

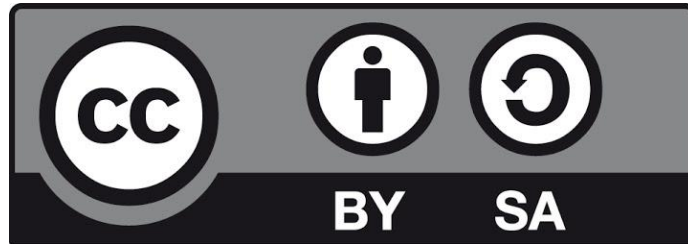
Το πρότυπο GSM

Εισηγητής: Χρήστος Δαλαμάγκας

cdalamagkas@gmail.com

Άδεια χρήσης

Το παρόν εκπαιδευτικό υλικό υπόκειται στη διεθνή άδεια χρήσης Creative Commons Attribution-ShareAlike 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>).



Το πρότυπο GSM (1991)

- Το πλέον κυρίαρχο πρότυπο στην αγορά των κινητών επικοινωνιών
- Η πρώτη προσπάθεια για ψηφιοποίηση της υποδομής κινητών επικοινωνιών
- Κρυπτογράφηση παντού (όχι και τόσο ασφαλής)
- Αρχικά, υλοποιούσε μεταγωγή κυκλώματος, στα επόμενα χρόνια πέρασε στη μεταγωγή πακέτου
- Συχνότητες: Κυρίως στις περιοχές 850, 900 MHz
- TDMA (Time Division Multiple Access): Το κινητό δεν εκπέμπει συνεχώς αλλά μία φορά κάθε 4,615 msec ή ισοδύναμα 217 φορές το δευτερόλεπτο.
- DS-1800: Εκδοχή του προτύπου GSM που χρησιμοποιεί την περιοχή γύρω στα 1800 MHz

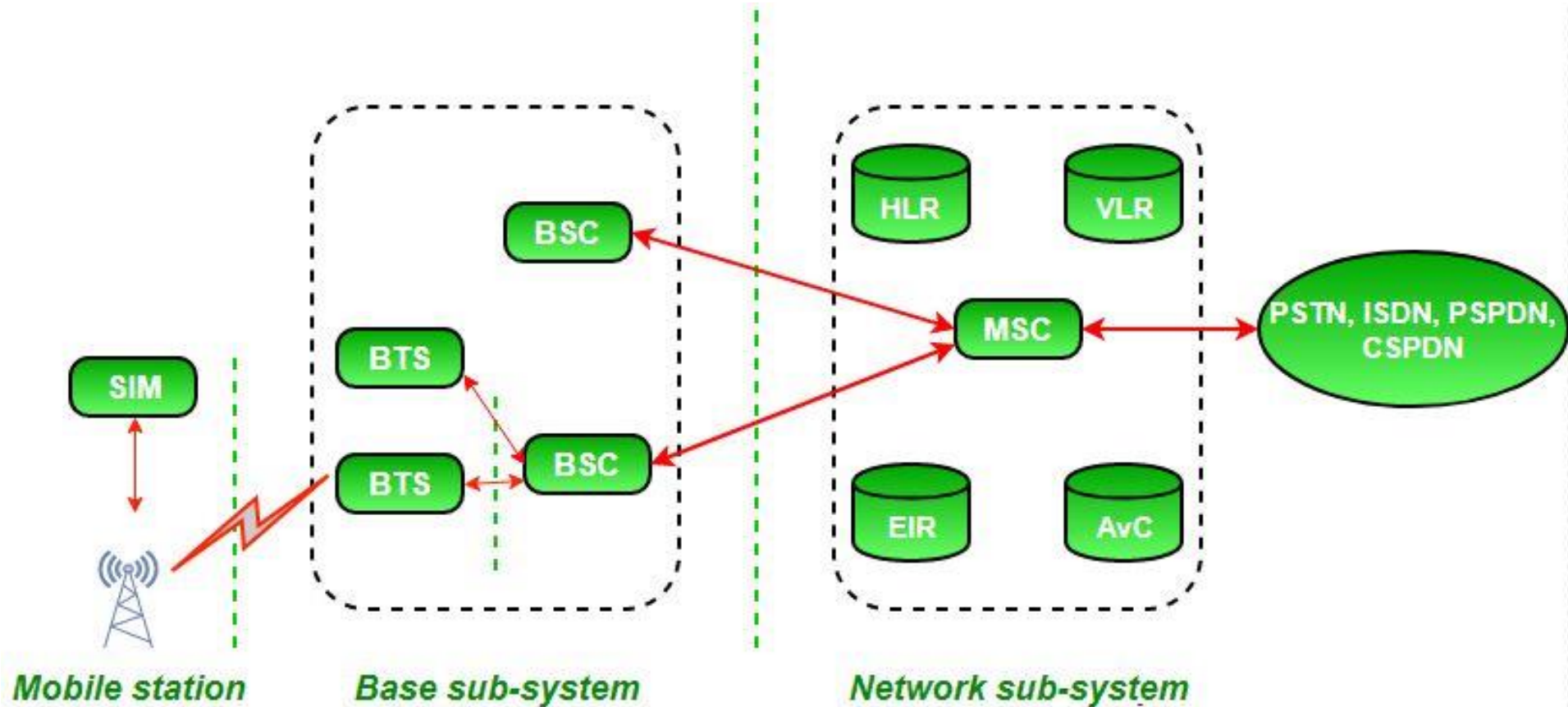
Συστατικά ενός δικτύου GSM - Σύνοψη

- Κινητό Τερματικό
- Δίκτυο πρόσβασης, το οποίο αποτελείται από Συστήματα σταθμών βάσης, κάθε ένα εκ των οποίων αποτελείται από τα εξής:
 - Ελεγκτής σταθμού βάσης
 - Σταθμός βάσης
- Δίκτυο κορμού, που αποτελείται από
 - Κέντρα μεταγωγής
 - Βάσεις δεδομένων

Public land mobile network (PLMN)

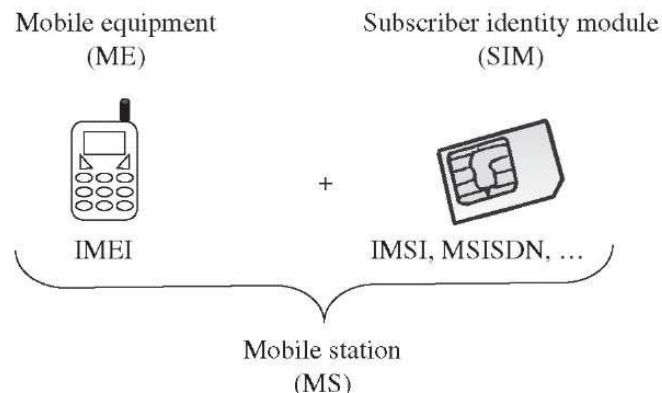
- Ένα δίκτυο GSM που διαχειρίζεται ένας πάροχος
- Κάθε πάροχος έχει το δικό του PLMN
- Ένα PLMN περιέχει τα εξής:
 - Δίκτυο Πρόσβασης
 - Δίκτυο Κορμού
 - Βάσεις Δεδομένων
- Μπορεί να θεωρηθεί κομμάτι ή επέκταση του Δημόσιου Τηλεφωνικού Δικτύου (Public Switched Telephone Network – PSTN)

Δικτυακή Δομή PLMN



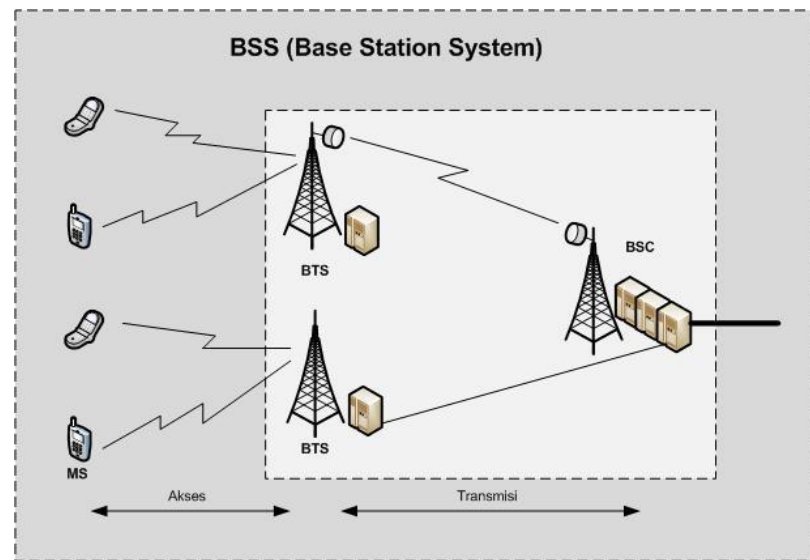
Τερματικό χρήστη

- Mobile Terminal (MT): Η φυσική συσκευή του χρήστη που αποκτά πρόσβαση στο δίκτυο
- Στη συσκευή συνδέεται μια Κάρτα ταυτότητας (Subscriber Identity Module – SIM)
 - Πιστοποιεί την ταυτότητα του συνδρομητή
 - Η φορητότητα της κάρτας κάνει εφικτή την πώληση MT από μη εξειδικευμένους πωλητές
- International Mobile Equipment Identity (**IMEI**): Ένας αριθμός, αποθηκευμένος στη συσκευή, που αποτελεί μοναδικό αναγνωριστικό μιας συσκευής
- International mobile subscriber identity (**IMSI**): Το αναγνωριστικό ενός συνδρομητή, μοναδικό σε όλα τα κυψελωτά δίκτυα

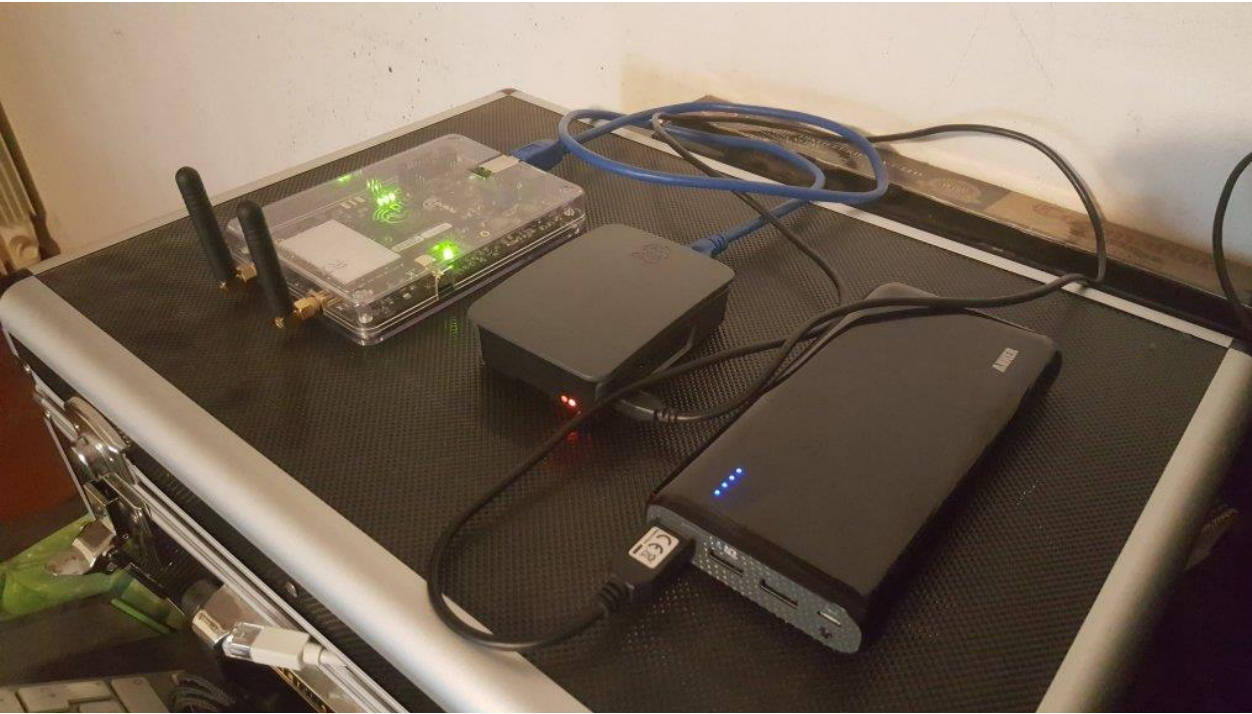


Δίκτυο Πρόσβασης

- Base Station System (BSS): Παρέχει τη δυνατότητα στους χρήστες να επικοινωνούν με το δίκτυο κορμού. Αποτελείται από:
 - Έναν BSC
 - Πολλούς BTS
- Base Transceiver Station (BTS): Κεραίες, διατάξεις εκπομπής/λήψης, βασικές λειτουργίες modem και επεξεργασίας σήματος
- Base Station Controller (BSC): Δίνει εντολές στους BTS και τα MT
 - Συνδέεται με πολλά BTS, αλλά αποκλειστικά με ένα MSC
 - Διαχειρίζεται τις διαπομπές



Base Transceiver Station



<https://www.evilssocket.net/2016/03/31/how-to-build-your-own-rogue-gsm-bts-for-fun-and-profit/>



Base Station Controller



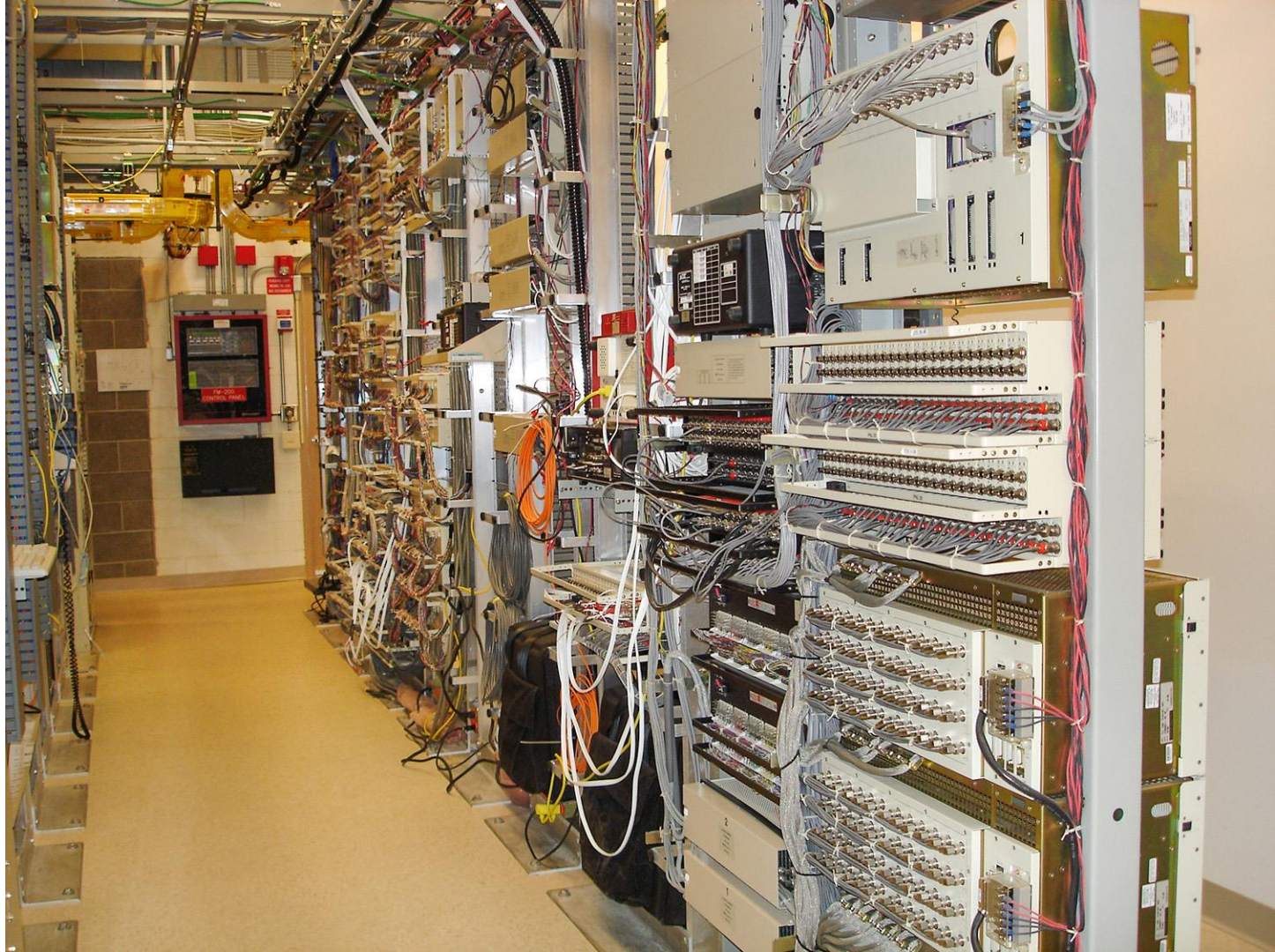
Δίκτυο Κορμού

- Mobile Switching Centre (MSC): Κυρίως ελέγχει τις κλήσεις των συνδρομητών. Πιο συγκεκριμένα:
 - Ελέγχει πολλά BSC
 - Διασυνδέει τα BSC με άλλα MSC
 - Επικοινωνεί με άλλα MSC και άλλα δίκτυα μέσω της σηματοδοσίας SS7
 - Διαχειρίζεται την κινητικότητα των χρηστών και τις διαπομπές
 - Εγκαθιδρύει/Διαχειρίζεται τις κλήσεις και τις συνδέσεις από άκρο σε άκρο (end-to-end)
- Gateway MSC: Διασυνδέει το PLMN με άλλα δίκτυα (GSM άλλου παρόχου, PSTN, DSL κλπ)

Mobile Switching Centre



Mobile Switching Centre



Δίκτυο Κορμού – Βάσεις Δεδομένων

- Home location register (HLR): Περιέχει λεπτομέρειες για κάθε συνδρομητή που είναι εξουσιοδοτημένος να χρησιμοποιεί το δίκτυο GSM
 - Κάθε πάροχος (δλδ κάθε PLMN) έχει μόνο μια **λογική** HLR
 - Κάθε MSC συνδέεται με ένα φυσικό HLR. Όλα τα φυσικά HLR έχουν τα περιεχόμενα του λογικού HLR
 - Η HLR αποθηκεύει λεπτομέρειες για κάθε κάρτα SIM που έχει εκδώσει ο πάροχος
 - Το IMSI είναι το πρωτεύον κλειδί της βάσης δεδομένων HLR
 - MSISDN: Ο τηλεφωνικός αριθμός του συνδρομητή, επίσης πρωτεύον κλειδί
 - Η HLR γνωρίζει σε ποιο MSC/VLR βρίσκεται ο κάθε συνδρομητής

Δίκτυο Κορμού – Βάσεις Δεδομένων

- Visitor Location Register (VLR): Η ΒΔ με τους χρήστες που χρησιμοποιούν το MSC
 - Γνωρίζει την ακριβή θέση του κάθε MT που χρησιμοποιεί το MSC
 - Κάθε MSC έχει τη δική του VLR
 - Οι πληροφορίες των συνδρομητών της κάθε VLR λαμβάνονται από την HLR
 - Η καταχώρηση στη VLR διαγράφεται όταν ο συνδρομητής μετακινηθεί από την περιοχή εξυπηρέτησης του MSC

Short Message Service – SMS

- Βασική υπηρεσία δεδομένων για ανταλλαγή μηνυμάτων
- Ένα μήνυμα SMS έχει μήκος 160 χαρακτήρων
- SMS Center (SMSC): Το κέντρο μεταγωγής που αναλαμβάνει την αποθήκευση, προώθηση, μετατροπή και παράδοση μηνυμάτων SMS
- Για να στείλει ένα SMS ο συνδρομητής σε έναν άλλον, χρησιμοποιεί τον τηλεφωνικό αριθμό του SMSC για να προωθήσει εκεί το μήνυμα
- Το SMSC αναλαμβάνει μετά την παράδοση του μηνύματος
- Ο τηλεφωνικός αριθμός του SMSC είναι αποθηκευμένος στην κάρτα SIM