كلمه الكاتب

اللهم مصلي وسلم علي أفضل الأنبياء والمرسلين

سيدنا محمد

عليه وعلي اله وصحبه أجمعين

أما بعد

فلا خير في من يعرف العلم ويكتمه

واتمني من الله ان يعينني علي ان اعلم الناس كل ما اعرفه وما لا اعرفه

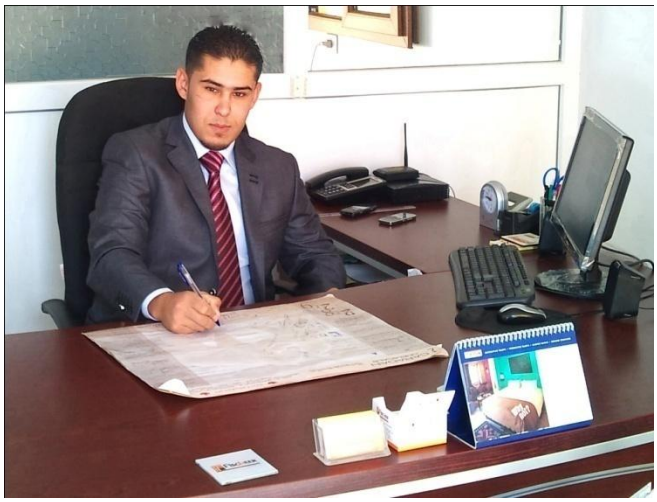
راجيا من الله ان يعتبره جهادا عنده ويجزيني عليه الأجر والثواب الجزيل

وطالبا من كل من يقرأ كتابي هذا بالدعوة الصالحة لي ولوالدي علي طول الدوام

والله علي ما أقوله شهيد

اخوكم في الله

المهندس محمد ابوحولي



السيره الذاتيه للكاتب

البيانات الشخصية

الاسم : محمد نصر علي ابوحولي

الجنسية : ليبي

مكان وتاريخ الميلاد : 1989 ,طرابلس \ ليبيا

البريد الإلكتروني : Eng.Mahammed@hotmail.com

المؤهلات العلمية

1- حاصل علي درجه الدبلوم العالي في الهندسة الكهربائية والالكترونية قسم (الاتصالات)

2- حاصل علي الرخصة الدولية لقياده الحاسوب (icdL)

3- خبره في استخدام الحاسوب والانترنت

4- خبره في لغات البرمجة التالية :

Visual Basic & VB.Net , java, Assembly , HTML

ارحب بعروض العمل واي استفسار علي

Eng.Mahammed@hotmail.com

عنوان هذا الكتاب هو محاكاة عملية الاتصال في نظام GSM

بين هاتفين وشبكتين مختلفتين

ومعرفة المسار الذي يتبعه الهاتف عند إجراء عملية الاتصال في نفس الشبكة

وفي شبكة أخري

وكذلك التطرق إلي خدمة التجوال العالمي

فبسم الله نبدأ الشرح

مقدمـــــة Introduction

منذ بدء استخدام الاتصالات الراديوية والمتخصصون في الاتصالات اللاسلكية يهدفون لتوفير خدمة هاتفية لكل مشترك على حده ، وذلك باستخدام جهاز هاتف شخصي له رقم يخص المشترك الذي يحمله ، وهذه الأجهزة تتصل بمراكز تنظيم ثابتة يتم ربطها بمراكز الهواتف داخل البلد وبالتالي بشبكة الهواتف العالمية وهذا ما يطلق عليه الاتصالات الشخصية، ويمثل الهاتف الخلوي الحلقة الأولى في طريق تحقيق الهدف.

قبل سبعينات القرن الماضي لم يكن الهاتف الخليوي ممكن التحقيق لسببين، أولهما عدم إتاحة جزء من المدى الطيفي الترددي بحيث يسمح لكل مشترك، والثاني أن الأجهزة الإلكترونية التي كان يجب أن يستخدمها المشترك لتحقيق نظام الهاتف اللاسلكي كانت ثقيلة الوزن وباهظة التكاليف.

مع بداية سبعينات القرن الماضي والتطور المذهل في تقنية وهندسة دوائر أشباه الموصلات المتكاملة تمكنت الصناعة من إنتاج أجهزة لاسلكية صغيرة الحجم والوزن وذات أداء فائق بالإضافة إلى معقولية سعرها وتمكنت هذه الأجهزة من استخدام عدد من القنوات اللاسلكية التي تعمل بنظام تعدد الوصولية بتقسيم التردد (**Frequency Division Multiple Access FDMA**) ومعنى تعدد الوصولية هو أنه يتواجد عدد كبير من المشتركين إلا أن عددا صغيرا منهم هو الذي يستطيع الكلام في اللحظة ذاتها، وبالتالي النظام لا ينشغل بهم إلا إذا طلب أحدهم المكالمة وعندئذ يعمل نظام FDMA في البحث عن قناة غير مستخدمة أو خالية ليعطيها له ويتم هذا البحث عن طريق معالج بيانات دقيقة (Microprocessor) يستخدم بروتوكول رياضي محدد لتنظيم هذه العملية.

في نظام الهاتف اللاسلكي يتم استخدام محطات إرسال ذات قدرات عالية لتمكين كل قناة من القنوات من تغطية المدينة أو المقاطعة بأكملها، وعند استخدام قناة معينة من قبل أحد المشتركين تصبح هذه القناة غير متاحة للمشتركين الآخرين داخل المدينة أو المقاطعة نفسها. ولمعالجة هذه المشكلة فقد تم تعديل هذا النظام وذلك بإشراك عدد من المشتركين في قناة واحدة في نفس الوقت باستخدام عدد من محطات الإرسال بدلا من محطة واحدة مع تصغير المساحة التي تغطيها كل محطة ويطلق على كل مساحة اسم خلية (cell) بحيث لا تتداخل هذه المساحات، وبالتالي يمكن إعادة استخدام المدى الطيفي الترددي للخلية ذاتها على قنوات كثيرة يقع كل منها في خلية منفصلة عن الخلايا الأخرى وهو ما يسمى بنظام الهاتف الخلوي

(cellule telephone system).

The Main Aspects of Cellular Network Planning
أسس تصميم الشبكة الخليوية

1 – Radio Propagation :
الطبيعة الجغرافية للمكان المدروس و الواقع السكاني كما أن الناحية الطوبولوجية و تضاريس المنطقة تلعب دوراً في تحديد المعطيات التي يتم على أساسها تصميم نظام راديوي .

2 – Frequency Regulation and Planning :
حيث توجد في أغلب البلدان هيئة مركزية للتخطيط و ذلك لتوزيع الحزم الترددية بحيث تخفض ظاهرة التداخل بين الحزم الترددية لأدنى مستوى .

3 – Modulation :
كانت الأنظمة التماثلية تستخدم نظام التعديل narrow band FM نظراً لفعاليته تجاه ظاهرة الخفوت Fading أما في الأنظمة الرقمية المستخدمة حالياً فيستخدم نظام التعديل DQPSK في أمريكا الشمالية و التي تستخدم نظام الاتصال IS-95 . بينما يستخدم في نظام GSM نظام التعديل GMSK .

4 – Antenna Design :
في المناطق النائية ذات الكثافة السكانية القليلة تستخدم الهوائيات غير الموجهة و هذا مفيد لبعض الشركات في بداية تأسيسها حيث تستفيد من خواص هذه الهوائيات لتغطية أكبر مساحة ممكنة و بأقل رأس مال . ولكن مع ازدياد الطلب على استخدام هذه الشبكات تم اعتماد أشكال أخرى لتحسين سعة النظام System Capacity مثل استبدال الهوائيات غي الموجهة بهوائيات موجهة أي إعادة تقسيم الخلايا لاستيعاب عدد أكبر من المشتركين .

5 – Transmission Planning :
يتم الاهتمام بطبيعة أو بنية الإشارة أو القنوات Channels و كيفية تحسين أداء مكونات عملية الإرسال مثل : signal power , bandwidth , capacity , stability .....

6 – Switching Exchange :
أي تطوير المقاسم الموجودة لتتلاءم مع أنظمة الاتصالات الخليوية .

7 – Teletraffic :
و يتم دراسة عدد المشتركين الذين يمكنهم استثمار الشبكة أو النظام وفقاً لدرجة معينة من الخدمات المقدمة من الشبكة و كذلك توزيع الأقنية Channels على المشتركين .

8 – Software Design :
نتيجة استخدام microprocessors في مكونات النظام و كذلك في mobile فلا بد من تصميم تطبيقات software لتشغيل هذه المكونات .

مكونات نظام GSM

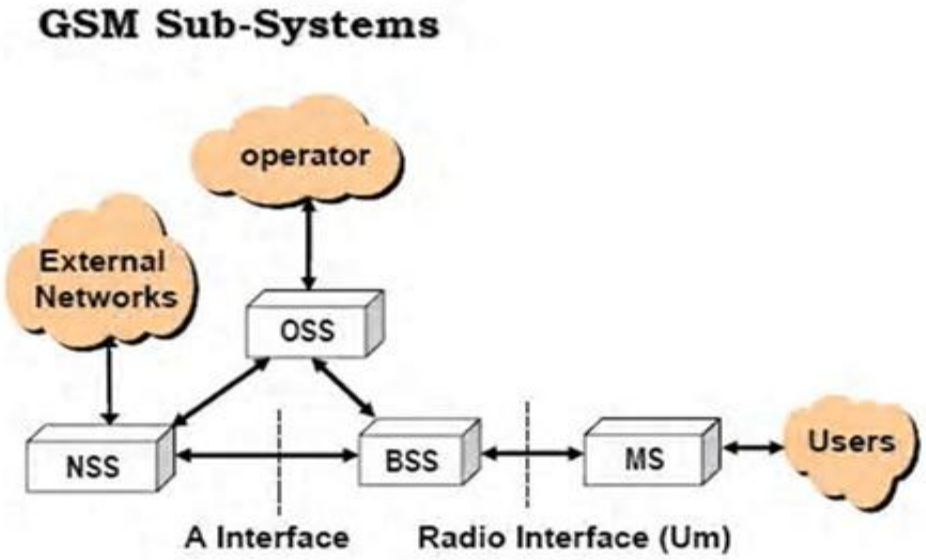
الأجزاء الأساسية المكونة لشبكة GSM

تتألف شبكة GSM من الأنظمة الفرعية التالية:

نظام محطة القاعدة Base Station Subsystem (BSS) :

نظام تبديل الشبكة Network Switching Subsystem (NSS) .

نظام التشغيل Operations Subsystem (OSS).



- المحطة المتنقلة Mobile Station (MS) تتألف من :

١. الجهاز النقال Mobile Equipment (ME).

٢. وحدة تعريف المشترك subscriber identity module (SIM).

- نظام محطة القاعدة (BSS) يتألف من الوحدات التالية :

١.محطة القاعدة Base Transceiver Station (BTS) .

٢.متحكم محطة القاعدة Base Station Controller (BSC) .

٣.وحدة التكييف ومعدّل التشفير Transcoding Rate and Adaptation Unit (TRAU) .

- نظام تبديل الشبكة (NSS) يتألف من الوحدات التالية :

١.مركز تبديل خدمات النقال Mobile Services Switching Center (MSC) .

٢. مسجل موقع محلي Home Location Register (HLR) .

٣.مسجل موقع زائر Visitor Location Register (VLR) .

٤.مسجل هوية الأجهزة Equipment Identity Register (EIR) .

تكوّن هذه العناصر مجتمعة ما يعرف بـــ **Public Land Mobile Network (PLMN)** . وهي تشكل المجموع الكلي للخلايا المخدمة من قبل مشغل شبكة واحد .

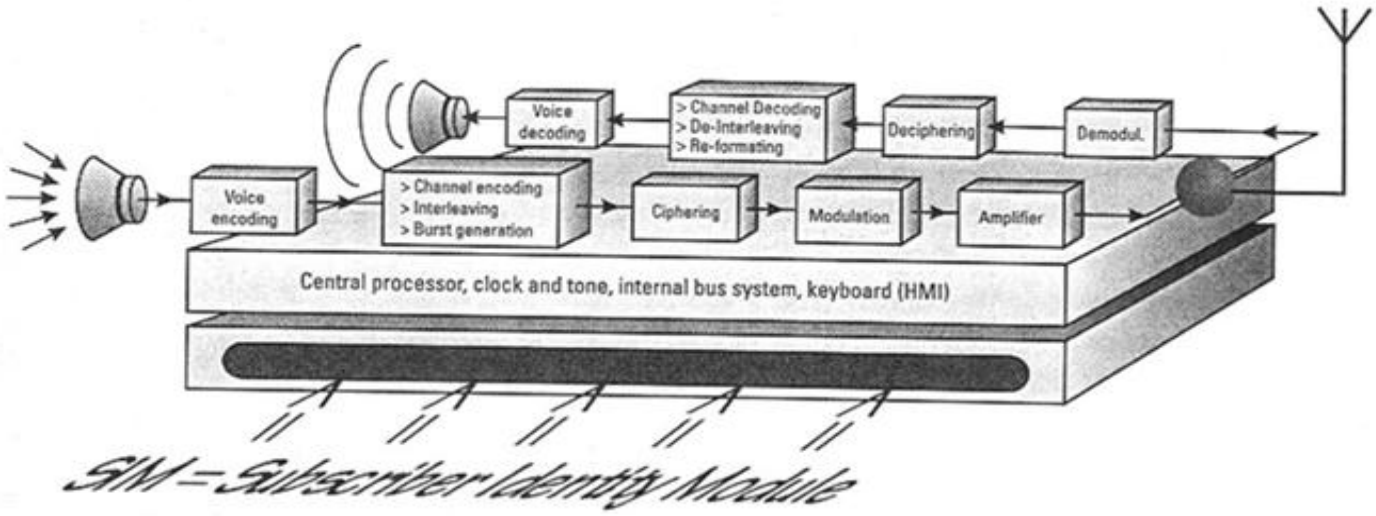
- المحطة المتنقلة Mobile Station (MS) :

تتألف المحطة MS من جزأين :

١- الجهاز النقال Mobile Equipment (ME) :

هو عبارة عن حاسب صغير يحوي على معالج وذاكرة و وحدات دخل وخرج و مودم إرسال استقبال .وعن طريق الجهاز النقال يستطيع المشترك التواصل مع الشبكة.

الشكل التالي يوضح عملية الإرسال والاستقبال في الهاتف الخلوي والتي سنأتي على ذكرها لاحقا.



تكوّن هذه العناصر مجتمعة ما يعرف بـــ **Public Land Mobile Network (PLMN)** . وهي تشكل المجموع الكلي للخلايا المخدمة من قبل مشغل شبكة واحد .

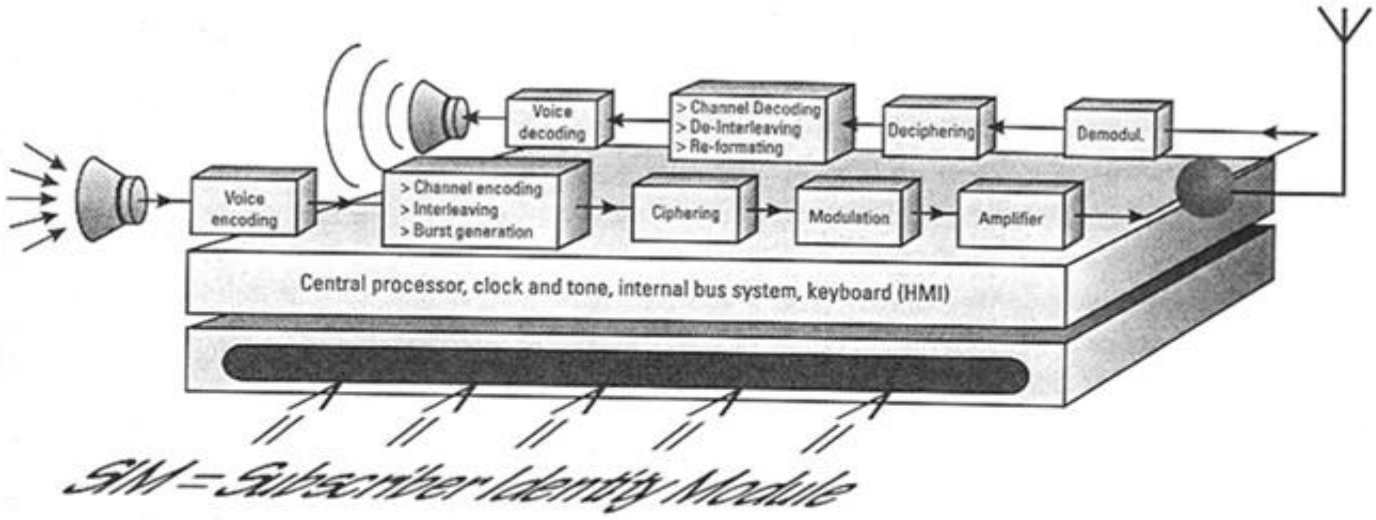
- المحطة المتنقلة Mobile Station (MS) :

تتألف المحطة MS من جزأين :

١- الجهاز النقال Mobile Equipment (ME) :

هو عبارة عن حاسب صغير يحوي على معالج وذاكرة و وحدات دخل وخرج و مودم إرسال استقبال .وعن طريق الجهاز النقال يستطيع المشترك التواصل مع الشبكة.

الشكل التالي يوضح عملية الإرسال والاستقبال في الهاتف الخلوي والتي سنأتي على ذكرها لاحقا.

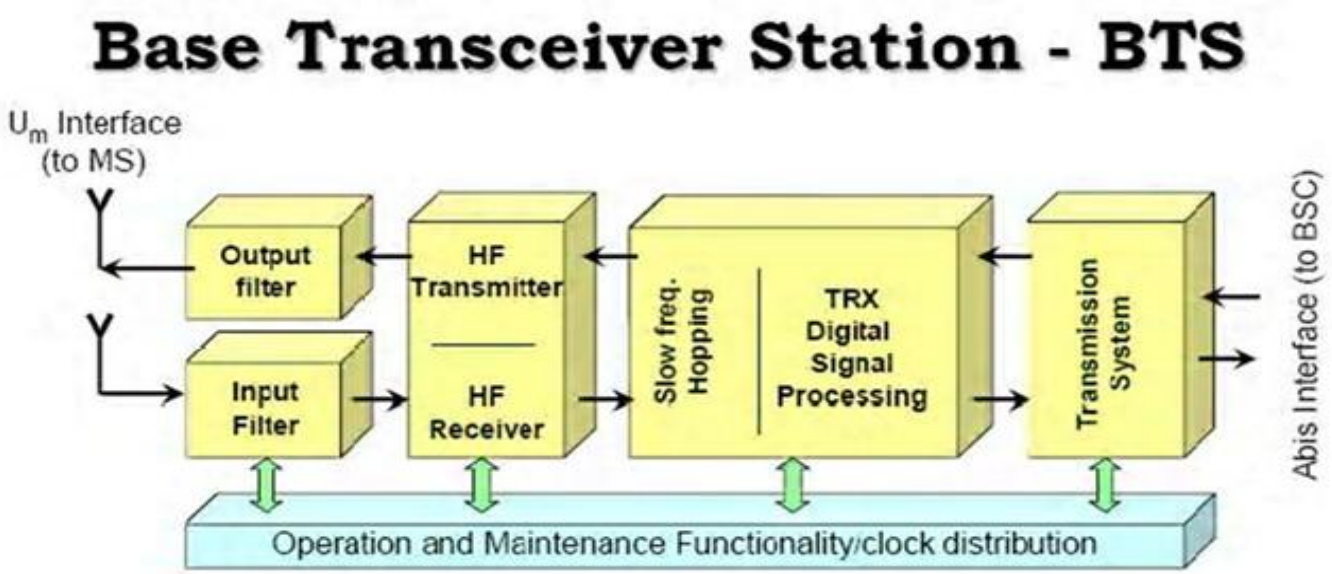


- نظام محطة القاعدة Base Station Subsystem (BSS) :

تتألف BSS من :

١- محطة قاعدة واحدة (BTS) أو أكثر من واحدة :

إن BTS تقدم اتصال فيزيائي ما بين المحطات المتنقلة و الشبكة حيث تقوم BTS بإرسال البيانات للهاتف الخلوي واستقبالها منه وذلك عن طريق Air-interface. تتصل BTS مع BSC بواسطة Abis-interface الشكل التالي عبارة عن مخطط صندوقي لتدفق الإشارة في BTS مع TRX واحدة .



تتألف BTS من الوحدات التالية :

١) وحدة الإرسال والاستقبال Transmitter/Receiver Module (TRX) :

تعتبر وحدة الإرسال والاستقبال الجزء الأكثر أهمية في BTS .

تتألف هذه الوحدة من :

قسم الترددات المنخفضة لمعالجة الإشارة الرقمية .

قسم الترددات العالية من أجل التعديل GMSK وفك التعديل .

وكلا هذين القسمين يكونان موصولين بواسطة وحدة قفز ترددية مدمجة أو منفصلة .

٢) وحدة العمليات والمحافظة Operation and Maintenance Module (O&M) :

تتألف هذه الوحدة على الأقل من وحدة مركزية واحدة والتي تدير الأقسام الأخرى لـ BTS .وتبعا لوظائف هذه الوحدة فهي تتصل بشكل مباشر مع BSC . هذا الاتصال المباشر يسمح لوحدة O&M بأن تعالج الأوامر القادمة من BSC وَ MSC مباشرة وتقرر النتائج .

الوحدة المركزية تحتوي على برمجيات عمليات TRXs مما يسمح بإعادة تحميلها عند الحاجة إلى ذلك .

٣) وحدة إشارة ساعة Clock Module :

تعتبر هذه الوحدة جزء من الوحدة O&M . يتطلب أن تكون كل وحدات الإرسال والاستقبال لـــBTS تستخدم نفس إشارة الساعة وذلك لإنجاز العمليات بشكل دقيق ويجب أن تكون إشارة الساعة ذات دقة عالية .

٤) مرشحات دخل وخرج Input and Output Filters :

لهذه المرشحات أهمية في تحديد عرض حزمة الإشارات المرسلة والمستقبلة .

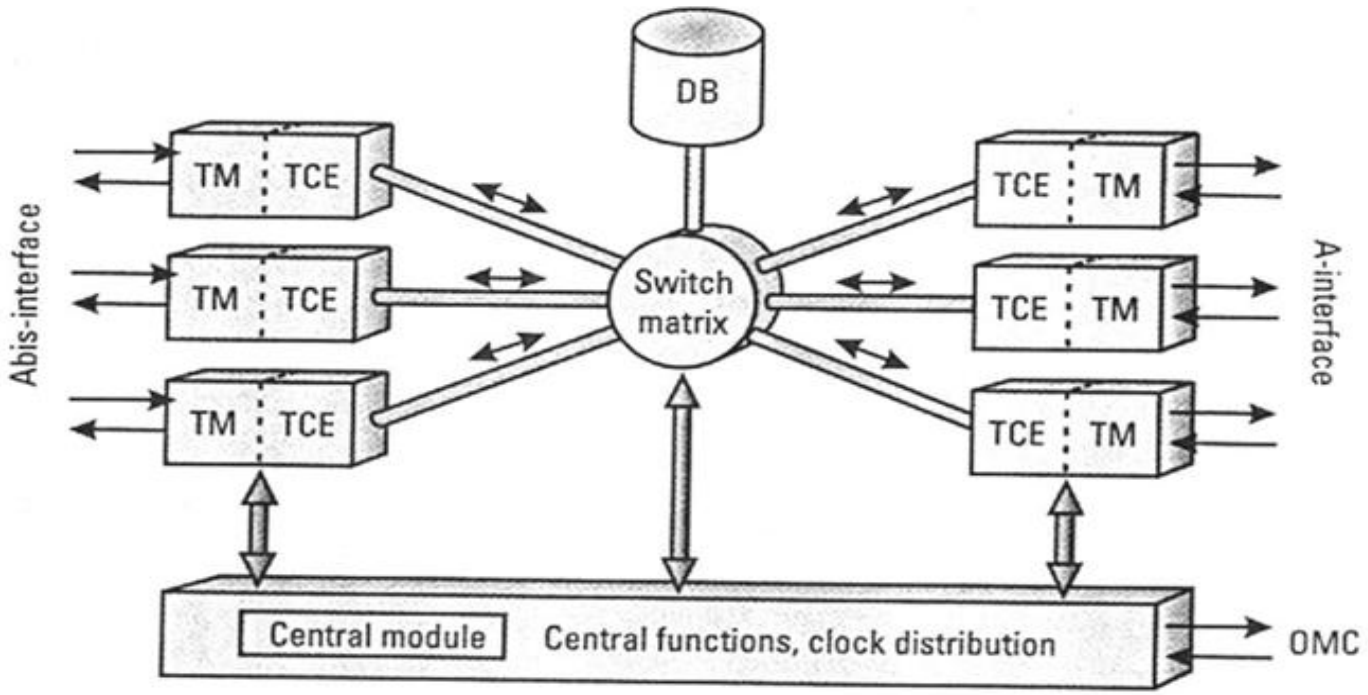
تعمل هذه المرشحات مع كل ترددات الأنظمة GSM900,DCS1800,PCS1900 ويتم التحكم بوضعية هذه المرشحات تبعاً لتغير التردد بواسطة وحدة O&M .

٢- متحكم محطة القاعدة Base Station Controller (BSC) :

تعتبر BSC مركز BSS (Base Station Sub-System)

تستطيع BSC أن تتخاطب مع عدة BTS .

الشكل التالي عبارة عن المخطط الصندوقي لـ BSC :



تتألف BSC من الوحدات التالية:

١) مصفوفة التبديل Switch Matrix :

مهمة هذا الجزء هو تبديل قنوات النقل (إشارات A-interface القادمة من MSC) إلى قنوات النقل Abis-interface الصحيحة ، والعكس .

أي أن هذه المصفوفة تراعي وظيفة التبديل إضافة إلى إمكانية استخدامها كممر تحكم داخلي .

٢) عناصر التحكم الطرفية لـــ Abis-interface :

إن الاتصال مع BTS تتم بواسطة عناصر التحكم الطرفية لـــ Abis-interface والتي يصطلح على تسميتها (Abis TCEs) .

هذه العناصر تكون مستقلة عن الوحدة المركزية لـــ BSC .

عدد عناصر Abis TCEs التي تحتويها BSC تعتمد على عدد BTS المرتبطة معها وكذلك على نوعية تصميم النظام .

يمكن أن نذكر هنا الوظائف الرئيسية لـ Abis TCES :

إنشاء ارتباطات مع BTS النظيرة (تدعى ارتباطات LAPD) .

تحويل بيانات الإشارات والحمولة الصافية .

تكون مسؤولة عن إدارة الموارد الراديوية لـ BTS .

٣) عناصر التحكم الطرفية لـــ A-interface :

إن الاتصال مع MSC تتم بواسطة عناصر التحكم الطرفية A-interface والتي يصطلح على تسميتها (A-TCES) .

بالرغم من أن BSC تتصل مع MSC واحدة فإننا نجد العديد من A-TCES حيث يتم عن طرق A-interface نقل الجزء الرئيسي لبيانات الإشارات والحمولة الصافية لـــ BSS.

٤) قاعدة بيانات Data Base (DB) :

تحتوي BSC على قاعدة بيانات ضخمة التي تلعب دورا في إدارة BSS كاملة .

قاعدة بيانات BSC تحتوي على برمجيات عمليات BTS كاملة وذلك للاتصال مع BTS . كما إنها تحتوي على كل المعلومات الخاصة بـــ BSS مثل الترددات المخصصة لها .

٥) وحدة مركزية Central module :

إن أحد الوظائف الرئيسة لهذه الوحدة هو أن تقرر إذا كان handover يجب أن يحدث أم لا بالإضافة إلى التحكم بالطاقة . هذه الوحدة تتصل بشكل مباشر مع O&M.

٣- وحدة التكييف ومعدّل التشفير Transcoding Rate and Adaptation Unit (TRAU):

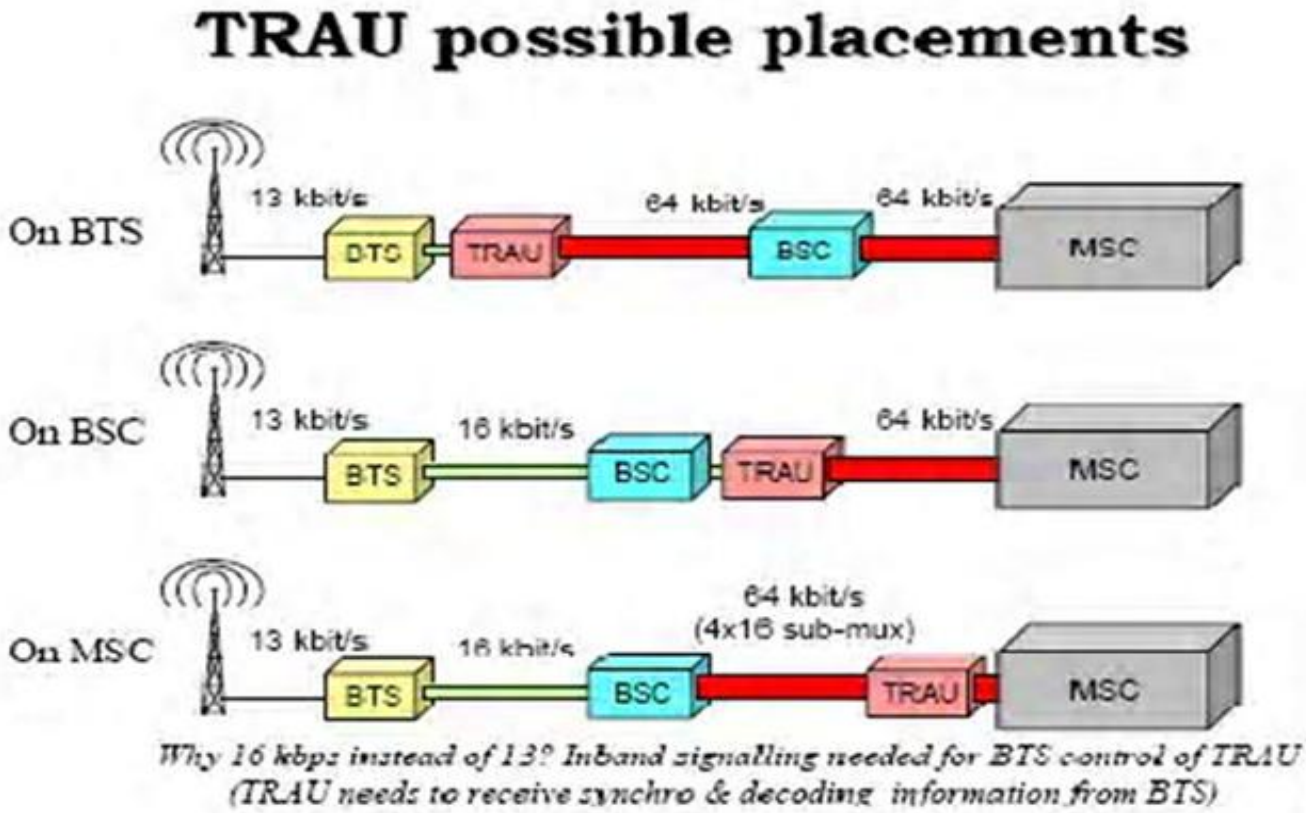
يتم في هذه الوحدة تحويل الكلام الرقمي PSTN PCM إلى كلام مرمز GSM RELP والعكس بالعكس وذلك بعملية ضغط وفك ضغط للمعلومات ما بين MS وَ TRAU .

يوجد عدة نماذج لإجراء عملية الضغط :

half rate channel : يتم ضغط الكلام من 64 kbps إلى 8 kbps . ويكون معدل البت لإشارة الكلام مساويا 6.5 kbps ، ومعدل البت لإشارة معلومات التحكم لـ TRAU مساويا 1.5 kbps .وفي المقابل وبعملية معاكسة يحول الكلام المرمز بسرعة 8 kbps إلى تقنية PCM بسرعة 64 kbps .

Full rate channel : يتم ضغط الكلام من 64 kbps إلى 16 kbps . ويكون معدل البت لإشارة الكلام مساويا 13 kbps ، ومعدل البت لإشارة معلومات التحكم لـ TRAU مساويا 3 kbps . وفي المقابل وبعملية معاكسة يحول الكلام المرمز بسرعة 16 kbps إلى تقنية PCM بسرعة 64 kbps .

الشكل التالي يوضح نماذج متاحة لتوضع TRAU:

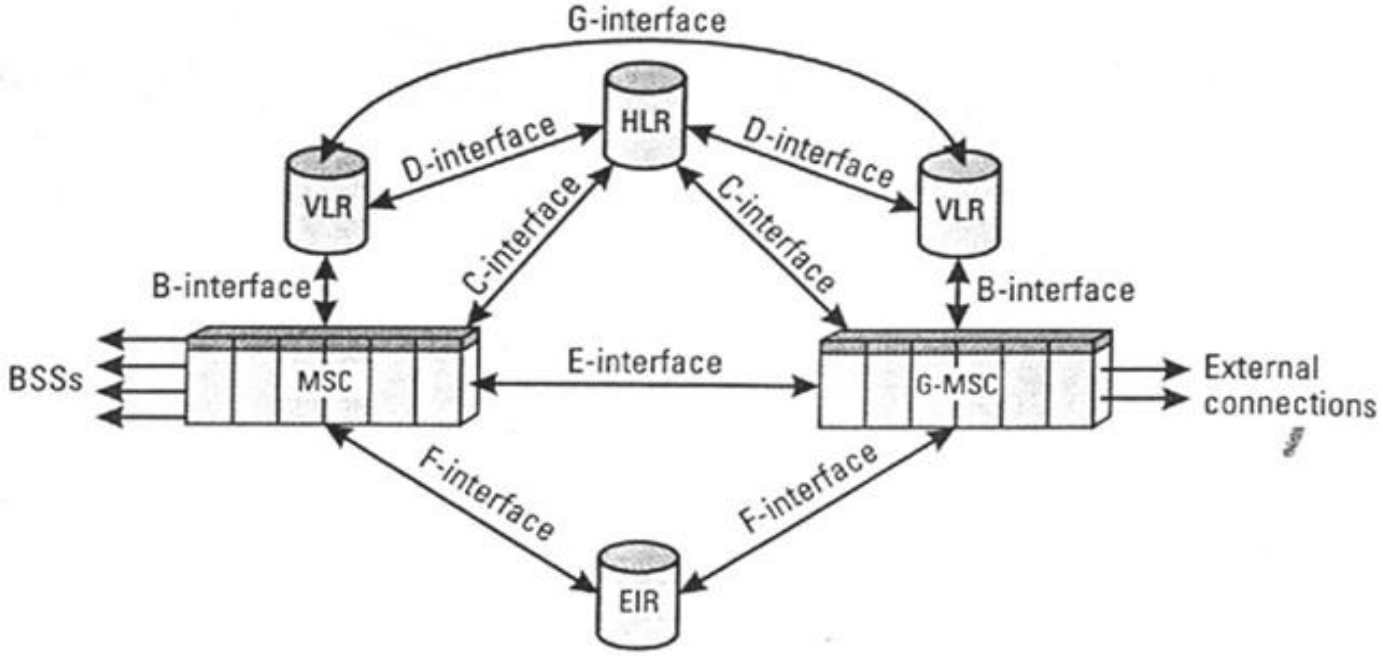


- نظام تبديل الشبكة (NSS) Network Switching Subsystem :

إن نظام تبديل الشبكة (network switching system) يلعب القسم المركزي لأي شبكة متحركة . حيث إن عناصر الشبكة المختلفة لـ NSS تكون مسؤولة عن وظائف التحكم وتحتوي على قاعدة بيانات تكون مطلوبة لتأسيس كل عمليات الاتصال .

إن عناصر النظام NSS ترتبط مع بعضها البعض بشكل مباشر أو غير مباشر .

التركيب البنيوي لـــ NSS أكثر مرونة من التركيب الهرمي لـــ BSS . إن عدة MSC يمكن لها أن تستخدم VLR واحدة . ويكون اختيار EIR اختياري .



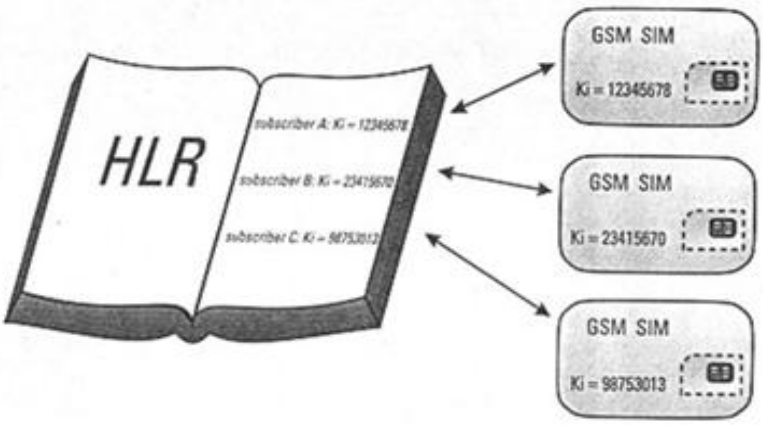
وفيما يلي شرح مبسط عن كل عنصر من عناصر NSS :

١- Home location register (HLR)and Authentication center (AUC) :

تمثل HLR قاعدة بيانات مرجعية للمشترك حيث تكون قادرة على إدارة بيانات مئات الألوف من المشتركين، تحتوي HLRعلى ما يلي :

- معلومات عن هوية المشترك (IMSI) .
- رقم هاتف المشترك(MSISDN).
- معلومات عن خدمات المشترك .
- معلومات عن VLR التي تخدم المشترك حاليا.

تحتوي وحدة AUC على معلومات الوثوقية والتشفير(الخوارزمية A3 ، الخوارزمية A8 ، مفتاح التوثيق Ki ، مفتاح التشفير Kc ، الرقم العشوائي RAND ، الاستجابة المؤشرة SRES) ، حيث تقوم بإجراء عمليات حسابية عليها وتقدمها إلى HLR. كالعامل Ki حيث يعرّف فقط في بطاقة SIM وَHLR فقط .



يعتبر مركز التوثيق AUC كقسم متكامل لـ HLR ،وتسمى الوصلة ما بين HLR وَ AUC بـ H-interface.
يحتوي AUC على معلومات الوثوقية والتشفير حيث يقوم بتقديمها إلى HLR وبالتالي يتم التأكد من الوثيقة وشرعية المشترك .

٢- Visitor Location register (VLR) :

إن VLR عبارة عن قاعدة بيانات تحتوي على معلومات مؤقتة عن المشتركين المتواجدين حالياً في منطقة MSC.

يمكن لـ VLR أن تخدم عدة MSC في حين MSC تستخدم دائماً VLR واحدة .

عند نقل مشترك من MSC إلى MSC أخرى ، فإن VLR المتصلة مع MSC – التي انتقل إليها المشترك – سوف تتطلب بيانات عن المحطة المتنقلة من HLR بمعنى تنتقل البيانات من VLR القديمة إلى VLR الجديدة، وعندها يستطيع المشترك إجراء عملية الاتصال دون الحاجة إلى HLR .

تحتوي VLR على ما يلي :

معلومات عن هوية المشترك (IMSI) .

معلومات عن هوية المشترك المؤقتة (TMSI) .

معلومات عن حالة المشترك (busy-free-no answer etc) .

معلومات عن هوية منطقة التوضع (LAI) .

معلومات عن رقم تجوال المحطة المتنقلة (MSRN) .

معلومات التوثيق والتشفير (RAND, SRES, KC, CKSN) .

معلومات عن الخدمات الإضافية .

تكون VLR مسئولة عن إدارة بيانات المشترك الحالية وفي منطقة خدمة MSC،وبالتالي فإن VLRيستخدم لكي يدعمHLR ويقلل الحمل الواقع عليه.

٣- Mobile Services Switching Center (MSC) :

يتصل عدد كبير من BSC إلى MSC بواسطة A-interface ، MSC تشبه كثيراً المقاسم حيث تقوم بوظائف التبديل ما بين المحطات المتنقلة.وبالتالي فإن الوظيفة الرئيسة لـ MSC هي توجيه المكالمات الواردة أو الخارجة إلى جهتها الصحيحة .تقوم MSC أيضاً بالتحكم بـ inter-MSC handovers .

عندما يوصل MSC مع شبكات أخرى فإنه يزود بوصلة تدعى بوابة عبور (Gateway) ، وعندئذ يشار إلى MSC بـ GMSC . وهذا يعني أن شبكة الهاتف العامة Public Switched Telephone Network (PSTN) يمكنها الوصول إلى الشبكة PLMN وبالتالي إمكانية الاتصال ما بين مشترك خلوي ومشترك PSTN بواسطة (GMSC) إضافة إلى إمكانية الاتصال ما بين مشترك خلوي وأي شبكة أخرى .

٤- Equipment Identity Register (EIR) :

تعتبر EIR قاعدة بيانات تحتوي على قوائم من تعاريف أجهزة الخلوي والتي يطلق عليها :

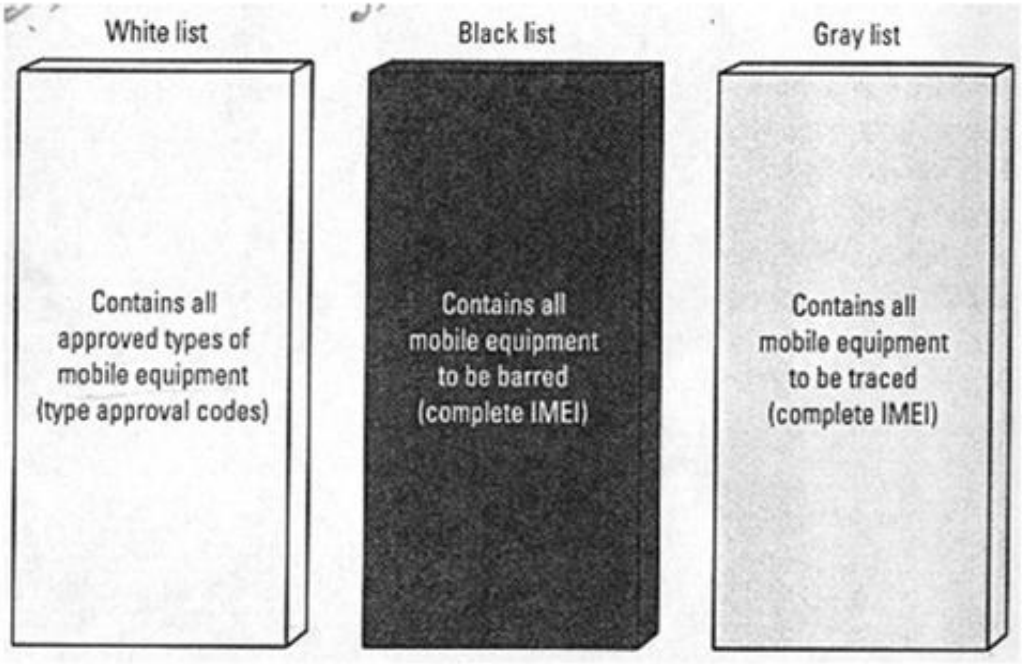
IMEI (International mobile equipment Identity) . إن IMEI هو عبارة عن رقم متسلسل ، وهو رقم لا يمكن لجهاز خلوي أن يتشابه فيه مع جهاز آخر ، و لا يمكن تغييره .

يمكن أن نقسم قاعدة بيانات EIR إلى ثلاث قوائم :

القائمة البيضاء : عبارة عن قائمة بالأنواع الصحيحة لأجهزة الخلوي والتي يمكن لها أن تعمل .

القائمة السوداء أو المحرمة :عبارة عن قائمة بأجهزة الخلوي المسروقة أو الممنوعة لأسباب تقنية .

القائمة الرمادية عبارة عن قائمة بأجهزة الخلوي المشكوك بها ، أو الأجهزة التي بها بعض المشاكل كأخطاء في البرمجة Software .



- نظام التشغيل والصيانة Operations and maintenance system :

يقوم هذا النظام بشكل عام بإدارة شبكة GSM يتكون من قسمين :

Network Management Center (NMC) : تكون مسؤولة عن إدارة الشبكة ككل ، ويوجد NMC واحدة للشبكة .

Operations and Maintenance Center (OMC) : تكون مسئولة عن إدارة شبكة PLMN في منطقة محددة ، وبالتالي يمكن أن يوجد OMCواحدة أو أكثر في الشبكة .

OMC تعتبر كقاعدة بيانات للشبكة ولديها القدرة على إدارة و مراقبة الشبكة .

التسلسل الهرمي لنظام GSM

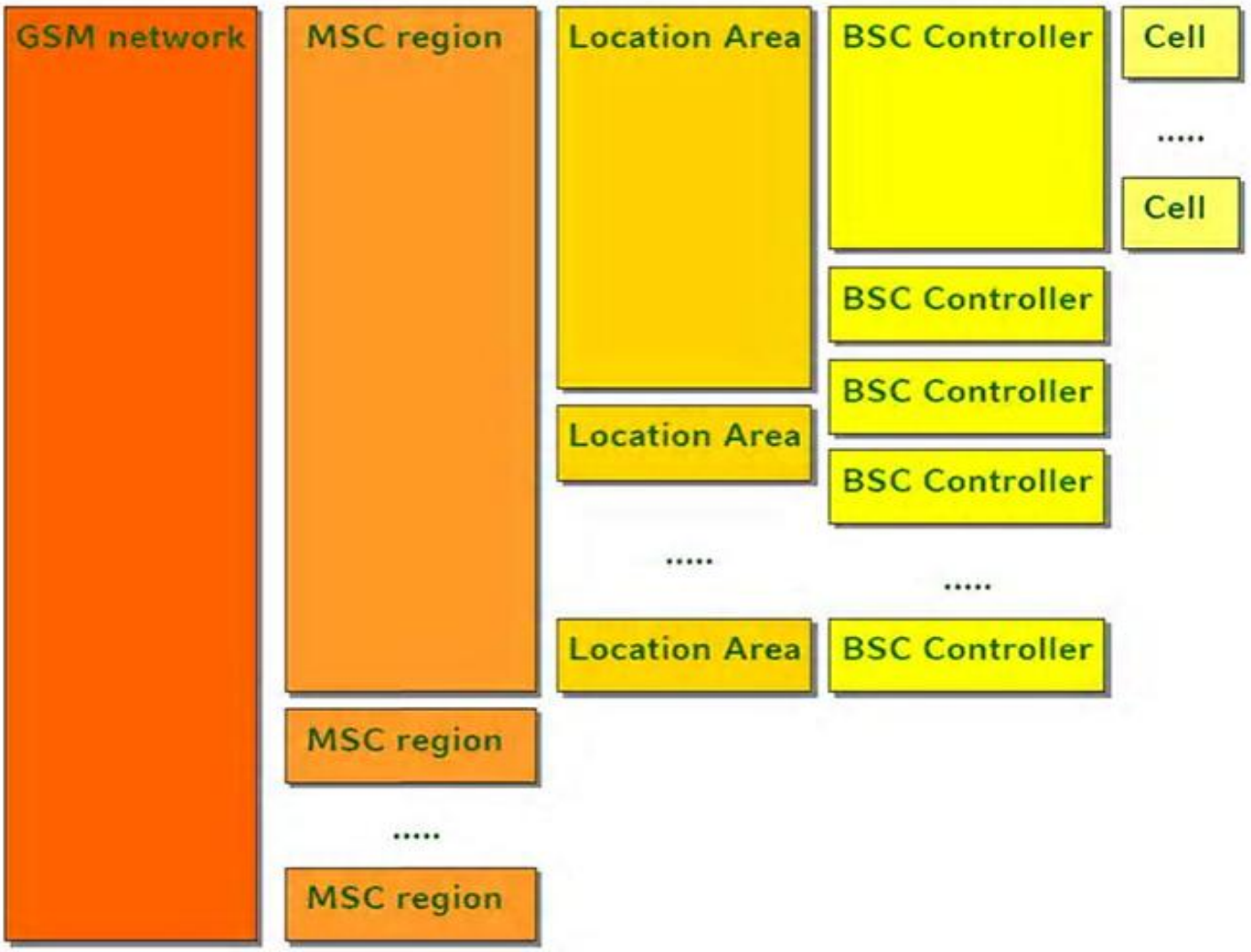
تتألف شبكة GSM على الأقل من منطقة إدارية واحدة والتي يخصص لها مركز تبديل خدمات (MSC) واحد.

المنطقة الإدارية تتألف على الأقل من منطقة توضع واحدة Location Area (LA).

منطقة التوضع Location Area (LA) تتألف بدورها من عدة مجموعات من الخلايا Cells .

مجموعة الخلايا يخصص لها متحكم محطة القاعدة Base Station Controller (BSC) .

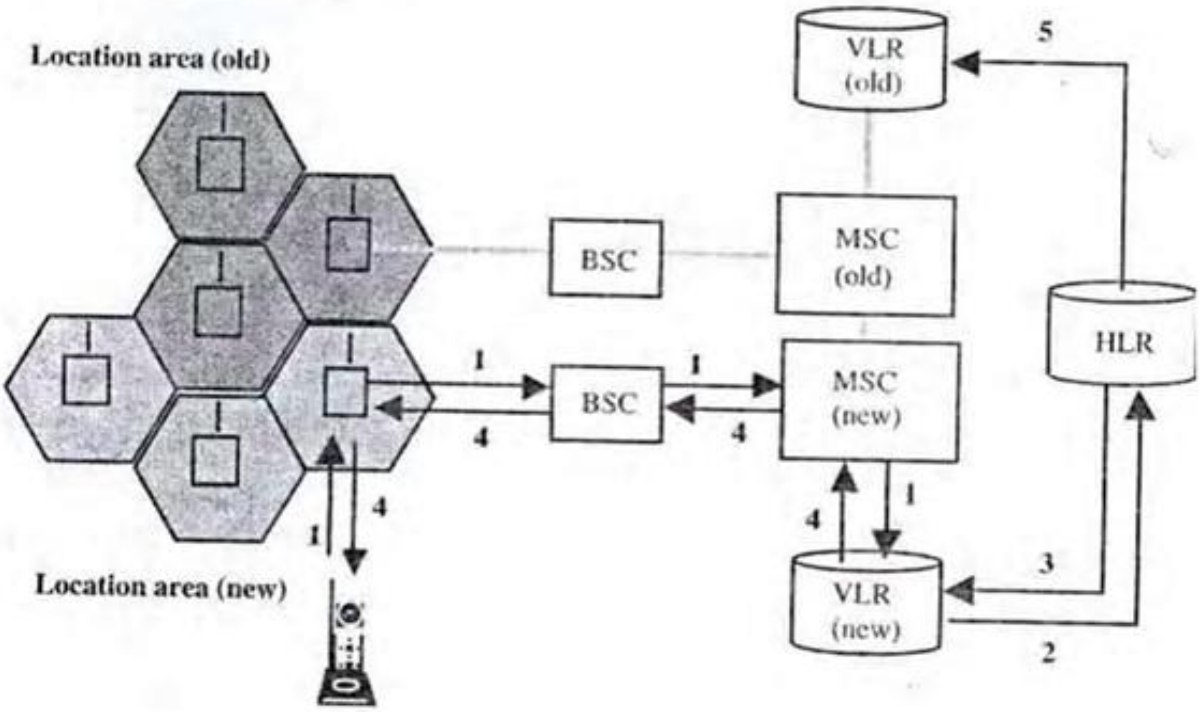
لكل LA يوجد على الأقل BSC ، ولكن الخلايا التابعة لـ BSC يمكن أن يكون لها مناطق توضع مختلفة LAs.



مراحل سير المكالمة في نظام الـ GSM

تحديث الموقع Location Updating :

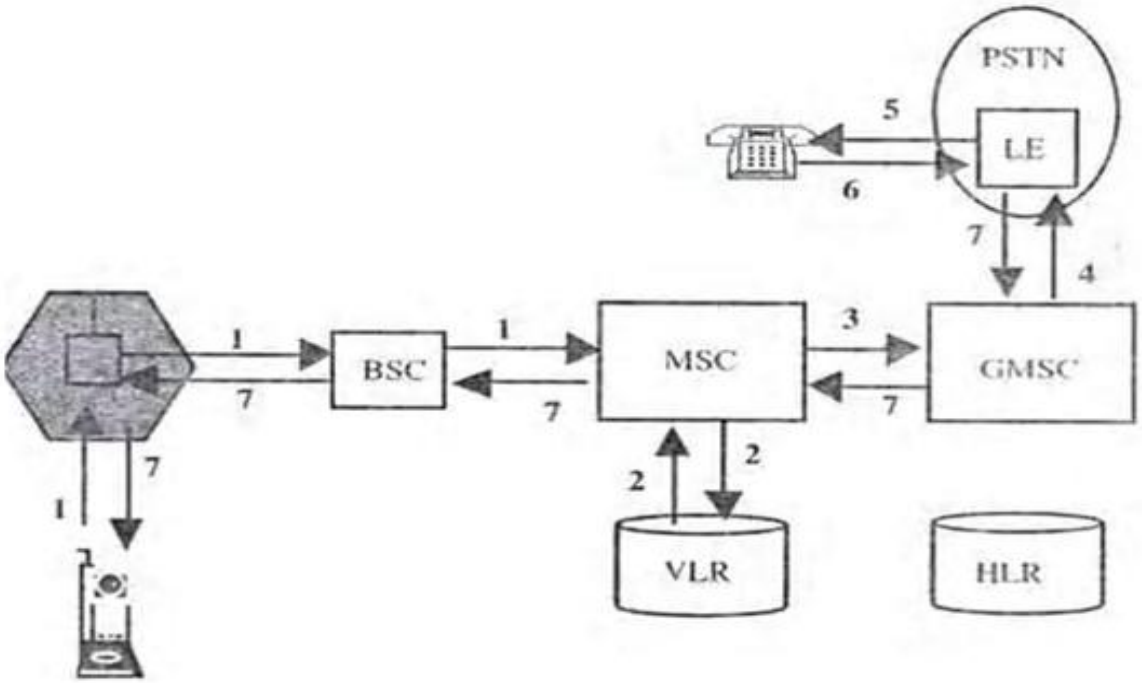
عندما ينتقل الموبايل من منطقة خدمة Service Area لأخرى فإن الشبكة يجب أن تعلم بذلك حتى تستطيع تحويل المكالمات الواردة لهذا المشترك إلى منطقة الخدمة الجديدة ، و هذا يتحقق من خلال عملية تحديث الموقع Location Updating و ذلك عندما يكون الـ MS بحالة Active .
منطقة الخدمة هي عبارة عن مجموعة خلايا متجاورة تعرف من خلال الرقم Location Area Identity (LAI) . و تتم هذه العملية وفق التسلسل التالي :



1- ترسل الـ MS طلب تحديث للموقع إلى الـ VLR الجديدة عبر الـ BSS و MSC .
2 - ترسل الـ VLR طلب تحديث الموقع إلى الـ HLR يتضمن عنوان الـ VLR الجديدة و الرقم IMSI للموبايل ، فيقوم الـ HLR بتحديث البيانات المتعلقة بهذا المشترك . إن عملية التحديث هذه لن تكون ضرورية إذا كانت منطقة الخدمة الجديدة تخدم من قبل نفس الـ VLR التي تخدم منطقة الخدمة القديمة .
3 - ثم يتم نقل البيانات الجديدة المتعلقة بهذا المشترك إلى الـ VLR الجديدة .
4 - يتم إرسال رسالة إجابة إلى الـ MS بنجاح عملية التحديث .
5 - تطلب الـ HLR من الـ VLR القديمة مسح البيانات المتعلقة بذلك المشترك .

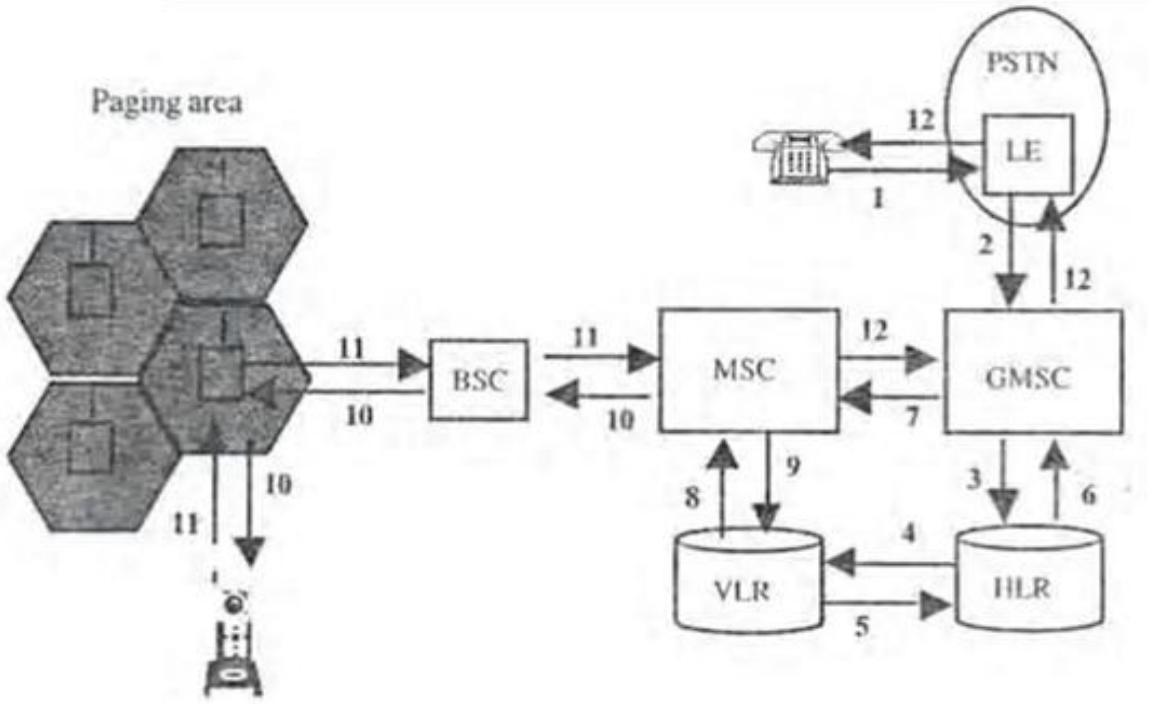
مراحل سير مكالمة من موبايل إلى هاتف أرضي :

عندما يطلب موبايل رقم هاتف أرضي و يضغط على زر الإرسال فإن الـ BSS تقوم بإجراء عمليات signaling (بروتوكولات الاتصال و التوثيق و التأكد من السماحية المعطاة للمشترك بالاتصال) .و من ثم يجري تأسيس الاتصال وفق التتابع التالي :



1 - ترسل الـ MS الرقم المطلوب إلى الـ MSC عبر الـ BSS .
2 - تتحقق الـ MSC إذا كان المشترك يحق له إجراء الاتصال و إذا كان ذلك محققا فإن الـ MSC تطلب من الـ BSS تأسيس القنوات اللازمة لإجراء هذا الاتصال .
3 - تحول الـ MSC الاتصال إلى بوابة العبور .
4 - تحول بوابة العبور الاتصال إلى المقسم الأرضي الذي يخدم الهاتف الأرضي المطلوب .
5 - يقوم المقسم بتنبيه الهاتف الأرضي المطلوب .
6 - يجيب الهاتف المطلوب على المقسم .
7 - المقسم بدوره يجيب على بوابة العبور و الـ MSC و الـ BSS ثم يكون الاتصال جاريا .

مراحل سير المكالمة من هاتف أرضي إلى هاتف في شبكة GSM :



1 - يدخل مشترك الهاتف الأرضي رقم MSISDN الخاص بمشترك شبكة الـ GSM .
2 - يقوم المقسم الأرضي بتحويل هذا الاتصال إلى بوابة العبور الخاصة بشبكة الـ GSM المطلوبة (GSM Gateway) .
3 - تقوم بوابة العبور من خلال الرقم MSISDN بتحديد الـ HLR التي تخدم المشترك المطلوب .
4 - تطلب الـ HLR من الـ VLR الحالية التي تخدم المشترك الرقم MSRN الخاص بالمشترك حتى يتم تحويل المكالمة إلى الـ MSC الحالية التي تخدم المشترك .
5 - تقوم الـ VLR بإعطاء الـ HLR الرقم MSRN .
6 - تقوم الـ HLR بنقل الرقم MSRN إلى بوابة العبور .
7 - اعتمادا على الرقم MSRN تقوم بوابة العبور بتحويل المكالمة إلى الـ MSC المطلوبة .
8 - تطلب الـ MSC من الـ VLR المخدمة للمشترك المطلوب أن تزودها بالرقم LAI الخاص بالمشترك المطلوب .
9 - تقوم الـ VLR بتزويد الـ MSC بالرقم LAI .
10 - تقوم الـ MSC بالبحث عن المشترك عبر الـ BSS بواسطة إشارة Paging ، و عندما يلتقط الـ MS هذه الإشارة يجيب بطلب إشارة Signaling لتأسيس الاتصال .
11 - تقوم الـ BSS بتأسيس الوصلات الراديوية المطلوبة .
12 - يجيب الـ MS و تم المكالمة بين الهاتفين .

استخدام برنامج محاكي لمحاكاة المراحل التي سيتبعها الهاتف عند إجراء عملية الاتصال

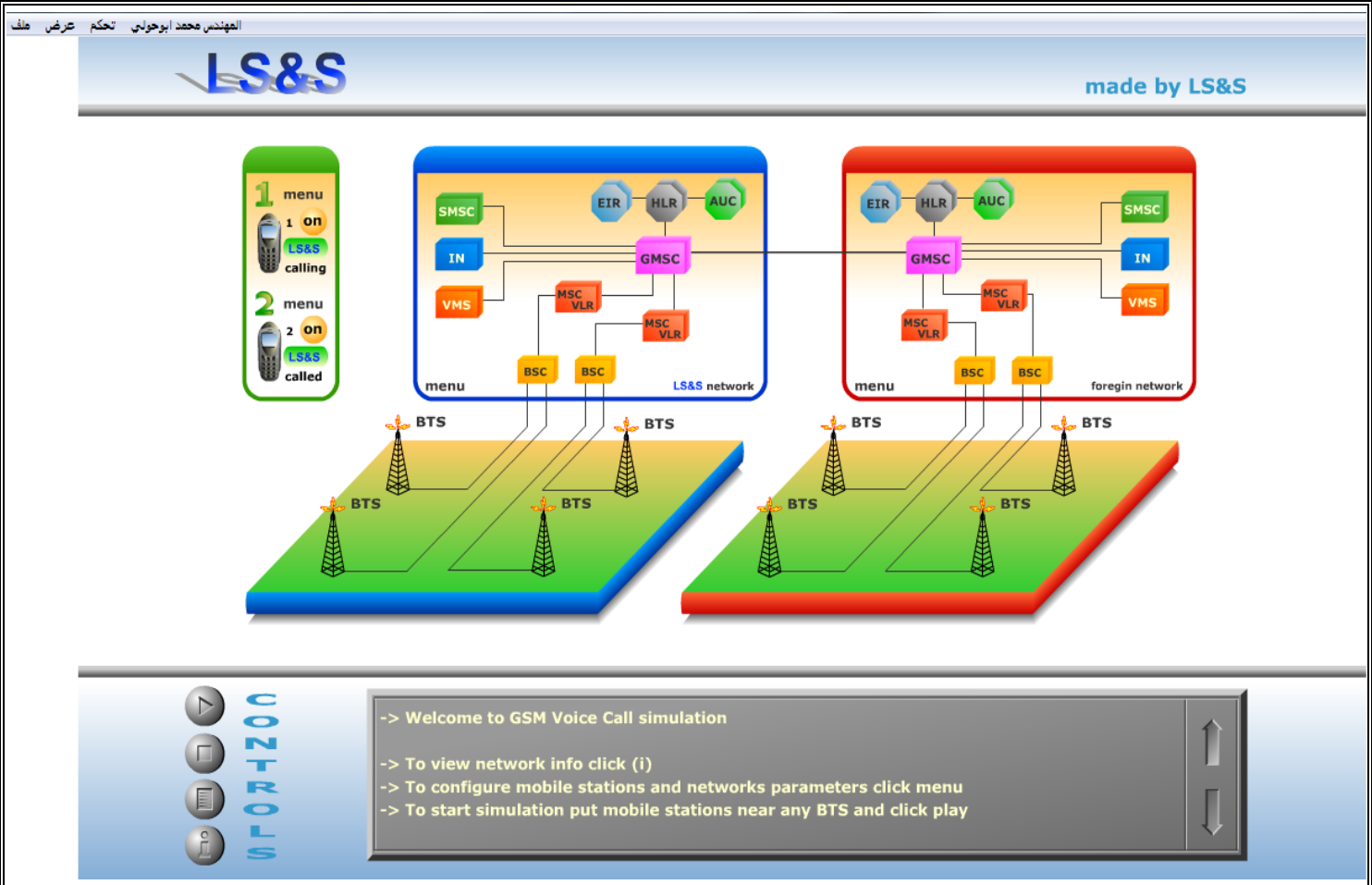
سواء بينه وبين هاتف أخر في نفس الشبكة او هاتف في شبكة مختلفة

تم برمجة الكتاب ليتم فتح البرنامج المحاكي تلقائيا عند تشغيل الكتاب

لتفادي فقدان البرنامج المحاكي أثناء عملية تحميل أو إعادة توزيع الكتاب

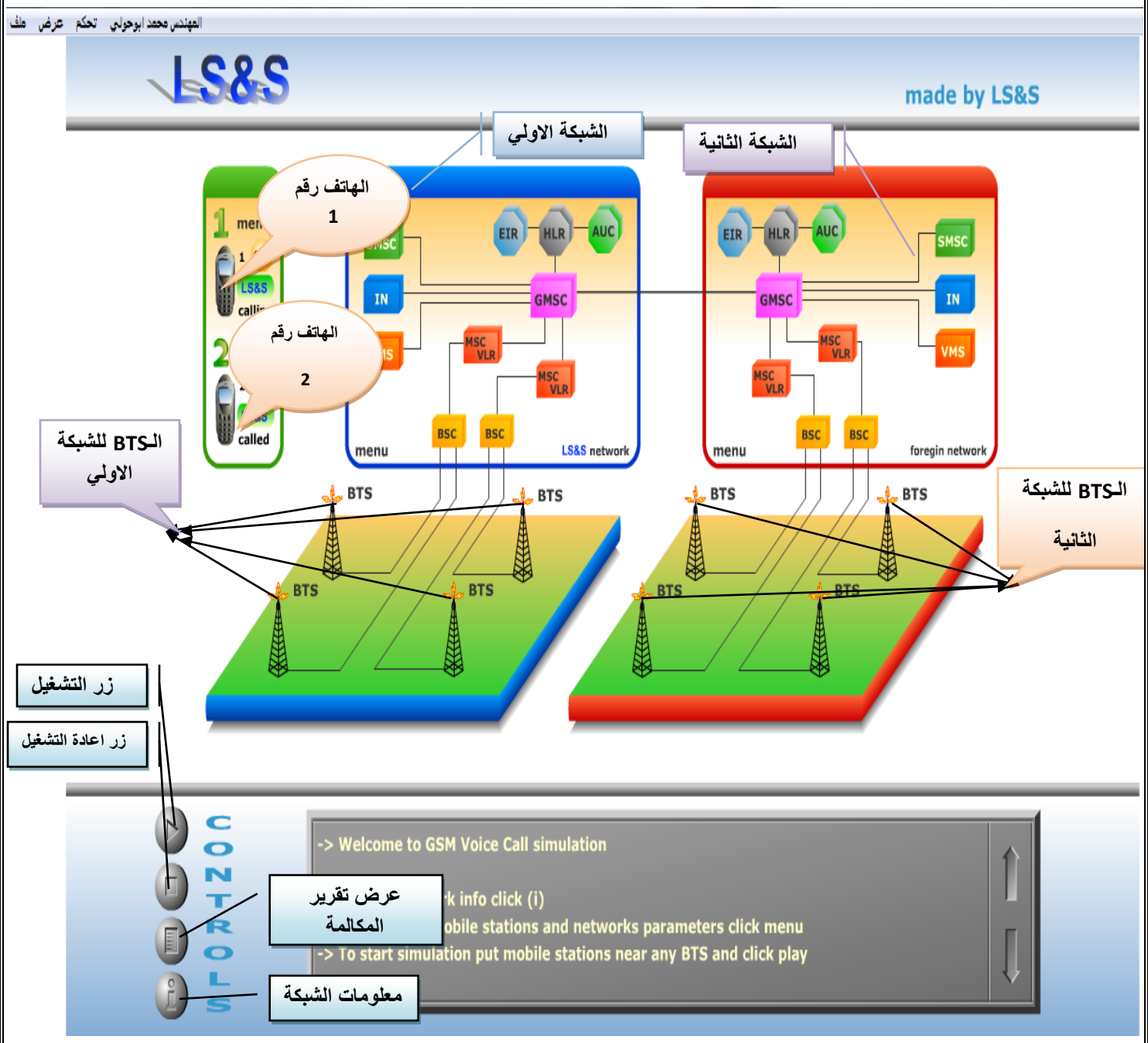
عند تشغيل البرنامج سيظهر الشكل التالي

اضغط Enter Simulation للدخول إلي المحاكي



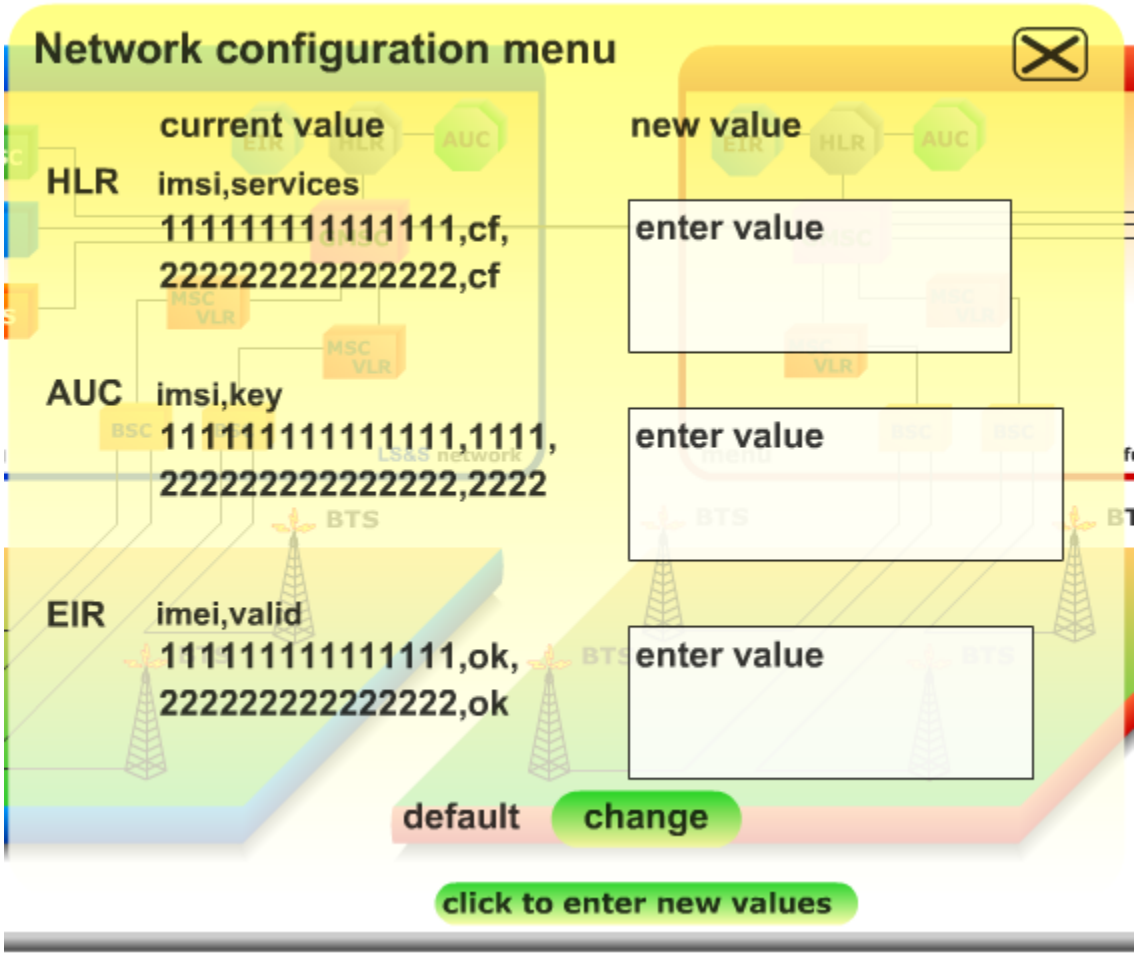
هذه هي الواجهة الرئيسية للبرنامج المحاكي

شرح واجهة البرنامج



لتعديل اعدادات اي من الشبكات اضغط علي كلمة Menu الموجودة اسفل مكونات الشبكة

ليظهر مربع الحوار التالي



المربع الأول هو لتعديل بيانات وإعدادات الـHLR حيث يحتوي علي

International Mobile Subscriber Identity : IMSI

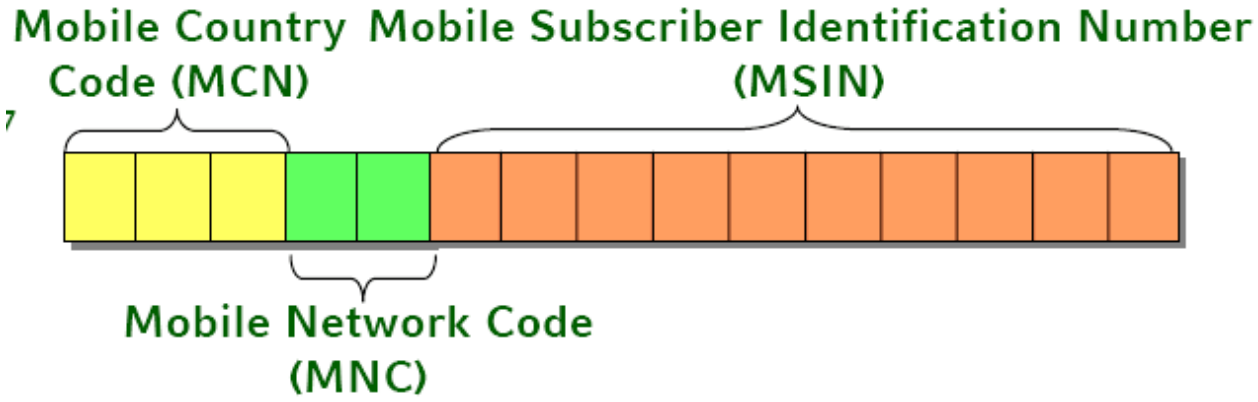
وهو رقم وحيد يخصص لكل مشترك بحث انه لا يمكن لمشترك ان يتشابة في هذا الرقم مع مشترك اخر من نفس الشبكة .

يقدم IMSI التسهيلات من اجل التحقق من هوية المشترك عبر المسار الراديوي وخلال الشبكة .

يخزن هذا الرقم في HLR و AUC و VLR و SIM .

يتكون IMSI من الاجزاء التالية :

1 - Mobile Country Code (MCC) : رمز البلد.
2 - Mobile Network Code (MNC) : رمز الشبكة.
3 - Mobile Station Identity Number (MSIN) : رقم تعريف المشترك .



المربع الثاني هو لتعديل بيانات وإعدادات الـAUC حيث يحتوي علي

IMSI: تم شرحة سابقا

Key : هو رمز يتم تحديدة من قبل الشركة ويتم تخزينة فيSIM

المربع الثالث هو لتعديل بيانات وإعدادات الـEIR حيث يحتوي علي

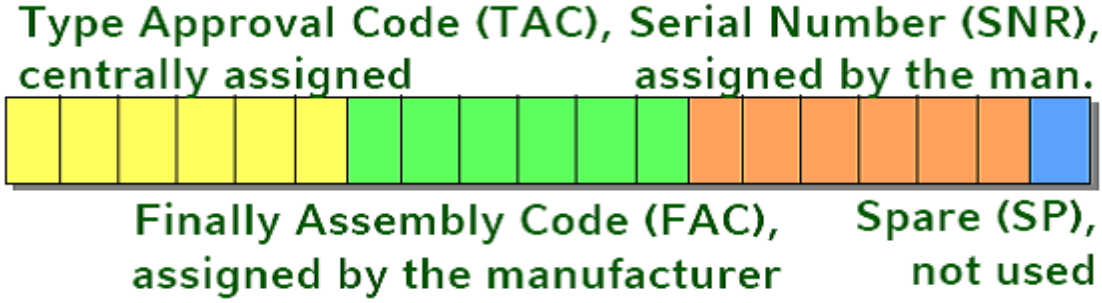
International Mobile Equipment Identity : IMEI

عبارة عن رقم تعريف الهاتف الخلوي العالمي . يخصص من قبل الشركة الصانعة للهاتف الخلوي ويتم تسجيله وتخزينه في EIR بواسطة مشغل الشبكة .

يقدم IMEI معلومات عن الهاتف الخلوي كالشركة الصانعة وتاريخ الصنع ويستخدم لأغراض الحماية .

يتكون IMEI من الاجزاء التالية :

1 - Type Approval Code (TAC) : يحدد هيكلية نظام GSM.
2 - Final Assembly Code (FAC): يعرف الشركة المصنعة.
3 - Serial Number (SNR) : رقم تسلسلي مقسم لست خانات وحيدة تخصصها الشركة المصنعة .
4 - Spare (SP) : وهي خانه غير مستعمله حاليا , قد تستعمل في المستقبل .



Valid : هو حالة رقم الـIMEI بالنسبة للشبكة من حيث إمكانية قبول المكالمة والخدمات الاخري أو لا

OK تعني أن الهاتف مسموح له بإجراء مكالمات والخدمات الاخري خلال الشبكة .

NO تعني أن الرقم محجوب آو ممنوع من استخدام خدمات الشبكة .

تستعمل هذه الخاصية في بعض الشبكات لمكافحة ومنع بعض أنواع الهواتف من إجراء المكالمة مثل منع الهواتف التقليدية او الغير أصلية من العمل علي الشبكة .

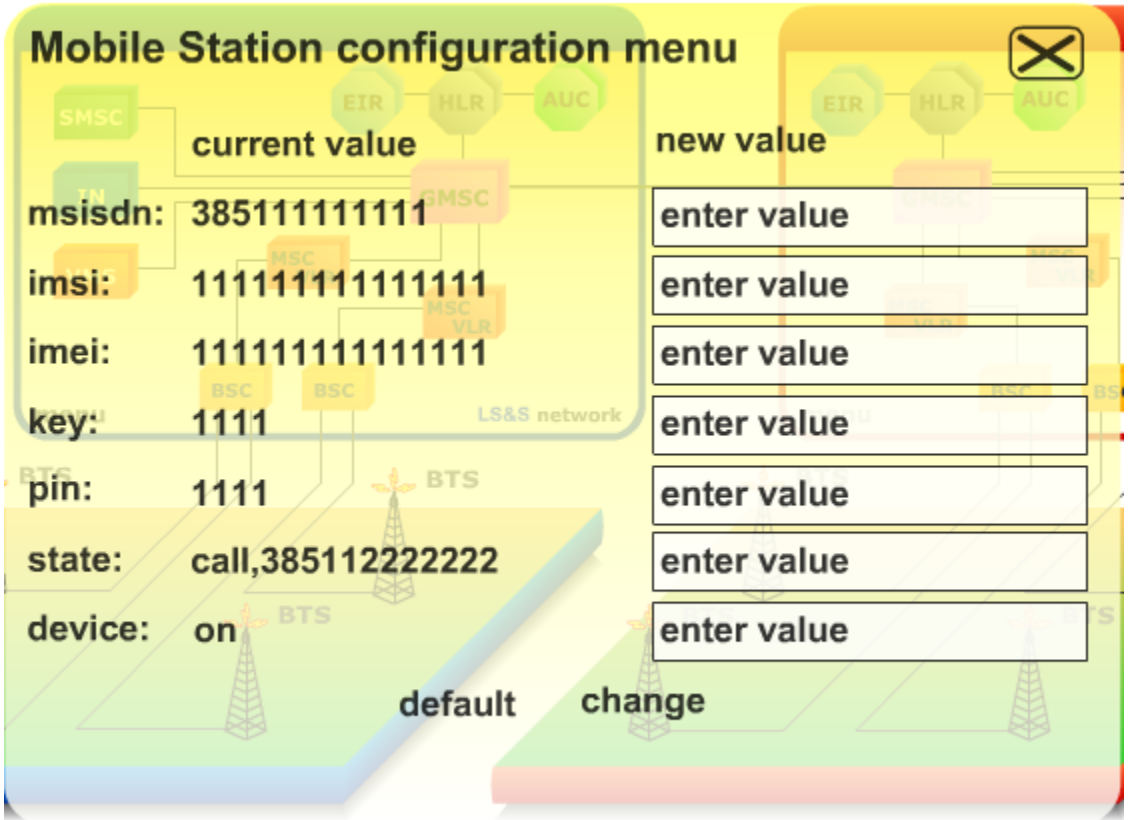
او لمكافحة سرقه الهواتف فعندما يسرق هاتف يتم تبليغ مشغل الشبكة عنه فيقوم مشغل الشبكة بوضع الـIMEI الخاص بالهاتف في خانة الغير مسموح لهم استعمال الشبكة وبذلك يصبح الهاتف لا يصلح للاستعمال في تلك الشبكة .

ولتغيير قيمة من القيم السابقة قم بإدخال القيمة الجديدة في مربع الحوار ثم اضغط علي Change

ولإعادة القيم إلي القيم الافتراضية اضغط علي Default

لتعديل اعدادات اي من الهواتف اضغط علي كلمة Menu الموجودة بجانب الهاتف

ليضهر مربع الحوار التالي



المربع الاول هو لتعديل بيانات وإعدادات الـMSISDN

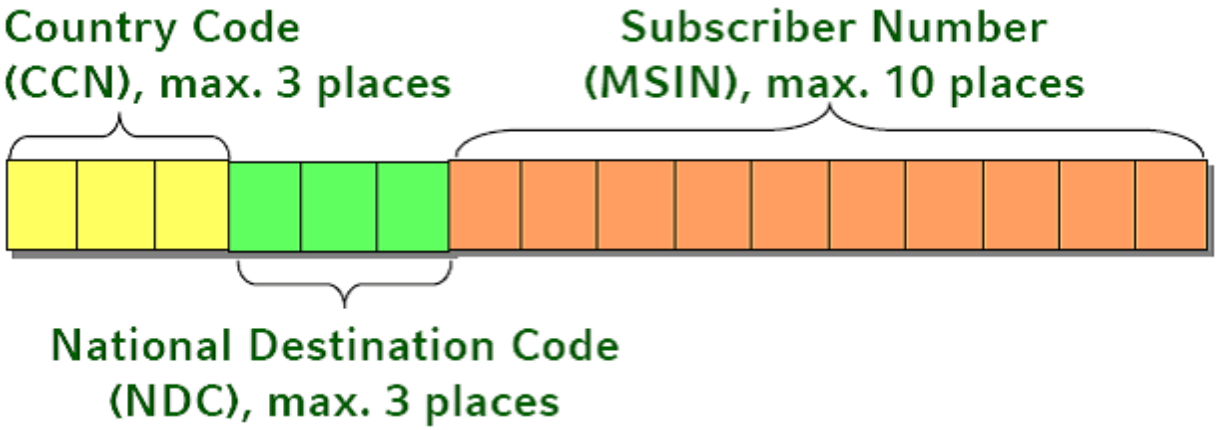
Mobile Subscriber ISDN (MSISDN)

عبارة عن رقم الهاتف الفعلي للمشترك النقال , بحيث لا بد ان يتوافق هذا الرقم مع خطة ترقيم PSTN/ISDN .

يخزن هذا الرقم بشكل رئيسي في HLR و VLR و SIM .

يتألف ISDN من الاجزاء التالية :.

1 - Country Code (CC) : رمز البلد وهو عبارة عن 3 أرقام كحد أقصي .
2 - National Destination Code (NDC) : رمز المشغل وهو عبارة عن 3 أرقام كحد أقصي .
3 - Subscriber Number (MSIN) : رقم المشترك وهو عبارة عن 10 أرقام كحد أقصي .



المربع الثاني هو لتعديل بيانات وإعدادات الـIMSI

تم شرحه سابقا

المربع الثالث هو لتعديل بيانات وإعدادات الـIMEI

تم شرحه سابقا

المربع الرابع هو لتعديل بيانات وإعدادات الـKey

تم شرحه سابقا

المربع الخامس هو لتعديل بيانات وإعدادات الـPin

هو رمز يتم أضافته من قبل مستعمل بطاقة الـSIM وذلك لتوفير حماية للبطاقة من استعمال غير مخول به من قبل شخص أخر إذا فقدت هذه البطاقة أو ضاعت ويطلب الهاتف هذا الرمز عند بداية تشغيل الهاتف او إعادة التشغيل .

المربع السادس هو لتعديل بيانات وإعدادات الـState

هي حالة الهاتف عند إجراء عملية الاتصال او عند بداية تشغيل المحاكي

يمكن تغييرها الي الانتظار باستبدال القيمة الموجودة بـWait

القيمة الموجودة هنا ااي call,385112222222

تعني ان حالة الهاتف هنا ان يقوم بالاتصال بالرقم385112222222

هذا الرقم هو نفسه الـMSISDN للهاتف رقم 2 في المحاكي

يراعي هنا ان الهاتف رقم2 في المحاكي يجب ان تكون حالتة هيWait لكي تتم عملية الاتصال

ويمكن تغيير حالة الهاتف بإضافة القيمة الجديدة ثم الضغط عليChange

المربع الأخير هو لتعديل بيانات وإعدادات الـdevice

هذه الخانة خاصة بحالة جهاز الهاتف من حيث التشغيل او الايقاف

يمكن تغيير حالة الهاتف إلي مقفل وذلك بإدخال القيمةOFF والضغط عليChange

هنا يجدر الاشاره انه يجب ادخال رمز الـPIN

وهنا هو 1111 اذا كان الهاتف رقم1

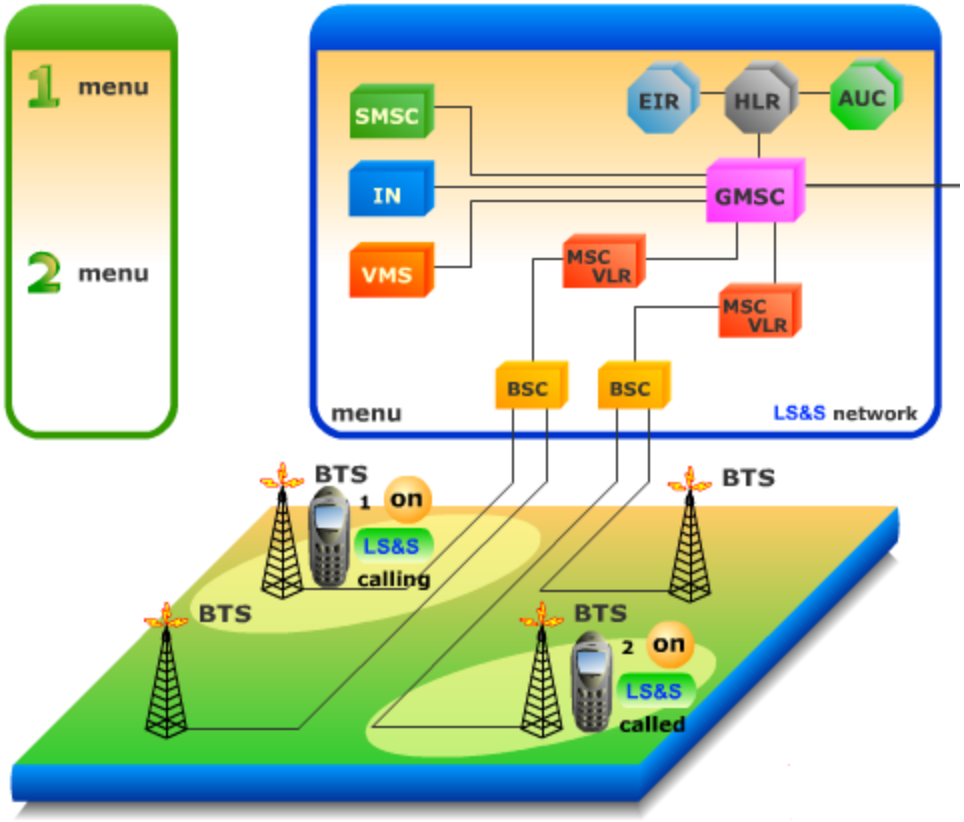
او 2222 اذا كان الهاتف رقم2

اذا لم يتم تغييرها

بعد الانتهاء من شرح إعدادات البرنامج المحاكي لمنظومة الاتصال سنقوم بأول عملية محاكاة بواسطته

إجراء اتصال بين هاتفين من نفس الشبكة.

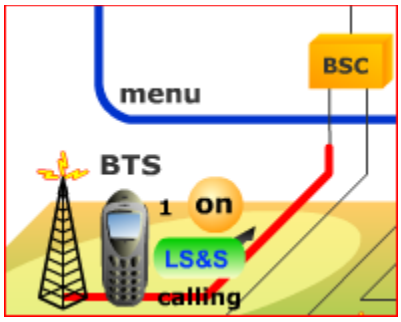
نقوم بسحب الهاتف وأفلاتة في نطاق احد خلايا الـBTS في شبكة واحدة



بعدها نقوم بالضغط علي زر لتشغيل المحاكي وبدء عملية الاتصال

يبدأ الهاتف بطلب الاتصال ويقوم بالبحث عن اقرب BTS التي يقع في نطاقها

بعدها تقوم الـBTS الموجود في الهاتف بإرسال الطلب الهاتفي إليBSC



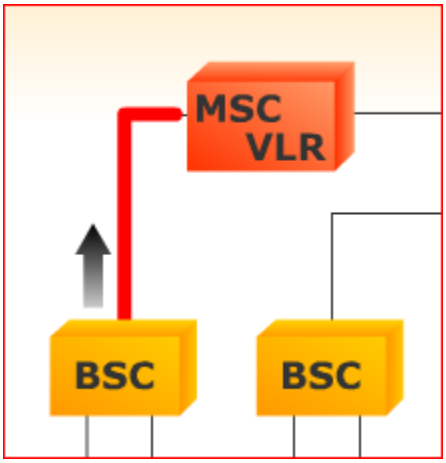
بعدها سوف تقوم محطة القاعدة بإرسال اشاره إلي(MSC\VLR)

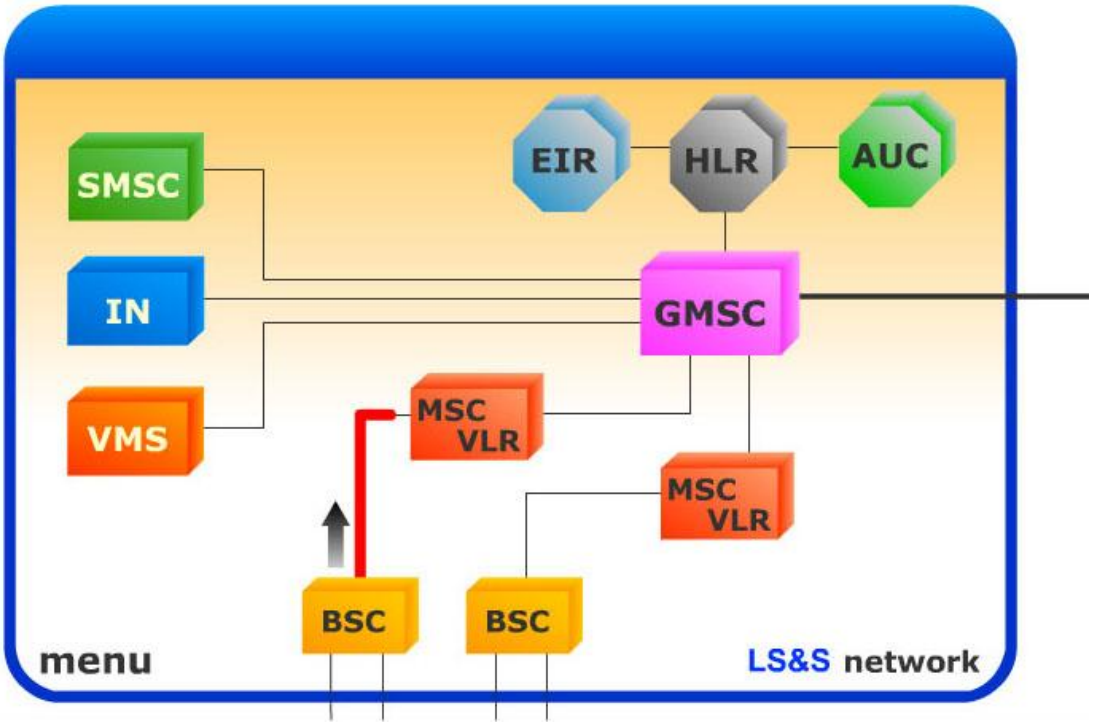
(Mobile Service Switching Center / Visitor Location Register)

حيث(MSC) هو المسئول علي تحويل المكالمات بين الهواتف النقالة بين بعضها

البعض أو بين الهواتف النقالة وشبكه الهواتف العامة

(VLR) هو الذي يحتوي علي جميع البيانات لجميع مشتركي النقالات الزائرين





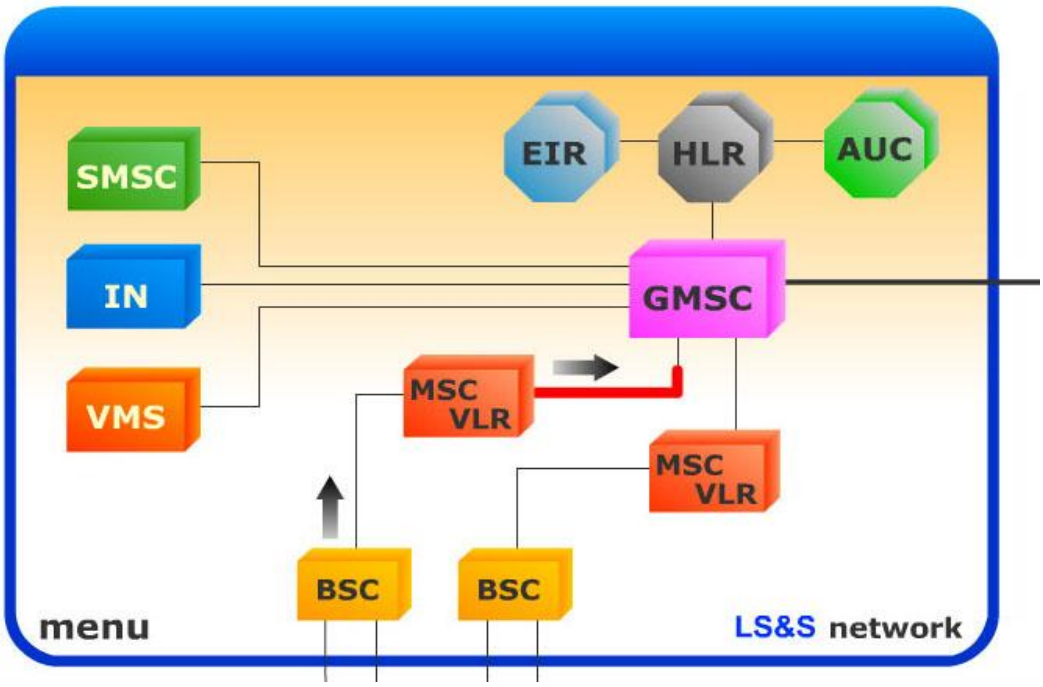
بعدها يقوم(MSC\VLR) بتحويل الاشاره إلي (GMSC)

حيث (GMSC)

هو عبارة عن نقطة الوصل بين شبكة الموبايل اللاسلكية وشبكة التلفون الثابتوالشبكات الاخري

Public Switching Telephone Network PSTN

وهو المسئول أيضا عن توجيه المكالمات من التليفون الأرضي والتليفون المحمول والعكس بالعكس



بعدها يقوم(GMSC) بإرسال الاشاره إلي(AUC – HLR – EIR)

(Authentication Center – Home Location Register–Equipment Identity Register)

وذلك للتأكد من شرعيه المكالمة وللحماية من الاختراق

(AUC)

من المميزات الهامة في (GSM) تمتعه بدرجة عالية من الأمن المعلوماتي و ذلك عبر عدة وظائف أمنيةيقوم بها النظام .

(AUC) هو المسؤول عن اغلب هذه الوظائف في شبكة (GSM)

فهو يقوم بتخزين معلومات السرية عن المشتركين مما يتيح لصاحب هذه المعلومات فقط بالعبور إلى الشبكة الخلوية (تحقيق هوية المشترك) وبذلك تتم حماية المشتركين من الاستخدام الاحتيالي لحسابهم

كما يقوم (AUC) بدور هام في عمليات التحقق

(HLR)

قاعدة بيانات تحتوي على معلومات عن المشتركين المسموح لهم بالتنقل بهواتفهم في المناطق الجغرافية لشبكات تستخدم تقنيات مختلفة مثل :

(GSM و AMPS).

(EIR)

وهو يشارك في الوظيفة الأمنية ويكون دوره التأكد من شرعية أجهزة الموبايل (ME)

ومعرفة (هل هي مسروقة او غير مسجلة في الشبكة) وذلك عن طريق(IMEI) الموجود في كل جهاز

(International Mobile Station Equipment Identity)

وفق الخطوات التالية :

1.يطلب (MSC/VLR). الـ (IMEI) من (MS)

2.يرسل (MSC/VLR). الـ (IMEI) إلى (EIR)

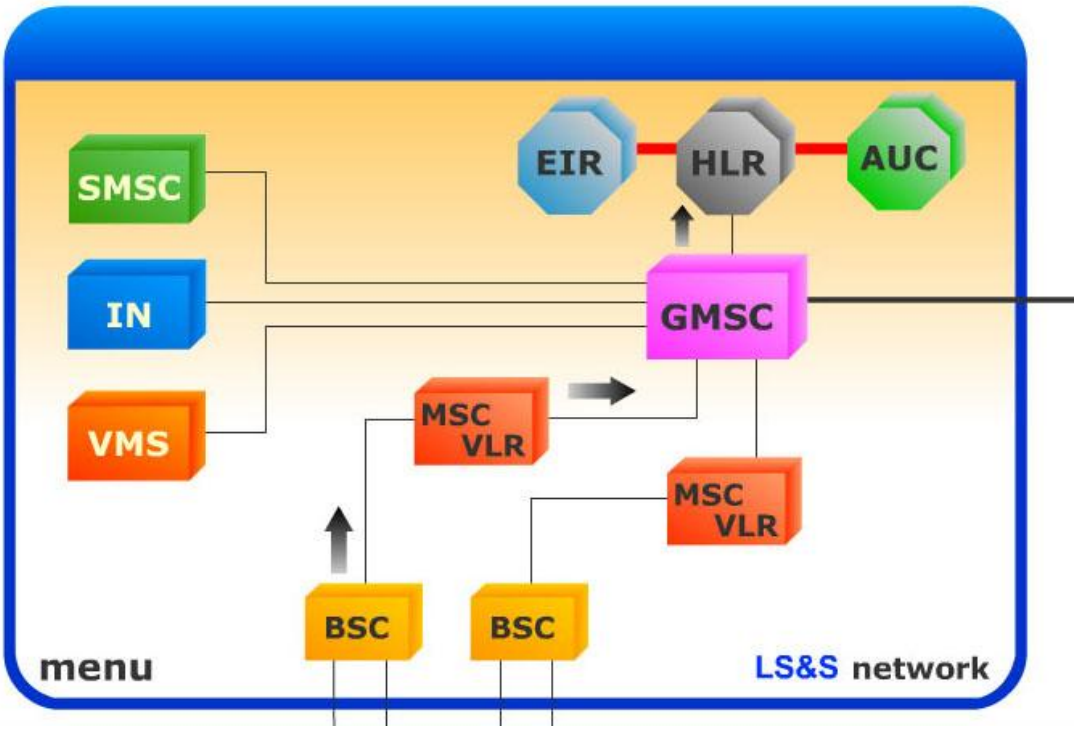
3. يقوم (EIR) بمطابقة (IMEI) مع ثلاثة قوائم من أرقام(IMEI)

المخزنة لديه وهذه القوائم هي :

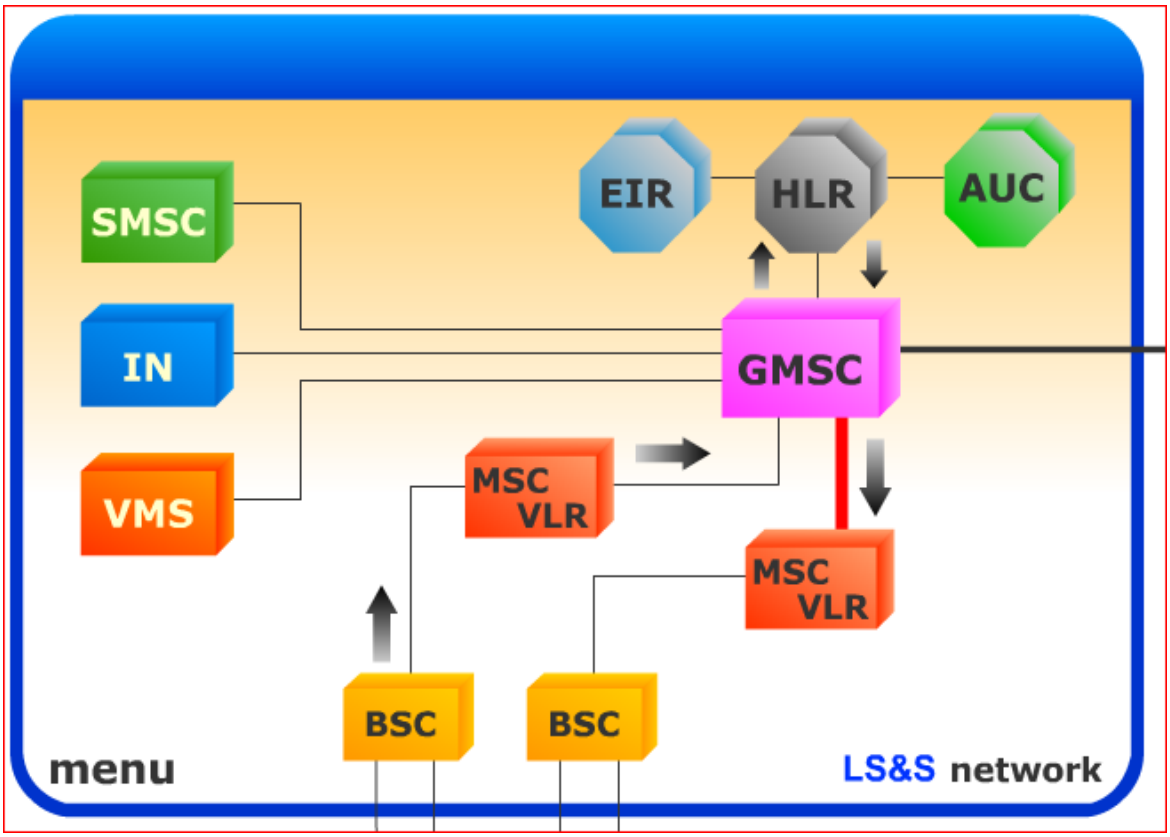
(القائمة السوداء – القائمة الرمادية – القائمة البيضاء).

4 . يرسل(EIR) نتيجة المطابقة وشرعيه الجهاز إلي(MSC/VLR)

للسماح أو منعه من دخول ألشبكه

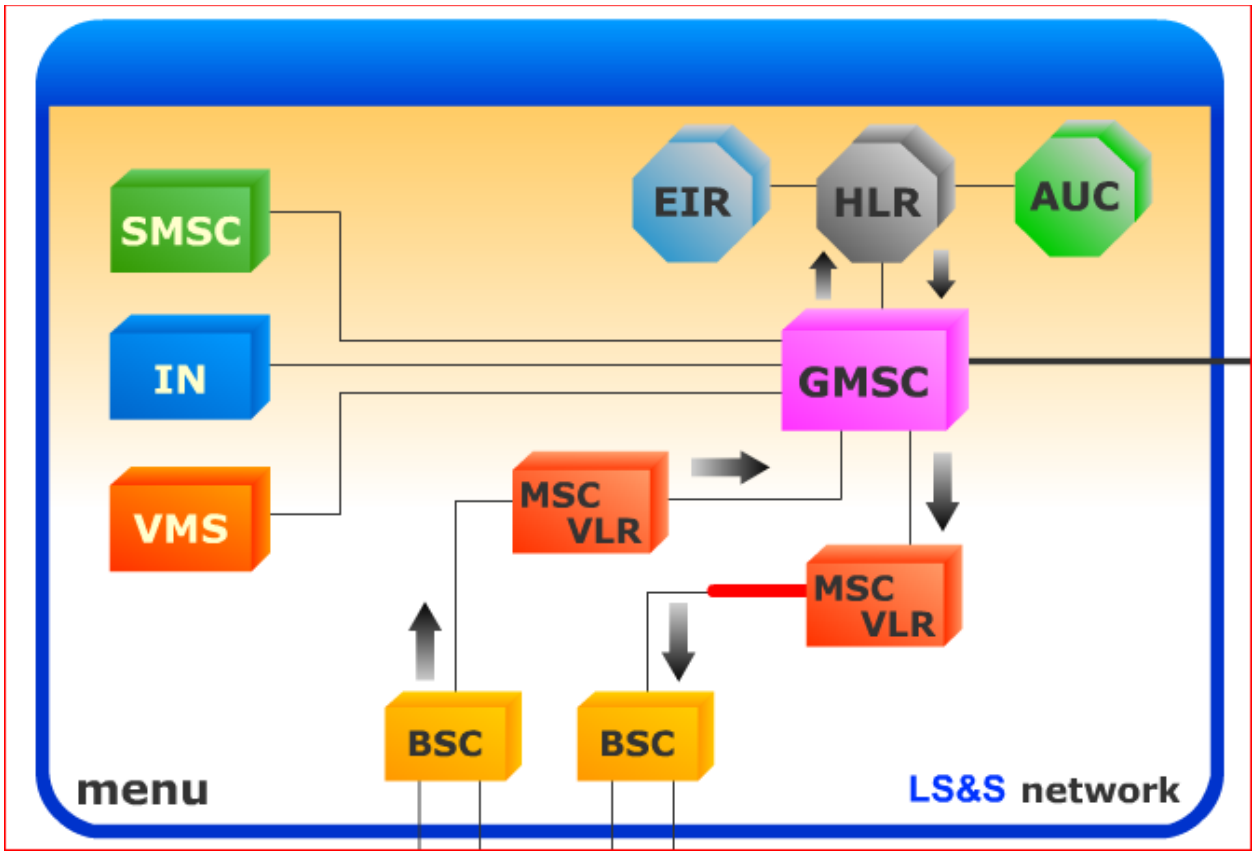


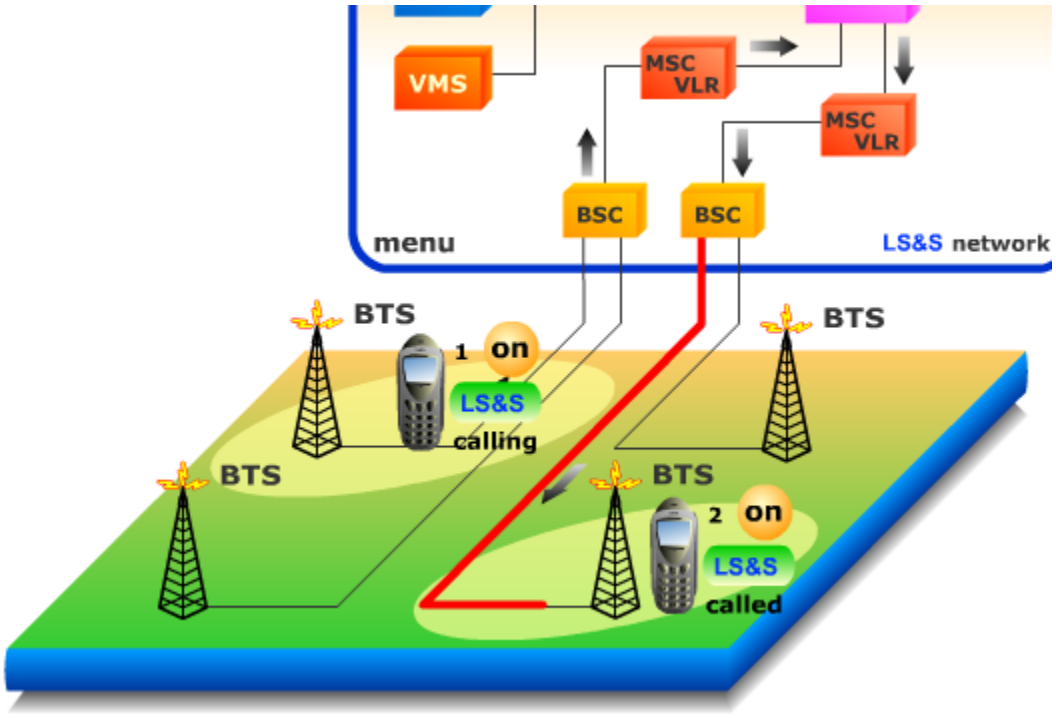
بعدها يقوم نضام(GMSK) بتحويل الاشاره إلي (MSC \ VLR)



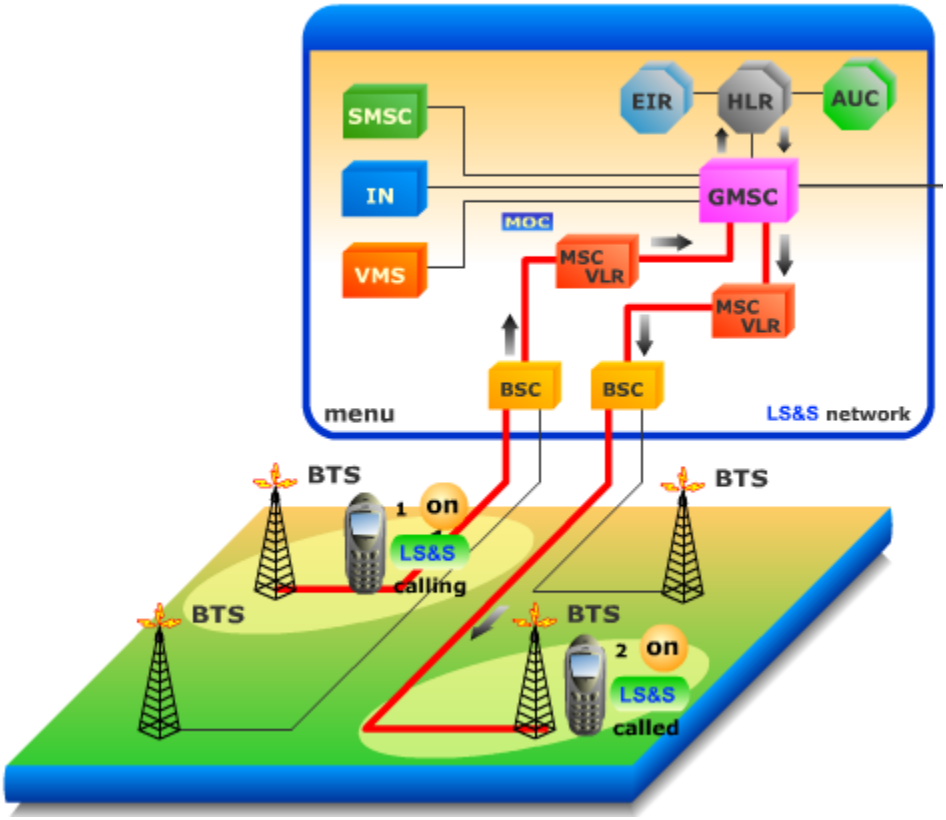
بعدها تقوم(MSC \ VLR)بإرسال الاشاره إلي محطة (BTS)

ومنها إلي الهاتف الجوال





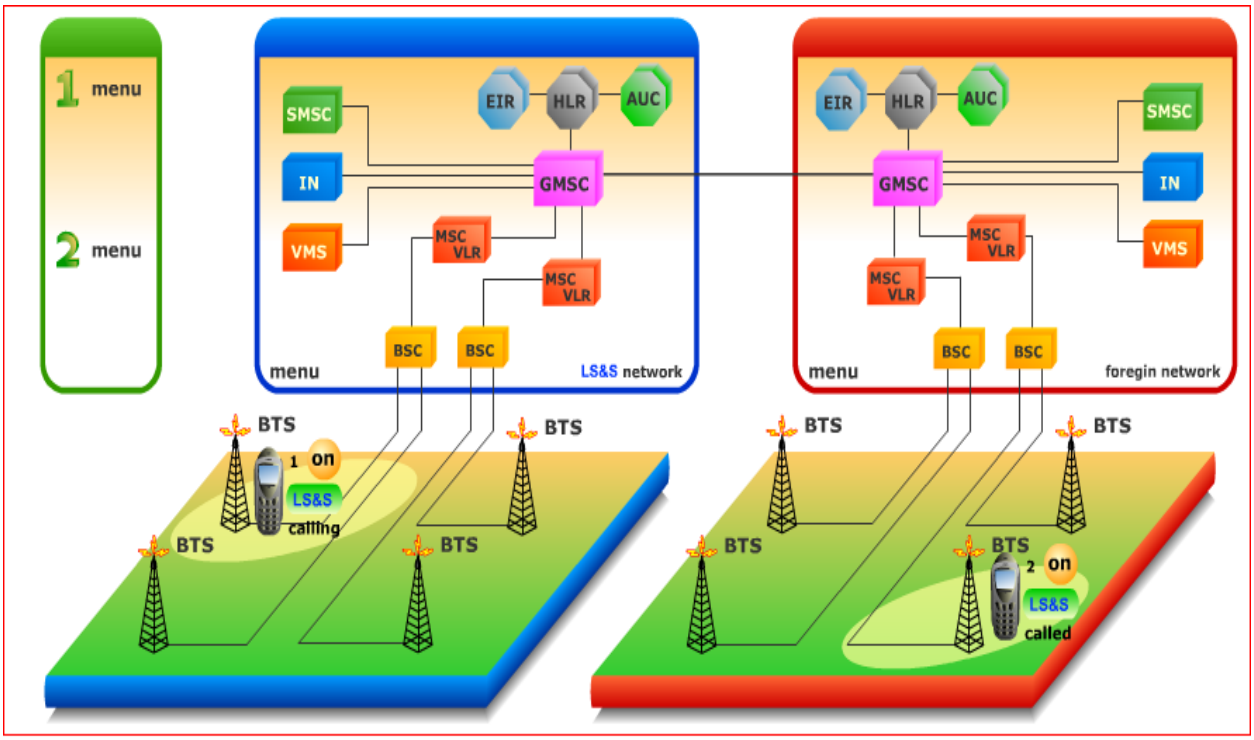
وهذه هي الخطوط التي يتبعها الهاتف المحمول لإجراء اتصال بين واحدة



ولا يوجد اختلاف لو تم تغيير الـBTS

إجراء اتصال بين هاتفين من شبكتين مختلفتين.

نقوم بوضع الهواتف في نطاق الـBTS في الشبكات المختلفة



نقوم بالضغط علي كلمة LS&S الموجودة بجانب الهاتف الثاني لتتحول الي Foregin

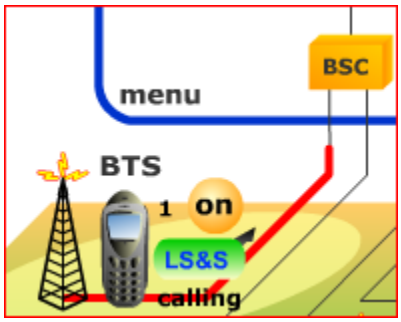
هذة الخطوة تعني ان الهاتف رقم2 هو هاتف يتبع للبشكة Foregin

ولا يحتوي شريحة تشتغل علي الشبكة LS&S

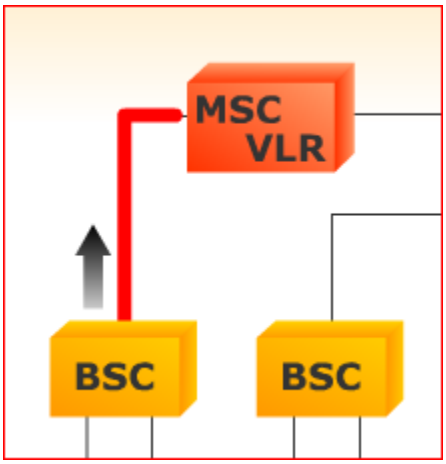
نقوم بتشغيل المحاكي

يبدأ الهاتف بطلب الاتصال ويقوم بالبحث عن اقرب BTS التي يقع في نطاقها

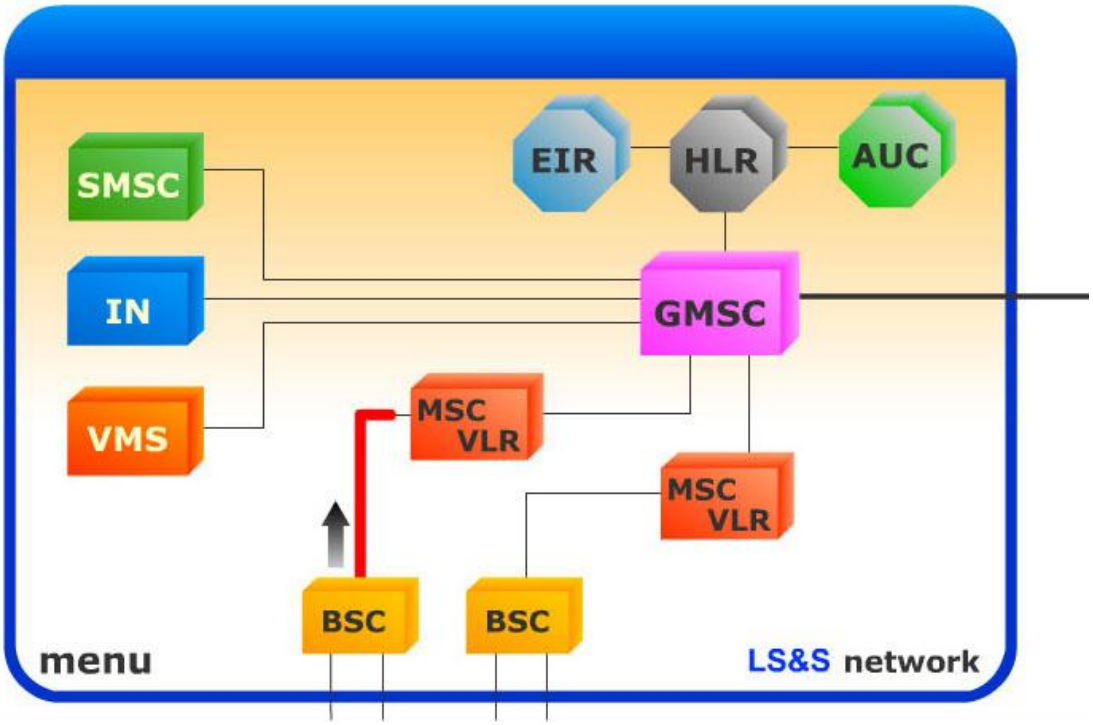
بعدها تقوم الـBTS الموجود في الهاتف بإرسال الطلب الهاتفي إليBSC



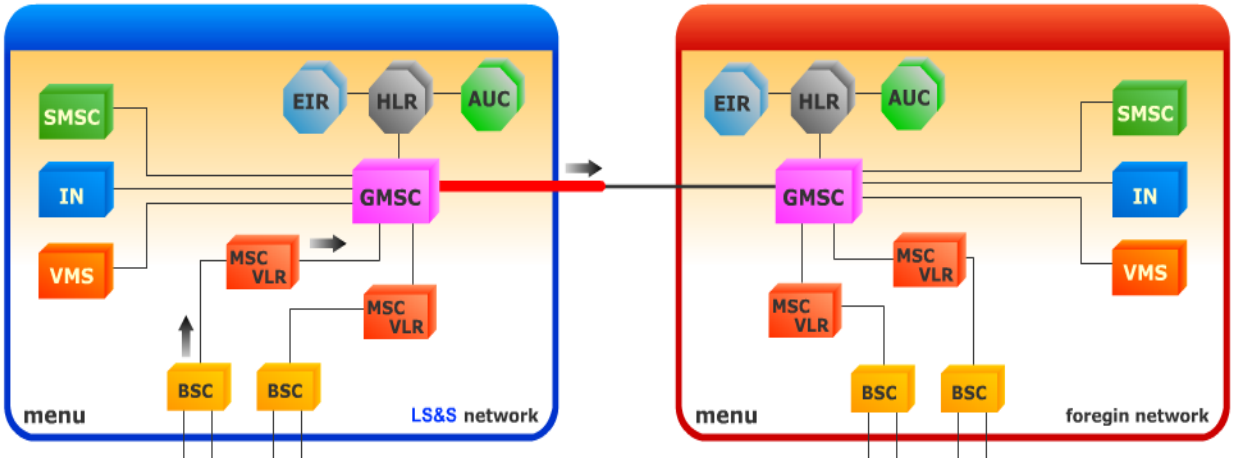
بعدها سوف تقوم محطة القاعدة بإرسال اشاره إلي(MSC\VLR)



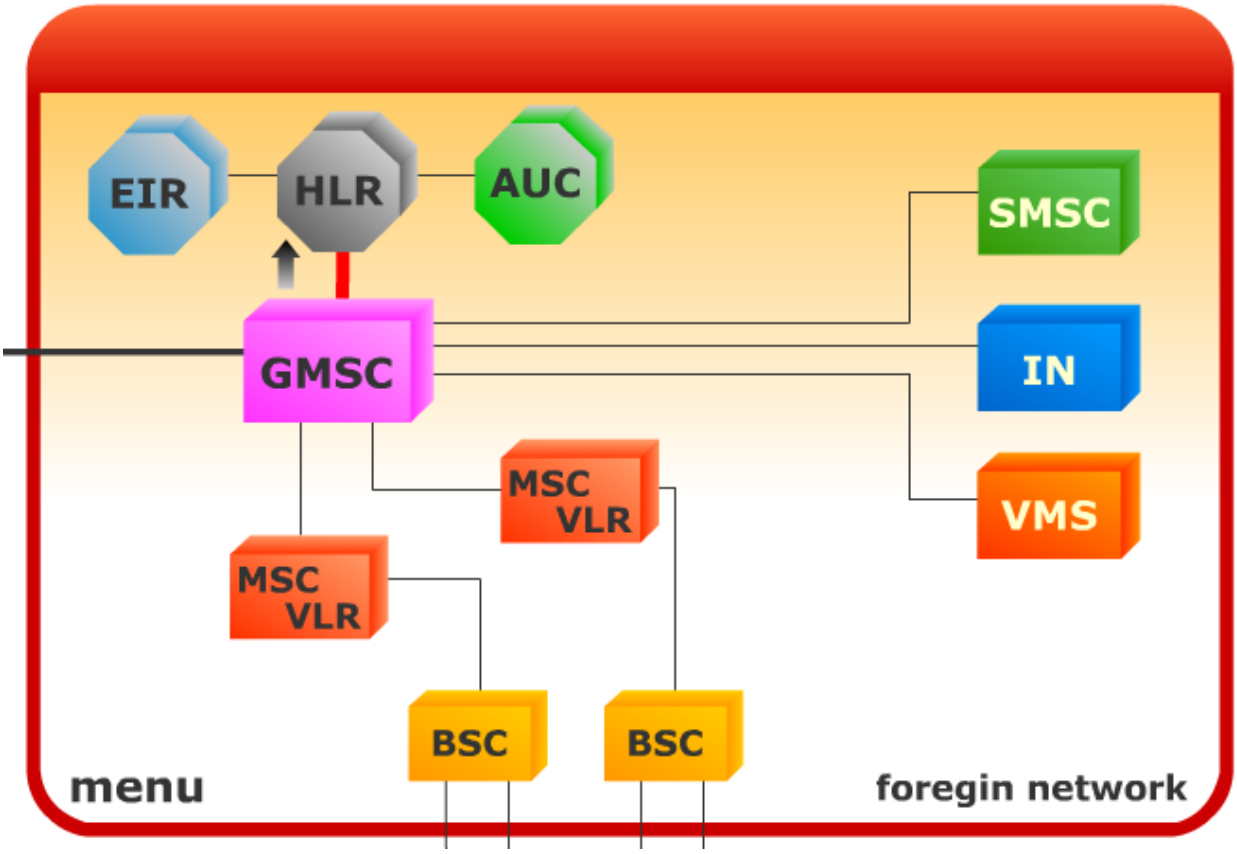
بعدها يقوم الـ(MSC\VLR) بإرسال الإشارة إلي GMSC



بعدها يقوم GMSC بتحويل الطلب الهاتفي الي الشبكة الاخري عبر مخاطبةGMSC الخاص بالشبكة



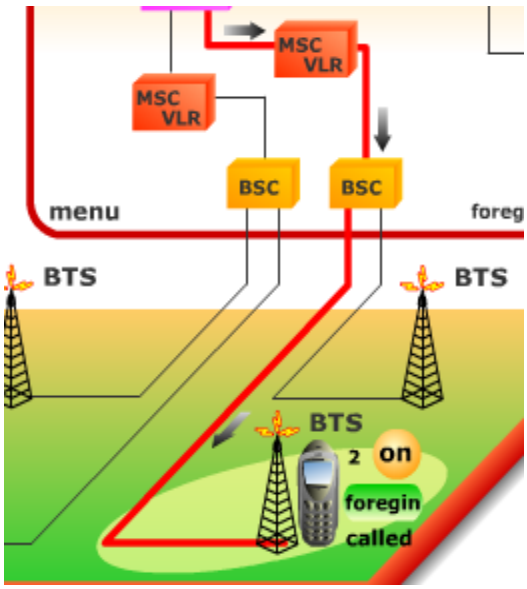
بعدها يقوم الــGMSC بتحويل الاشارة الي (AUC – HLR – EIR)



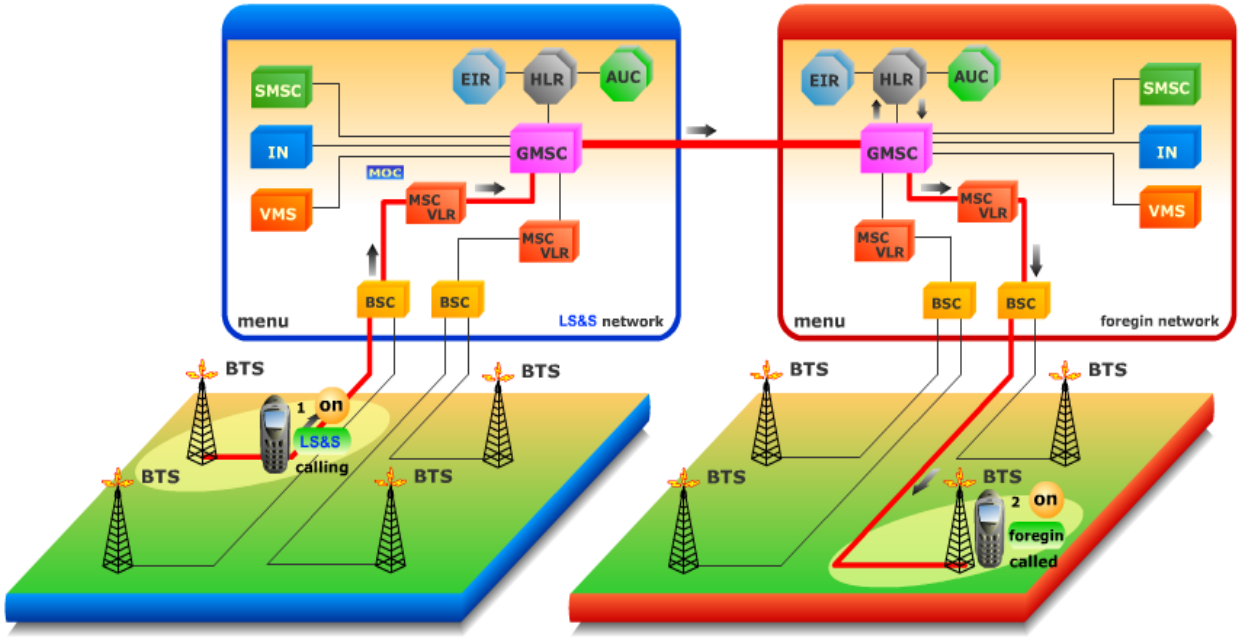
بعد التحقق من سلامة وصحة المكالمة

يوجهة الــGMSC الطلب الهاتف الي (MSC/VLR)

وبدورة يقوم الــ(MSC/VLR) بتحويل الطلب الي الــBSC وينتقل الطلب الي الــBTS الموجود فيها الهاتف النقال



وهذة هي الخطوات كاملة التي يتبعها الهاتف في حاله اجراء مكالمة لشبكة اخري غير التي يعمل في نطاقها



خدمة التجوال العالمي.

تعريف بالخدمة

هي خدمة تقوم بها شركات تشغيل الهواتف المحمولة فيما بينها تقضي بتمكين هاتف من شركة او من بلد اخر من العمل تحت شبكة أخري ويمكنه استعمال خدمات وإمكانيات الشبكة الخارجية لغرض تمكين المشتركين من التجول في جميع أنحاء العالم بشريحة هاتف ورقم موحد في بلدان عديدة.

يسمح للهاتف بالعمل في نطاق الـBTS للشركات الأجنبية وذلك بموائمة التردد ويمكن للهاتف ان يجري مكالمة ويستقبلها ويرسل رسائل نصية تحت أشارة الـBTS في الدول الاخري

ميزة هذه الخدمة هي التمتع برقم موحد وعدم الاضطرار الي البحث عن مشغل جديد كلما انتقلت الي دولة او إقليم غريب

ولاكن عيبها يكمن في التكلفة العالية والسعر المرتفع لتسعيرة المكالمات ونقل البيانات

ففي ليبيا مثلا عند استعمال شريحة من شركة (المدار الجديد) في السعودية خلال موسم الحج تكلفة الدقيقة ترتفع ثلاث أضعاف عند إجراء عملية الاتصال .

وحتى عند استقبال المكالمة عبر تلك الشريحة يجب دفع رسوم تحددها الشركة

ويمكن تعبئة الرصيد من خلال بطاقات احدي الشركات الموجودة في السعودية

اعتقد ان شركة (المدار الجديد) موقعة خدمة التجوال العالمي مع شركة (موبايلي) السعودية

محاكاة عملية التجوال العالمي.

فلنفرض في البداية ان شبكة LS&S هي شبكة المدار الجديد

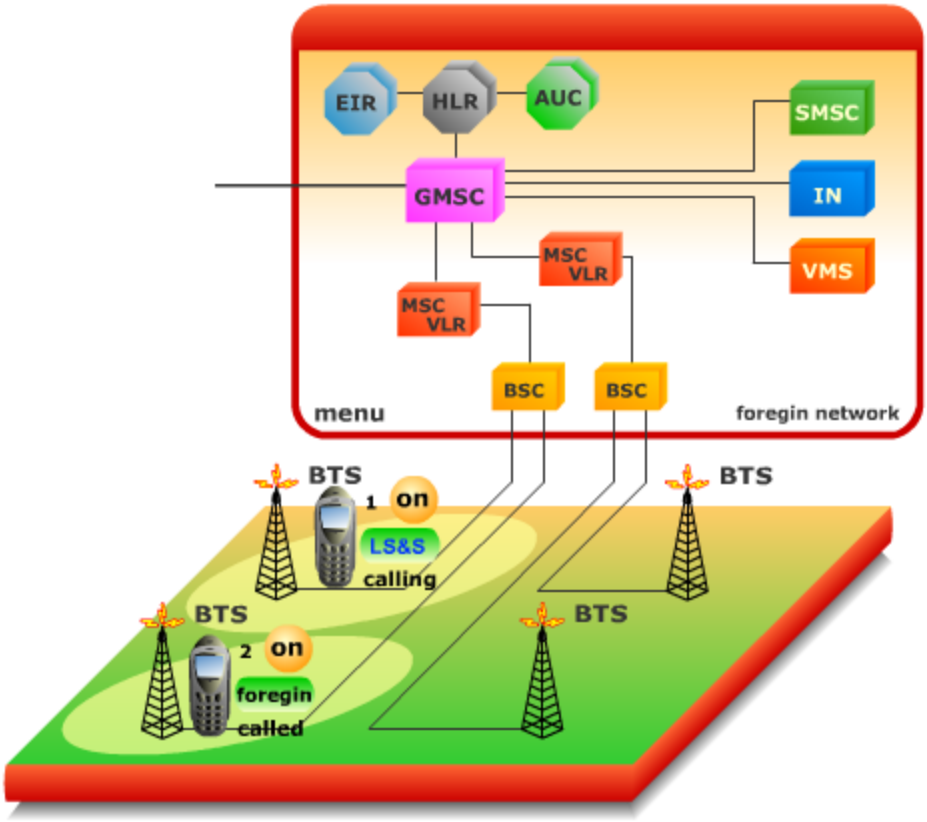
وشبكة Foregin هي شبكة موبايلي

سنقوم بأجراء عملية الاتصال بين شخص يحمل شريحة المدار الجديد موجود في السعودية وشخص يحمل شريحة موبايلي موجود في السعودية.

حيث الهاتف الذي يحمل شريحة المدار الجديد هو من سيجري الاتصال والهاتف الاخر سيستقبل المكالمة .

نقوم بوضع الهاتف رقم 1 (الهاتف الذي يشتغل بشريحة المدار الجديد) في احد الـBTS التابعة لشركة موبايلي

ونقوم بتعديل الهاتف رقم 2 بالضغط علي زر LS&S لتصبح Foregin



نقوم ببدء عملية الاتصال

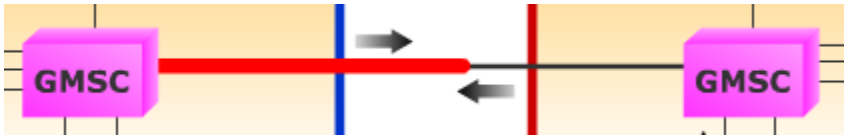
يقوم الهاتف 1 بالبحث عن اقرب BTS تابعة لشركة موبايلي هو واقع في نطاقها ليرسل عبرها الطلب الهاتفي

بعدها يقوم الـBTS بإرسال الطلب الي الـــBSC ومنه الي الـــ(MSC/VLR) ثم الي GMSC

يقوم الـــGMSC بالطلب من شركة المدار الجديد بتزويد بشركة موبايلي عن معلومات عن الهاتف المتصل

مثل الرقم الهاتف وإمكانية الاتصال وتسعيرة المكالمة وغيرة من المعلومات الضرورية ألازمة لعملية الاتصال

وذلك عبر التخاطب بين كلا من الـGMSC التابع لشركة موبايلي و الـــGMSC التابع لشركة المدار الجديد



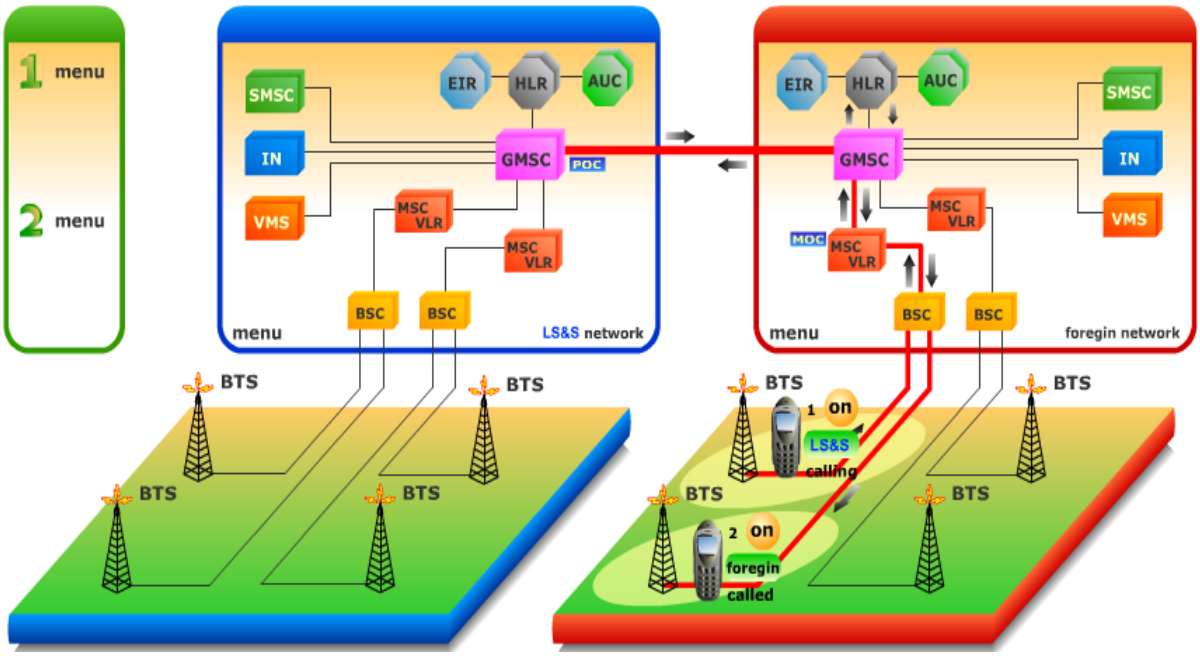
بعد ان تحصل الشبكة الخاصة بموبايلي بالمعلومات الازمة تقوم باجراء عملية الاتصال بشكل طبيعي

بأن يقوم الـــGMSC بارسال الطلب الي(AUC – HLR – EIR)

للتحقق من سلامة المكالمة ثم توجيه الطلب الي الهاتف الذي يعمل تحت شبكة موبايلي

بالمرور عبر كلا من (MSC/VLR) ثم الي BSC ثم الي الـBTS ومنها الي الهاتف .

هذة واجهة البرنامج المحاكي بعد إتمام عملية الاتصال



ملاحظة

لا يوجد اختلاف لو في الإجراءات لو كان المتصل شخص يحمل شريحة موبايلي موجود في ليبيا

سنقوم الان بمحاكة عملية اتصال اخري بين شبكتين

لاكن في هذة المرة سنزيي الأمر تعقيدا

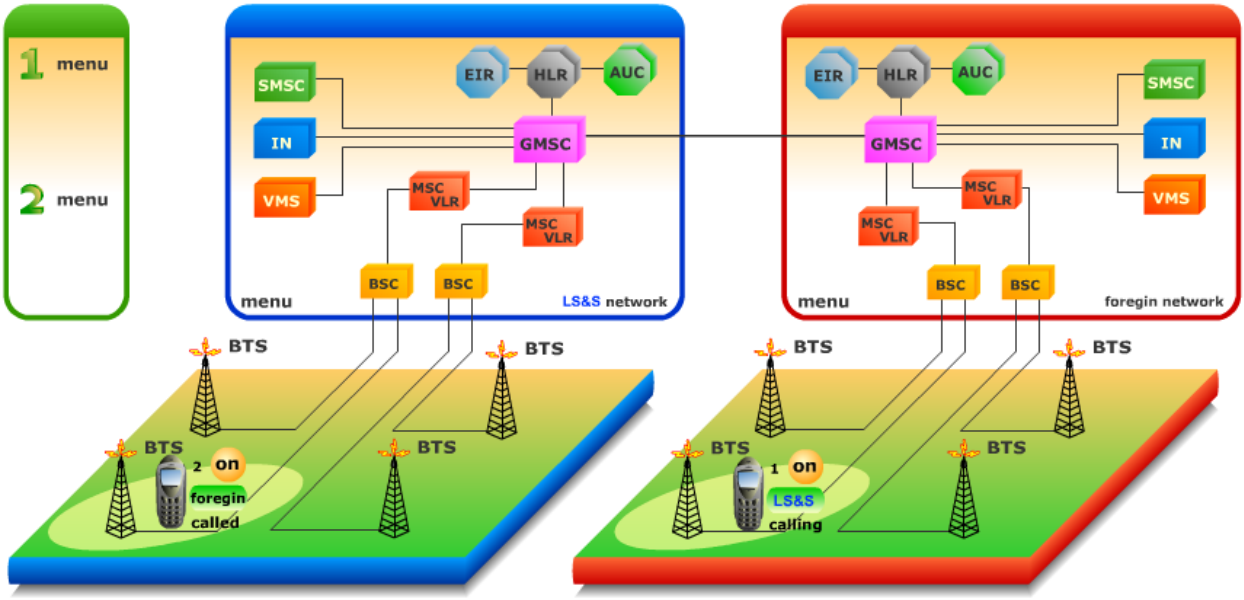
ستكون عملية الاتصال بين شخص يحمل شريحة المدار الجديد وموجود في السعودية

وبين شخص اخر يحمل شريحة موبايلي وموجود في الأراضي الليبية

سيكون كلتا الهاتفين يستعمل خدمة التجوال العالمي

اولا نقوم بوضع الهاتف رقم 1 في نطاق احد الـــBTS التابعة لشبكة Foregin

ونضع الهاتف رقم 2 في نطاق احد الـــBTS التابعة لشبكة LS&S ونقوم بتغيير شبكته الي Foregin بالضغط علي كلمة LS&S الموجودة بجانب الهاتف رقم 2 لتصبح Foregin



بعدها نقوم بتشغيل المحاكي

سيقوم الهاتف رقم 1 (الذي يحمل شريحه المدار الجديد وموجود بالسعودية) بالبحث عن اقربBTS ويقوم بارسال الطلب الهاتفي

تقوم الـBTS بتحويل الطلب الي الـBSC

من الـBSC تتجه المكالمة الي الـ(MSC/VLR) ثم الي GMSC

بعدها

يقوم GMSC شركة موبايلي بارسال الطلب وتحويله الي GMSC شركة المدار الجديد بغرض الاستفسار علن الرقم الذي يتبعها والموجود بالسعودية

يعيد الـGMSC التابع لشركة المدار الجديد الرد علي الـGMSC شركة موبايلي والرد يتضمن المعلومات المطلوبة

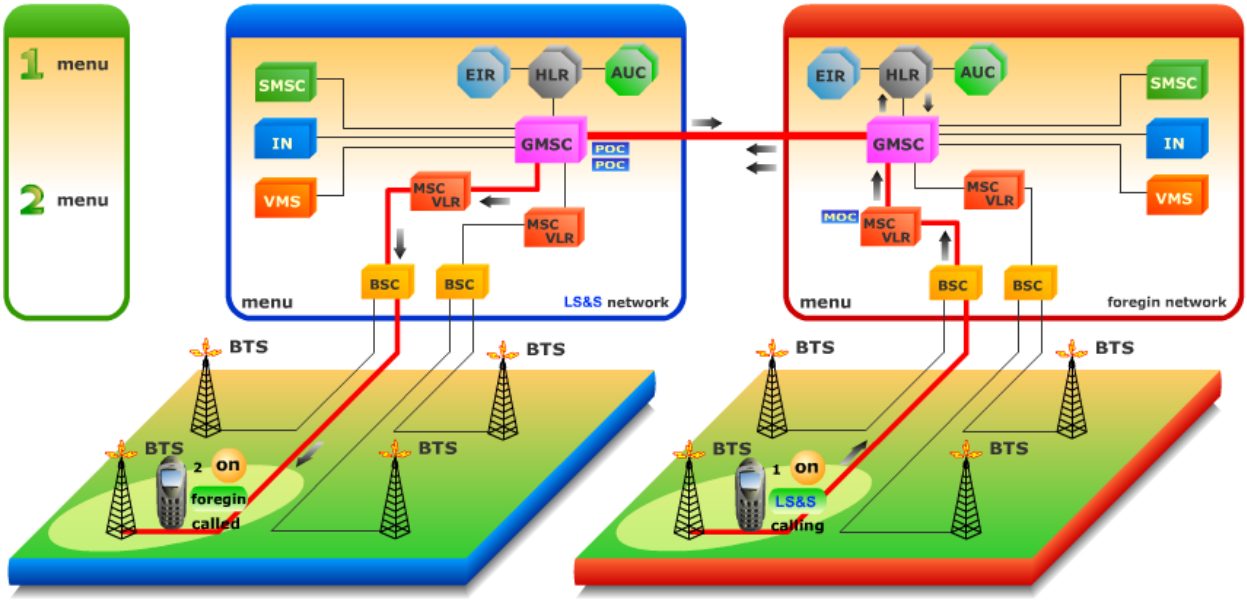
بعدها يقوم GMSC شركة موبايلي بتحويل الطلب الي (AUC – HLR – EIR) بغرض التحقق من صحة المكالمة

بعد التأكد من المكالمة يعيد (AUC – HLR – EIR) الطلب الهاتفي الي GMSC التابع لشركة موبايلي

يقوم GMSC التابع لشركة موبايلي بإرسال الطلب الي GMSC التابع لشركة المدار الجديد مرة اخري لتحويله الي الهاتف الذي سيستلم المكالمة والموجود في نطاق خدمة شركة المدار الجديد

بعدها يقوم GMSC التابع لشركة المدار الجديد بتحويل المكالمة الي الـ(MSC/VLR)

ومن الـ(MSC/VLR) ينتقل الطلب الهاتفي الي الـBSC ومنها الي الـBTS الموجود فيها الهاتف الذي يحمل شريحة شركة موبايلي والمتواجد تحت نطاق تغطية شركة المدار الجديد



بعض التعديلات والخيارات الموجودة في المحاكي.

طريقة تغيير حالة الهاتف

نعني هنا تغيير حالة الهاتف من حيث ان عند بداية تشغيل المحاكي هل سيتصل ام سيتصل به

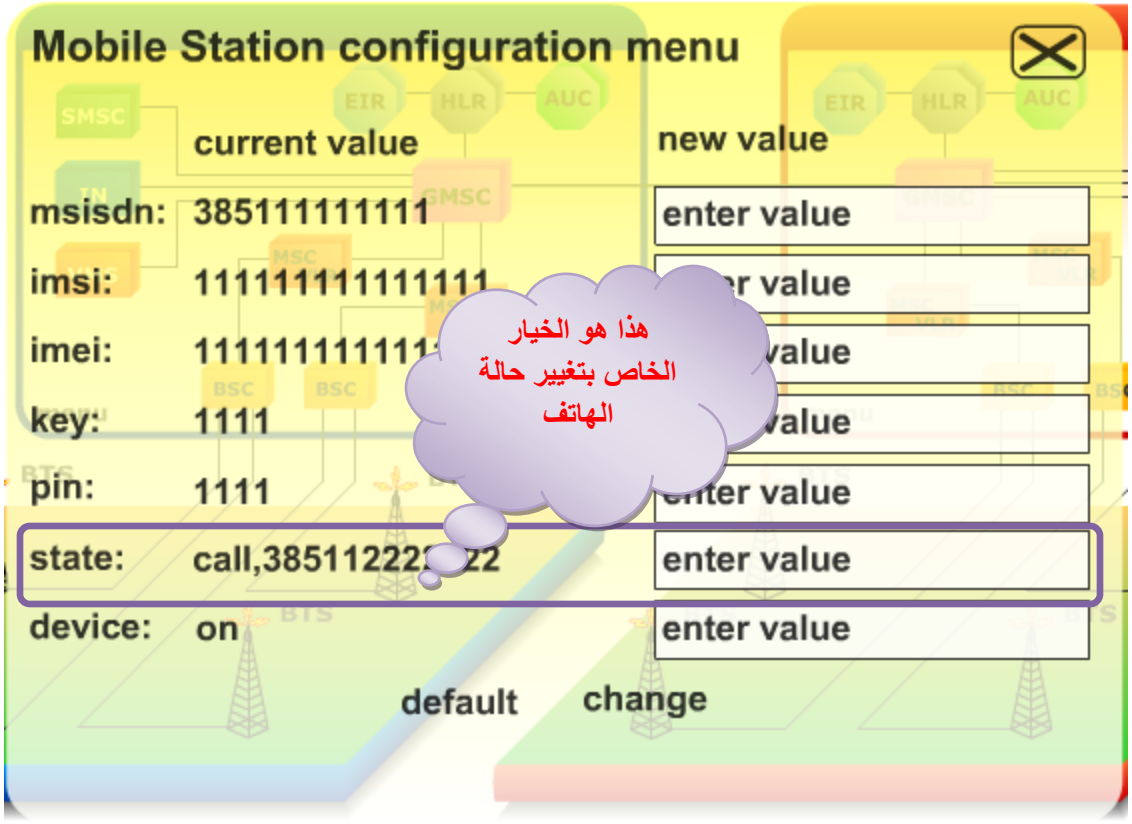
لتغيير ذلك نضغط علي كلمة Menu الموجودة بجانب الهاتف المراد تغيير حالته

وتغيير الخيار السادس الخاص بالحالة.

لجعل الهاتف رقم 2 هو من يقوم بالاتصال

قم بتغيير حالته الي call, 385111111111

وقم بتغيير حالة الهاتف رقم 1 الي Wait



طريقة تغيير رقم الهاتف

يمكن تغيير رقم الهاتف في البرنامج المحاكي

ولاكن عند تغيير رقم الهاتف في البرنامج يلزم تغيير الرقم في كل اعدادات البرنامج

كتغيره عند الشبكة وتغيره في قائمة الارقام المسموح بها

لتغيير رقم الهاتف اضغط علي كلمة Menu الموجودة بجانب الهاتف

وقم بتغيير الخيار الاول الخاص برقم الهاتف

ملاحضة

رقم الهاتف مقسم الي 12 رقم كما سبق توضيحه

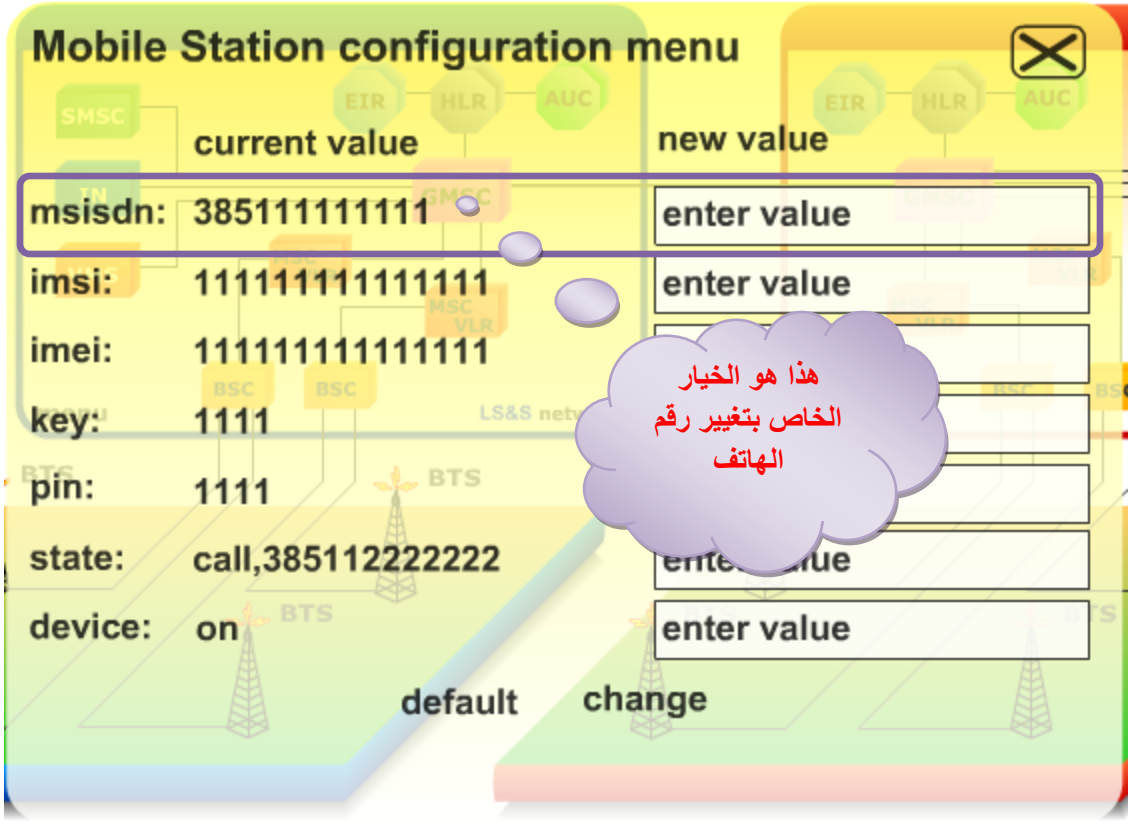
385111111111

الثلاثة الاولي خاصه بعنوان الدولة يمكن تغييرها

اما الرقمين الذي يليانها فهم رمز الشبكة لا يمكن تغييرهم

وهم اما 11 او 22

اما الارقام الباقية فهي رقم الهاتف ويمكن تغييره



كذلك يمكن تغيير IMSI و IMEI و KEY

ويجب عند تغييرهم تغيير إعدادات الشبكات وإدخال القيم الجديدة

منع هاتف من الاتصال او حجب الخدمة عنه

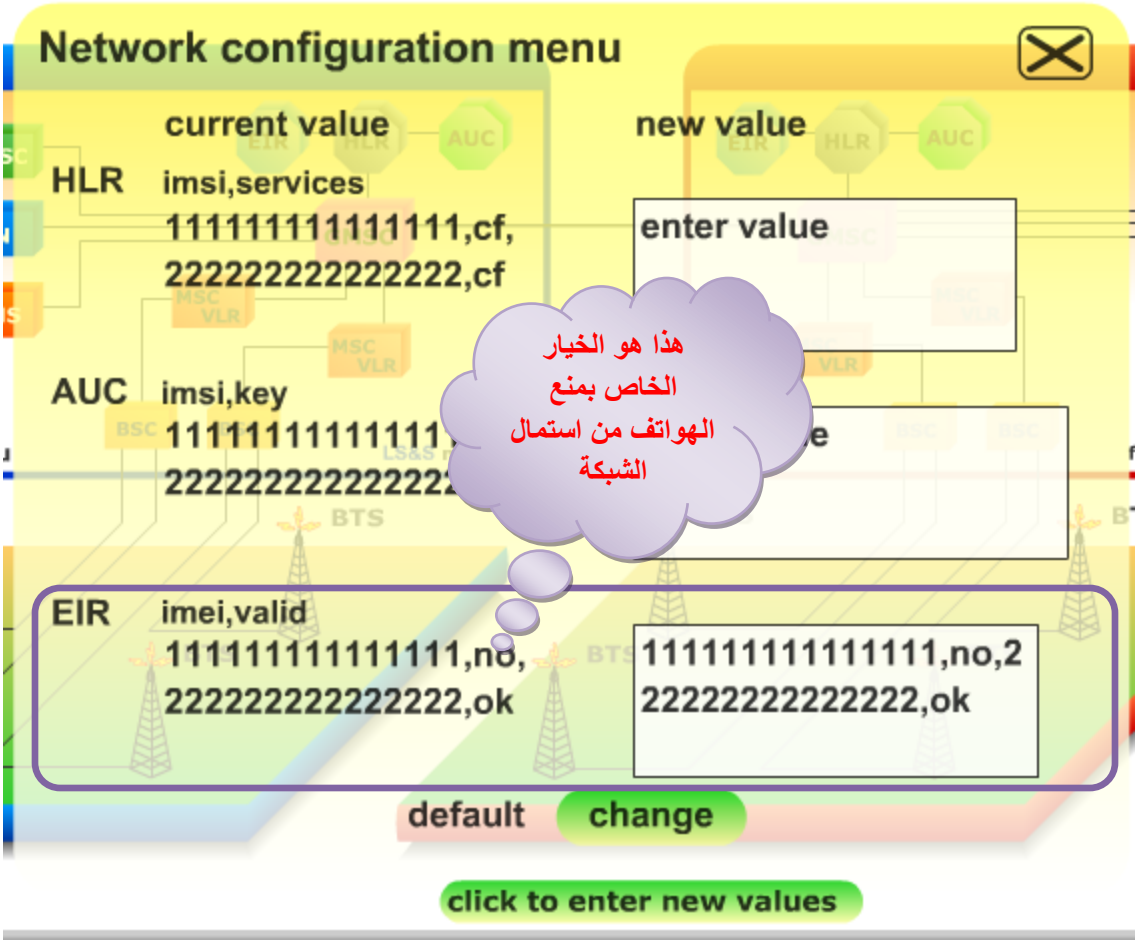
يمكن حجب الخدمة عن هاتف او منعه من الاتصال وذلك بوضع رقمIMEI الخاص بالهاتف في خانة الممنوع من استعمال الشبكة

لعمل ذلك نقوم بالضغط علي Menu الموجودة في الشبكة التي تريد منع الهاتف من استعمالها

والتعديل في مربع الادخال الاخير الخاص بقسم الـEIR

وتعديل احد ارقام الـIMEI وكتابة مقابلة بدل كلمه OK كتابة NO

ليتحول الهاتف الذي يحمل رقم الـIMEI الي هاتف ممنوع من استعمال تلك الشبكة

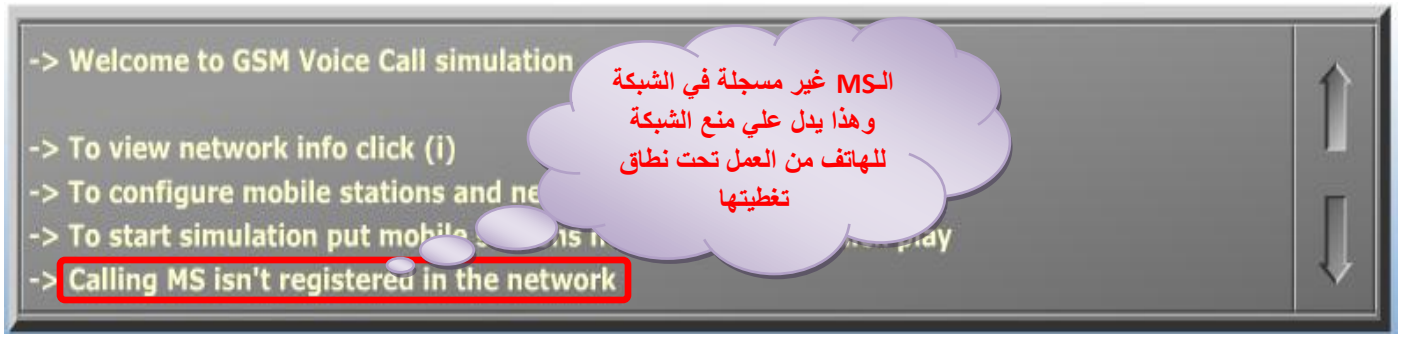


عند منع هاتف من استعمال شبكة معينة

وقمت بوضعه داخل نطاق تغطيتها لتجري فيه مكالمة

فلن تتم المكالمة وذلك لأن الشبكة لن تتعرف علي الهاتف

وسيضهر في شريط التوضيح في المحاكي ما يدل علي ان الهاتف غير متعرف علي



بهذا السطر نكون أخوتي في الله قد انتهينا من محاكاة عملية الاتصال بين هاتفين

وتم التطرق الي مكونات نضام الـGSM

تم بحمد الله في

2011-8-11

الموافق

11-رمضان-1432

وفي النهاية

أتمني ان تدعوا لي بالتوفيق في حياتي وبالرحمة بعد مماتي

ساهم في نشر الكتاب ولك الأجر بأذن الله

وانتظروني في كتب وبرامج أخري

أخوكم في الله

المبرمج الليبي

المهندس محمد ابوحولي

Eng.Mahammed@hotmail.com

+218926072758

والله أسأله قبول برامجي * مني وأشكره لما أعطاني**

صلي الإله علي النبي محمدا * ما ناح قمريٌ علي الاغصاني**

وعلي جميع بناته ونسائه * وعلي جميع الصحب والاخواني**

بالله قولو كلما استعملتموه * رحم الإله ثراك يا ورشفاني**