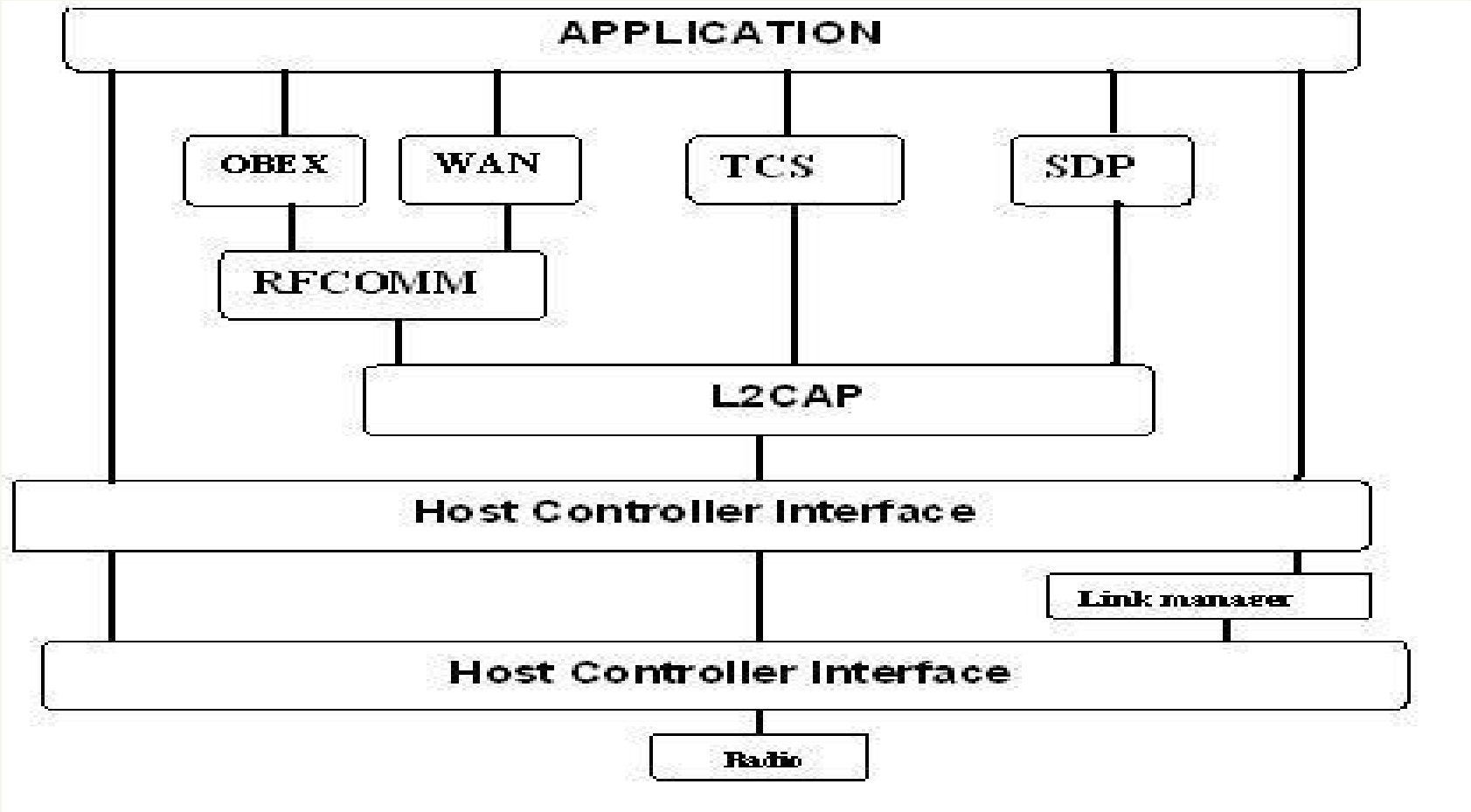
- Παρέχει τρεις λειτουργίες σε ένα τηλέφωνο
- Λειτουργεί σαν Hi-tec χαρτοφύλακας
- Παρέχει έναν αυτόματο συγχρονισμό
- Ταυτόχρονος χειρισμός δεδομένων και μετάδοσης φωνής.
- Ικανότητα για εγκατάσταση ad hoc συνδέσεις

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ

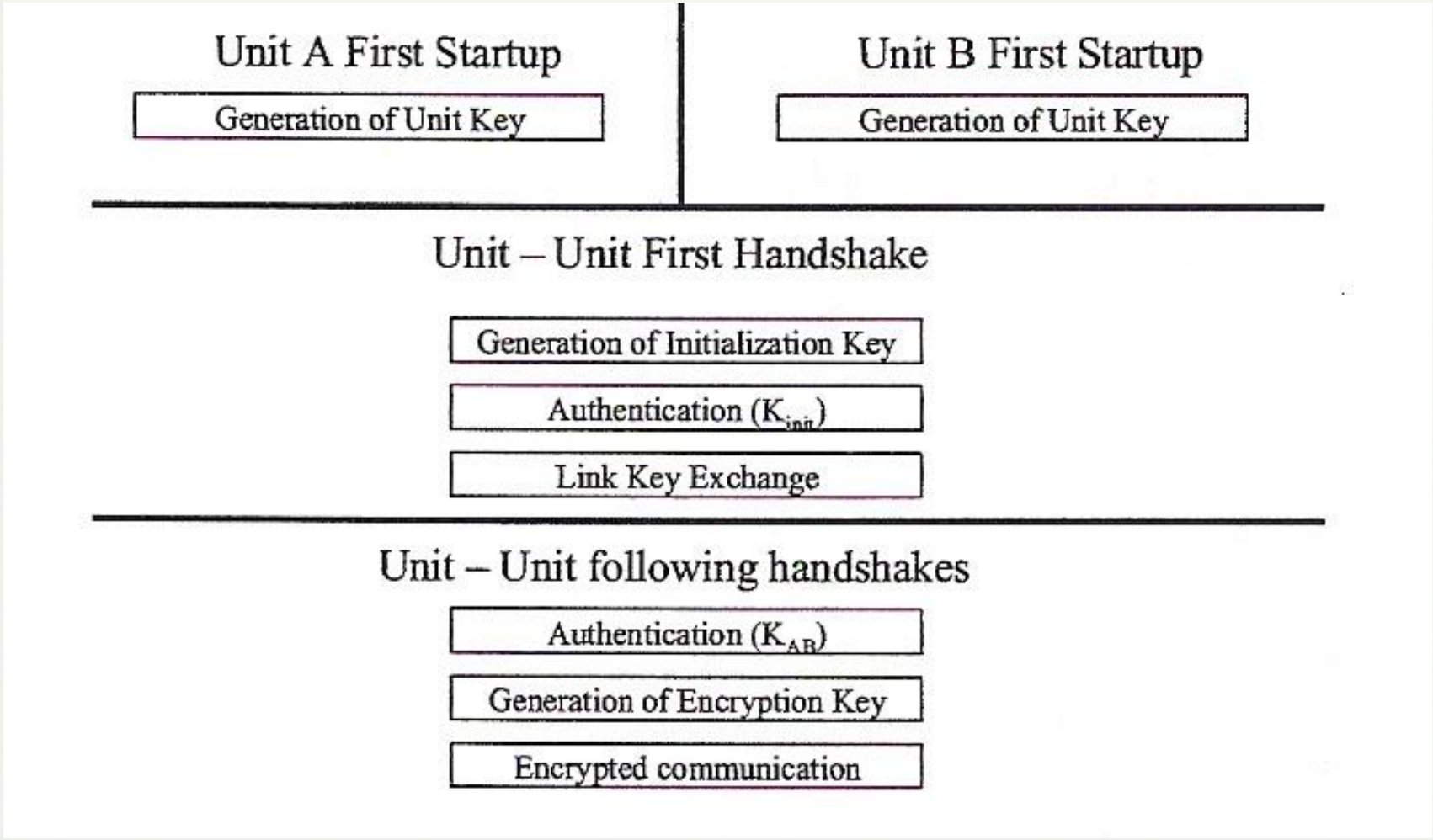
- Power level
- Ραδιοσυχνότητα(radio frequency
- Frequency Hopping Spread Spectrum

  - Χρονικός συγχρονισμός
  - Διανομή πληροφορίας
  - Επιλογή συχνότητας
  - Συχνότητα hop

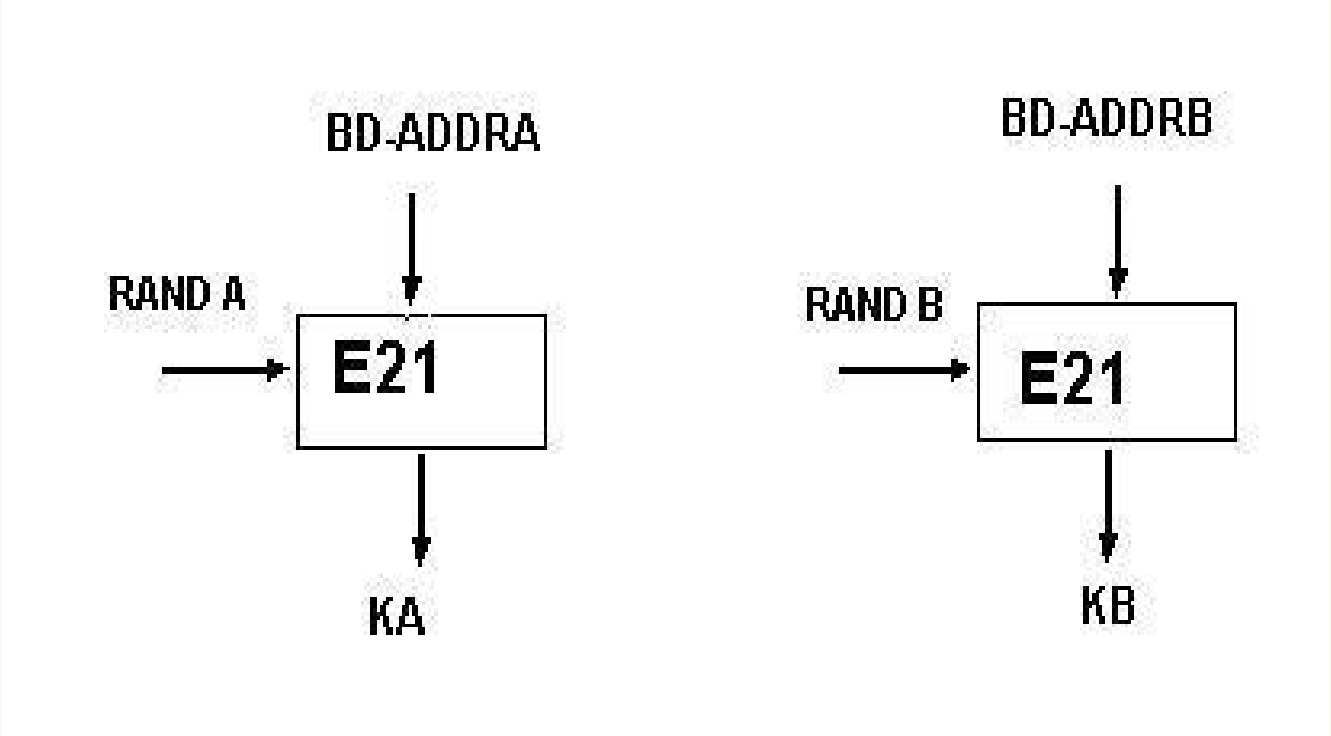
ΑΡΧΙΤΕΚΤΟΝΙΚΗ



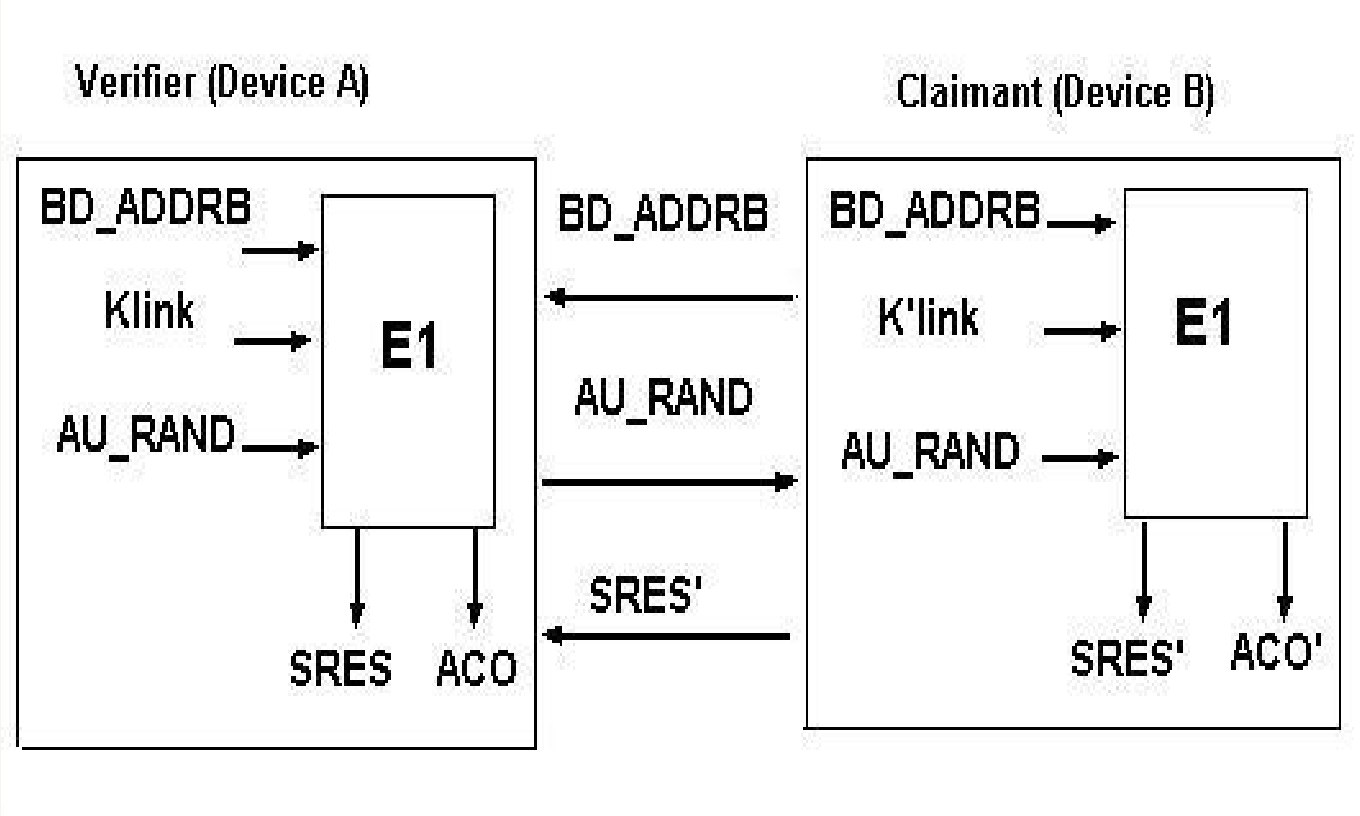
ΑΣΦΑΛΕΙΑ


Unit A First Startup
Generation of Unit Key
Unit B First Startup
Generation of Unit Key
Unit – Unit First Handshake
Generation of Initialization Key
Authentication (K_{init})
Link Key Exchange
Unit – Unit following handshakes
Authentication (K_{AB})
Generation of Encryption Key
Encrypted communication

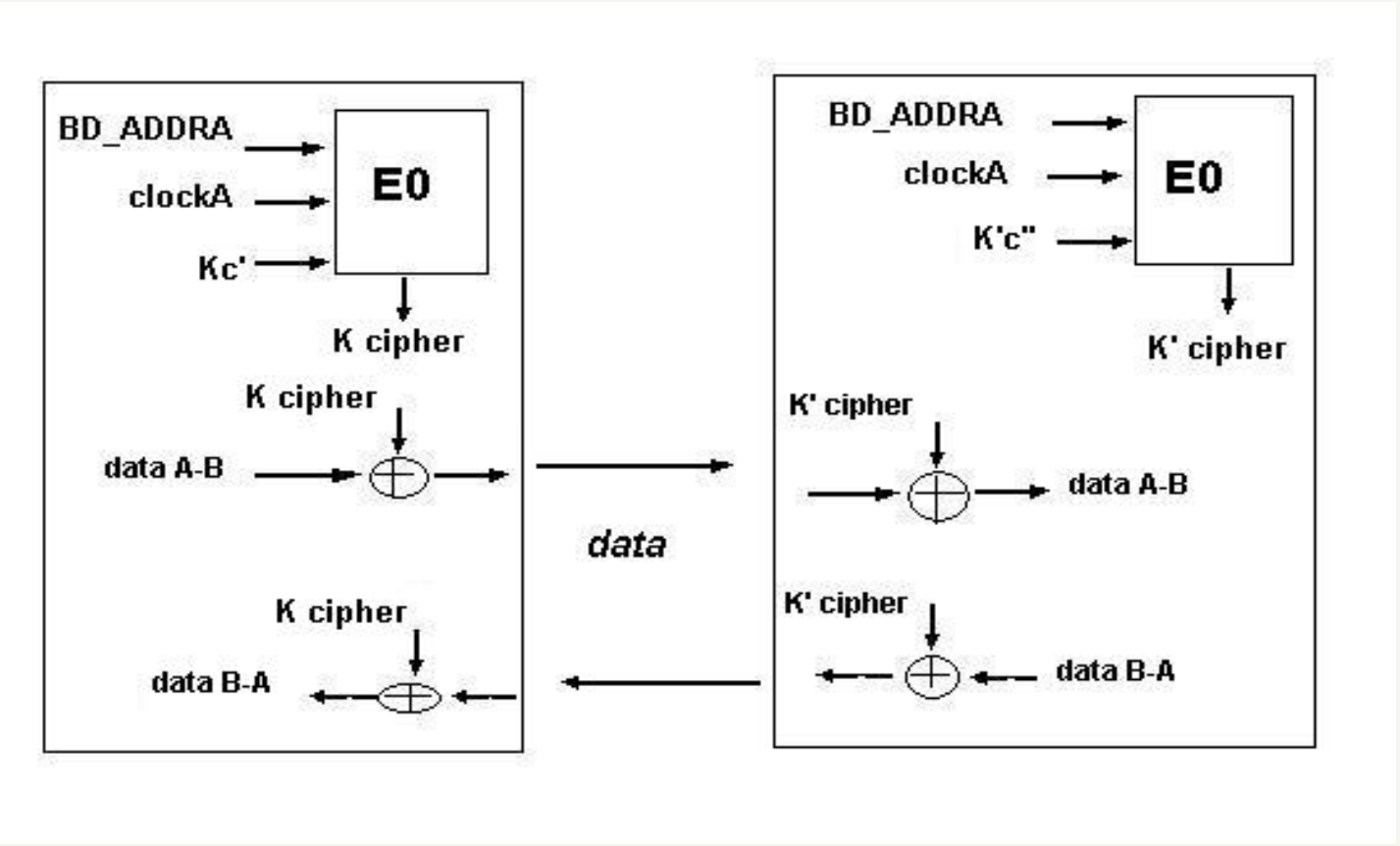
ΠΑΡΑΓΩΓΗ ΚΛΕΙΔΙΟΥ ΜΟΝΑΔΑΣ



ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ



ΚΡΥΠΤΟΓΡΑΦΗΣΗ



ΔΙΚΤΥΑ AD HOC

- Διαθεσιμότητα (availability)
- Εξουσιοδότηση και κλειδί διαχείρισης (authorization and key management)
- Εμπιστευτικότητα και ακεραιότητα (confidentiality and integrity)

ΑΔΥΝΑΜΙΕΣ ΑΣΦΑΛΕΙΑΣ

- Υποκλοπή (eavesdropping) και προσωποποίηση (impersonation)
- Location Attacks
- Στην αυθεντικοποίηση
- Στην κρυπτογράφηση

ΜΕΤΡΑ ΣΤΙΣ ΕΠΙΘΕΣΣΕΙΣ

- Μήκος PIN
- Προστασία κλειδιού μονάδας
- Ασφάλεια επιπέδου εφαρμογής (application layer security)
- Προστασία στις επιθέσεις ενδιάμεσων χρηστών
- Φυσική προστασία (physical protection).
- Κρυπτογραφημένο κείμενο (cipher)

ΣΥΓΚΡΙΣΗ BLUETOOTH ΜΕ 802.11

- Το Bluetooth χρησιμοποιεί την τεχνολογία FHSS ενώ το 802.11 χρησιμοποιεί την DSSS .
- Το Bluetooth έχει ταχύτητα 1Mbps ενώ το 802.11 έχει 2Mbps.
- Το Bluetooth έχει εμβέλεια στα 10μ ενώ το 802.11 στα 100μ.
- Το κόστος κατασκευής του 802.11 είναι πολύ υψηλότερο από αυτό του Bluetooth.

ΜΕΛΛΟΝΤΙΚΕΣ ΕΞΕΛΙΞΕΙΣ

- Γίνεται έρευνα από την ομάδα εργασίας για υψηλότερες ροές δεδομένων.
- Το AFH (Adaptive frequency hopping) μπορεί να μειώσει την απώλεια πακέτων εάν εφαρμόζεται κατάλληλα.
- Στις έξυπνες κεραίες υπάρχει η δυνατότητα να αυξηθεί η επεξεργασία σήματος ακόμη περισσότερο.

ΣΑΣ ΕΥΧΑΡΙΣΤΩ !