## Пособие по обучению продукту «Облачная АТС от Билайн».

## От автора

Данное руководство призвано в первую очередь для инженеров, чья работа связана с диагностикой проблем на мобильной сети и услугой с «Облачная АТС от Билайн».

Также материал будет полезен своей теоретической стороной для инженеров, которые хотят получить базовые знания в области работы мобильной сети и диагностики проблем на ней.

В данном материале будут рассмотрены основные элементы сети GSM, их назначение, расположение, взаимодействие, также будет разобрана модель входящего вызова, как основа для приобретения навыков диагностики проблем. Также будет разобрана сеть ОКС №7 в объеме, необходимом для базового понимания работы и диагностики проблем на сети сигнализации. В дополнение к этому рассматривается работа с аналитическим комплексом мониторинга «Polystar OSIX». В конце теории будет рассмотрена услуга «Облачная АТС от Билайн» как основа для понимания работы VAS услуг.

Хотелось бы отметить, что данное руководство не является исчерпывающим, а дает лишь начальный уровень знаний, который, безусловно, требуется пополнять и расширять. В вашем распоряжении всегда есть материалы в сети Интернет, материалы на внутреннем корпоративном портале, а, также, в конце будет дан перечень книг и статей, которые могут быть полезны при работе и дальнейшем изучении мобильной связи.

## Сеть GSM – как основа современной мобильной связи

## История

2G (2-джи) — аббревиатура для обозначения второго поколения беспроводной телефонной технологии.

Второе поколение сотовой связи 2G было запущено в коммерческую эксплуатацию по стандарту GSM в Финляндии компанией Radiolinja (сейчас является частью Elisa Oyj) в 1991. Тремя основными преимуществами сетей 2G по сравнению с предшественниками было то, что телефонные разговоры были зашифрованы с помощью цифрового шифрования; система 2G была значительно более эффективной; представила услуги передачи данных, начиная с текстовых сообщений СМС.

Технология 2G позволила различным мобильным сетям предоставлять услуги, такие, как текстовые сообщения, сообщения с изображениями и ММС (мультимедийные сообщения). Технология 2G достаточно безопасна как для отправителя, так и для получателя. Все текстовые сообщения зашифрованы в цифровой вид. Это цифровое шифрование передаёт данные таким образом, что только тот приёмник, которому они предназначены, может получить их и прочитать.

После того, как технология 2G была запущена, предыдущая технология была названа 1G (DAMPS). В то время как радиосигналы сети 1G являются аналоговыми, радиосигналы в сетях 2G являются цифровыми. Обе системы используют цифровые сигналы для подключения к базовой станции сотовой связи (которые прослушивают телефоны) к остальной части телефонной системы. 2G была заменена на новые технологии, такие, как 2.50G, 2.750G, 3,6G, и 4,20G; однако, сеть 2G до сих пор используется во многих частях мира.

Сеть 2G была построена, в основном, для голосовых услуг и медленной передачи данных (технология CSD). Скорость передачи данных — до 19,5 кБит/с

## 2.5G (GPRS)

Аббревиатура 2.5G («второе с половиной поколение») используется для описания систем 2G, в которых реализовывались домены с коммутацией пакетов в дополнение к доменам с коммутацией каналов. Это не обязательно обеспечивает более быстрое исполнение услуг, поскольку связывание временных интервалов используется также для услуг передачи данных с коммутацией каналов (HSCSD). Первым крупным шагом в эволюции GSM к 3G было введение General Packet Radio Service (GPRS).

Сети CDMA2000 аналогично развивались за счёт внедрения 1xRTT. Сочетание этих возможностей и стало известно, как 2.5G. GPRS может обеспечить скорость передачи данных от 56 кбит/с до 115 кбит/с. Он может быть использован для таких услуг, как доступ к WAP (беспроводному протоколу передачи данных), мультимедийных сообщений (MMS), а также для интернет-услуг связи, таких как электронная почта и World Wide Web Access.

Как правило, в сетях GPRS плата взимается за мегабайт переданного трафика, в то время как в случае традиционной сети с коммутацией каналов плата взимается за минуту соединения, не зависимо от того, сколько трафика пользователь использует. 1xRTT поддерживает двунаправленные (вверх и вниз) пиковые передачи данных до 153,6 кбит/с, обеспечивая среднюю пропускную способность 80—100 кбит/с в коммерческих сетях. Она также может быть использована для WAP, SMS и услуги MMS, как и для доступа в Интернет.

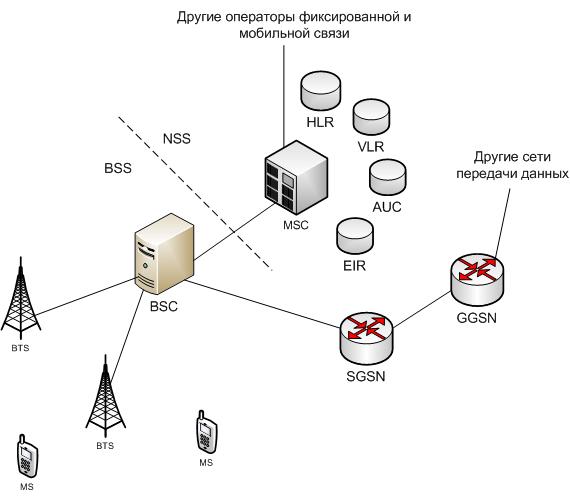
2.75G (EDGE)

GPRS1 сети превратились в сети EDGE с введением 8PSK кодирования. Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), или IMT Single Carrier (IMT-SC) является обратно совместимой цифровой мобильной технологией, которая позволяет улучшить скорость передачи данных, являясь расширением поверх GSM. EDGE была введена в сетях GSM с 2003 — первоначально фирмой Cingular (ныне AT&T) в США.

EDGE стандартизована 3GPP как часть семейства GSM, и это обновление, обеспечивающее потенциально трёхкратное увеличение мощности сетей GSM/GPRS. Скорость передачи данных — до 474 кбит/с.

## Структура сети GSM

Итак, рассмотрим основные элементы, входящие в состав системы GSM:



Сеть GSM делится на 2 системы. Каждая из этих систем включает в себя ряд функциональных устройств, которые, в свою очередь являются компонентами сети мобильной радиосвязи.

Данными системами являются:

* Система коммутации – **Network Switching System (NSS)**
* Система базовых станций - **Base Station System (BSS)**

Система **NSS** выполняет функции обслуживания вызовов и установления соединений, а также отвечает за реализацию всех назначенных абоненту услуг. NSS включает в себя следующие функциональные устройства:

* Центр коммутации мобильной связи (**MSC**)
* Домашний регистр местоположения (**HLR**)
* Визитный регистр местоположения (**VLR**)
* Центр аутентификации (**AUC**)
* Регистр идентификация абонентского оборудования (**EIR**).

Система **ВSS** отвечает за все функции, относящиеся к радиоинтерфейсу. Эта система включает в себя следующие функциональные блоки:

* Контроллер базовых станций (BSC)
* Базовую станцию (BTS)

**MS** (т.е. телефон абонента) не принадлежит ни к одной из этих систем, но рассматривается как элемент сети.

Теперь рассмотрим перечисленные элементы более подробно:

## Состав системы коммутации NSS

### Центр коммутации мобильной связи (MSC)

MSC является главным элементом системы GSM, он осуществляет контроль за BTS и BSC, расположенные в его зоне обслуживания.

Основная функция MSC заключается в установлении соединения между абонентами сети. Через него также осуществляется выход на другие сети связи: стационарную телефонную сеть, сети междугородной связи, другие сотовые сети.

### Домашний регистр местоположения (HLR)

HLR содержит информацию об абонентах, которые приписаны к оператору связи. В нем хранится информация о подключенных услугах, о состоянии абонента (включен, выключен, активное соединение), местоположении и некоторая другая информация, в том числе информация o CAMEL-подписках.

### Визитный регистр местоположения (VLR)

В VLR хранится информация об активных абонентах, которые находятся в зоне обслуживания данного MSC. В него занесены данные и о домашних абонентах, приписанных к данному MSC и о так называемых роумерах – абонентах, для которых данный MSC гостевой. Это могут быть абоненты других операторов связи, либо абоненты того же оператора, но из других регионов. В VLR информация поступает из HLR.

### Центр аутентификации (AUC)

AUC предназначен для аутентификации абонентов. Эта процедура предназначена для предотвращения несанкционированного доступа в сеть. Каждый раз, когда абонент включает свой телефон, совершает голосовой вызов, отправляет SMS и т.п. сеть предлагает пройти процедуру аутентификации. Её осуществляет MSC на основании данных полученных из AUC и от MS.

### **Регистр идентификации абонентского оборудования (EIR**)

EIR – это база данных, содержащая информацию о идентификационных номерах мобильных телефонов GSM. Данная информация необходима для осуществления блокировки краденых трубок. EIR не является обязательным элементом сети. В мире существует лишь несколько операторов, которые внедрили его в своей сети.

## Состав системы базовых станций BSS

### Контроллер базовых станций (BSC)

BSC управляет всеми функциями, относящимися к работе радиоканалов в сети GSМ. Это коммутатор большой емкости, который обеспечивает такие функции, как хэндовер MS, назначение радиоканалов и сбор данных о конфигурации сот. Каждый MSC может управлять несколькими BSC.

### Базовая станция (BTS)

BTS управляет радиоинтерфейсом с MS. BTS включает в себя такое радиооборудование, как трансиверы (приемо-передатчики) и антенны, которые необходимы для обслуживания каждой соты в сети.

## Пакетная передача данных и элементы сети, относящиеся к ней

### Узел обслуживания абонентов GPRS (SGSN)

Пакетные данные в отличии от голосового трафика передаются от подсистемы базовых станций не в сторону MSC, а в сторону SGSN. Этот элемент представляет собой маршрутизатор с расширенными функциями. На него возложены функции установления сессии пакетной передачи данных, маршрутизации пакетов, начисления платы за предоставленные услуги.

### Шлюзовой узел GPRS (GGSN)

GGSN представляет собой шлюз сети. Если пакеты маршрутизируются за пределы сети оператора, то они попадают именно в GGSN. Этот элемент часто конструктивно объединяется вместе с SGSN в одном устройстве.

## Третье поколение сетей (UMTS//3G)

### История

UMTS (англ. Universal Mobile Telecommunications System — Универсальная Мобильная Телекоммуникационная Система) — технология сотовой связи, разработана Европейским Институтом Стандартов Телекоммуникаций (ETSI) для внедрения 3G в Европе. В качестве способа передачи данных через воздушное пространство используется технология **W-CDMA**, стандартизованная в соответствии с проектом 3GPP, ответ европейских учёных и производителей на требование IMT-2000, опубликованное Международным союзом электросвязи как набор минимальных критериев сети сотовой связи третьего поколения.

С целью отличия от конкурирующих решений UMTS также часто называют 3GSM с целью подчеркнуть принадлежность технологии к сетям 3G и его преемственность в разработках с сетями стандарта GSM.

UMTS, используя разработки W-CDMA, позволяет поддерживать скорость передачи информации на теоретическом уровне до 21 Мбит/с (при использовании HSPA+). В настоящий момент самыми высокими скоростями считаются 384 Кбит/с для мобильных станций технологии R99 и 7,2 Мбит/с для станций HSDPA в режиме передачи данных от базовой станции к мобильному терминалу.

Это является скачком по сравнению со значением в 9,6 Кбит/с при передаче данных по каналу GSM или использованием в соответствии с технологией HSCSD нескольких каналов 9,6 Кбит/с (при этом максимально достигаемая скорость — 14,4 Кбит/с в CDMA One), и, наряду с другими технологиями беспроводной передачи данных (CDMA2000, PHS, WLAN), позволяет получить доступ к Всемирной Паутине и другим сервисам посредством использования мобильных станций.

### 3,5G (HSDPA)

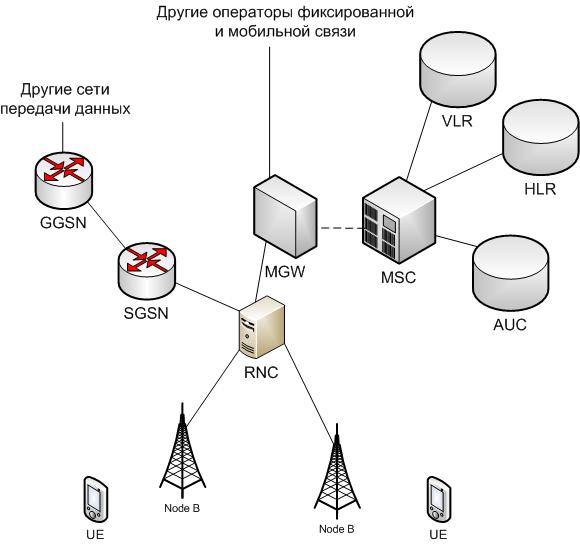
Начиная с 2006 года, на сетях UMTS повсеместно распространяется технология высокоскоростной пакетной передачи данных от базовой станции к мобильному терминалу HSDPA, которую принято относить к сетям поколения «3,5G».

К началу 2008 года HSDPA поддерживала скорость передачи данных в режиме «от базовой станции к мобильному терминалу» до 7,2 Мбит/с. Также ведутся разработки по повышению скорости передачи данных в режиме от мобильного терминала к базовой станции HSUPA.

UMTS позволяет пользователям проводить сеансы видеоконференций посредством мобильного терминала, однако опыт работы операторов связи Японии и некоторых других стран показал невысокий интерес абонентов к данной услуге. Гораздо более перспективным представляется развитие сервисов, предлагающих загрузку музыкального и видео контента: высокий спрос на услуги такого рода был продемонстрирован в сетях 2,5G.

## Структура сети UMTS (3G)

Рассмотрим структуру системы UMTS и ее основные отличия от стандарта второго поколения GSM.



### Подсистема коммутации

В первых релизах стандарта UMTS (R99, R4) подсистема коммутации не отличалась по своей структуре от той же подсистемы сетей второго поколения. В нее входили MSC – Mobile Switching Centre, который выполнял функции коммутации, установления соединения, тарификации и др., а также ряд регистров HLR, VLR, AUC, которые предназначены для хранения абонентских данных. В более поздних релизах (R5, R6, R7, R8) функции MSC были разделены между двумя устройствами: MSC-Server и MGW (Media gateway). MSC-Server отвечает за установление соединений, тарификацию, выполняет некоторые функции аутентификации. MGW представляет собой коммутационное поле, подчиненное MSC-Server.

### Подсистема базовых станций

В сети UMTS по сравнению с сетью GSM наибольшие изменения претерпела подсистема базовых станций. Отмеченные выше преимущества достигаются в первую очередь за счет новой технологии передачи информации между базовой станцией и телефоном абонента.

Итак, рассмотрим основные элементы, входящие в подсистему базовых станций:

* **RNC (Radio Network Controller)** – контроллер сети радиодоступа системы UMTS. Он является центральным элементом подсистемы базовых станций и выполняет большую часть функций: контроль радиоресурсов, шифрование, установление соединений через подсистему базовых станций, распределение ресурсов между абонентами и др. В сети UMTS контроллер выполняет гораздо больше функций нежели в системах сотовой связи второго поколения.
* **NodeB** – базовая станция системы сотовой связи стандарта UMTS.

Основной функцией NodeB является преобразование сигнала, полученного от RNC в широкополосный радиосигнал, передаваемый к телефону. Базовая станция не принимает решений о выделении ресурсов, об изменении скорости к абоненту, а лишь служит мостом между контроллером и оборудованием абонента, и она полностью подчинена RNC.

Оборудование абонента получило название UE (User Equipment). Тем самым подчеркивается, что в отличии от предшествующих стандартов в UMTS может быть не только обычный телефон, но и смартфон, ноутбук, стационарный компьютер и т.п.

Пакетные данные в сети UMTS передаются от MGW к известному нам по системе GSM элементу SGSN, после чего через GGSN поступают к другим внешним сетям передачи данных, например, Internet.

Как правило, SGSN и GGSN сети GSM применяются для тех же целей и в сети UMTS. Производится только коррекция программного обеспечения данных элементов.

## Сети четвертого поколения. LTE

## 4G. LTE - Long Term Evolution

### История

Стандарты третьего поколения позволяют предоставить широкий перечень мультимедийных услуг и поддерживают скорости передачи данных до 14Мбит/сек. Это вполне соответствует запросам абонентов в настоящее время. Однако, объемы передаваемой информации в телекоммуникационных сетях растут с каждым днем. Чтобы удовлетворить потребности пользователей по скорости передачи данных и набору услуг хотя бы на 20 лет вперед необходим новый стандарт, уже четвертого поколения.

Работа над первым стандартом четвертого поколения - LTE (Long Term Evolution) началась в 2004 году организацией 3GPP. Главными требованиями, которые предъявлялись в процессе работы над стандартом были следующие:

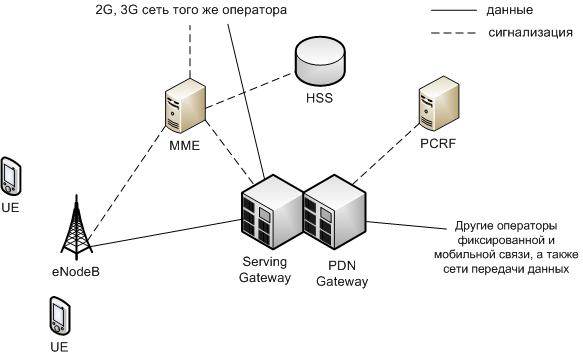
* Скорость передачи данных выше 100 Мбит/сек.
* Высокий уровень безопасности системы
* Высокая энергоэффективность
* Низкие задержки в работе системы
* Совместимость со стандартами второго и третьего поколений

В конце 2009 года в Швеции была запущена в коммерческую эксплуатацию первая сеть стандарта LTE.

Сети LTE поддерживают скорости передачи данных до 326,4 Мбит/сек. К примеру, загрузка фильма в хорошем качестве займет менее одной минуты. Таким образом, верхняя планка по скорости передачи данных практически снимается.

### Структура сетей LTE

Рассмотрим структуру сети LTE:



Из схемы сети LTE, представленной выше, уже видно, что структура сети сильно отличается от сетей стандартов 2G и 3G.

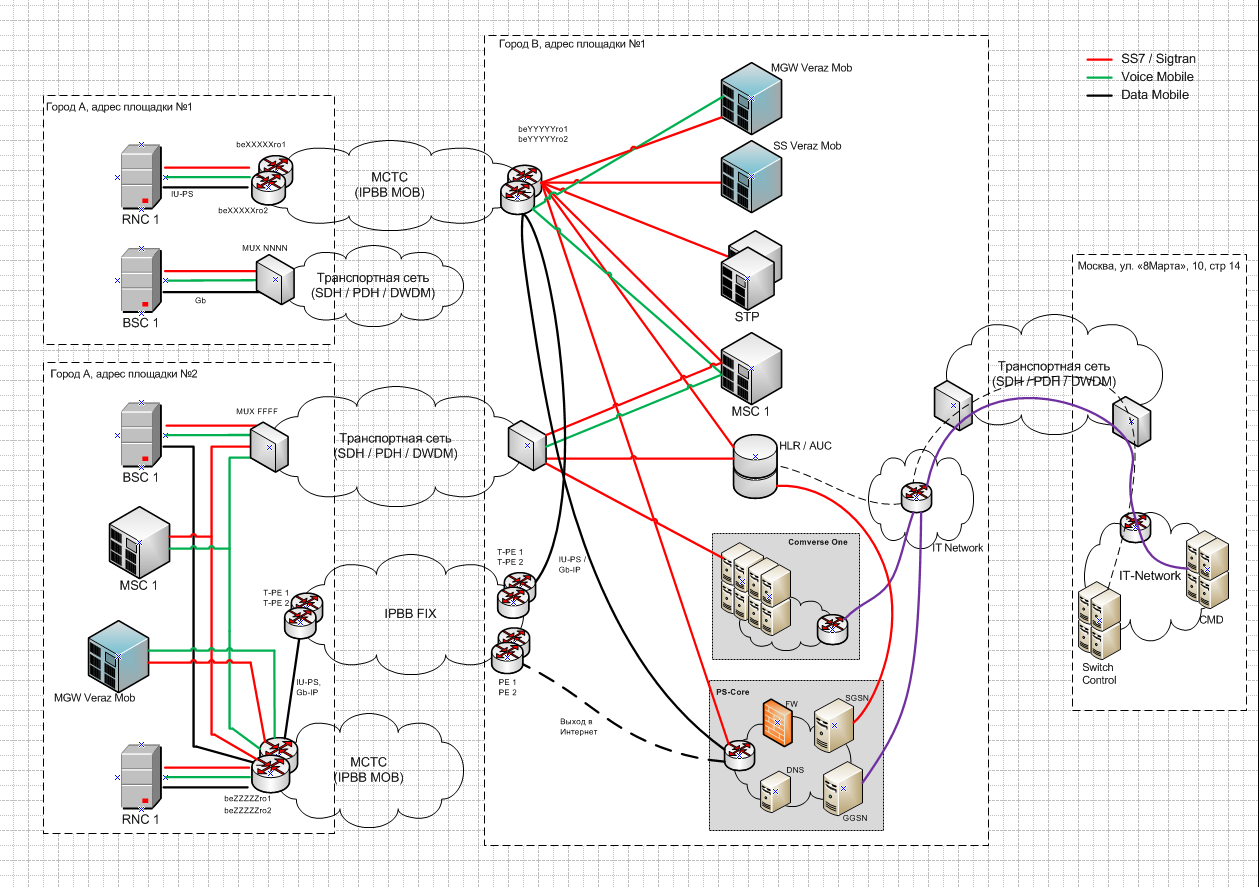
Существенные изменения претерпела и подсистема базовых станций, и подсистема коммутации. Была изменена технология передачи данных между оборудованием пользователя и базовой станцией. Также подверглись изменению и протоколы передачи данных между сетевыми элементами. Вся информация (голос, данные) передается в виде пакетов. Таким образом, уже нет разделения на части обрабатывающие либо только голосовую информацию, либо только пакетные данные.

Можно выделить следующие основные элементы сети стандарта LTE:

* **Serving SAE Gateway** или просто Serving Gateway (SGW) – обслуживающий шлюз сети LTE. Предназначен для обработки и маршрутизации пакетных данных поступающих из/в подсистему базовых станций. По сути, заменяет MSC, MGW и SGSN сети UMTS. SGW имеет прямое соединение с сетями второго и третьего поколений того же оператора, что упрощает передачу соединения в /из них по причинам ухудшения зоны покрытия, перегрузок и т.п.
* **Public Data Network (PDN) SAE Gateway** или просто PDN Gateway (PGW) – шлюз к/от сетей других операторов. Если информация (голос, данные) передаются из/в сети данного оператора, то они маршрутизируются именно через PGW.
* **Mobility Management Entity (MME)** – узел управления мобильностью. Предназначен для управления мобильностью абонетов сети LTE.
* **Home Subscriber Server (HSS)** – сервер абонентских данных. HSS представляет собой объединение VLR, HLR, AUC выполненных в одном устройстве.
* **Policy and Charging Rules Function (PCRF)** – узел выставления счетов абонентам за оказанные услуги связи.

Все перечисленные выше элементы относятся к системе коммутации сети LTE. В системе базовых станций остался лишь один знакомый нам элемент – базовая станция, которая получила название **eNodeB**. Этот элемент выполняет функции и базовой станции, и контроллера базовых станций сети LTE. За счет этого упрощается расширение сети, т.к. не требуется расширение емкости контроллеров или добавления новых.

## Структура мобильной сети Билайн



На схеме представлена типовая реализация работы узлов мобильной сети Вымпелком. Особое внимание стоит уделить взаимосвязи между городами – в современных сетях используются стыки IPBB между роутерами beXXXXro1/2 и beYYYYro1/2, связность и наличие между ними трафика можно отслеживать на ресурсе <https://manager.sovintel.net/mrtg/> (вкладка MSTN). В частности, это может потребоваться для диагностики аварий, связанных с обрывом ВОЛС и определения корректного влияния.

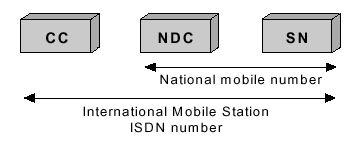
## Идентификаторы сети GSM

Идентификаторы сети – ряд номеров, которые сеть GSM использует для определения местоположения абонента при установлении соединения. Данные идентификаторы используются для маршрутизации вызовов к MS. Важно, чтобы каждый идентификационный номер был уникальным и был всегда корректно определён.

## Идентификаторы абонентов

### Номер мобильной станции (MSISDN)

Номер абонента (Mobile Station ISDN number – **MSISDN**) уникально определяет абонирование мобильного абонента в номерном плане сети PSTN. Данный номер набирается при установлении входящего соединения к абоненту сети мобильной связи.



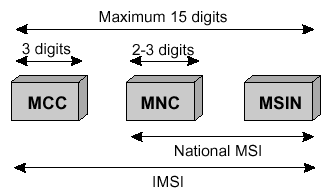
* **CC** (Country Code) - код страны
* **NDC** (National Destination Code) - национальный код пункта назначения
* **SN** (Subscriber Number) – номер абонента

Для каждой сети PLMN существует свой NDC. Например, в Ирландии NDC может быть 086 и 087, что указывает на наличие двух операторов PLMN. В России для каждой PLMN определены несколько NDC. Интернациональный номер MSISDN может быть переменной длины. Максимальная длина составляет 15 цифр, префиксы не включаются (+7). Входящее соединение с абонентом МГТС осуществляется набором +7 495 XXX XXXX.

### Интернациональный идентификатор мобильного абонента (IMSI)

International Mobile Subscriber Identity (**IMSI**) уникален для каждого оператора. По данному номеру происходит идентификация абонента через радиоэфир и через всю сеть. Данный номер используется для сигнализации PLMN. IMSI хранится в SIM, в HLR и в обслуживающем VLR.

IMSI состоит из трёх основных частей:



* **MCC** (Mobile Country Code) - код страны.
* **MNC** (Mobile Network Code) – код сети мобильной связи.
* **MSIN** (Mobile Station Identification Number) – идентификационный номер MS

Согласно спецификациям GSM, максимальная длина IMSI составляет 15 цифр.

### Временный идентификатор мобильного абонента (TMSI)

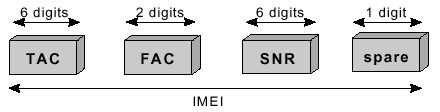
Temporary Mobile Subscriber Identity (**TMSI**) - временный номер IMSI, который дается MS при её регистрации. Он используется для того, чтобы защитить абонента от прослушивания и несанкционированного доступа в радиочастотном тракте.

TMSI используется только для локального абонирования (только в одной зоне MSC/VLR) и изменяется при изменении местоположения (Location Update). Структура TMSI может быть определена каждым оператором, но не может превышать 8 цифр. Поскольку TMSI имеет в два раза меньший размер, чем IMSI, пейджинг в одном кадре осуществляется для двух абонентов, что также сокращает нагрузку на процессор.

### Идентификационный номер оборудования MS (IMEI)

International Mobile Equipment Identity (**IMEI**) используется для уникальной идентификации мобильного оборудования в сети. Данный код используется в процедурах обеспечения безопасности связи для идентификации украденного оборудования и предотвращения неавторизованного доступа в сеть. Согласно спецификациям GSM, длина IMEI составляет 15 цифр:

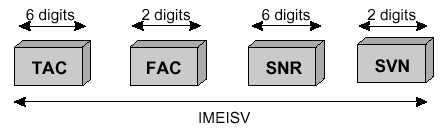
* **TAC** (Type Approval Code) - код утвержденного типового образца.
* **FAC** (Final Assembly Code) - код окончательно собранного изделия, присваивает производитель.
* **SNR** (Serial Number) - индивидуальный серийный номер. Идентифицирует полностью все оборудование с учетом кодов TAC и FAC
* **Spare -** свободные цифры. Зарезервированы для будущего использования. Когда данный код передается в MS, значение данного кода должно быть всегда «0».



### Интернациональный идентификатор оборудования MS и номер программного обеспечения (IMEISV)

International Mobile Equipment Identity и Software Version number (**IMEISV**) обеспечивает уникальную идентификацию каждой MS, а также обеспечивает соответствие версии программного обеспечения, инсталлированного в MS, разрешенному оператором. Версия программного обеспечения является важным параметром, так как от этого зависят услуги, доступные для MS, а также способность выполнять речевое кодирование. Так, например, PLMN необходимо знать возможности речевого кодирования MS при установлении соединения (например, half rate/full rate, и т д.). Данные возможности отображаются с помощью IMEISV.

Идентификатор IMEISV состоит из:

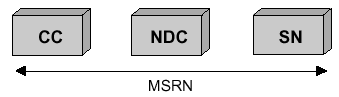
****

**SVN** (Software Version Number) - номер программной версии, позволяет производителю MS идентифицировать различные версии программного обеспечения утверждённого типового образца MS. SVN со значением 99, зарезервирован для будущих целей.

## Идентификаторы местоположения

### Номер MS в роуминге (MSRN)

Mobile Station Roaming Number (**MSRN**) - временный сетевой номер, назначаемый в течение установления соединения для MS, находящейся в роуминге. MSRN состоит из трёх частей:



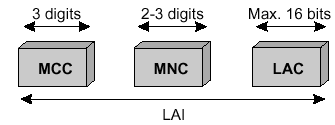
В этом случае SN означает адрес обслуживающего MSC/VLR.

### Идентификатор местоположения (LAI)

Location Area Identity (**LAI**) – временный сетевой идентификатор, который тоже требуется для маршрутизации вызовов. Данный код введён для двух целей:

1. Пейджинг. В этом случае LAI используется для информирования MSC о LA, в которой находится MS.
2. Обновление местоположения абонента

LAI состоит из следующих блоков:

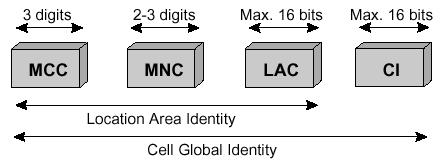
****

Location Area Code (**LAC**) - код местоположения, максимальная длина LAC составляет 16 бит, что позволяет определить 65536 различных LA внутри одной PLMN.

### Глобальный идентификатор соты CGI

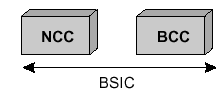
Cell Global Identity (CGI) используется для идентификации индивидуальной соты внутри LA. Идентификация соты осуществляется посредством добавления параметра Cell Identity (CI) к компонентам LAI. CI имеет размер 16 бит.

CGI состоит из:

****

### Идентификационный код БС (BSIC)

Base Station Identity Code (**BSIC**) дает возможность MS различать соты. BSIC состоит из:

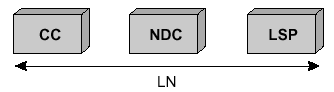
****

* **NCC** - National Color Code (национальный цветовой код). Используется для того, чтобы разграничивать зоны действия операторов в тех местах, где сети операторов перекрывают друг друга.
* **BCC** – Base station Color Code (цветовой код базовой станции). Используется для того, чтобы различать между собой базовые станции, использующие одинаковые частоты.

### Номер местоположения LN

Location Number (**LN**) – номер определённой географической зоны LA, зона обслуживания MSC/VLR. Данный номер используется для регионального/локального абонирования услуг сети мобильной связи и для тарификации на основе географического местоположения абонента.

LN состоит из:

****

**LSP** Locally Significant Part. Локально важная часть

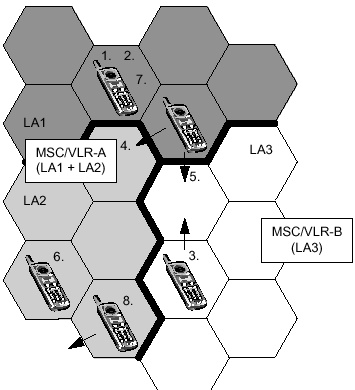
### Конфиденциальная процедура идентификации абонента

Каждый раз, когда MS делает запрос на системные процедуры (LU, попытка вызова или активация сервиса) MSC/VLR ставит новый TMSI.в соответствие с IMSI MSC/VLR передаёт TMSI в MS, которая хранит его в SIM-карте. Сигнализация между MSC/VLR и MS использует только на основе TMSI. Таким образом, реальный номер абонента IMSI не передается через радиоэфир. TMSI в два раза короче IMSI, следовательно, в одном сообщении можно передать пейджинг для двух абонентов. IMSI используется тогда, когда процедура Location Updating выполнена неудачно или не назначен TMSI.

Теперь рассмотрим состояния MS в зависимости от различных сценариев.

## Варианты сценариев обслуживания вызовов

## Варианты сценариев обслуживания вызовов: MS в состоянии IDLE

****

1. Регистрация в сети, регистрация IMSI (**IMSI attach**)

2. Обновление местоположения (**Location updating**)

3. Смена соты внутри LA

4. Обновление местоположения внутри одного MSC/VLR

5. Обновление местоположения при входе в зону действия нового MSC/VLR

6. Обновление местоположения, тип - периодическая регистрация.

7. Отключение от сети (**IMSI detach**)

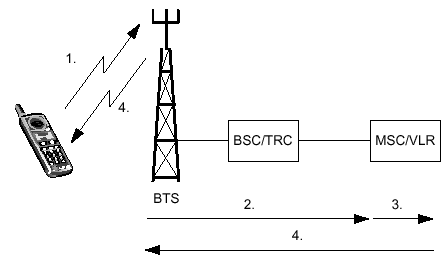
8. Полное отключение от сети (отсутствует информации о местонахождении MS) (**Implicit detach)**

### Включение MS в сеть

#### IMSI Attached

Когда абонент включает MS (включает питание на MS), выполняется процедура IMSI attach, которая содержит в себе следующие шаги:

1. MS передаёт в сеть сообщение «IMSI attach» указывая на то, что она изменила своё состояние из неактивного в IDLE.
2. VLR определяет, существует ли запись об этом MS. Если нет, то VLR связывается с HLR, к которому приписана данная MS, и копирует в себя данные абонирования этого абонента.
3. После этого VLR осуществляет обновление состояния MS и переводит это состояние в IDLE.
4. На MS передается уведомление.

****

#### Обновление местоположение (LU), тип - IMSI attach

Если MS изменила LА будучи в состоянии OFF, то процедура IMSI attach может привести к обновлению местоположения MS. VLR в течение выполнения процедуры IMSI attach может определить, что текущий идентификатор LAI мобильной станции отличается от LAI, хранящегося в SIM-карте MS. Если это так, то VLR обновляет информацию о LAI мобильной станции.

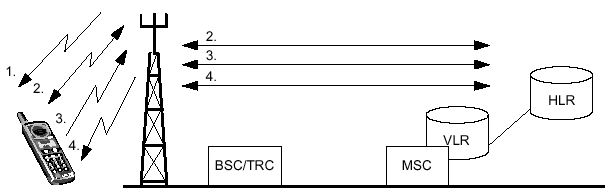
### Сетевой роуминг

#### Смена соты внутри LA

MS постоянно находится процессе перемещения по всей сети. Информация о местоположении MS отображается с помощью параметра зоны местоположения **Location Area** (LA) и хранится в VLR. Если MS меняет соты внутри одной LA, процедура обновления местоположения в сети не выполняется. Информацию о том, что новая сота принадлежит той же LA, мобильная станция получает из канала BCCH соседних сот. По каналу BCCH передается LAI сот. MS сравнивает принятое значение LAI с новым LAI. Если LAI совпадают, то это означает, что обновление местоположения выполняться не будет и нет необходимости оповещать об этом сеть.

#### Обновление местоположения внутри одного MSC/VLR

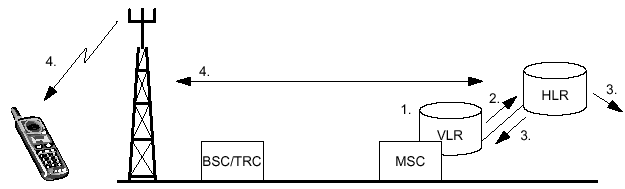
Если MS обнаруживает изменения в LAI на основе анализа информации, передаваемой по каналу BCCH, она информирует об этом сеть. Когда MS передает сообщение об обновлении местоположения, MSC/VLR определяет, зарегистрирован ли данный абонент в этом VLR, или он переместился в зону обслуживания данного MSC/VLR из зоны обслуживания другого MSC/VLR.

****

1. MS прослушивает BCCH в новой соте, чтобы определить LAI. Новый LAI сравнивается со старым. Если существует различие, то необходимо провести обновление местоположения.
2. MS устанавливает соединение с сетью через SDCCH. Выполняется аутентификация.
3. Если аутентификация прошла успешна, MS делает запрос в систему об обновлении местоположения.
4. Система подтверждает LU и дает команду базовой и мобильной станциям на освобождение канала.

#### Обновление местоположения при входе в зону обслуживания нового MSC/VLR

Обновление местоположения (LU) осуществляется тогда, когда MS перемещается в новую LA. Однако мобильной станции неизвестно, принадлежит ли LA новому MSC/VLR. Когда новый VLR принимает запрос об LU, то выполняется следующее:

****

1. Выполняется аутентификация. Если аутентификация прошла успешно, VLR проверяет свою БД, чтобы определить, есть ли там информация о данном абоненте.
2. Когда VLR не находит информации о MS, он передаёт запрос в HLR абонента для осуществления копирования данных об этом абоненте в свой VLR.
3. HLR передаёт информацию в VLR и обновляет у себя информацию о местоположении MS.
4. VLR записывает информацию об MS, включающую в себя данные о последнем местоположении и состоянии IDLE. VLR передает оповещение в MS.

#### Обновление местоположения, тип - периодическая регистрация

Периодическая регистрация – это услуга, которая позволяет MS посылать регистрационные сообщения через определённые интервалы времени. В случае, если MS не регистрируется через определённый интервал времени, то система помечает MS как выключенную (detached). Последнее случается тогда, когда MS оказывается вне зоны обслуживания сети или в этом случае, когда системе нет необходимости осуществлять пейджинг на мобильную станцию. В случае, если сеть использует процедуру периодической регистрации, информация о периоде регистрации мобильной станции передается по каналу BCCH. Периодическая регистрация использует системное сообщение **acknowledgment message**. MS пытается зарегистрироваться в сети до тех пор, пока она не получит данное сообщение.

### Отключение от сети

#### Отключение IMSI (IMSI Detach)

Отключение IMSI указывает сети, что MS перешла в неактивное состояние. MS при отключении от сети направляет в сеть сообщение о своем отключении. VLR, получив такое сообщение, отмечает соответствующий IMSI как отключенный. HLR при этом не уведомляется. На MS не отправляется никакого подтверждающего сообщения.

#### Полное отключение от сети (Implicit Detach)

Если MS направляет в сеть сообщение об отключении в условиях плохого качества обслуживания, система может не расшифровать информацию о выключении MS. Так как на MS не отправляется никакого подтверждающего сообщения, дальнейшие попытки сообщить об отключении не делаются. С помощью метода периодической регистрации сеть по истечении периода регистрации определит, что MS отключена. После этого VLR выполнит скрытое отключение, отмечая MS как отключенную. (Implicit Detach).

В случае, если MS выходит из зоны обслуживания сети и не выходит на связь в течение периода регистрации, то система также отмечает состояние MS как Implicit Detach.

#### Удаление из VLR информации о MS (MS Purging)

Эта процедура используется для того, чтобы информировать HLR о предстоящем удалении информации о конкретном MS из VLR. После удаления из VLR этой информации HLR устанавливает флажок, указывающий на то, что данные о MS удалены и воспринимает эту MS как недоступную. Это исключает лишние процессы в сети, а также сокращает затраты ресурсов на проверку базы данных абонента.

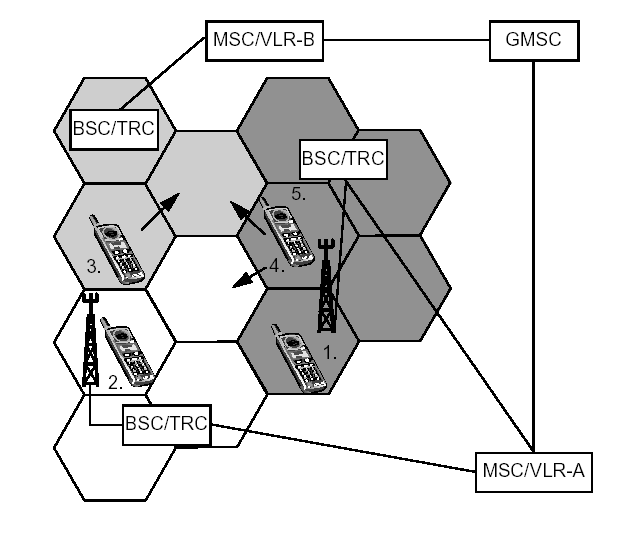
Рассмотрим пример, когда MS из России перемещается в Германию и производит обновление данных о местоположении в MSC/VLR сети GSM в Германии. Далее абонент переезжает обратно в Россию. Переезд из Германии в Россию занимает некоторое время. На протяжении этого времени MS абонента находится в неактивном режиме. Если не применять процедуру удаления данных об MS (MS Purging), то при поступлении вызова к данному абоненту HLR определяет MS как зарегистрированную в MSC/VLR Германии и направляет вызов в сеть GSM Германии. Затем MSC/VLR сети GSM Германии уведомляет HLR, что абонент недоступен.

При применении процедуры удаления данных об MS (MS Purging) запись российского абонента будет удалена из MSC/VLR Германии и при поступлении входящего вызова к этому абоненту HLR видит, что MS недоступна и, следовательно, не направляет вызов в MSC/VLR Германии.

## Варианты сценариев обслуживания вызовов

##### **MS в активном режиме**

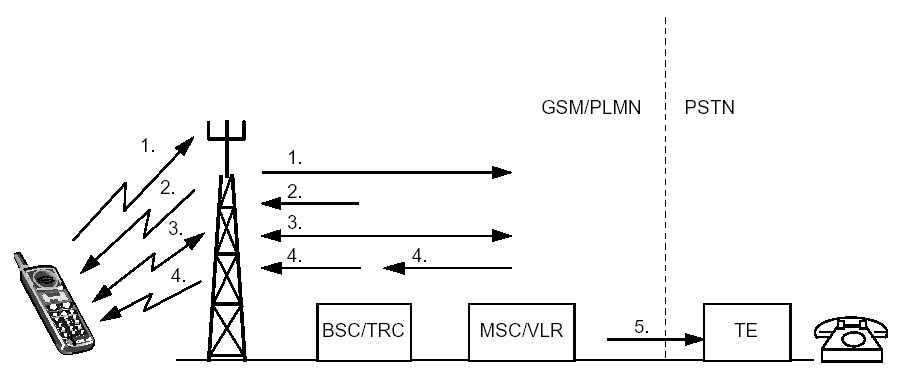
MS находится в активном режиме тогда, когда она занята обслуживанием вызова, это состояние не зависит от вида трафика (речевого, факсимильного или передачи данных) и типа соединения (входящего или исходящего).



1. Исходящий вызов от MS (тип трафика: речевой, факсимильный, передача данных или сообщения SMS).
2. Входящий вызов к MS (тип трафика: речевой, факсимильный, передача данных, сообщений SMS или рассылка сообщений оператора (cell broadcast)).
3. Хэндовер внутри BSC
4. Хэндовер между разными BSC внутри одного MSC
5. Хэндовер между разными MSC

##### **Исходящий вызов (MS – PSTN)**

В этом разделе описывается процесс обслуживания исходящего вызова, направленного от MS в сеть общего пользования. Передача информации и данных описываются отдельно.



* 1. MS использует канал RACH для запроса сигнального канала.
  2. BSC/TRC назначает канал AGCH.
  3. MS через SDCCH направляет в MSC/VLR запрос на установление соединения. Все процессы сигнализации, предшествующие установлению соединения на канале трафика, проходят через канал SDCCH. К процессам сигнализации относятся:

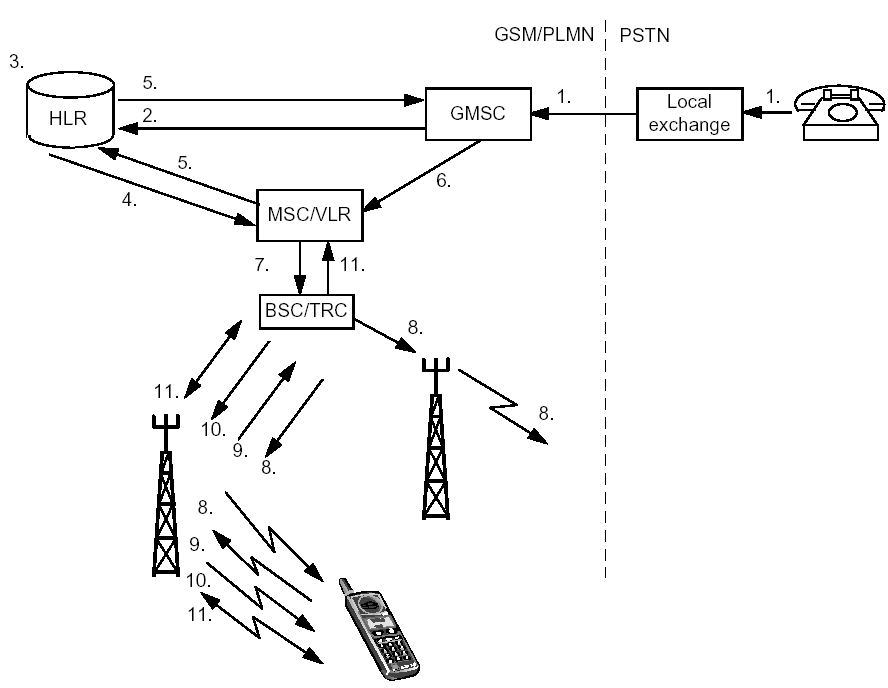
Отметка в VLR активного состояния MS (IMSI Attach).

* + - Процедура аутентификации.
    - Идентификация оборудования.
    - Передача в сеть цифр В-номера абонента (набираемый номер).
    - Проверка статуса услуги «Запрет на исходящую связь» для данного абонента (инициирована/неинициирована)
  1. MSC/VLR дает команду BSC/TRC назначить свободный TCH. BТS и MS получают команду настроиться на заданный TCH.
  2. MSC/VLR направляет В-номер абонента на PSTN для установления соединения.
  3. При ответе абонента связь считается установленной.

##### **Входящий вызов (PSTN - MS)**

Главным отличием процедуры обслуживания входящего вызова от исходящего вызова является то, что при поступлении входящего вызова на MS неизвестно точное местоположение абонента. Следовательно, прежде чем установить связь с MS, необходимо передать вызывное сообщение (пейджинг) для определения местоположения MS.

Ниже приведено описание процедуры установления соединения для входящего вызова от абонента PSTN к мобильному абоненту. Вызов с MS на MS происходит по той же схеме. Отличие только в том, что при входящей связи от MS установление соединения с MSC/VLR проходит через GMSC, а не через узел PSTN.



1. Абонент PSTN набирает номер MS (MSISDN). MSISDN анализируется в PSTN, которая определяет, что осуществляется вызов абонента мобильной сети. Устанавливается связь с GMSC, которому принадлежит MS.
2. GMSC анализирует MSISDN, чтобы выяснить, в каком HLR зарегистрирован MS. Затем GMSC запрашивает у HLR информацию о том, как маршрутизировать вызов на обслуживающий его MSC/VLR.
3. HLR устанавливает соответствие между MSISDN и IMSI и определяет, какой MSC/VLR обслуживает MS в настоящее время. HLR также проверяет, активизирована ли услуга «Переадресация вызова». Если услуга в активном состоянии, GMSC переадресует вызов на заданный номер.
4. HLR запрашивает MSRN у обслуживающего MSC/VLR.
5. MSC/VLR возвращает MSRN через HLR на GMSC.
6. GMSC анализирует MSRN и совершает вызов на него в сторону MSC/VLR
7. MSC/VLR располагает информацией о том, в какой LA находится MS. Пейджинговое сообщение направляется на BSC, который контролирует эту LA.
8. BSC направляет пейджинговые сообщения на все BТS, которые распространяют ее в нужной LA. BТS передают это сообщение по радиоинтерфейсу, используя канал РСН. Для пейджинга сеть использует IMSI или TMSI, действительный только в зоне обслуживания текущего MSC/VLR.
9. Когда MS определяет, что пейджинговое сообщение предназначено именно ей, она отправляет запрос на выделение канала SDCCH.
10. BSC обеспечивает SDCCH, используя AGCH (передает по каналу AGCH номер канала SDCCH, назначенный данной MS).
11. Канал SDCCH используется для процедуры установления соединения. По этому каналу передается информация о номере канала TCH, назначенного данному MS на время установления соединения.
12. Мобильный телефон начинает звонить. Когда абонент ответит, соединение считается установленным.

После того как какая-либо сторона завершит соединение в сеть придут сообщения **DISCONNECT** по протоколу DTAP и **REL** протокола ISUP, в которых будут содержаться причины разъединения вызова, которые описаны стандартом Q.931 ([вики-статья](https://ru.wikipedia.org/wiki/Q.931)). Более подробно причины расписаны в данном [материале](http://www.solyar.ru/glossary/110/isdn-prichiny-razedineniya/).

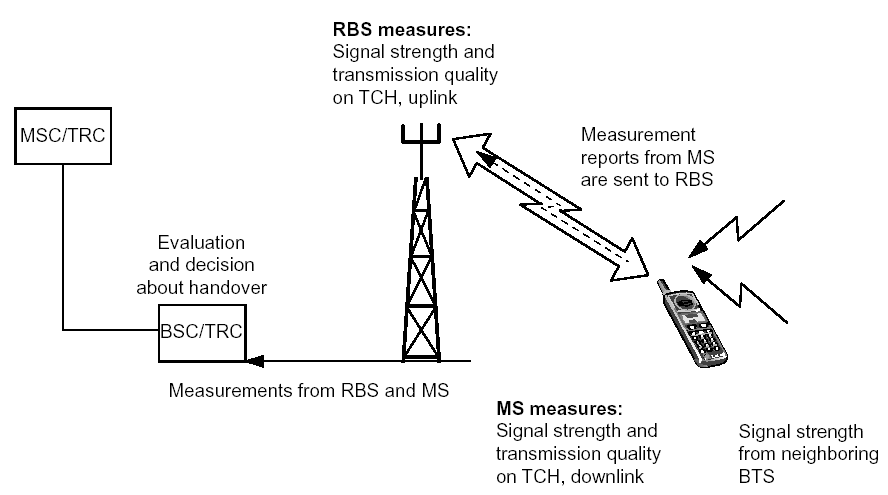
Теперь предлагаю ознакомиться с процедурой **хэндовера**, которая помимо полезных действий, иногда может служить причиной разъединения вызовов, если данная процедура пройдет некорректно.

##### **Хэндовер (Handover)**

В терминологии GSM процесс смены сот во время соединения называется хэндовером. Выбор лучшей соты и измерения ее параметров производятся с помощью MS и BТS. Так как MS в выборе хэндовер играет важную роль, такой тип хэндовера часто называется хендовером с участием мобильных систем (МАНО – Mobile Assisted HandOver).

###### **Процедура осуществления хэндовера (Locating)**

MS измеряет уровни и качество сигнала своей собственной соты и уровни сигналов несущей ВССН соседних сот. Передача запроса на выполнение измерения производится в направлении dawlink, когда MS находится в активном режиме. Результаты замеров отправляются на BТS по каналу SACCH через определенные интервалы времени. Обслуживающая BТS, получая от MS данные измерений, также осуществляет измерения.

****

Измерения от BТS и MS передаются в форме отчетов об измерениях (Measurement Reports). Основываясь на этих отчетах, BSC принимает решение о необходимости выполнения хэндовера. Если BSC принимает решение о выполнении хэндовера, он определяет, в какую соту будет передаваться управление. Этот процесс называется процедура осуществления хэндовера (locating).

Как только определяется, что какая-то из соседних сот лучше, чем обслуживающая сота, осуществляется хэндовер.

Другой причиной осуществления хэндовера является величина временной задержки (ТА). Если она превышает установленное оператором пороговое значение, осуществляется хэндовер. Обычно это происходит во время перемещения MS от одной соты к другой.

Как только MS переместится в другую соту, новая BТS информирует MS о новых соседних несущих ВССН. Последнее делается для того, чтобы могли быть произведены новые измерения. Если MS также переключается на новую LA, то новые данные об изменении местоположения будут обновлены по окончании разговора.

Хэндовер может использоваться для распределения нагрузки между сотами. Во время попытки установления соединения в перегруженную соту MS может быть перенаправлена в соту с меньшим трафиком, где качество соединения приемлемое.

Ниже приводятся различные типы хэндоверов:

* Хэндовер внутри соты;
* Хэндовер между сотами, контролируемыми одной и той же BSC;
* Хэндовер между сотами, контролируемыми разными BSC, но одной и то же MSC/VLR;
* Хэндовер между сотами, контролируемыми разными MSC.

Каждый из этих случаев описывается более подробно ниже.

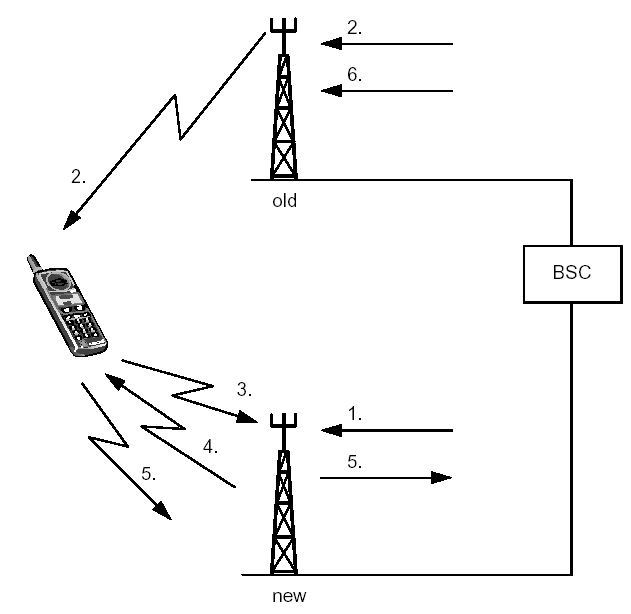
###### **Хэндовер внутри соты**

Этот тип хэндовера применяется в том случае, если BSC определяет, что качество соединения слишком низкое, но нет никаких данных об измерениях, указывающих на то, что есть сота с лучшими значениями параметров. В этом случае BSC определяет другой канал (частоту) в этой же самой соте, где качество может быть лучше, и MS перенастраивается на этот канал.

Примечание: BSC всегда пытается сначала использовать хэндовер на частотный канал другой соты. В случае, если такого канала нет, применяется внутрисотовый хэндовер.

###### **Хэндовер между сотами, контролируемыми одним и тем же BSC**

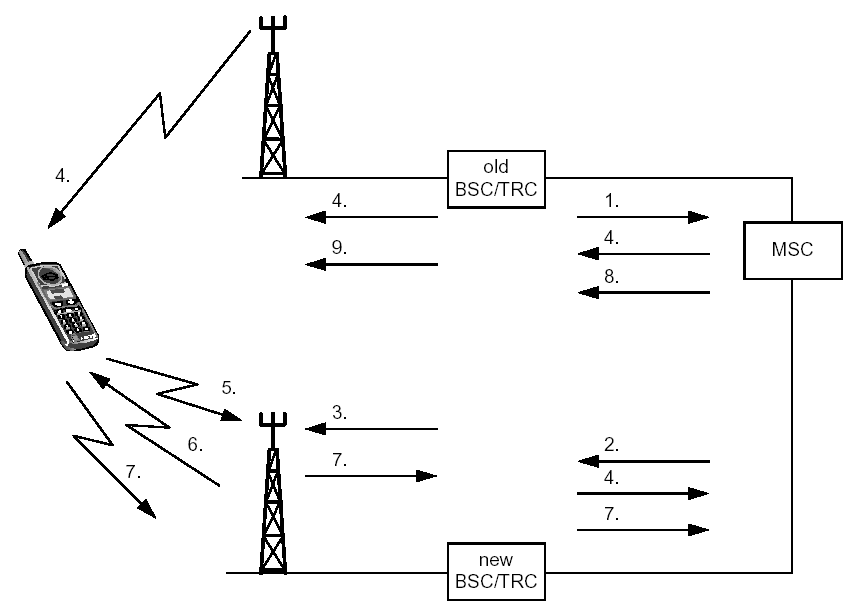
MSC/VLR не участвует в выполнении междусотового хэндовера между двумя сотами, контролируемыми одной и той же BSC. MSC/VLR будет информирован об осуществлении хэндовер. Если хэндовер охватывает разные LA, то обновление данных о местоположении будет выполнено сразу же, как только соединение завершиться.



1. BCS посылает команду на новую BTS для занятия TCH.
2. BSC через предыдущую BTS отправляет на MS сообщение о том, на какую частоту и какой временной интервал (TS) необходимо произвести замену, а также какую выходную мощность нужно использовать. Эта информация отправляется на MS по каналу FACCH.
3. MS настраивается на новую частоту и передает пакет доступа для выполнения хэндовера в нужный временной интервал. Так как MS еще не имеет информации о ТА, то пакеты для хэндовера очень короткие (только 8 бит информации).
4. Когда новая BTS определяет пакеты, содержащие информацию, необходимую для выполнения хэндовера, она отправляет информацию о ТА по FACCH.
5. MS отправляет полное сообщение для хэндовера на новую BSC через новую BS.
6. BSC сообщает предыдущей BTS о необходимости освободить ранее использовавшийся ТСН.

###### **Хэндовер между сотами, контролируемыми разными BSC, но одним и тем же MSC/VLR**

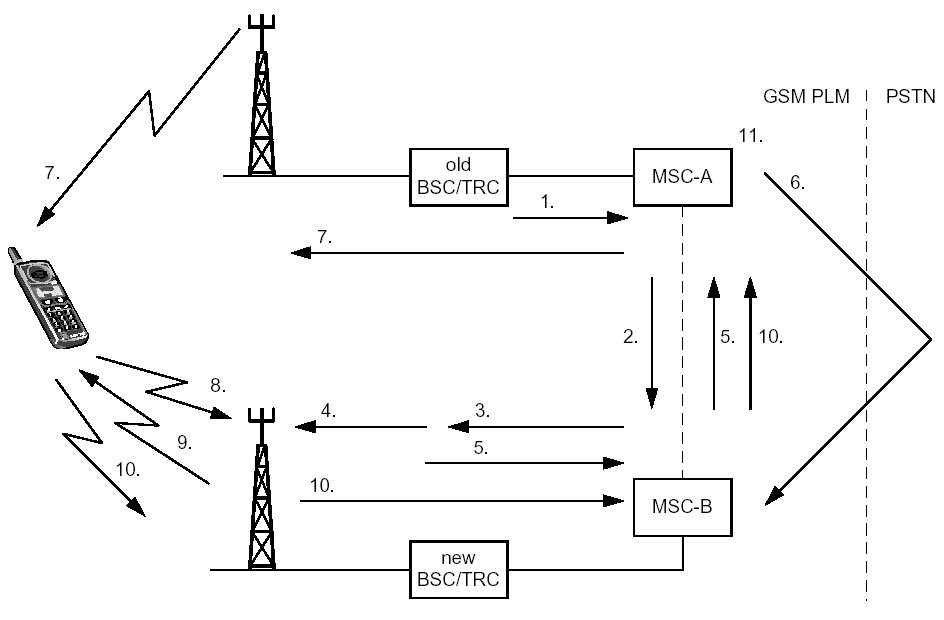
Если в хэндовере задействован другой BSC, то для установления соединения между этими BSC должен использоваться MSC/VLR.



1. Обслуживающий (предыдущий BSC) отправляет в MSC сообщение, содержащее идентификатор нужной соты, с требованием на выполнение хэндовера.
2. MSC располагает информацией о том, какой из BSC контролирует эту соту и отправляет запрос на хэндовер на эту BSC.
3. Новый BSC дает команду нужной BTS для выделения канала ТСН.
4. Новый BSC отправляет сообщение на MS через MSC и предыдущую BTS.
5. MS настраивается на новую частоту и передает пакет доступа для хэндовера, который будет выполняться в указанный временной интервал.
6. Новая BTS отправляет информацию о величине ТА.
7. MS отправляет полное сообщение о хэндовере на MSC через новый BSC.
8. MSC отправляет предыдущему BSC команду на освобождение ранее использовавшегося канала ТСН.

###### **Хэндовер между сотами, контролируемыми разными MSC**

Хэндовер между сотами, контролируемыми разными MSC, может применяться внутри одной РLMN. Соты, контролируемые разными MSC/VLR, соответственно, контролируются разными BSC.



1. Обслуживающий (предыдущий) BSC отправляет сообщение с требованием на хэндовер на обслуживающий MSC (MSC-A) с идентификацией нужной соты.
2. MSC-A определяет, что эта сота принадлежит другой MSC (MSC-B) и запрашивает ее.
3. MSC-B определяет номер хэндовера для перемаршрутизации. Далее запрос на хэндовер отправляется на новую BSC.
4. Новый BSC отправляет команду нужной BTS для занятия ТСН.
5. MSC-B получает информацию и передает ее на MSC-A вместе с номером хэндовера.
6. Установление соединения с MSC-B возможно через PSTN.
7. MSC-A отправляет команду на хэндовер на MS через предыдущий BSC.
8. MS настраивается на новую частоту и передает пакеты доступа в нужный временной интервал.
9. Когда новая BTS определяет пакеты для хэндовера, она отправляет информацию о временной задержке (ТА).
10. MS отправляет полное сообщение о хэндовере на предыдущий MSC через новый BSC и новый MSC.
11. После этого устанавливается новый путь в MSC-A и соединение устанавливается через него.
12. Предыдущий ТСН освобождается тем BSC, который ранее управлял соединением.

Предыдущий MSC (MSC-A) контролирует соединение до тех пор, пока оно не будет прекращено. Связано это с тем, что в нем содержится информация об абоненте и подробностях соединения, которые необходимы для тарификации.

MS после прекращения соединения должна обновить данные о местоположении, так как LA не может принадлежать более чем одной зоне обслуживания MSC. HLR передает данные в VLR-B для обновления в нем информации, а VLR-B, в свою очередь, передает в VLR-A команду на удаление всей информации о мобильном абоненте.

##### **Международный вызов**

Одной из основных характеристик GSM является возможность использования международного роуминга и осуществления международных соединений. Для того, чтобы абоненты могли воспользоваться услугой роуминга в сетях, принадлежащих операторам разных сетей сотовой связи, необходимо заключить между операторами роуминговое соглашение. Это же касается международного роуминга.

Процессы обслуживания международных вызовов при роуминге не отличаются от вариантов обслуживания вызовов абонентов, находящихся в пределах собственной сети. Но, тем не менее, рассмотрим два случая, характерных для случая роуминга.

##### **Включение IMSI (IMSI Attach)**

Когда MS требует обслуживания в режиме международного роуминга, происходит следующее:

1. MS включается и начинает сканировать все частоты GSM внутри одного частотного диапазона (GSM –900). Производится поиск несущей ВССН. MS настраивается на ту несущую ВССН, которая имеет наибольший уровень сигнала и считывает ее системную информацию. Так происходит распознавание сетевого оператора.
2. MS сравнивает идентификатор сети со списком запрещенных PLMN, хранящимся в памяти SIM. Этот список содержит все сетевые идентификаторы, с которыми домашний оператор не имеет роуминговых соглашений. Если сеть, на которую настроилась MS, является запрещенной, то MS продолжает поиск разрешенной сети.
3. Если MS не находит разрешенной сети, но идентифицировала запрещенную сеть, то она выдает сообщение «Только экстренные вызовы». Если MS находит разрешенную сеть, то она настраивается на нее и отправляет сообщение о регистрации IMSI (IMSI Attach).
4. Этот случай идентичен случаю нормальной регистрации IMSI (в собственной сети). Отличие состоит только в том, что абонентский HLR находится в другой стране.

##### **Вызов на MS**

Когда MS находится в международном роуминге и на нее поступает вызов, процедура идентична той, когда MS находится в своей собственной сети. Разница лишь в том, что используемые GMSC и HLR находятся в собственной сети, а MSC/VLR находится в сети другой страны.

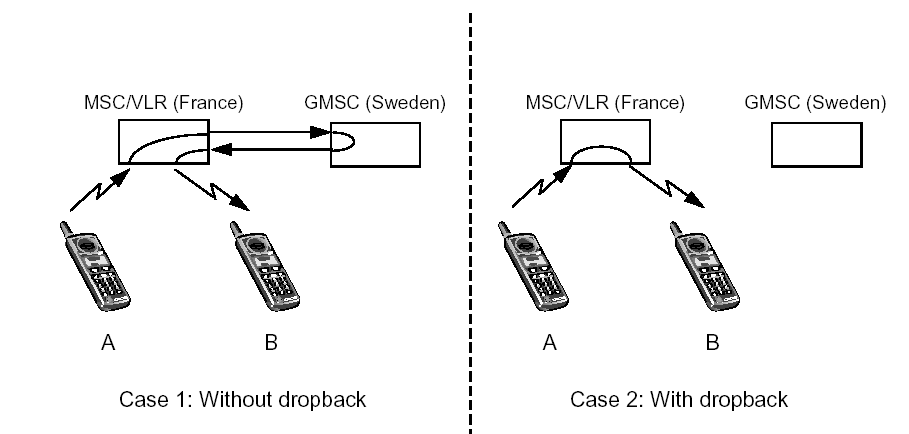
##### **Процедура Dropback**

Следующий случай показывает преимущество использования процедуры dropback. В данную процедуру вовлекается два абонента. Рассмотрим пример, когда:

* Абонент А из Франции находится во Франции, его MS контролируется собственной MSC.
* Абонент Из Швеции находится в настоящий момент в международном роуминге во Франции, его MS контролируется MSC/VLR-A.

Абонент А звонит абоненту В. Вызов маршрутизируется из Франции в Швецию.

Сеть Швеции определяет, что абонент В находится в зоне действия MSC/VLR-A во Франции и перенаправит вызов обратно во Францию. Абоненты соединяются друг с другом в сети GSM Франции и ведут разговор.



* **Без использования процедуры dropback:** разговор при вызове идет через GMSC Швеции
* **С использованием процедуры dropback:** разговор при вызове переключается внутри MSC/VLR-A, что существенно влияет на стоимость разговора.

**Передача коротких сообщений**

Служба коротких сообщений (SMS) предоставляет мобильным станциям средства для обмена текстовыми сообщениями, содержащими до 160 буквенно-цифровых символов. SMS-C (SMS Сеnter) является хранилищем и центром, перенаправляющим короткие сообщения.

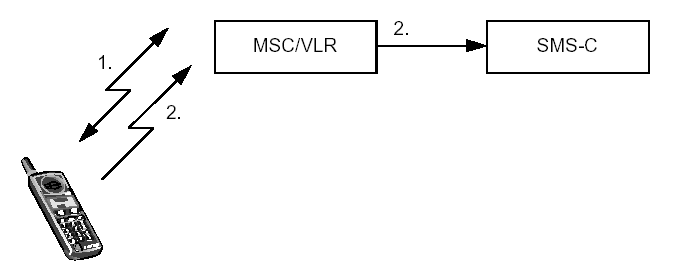
SMS поддерживает две основные услуги:

* Мобильный прием SMS: от SMS-C на MS
* Мобильная передача SMS: от MS на SMS-C

В обоих случаях MS находится в состоянии IDLE. Если MS находится в активном режиме, то короткие сообщения передаются по каналу SACCH. Пейджинг, установление соединения, аутентификация и т.д. в этом случае не требуется.

##### **Передача SMS с MS**

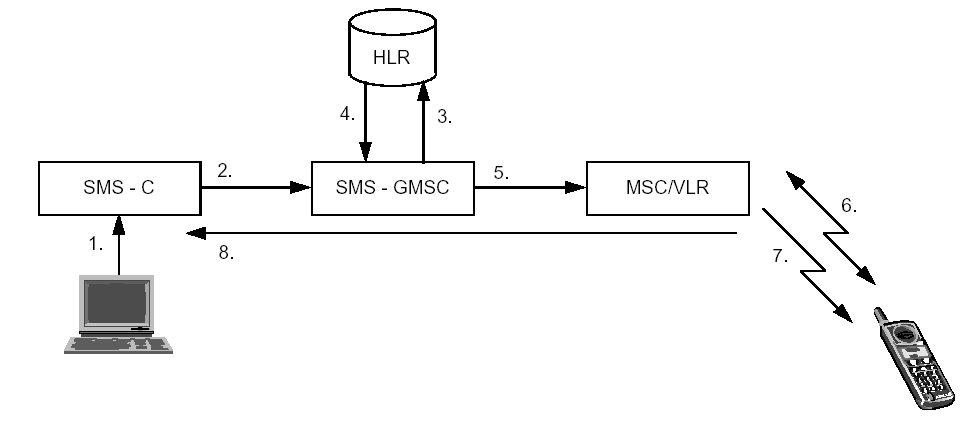
Мобильная передача SMS подразумевает передачу коротких сообщений от MS на SMS-C, который, в свою очередь, обеспечивает информацию о доставке сообщения, либо о его недоставке.



* MS устанавливает соединение с сетью, как в случае нормального установления соединения, используя сигнальные каналы RACH, AGCH, SDCCH.
* Если аутентификация прошла успешно, MS отправляет короткое сообщение по каналу SDCCH на SMS-C через MSC/VLR. SMS-C перенаправляет короткое сообщение в пункт назначения. Это может быть MS или терминал выделенной сети, например, РС.

##### **Прием SMS на MS**

Мобильный прием SMS - это возможность передачи коротких сообщений от SMS-C на MS.



1. Пользователь отправляет сообщение на SMS-C.
2. SMS-C отправляет сообщение на SMS-GMSC.
3. SMS-GMSC запрашивает HLR для маршрутизации вызова.
4. HLR возвращает информацию о маршруте на SMS-GMSC
5. SMS-GMSC перенаправляет сообщение на MSC/VLR.
6. На MS поступает вызывной сигнал, устанавливается соединение с сетью, так же как, для случая установления речевого соединения.
7. Если аутентификация успешна, то MSC/VLR передает короткое сообщение на MS, используя сигнальный канал SDCCH.
8. Если передача была успешной, то MSC/VLR отправляет отчет на SMS-C. Если нет, то MSC/VLR информирует HLR, и отчет о недоставке отправляется на SMS-C.

В случае неуспешной доставки, SMS-C информирует HLR и VLR о том, что сообщение ожидает отправки на MS. HLR затем проинформирует SMS-C о том, когда MS станет доступной.

Прием сообщений SMS-C может идти от различных источников, например, телекса, факсимильного аппарата, из сети Интернет.

## Система сигнализации ОКС №7

Система сигнализации № 7 - это универсальная многофункциональная система межстанционной сигнализации, ориентированная на поддержку практически всех уже известных, а также будущих услуг связи. Ее огромный потенциал объясняется блочной функциональной архитектурой, где над единой транспортной подсистемой (MTP) расположены подсистемы пользователей и приложений (TUP, ISUP, MAP, TCAP, MUP и т. д.), предназначенные для обеспечения соответствующих услуг связи. Экономический эффект от внедрения ОКС7 (общеканальной сигнализации) проявляется даже при обычной телефонной связи.

##### **Что такое сигнализация и почему № 7?**

На протяжении последних ста лет сигнализация развивалась в рамках традиционной телефонии, причем за последние два десятилетия ее эволюция ускорилась как никогда ранее благодаря сращиванию компьютерных и коммутационных технологий.

В контексте телефонии под сигнализацией понимается передача управляющей информации с целью установления/разъединения двухточечных соединений. Сигнализация бывает трех типов - абонентская, т.е. на участке между абонентским терминалом и коммутационной станцией, внутристанционная и межстанционная. Пример абонентской сигнализации приведен на рисунке, где показаны основные сигналы, передаваемые в процессе нормального установления/разъединения соединения между двумя абонентами, подключенными к одной коммутационной станции.



   Межстанционная сигнализация в свою очередь делится на два основных типа - сигнализация по выделенному каналу **CAS (Channel Associated Signalling)** и сигнализация по общему каналу **CCS (Common Channel Signalling)**. В системе использован принцип передачи управляющей информации по общему каналу сигнализации, отсюда ее сокращенное название по-русски - ОКС7. В первом случае (CAS) сигнальная информация передается либо непосредственно по разговорному каналу (внутриканальная сигнализация) либо по каналу, физически привязанному к нему. Во втором случае (CCS) сигнализация полностью отделена от разговорного тракта, и передача сигнальной информации осуществляется по специально выделенному высокоскоростному каналу, общему для пучка разговорных каналов.

На сегодняшний день известны два стандарта систем общеканальной сигнализации:

* CCITT Signalling System No. 6
* CCITT Signalling System No. 7

Первая из них была разработана в конце 60-х годов и по ряду причин сейчас практически не применяется. Вторая - CCITT No. 7 (SS7) появилась в конце 70-х годов и предназначена для использования на цифровых сетях с каналами не ниже 64 Кбит/с. Основными преимуществами SS7 являются:

* **СКОРОСТЬ** - в большинстве случаев время установления соединения не превышает одной секунды;
* **ВЫСОКАЯ ПРОИЗВОДИТЕЛЬНОСТЬ** - один канал сигнализации способен одновременно обслужить несколько тысяч телефонных вызовов;
* **ЭКОНОМИЧНОСТЬ** - по сравнению с системами CAS во много раз сокращается объем оборудования на коммутационной станции;
* **НАДЕЖНОСТЬ** - достигается за счет возможности альтернативной маршрутизации в сети сигнализации;
* **ГИБКОСТЬ** - система передает любые данные, не только данные телефонии.

##### **ОКС №7 - сигнализация будущего**

Популярные словосочетания и аббревиатуры, такие как ISDN, сети подвижной связи, интеллектуальные сети, в действительности, остаются лишь словами на бумаге без системы сигнализации № 7 (SS7) -- единственного средства, обеспечивающего внедрение и функционирование современных услуг связи на сетевом уровне.

Многие производители оборудования ISDN утверждают, будто их продукты обеспечивают "услуги ISDN". Однако область действия услуг, предоставляемых любым терминальным оборудованием ISDN или офисными АТС класса ISDN, ограничена пределами одной коммутационной системы, и не распространяется на абонентов других станций. Развитие сетей подвижной связи также невозможно без SS7. Порой конкурирующих между собой поставщиков услуг сотовой связи объединяет лишь SS7, необходимая для обеспечения автоматического обмена информацией о местонахождении абонента (роуминга). Наконец, для эффективного функционирования интеллектуальных сетей также требуется SS7.

Будучи разработанной для традиционной телефонии, в SS7 изначально были заложены большие возможности для управления другими услугами связи. Это объясняется прежде всего бумом на рынке услуг телекоммуникаций, который продолжается с начала 80-х годов и еще не достиг своего пика. Именно в 80-х годах SS7 интенсивно разрабатывалась ведущими производителями коммутационного оборудования и параллельно утверждалось в качестве стандарта CCITT.

Уже сейчас SS7 является обязательным элементом следующих цифровых сетей связи:

* **PSTN -** Public Switched Telephone Network
* **ISDN -**Integrated Services Digital Network
* **PLMN -**Public Land Mobile Network
* **IN -** Intelligent Network

   Взаимодействие данных систем также осуществляется посредством SS7.



В настоящее время практически всеми международными институтами стандартизации телекоммуникаций (ITU-T, ETSI, ANSI, ATM Forum и др.) разрабатываются стандарты SS7 для широкополосных сетей - Broadband-ISDN, Universal Mobile Telecommunications System, Broadband-IN.

##### **Структура сети сигнализации**

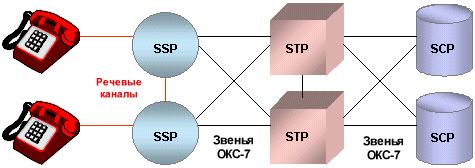
Сеть сигнализации, как и сети пакетной коммутации других типов, строится согласно следующим основным критериям:

* простота структуры сети
* надежность
* минимальные временные задержки
* оптимальная стоимость.

Этим критериям лучше всего будет соответствовать сеть с достаточно симметричной топологией и функционирующая в квази-связанном режиме (режим работы сети ОКС, при котором сигнальные единицы, относящиеся к обслуживаемому пучку линий (каналов) телефонной сети, проходят по одному определенному маршруту).

Многие национальные сети SS7 строятся по региональному принципу с иерархической системой транзитных пунктов сигнализации. Есть три типа пунктов сигнализации в сети ОКС №7:

* Узел Коммутации Услуг (**SSP**)
* Транзитный Пункт Сигнализации (**STP**)
* Пункт Контроля Сигнализации (**SCP**)



В рамках ТфОП/GSM/GSM для SS7 создается выделенная сеть сигнализации. В ней объединены несколько типовых устройств центров сигнализации), а для обмена сообщениями используются канальные интервалы сигнализации потоков Е1 (TS16).

Такая сеть включает в себя пункты передачи сигнальных сообщений (Signalling Transfer Point - STP), абонентские пункты сигнализации (Service Switching Point - SSP) и пункты предоставления дополнительных услуг (Service Control Point - SCP). С помощью STP в сети SS7 выполняется маршрутизация пакетов сигнальных сообщений. SSP отводится роль терминалов сетей передачи данных, а SCP, адаптированные в соответствии с концепцией интеллектуальных сетей, работают эквивалентно хостам и коллективным базам данных этих сетей.

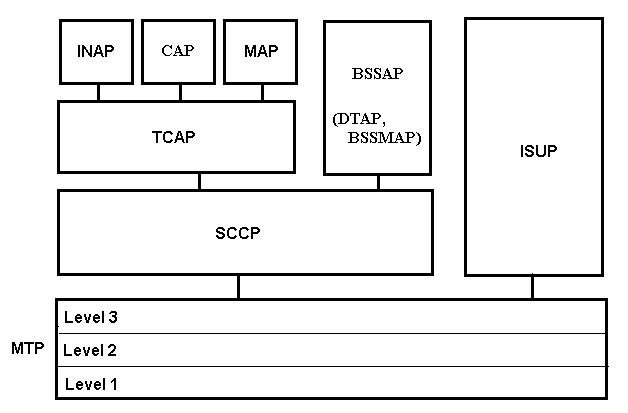
##### **SS7 и модель OSI**

Структура протокола SS7 сложнее структуры большинства протоколов сетей передачи данных и включает в себя множество уровней и подсистем. Это связано с тем, что протокол SS7 является средством для объединения различных сетей: ТфОП/GSM, ISDN, подвижной радиосвязи, а также предоставляет дополнительные возможности для создания глобальных сетей персональной связи (PCS) с международным роумингом. Наличие в структуре сети SS7 пунктов SCP способствует широкому внедрению интеллектуальных сетей, внося дополнительные уточнения и расширения в структуру протокола SS7.

Архитектура протоколов SS7 отражает историю ее создания. До 1984 года, когда в Красной книге CCITT была начата спецификация части транзакционных возможностей SS7, стек протоколов был совместим с моделью OSI только до третьего уровня, и то не полностью. Совместимость была достигнута дополнением системы протоколами **SCCP (Signalling Connection Control Part)** и **TCAP (Transaction Capabilities Application Part)**, что позволило реализовывать в SS7 услуги передачи данных по тем же принципам, что и в модели OSI.

На базе транзакционной части SS7 позднее были специфицированы протоколы **MAP (Mobile Application Part)** и **INAP (Intelligent Network Application Protocol)**, для которых существенным является обмен транзакциями между узлами сети и сетевыми базами данных.

Общая структура сети выглядит так:



## Подсистема MTP

Основным назначением подсистемы передачи сообщений (MTP - Massage Transfer Part) является обеспечение средств:

* надёжной передачи сигнальной информации подсистем пользователей через сеть сигнализации ОКС-7;
* выявления и устранения отказов системы и сети для обеспечения надежной передачи и доставки сигнальной информации.

В общем виде функции подсистемы MTP можно описать следующим образом:

* передача сигнальных единиц;
* приём сигнальных единиц;
* фазирование;
* коррекция ошибок;
* управление сетью.

Сами функции подсистемы передачи сообщений делятся на три группы:

* функции звена данных сигнализации;
* функции звена сигнализации;
* функции сети сигнализации.

Подсистема передачи сообщений MTP обеспечивает передачу информации в неискажённой форме, без потерь, дублирования и ошибок, в установленной последовательности от одного пункта сигнализации к другому. Причем эта подсистема не анализирует значения передаваемых сигнальных сообщений, формируемых различными подсистема пользователя. Благодаря такой независимости работы MTP от передаваемых сообщений существует также возможность реконфигурации и гибкого управления сигнальным трафиком при отказах или перегрузках в сети сигнализации.

В данном разделе важно отметить подуровень **MTP3**.

Третий уровень подсистемы передачи сообщений MTP3 соответствует **сетевому** уровню эталонной модели OSI и выполняет сетевые функции ОКС-7. Его основной целью является надёжная маршрутизация сообщений между сетевыми узлами ОКС-7.

Задачи третьего уровня делятся на две категории:

* обработка сигнальных сообщений (SHM – Signaling Message Handling);
* управление сетью сигнализации (SNM – Signaling Network Management).

Система обработки сообщений сигнализации (SHM) выполняет маршрутизацию сообщений для соответствующих сетевых адресатов. Каждый узел анализирует входящее сообщение на основе их кода пункта-получателя (**DPC – Destination Point Code**) c целью определить предназначено ли сообщение для данного узла. Если принимающий узел является пунктом назначения, входящее сообщение доставляется на соответствующему абоненту подсистемы MTP3. Если принимающий узел не является пунктом назначения и сообщение может быть маршрутизировано, то есть этот является транзитным пунктом STP, тогда делается попытка перенаправить сообщение далее. При этом каждый узел сигнализации также указывает при передаче свой код пункта-отправителя (**OPC – Origination Point Code**).

Система управления сетью сигнализации (SNM) – это набор сообщений и процедур, целью которых является обработка отказов в сети таким образом, чтобы сообщения могли достигать своих адресатов, если это возможно. Эти процедуры работают совместно для координации ресурсов системы ОКС-7, которые становятся доступными либо недоступными в соответствии с запросами абонентской нагрузки. Сетевые узлы соединяются друг с другом для того, чтобы получать информацию какие маршруты доступны для отправки сообщений, благодаря чему они могут соответственно корректировать маршруты для передачи сообщений.

Функции сети сигнализации MTP относятся к обмену сообщениями между пунктами сигнализации, являющимися узлами сети сигнализации. Эти функции и процедуры осуществляются подсистемой передачи сообщений на уровне 3.

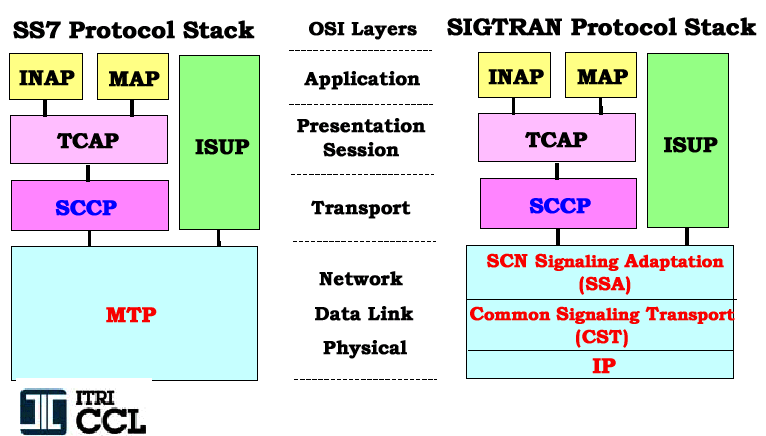
Функции сети сигнализации должны обеспечивать надёжную передачу сигнальных сообщений даже в случае отказа звеньев сигнализации и транзитных пунктов сигнализации. Следовательно, они включают соответствующие процедуры, необходимые для информирования удаленных пунктов сети сигнализации о последствиях какого-либо отказа и для обеспечения соответствующей реконфигурации маршрута сообщений через сеть сигнализации. Функции сети сигнализации обычно выполняются центральным или специализированным процессором системы коммутации.

## Подсистема SIGTRAN

Совершенствование IP-технологий в последнее время позволило усомниться в преимуществах традиционных сетей с коммутацией каналов, что подтверждается, в частности, появлением сетей VoIP операторского класса. Несмотря на то, что в этих сетях применяются свои протоколы, возникает потребность в передаче сигнализации ОКС7 через IP. Это связано как с необходимостью стыковки сетей VoIP и TDM, так и с теми преимуществами, которые дает использование IP-инфраструктуры для связи традиционных пунктов сигнализации.

Стандартизацией протоколов для передачи сообщений различных существующих систем сигнализации (ОКС7, Q.931, DPNSS, V5.2 и др.) через IP занимается рабочая группа IETF SIGTRAN. Для передачи сигнальных единиц ОКС7 через IP используются преимущественно три протокола или, иначе говоря, три уровня адаптации: M2PA (MTP2 Peer-to-peer Adaptation), M3UA (MTP3 User Adaptation) и SUA (SCCP User Adaptation). Каждый из них предназначен для решения своего круга задач.

Сравнение стеков представлено на картинке ниже:



Функционально система ОКС7 разделена на несколько уровней: внизу — общая подсистема передачи сообщений (MTP1, MTP2, MTP3), выполняющая функции 1-го, 2-го и частично 3-го уровней модели OSI, а выше — подсистемы различных пользователей.

Уровни MTP1 и MTP2 ОКС7 соответствуют физическому и канальному уровням модели OSI. На уровне MTP1 определены физические, электрические и функциональные характеристики звена данных сигнализации и средства доступа к нему, а на уровне MTP2 — функции и процедуры, связанные с передачей сигнальных сообщений по отдельному звену сигнализации.

Уровень MTP3 ОКС7 не полностью соответствует сетевому уровню модели OSI, поддерживая лишь ограниченные возможности адресации. На этом уровне определены функции и процедуры сети сигнализации по маршрутизации сообщений, а также другие действия, требуемые для сохранения или восстановления способности передачи сигнальных единиц в случае сбоев в сети сигнализации. В дальнейшем для соответствия сетевому уровню в стек ОКС7 была добавлена подсистема управления соединениями сигнализации (SCCP), которая предусматривала расширение адресации при помощи функции трансляции глобальных заголовков (GTT).

Основным отличием протоколов M2PA, M3UA и SUA друг от друга является функциональный уровень, на котором в шлюзе сигнализации завершается (терминируется) традиционный протокол ОКС7 (а через IP передаются сообщения более высоких уровней). Так, протокол M2PA предусматривает завершение на сигнальном шлюзе уровня MTP2, протокол M3UA — уровня MTP3, а при использовании SUA терминируется протокол SCCP.

##### **Протокол SCTP**

Все протоколы передачи ОКС7 через IP, разрабатываемые группой SIGTRAN, используют в качестве транспорта протокол SCTP (Stream Control Transmission Protocol) с его широкими возможностями по обеспечению отказоустойчивости. Функционально протокол SCTP заменяет уровни MTP1 и MTP2 в традиционной архитектуре ОКС7.

Протокол SCTP можно рассматривать как дальнейшее логическое развитие протокола TCP. Аналогом TCP-соединения для SCTP является понятие ассоциации, которая устанавливается между двумя оконечными устройствами. При этом одно устройство может быть определено несколькими IP-адресами, список которых передается при установлении ассоциации. Для передачи данных через ассоциацию используются все возможные комбинации адресов пары оконечных устройств.

Отказоустойчивость в таком случае обеспечивается за счет того, что разные IP-адреса присваиваются разным интерфейсам устройств, и трафик между ними передается по разным маршрутам. В случае отказа какого-либо оборудования в сети и недоступности одного или нескольких IP-адресов трафик продолжает передаваться между оставшимися адресами, и разрыва SCTP-ассоциации не происходит.

Вышеописанный механизм работы SCTP-ассоциации носит название SCTP multi-homing. К другим ключевым функциям протокола SCTP относятся:

* группировка различных сигнальных сообщений в одном пакете с одним SCTP/IP-заголовком (chunk bundling), что повышает эффективность использования полосы пропускания;
* последовательная доставка сообщений внутри различных потоков, что позволяет избежать ситуации, встречающейся при использовании протокола TCP, когда в случае потери одного пакета остальные задерживаются в буфере до успешной его перепосылки (head-of-line blocking);
* использование контрольных сумм для обеспечения безошибочной передачи пакетов, а также для защиты от атак.

##### **Уровень адаптации M2PA**

Протокол M2PA был разработан для прозрачного “с точки зрения” протокола MTP3 транзита сигнальных единиц через IP, т. е., другими словами, для сети сигнализации ОКС7 звено M2PA не отличается от традиционного. Неизменной остается вся функциональность сетевого уровня ОКС7: балансировка нагрузки между звеньями внутри пучка с помощью поля выбора звена сигнализации (SLS), обнаружение неисправностей, процедуры переключения на альтернативный маршрут (change-over) и возврата на первоначальный (change-back), контроль перегрузки звена через механизм задания порогов и т. д. Это ключевая особенность протокола M2PA; протоколы M3UA и SUA служат для доставки сигнальных единиц до оконечных устройств, и с их помощью транзит ОКС7 через IP организовать невозможно.

При использовании протокола M2PA сигнальные шлюзы выполняют функции обыкновенных транзитных пунктов сигнализации (STP), способных работать как с традиционными MTP2-звеньями ОКС7, так и с M2PA-звеньями на основе инфраструктуры IP. При этом благодаря использованию протокола SCTP поверх IP M2PA-звенья обеспечивают ту же степень надежности, что и TDM-звенья ОКС7, требуя, однако, существенно меньше сетевых ресурсов.

Внедрение M2PA-звеньев в существующую сеть ОКС7 можно рассматривать не только как способ повышения эффективности использования пропускной полосы, но и как один из шагов на пути построения сети следующего поколения (NGN), предусматривающей наличие единой транспортной инфраструктуры для всех видов услуг.

##### **Уровень адаптации M3UA**

Для установления разговорных соединений в ТфОП используется протокол ISUP. При взаимодействии ТфОП с VoIP-сетями сигнальные единицы этого протокола частично должны проходить по традиционной сети ОКС7, а частично — через сеть IP до программного коммутатора (softswitch). Для IP-участка архитектурой сетей NGN предусматривается использование уровня адаптации M3UA. Поверх M3UA может также работать не только протокол ISUP, но и другие протоколы ОКС7, использующие SCCP (MAP, INAP и пр.).

Основное преимущество применения протокола M3UA заключается в возможности стыковки IP-устройств с сетью ОКС7 без необходимости установки на этих устройствах интерфейсов Е1 и без поддержки ими уровней MTP ОКС7, что существенно упрощает и снижает их стоимость.

M3UA является протоколом типа клиент—сервер. В роли клиента выступает сигнальный шлюз, функции которого заключаются в завершении уровней MTP ОКС7 и дальнейшей передаче сигнальных единиц пользовательских подсистем на сервер.

Протокол M3UA обычно применяется для стыка с сетью ОКС7, если в качестве AS выступает программный коммутатор. Во всех остальных случаях, как правило, используется протокол SUA.

##### **Заключение**

В настоящее время протоколы SIGTRAN переходят из состояния “перспективной новинки” в ранг зрелых технологий, которые все чаще используют операторы связи во всем мире. В России, например, ряд операторов связи уже ввели в эксплуатацию транзитные участки ОКС7 через IP, работающие на основе M2PA-туннелей. Еще шире применяются протоколы M3UA и SUA, являющиеся наиболее эффективным средством доставки сигнализации ОКС7 до оконечных IP-устройств.

## Подсистема SCCP

Подсистема управления сигнализационным соединением (Signaling Connection Control Part - SCCP) используется для расширения подсистемы передачи сообщений третьего уровня MPT3 стека протоколов ОКС-7. SCCP обеспечивает выполнение дополнительных функций сетевого уровня - дает возможность передавать сигнальную информацию, не связанную с каналом и процедуры управления прикладными системами, а также обеспечивает альтернативные методы маршрутизации.

Протокол MTP изначально был разработан для передачи сообщений управления вызовами, которые поступают от подсистемы передачи телефонных вызовов пользователя TUP (Telephony User Part), то он используется только для передачи сигнальной информации, связанной с каналом. Совместно с МТР, подсистема SCCP может передавать сообщения сигнализации, не связанные с каналом. Такие сообщения используются для поддержки служб, таких как бесплатные междугородные звонки, службы переносимости местных номеров (Local Number Portability — LNP) и подключение вызова к занятому абоненту в интеллектуальных и мобильных сетях, при роуминге и отправке SMS-сообщений в мобильных сетях.

Подсистема SCCP обеспечивает такие дополнительные возможности при работе через подсистему МТР:

* расширяет функции подсистемы МТР до третьего уровня модели OSI;
* обеспечивает мощные и гибкие механизмы маршрутизации;
* повышает передающую способность, включая сегментацию/повторную сборку пакетов, размер которых превышает величину сигнальной единицы MSU (Message Signal Unit);
* обеспечивает работу служб передачи данных без установления соединения (connectionless service) и служб с установлением соединения (connection-oriented service);
* обеспечивает управление и адресацию подсистем (в первую очередь систем, управляемых базами данных).

Подсистема SCCP активно используется в сотовых сетях. Для передачи радиосообщений в GSM-сети используются подсистемы BSSMAP (Base Station Subsystem Mobile Application Part — протокол мобильной системы базовой станции) и DTAP (Direct Transfer Application Part — прикладной протокол прямой передачи). В сочетании с подсистемой ТСАР (Transfer Capabilities Application Part — подсистема обеспечения транзакций), подсистема SCCP может быть использована также в GSM-подсистеме NSS (Network Switching Subsystem — подсистеме сетевой коммутации) для передачи сигналов подсистемы MAP (Mobile Application Part — прикладной подсистемы мобильной связи) между ядрами GSM-компонентов, что дает конечному пользователю мобильность и возможность передачи коротких текстовых сообщений (SMS).

Например, когда реестр VLR (Visitor Location Register — реестр перемещающихся абонентов) для получения профиля подписчика делает запрос к реестру HLR (Home Locator Register - реестр собственных абонентов), подсистема SCCP отвечает за передачу запроса и ответа на него обратно к VLR.

Для обеспечения интеллектуальной сетевой функциональности в сотовой среде технология CAMEL (Customizable Application for Mobile Enhanced Logic - усовершенствованная логика пользовательских приложении в мобильной связи) также используют подсистему SCCP совместно со средствами ТCAP).

В общем случае SCCP предоставляет два класса сервисов: Connection-Oriented (СО), т.е. ориентированных на соединение и Connectionless (CL) – не ориентированных на соединение.

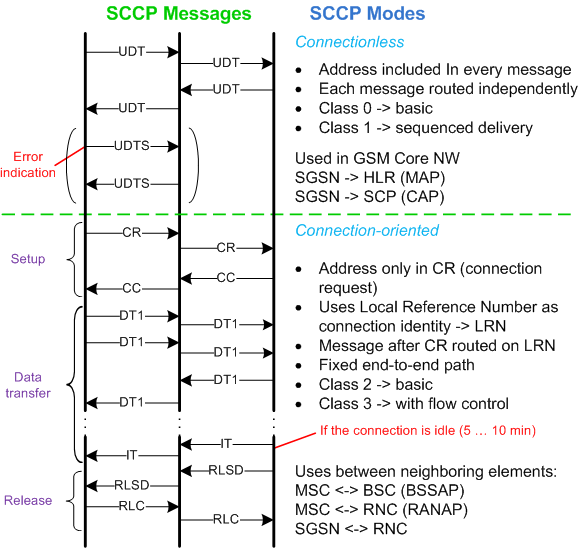
Уровень SCCP определяет четыре класса для протоколов передачи сообщений:

* Class 0 – Basic connectionless class
* Class 1 – In-sequence delivery connectionless class
* Class 2 – Basic connection-oriented class
* Class 3 – Flow control connection-oriented class

Давайте рассмотрим каждый из двух основных классов (CL и CO) в отдельности (см. Рис. 4).

В классе СL используются в основном сообщения UDT (Unidata), при этом каждое сообщение содержит адрес получателя, т.е. каждое сообщение — это фактически «самодостаточная» коммуникационная единица. Коммуникации, основанные на классе СО, используются между сетевыми элементами, которые фактически могут быть разнесены в архитектуре(ах) оператора, например, между: SGSN ↔ HLR, SGSN ↔ SCP (IN Platforms).

Во втором основном классе сервисов CO, между двумя сетевыми элементами, которые осуществляют коммуникацию, устанавливается виртуальный канал, при этом адрес получателя нужен только в начальные сообщения на установление коммуникации. Такой класс, в основном используется между «смежными» элементами, такими как: MSC ↔ BSC, MSC ↔ RNC, SGSN ↔ RNC. Схематично оба класса представлены на рисунке ниже:



##### **Типы сообщений**

В этом разделе рассмотрены примеры SCCP-сообщений, которые используются как в службах с установлением соединения, так и в службах без установления соединения.

**Запрос на соединение CR**

Во время фазы установления соединения используются **CR**-сообщения. Они передаются для установления сигнального соединения (виртуального соединения) между двумя сигнальными точками, от пользователя-отправителя к пользователю-получателю. Различные параметры сообщения задают различные требования к соединению. После получения CR-сообщения, подсистема SCCP инициализирует процедуру установки виртуального соединения (если это возможно).

В сотовых GSM-сетях CR-сообщение может использоваться между центром коммутации (Mobile Switching Center) и контроллером базовых станций (Base Station Controller) для установки сигнального соединения. Например, его параметр данных может содержать запрос на обновление информации о местоположении абонента подсистемы приложений базовых станций (Base Station Subsystem Application Part — BSSAP) или же запрос на переключение канала в подсистеме BSSAP.

**Подтверждение соединения СС**

В процессе отработки фазы установления соединения используются **СС**-сообщения. Такие сообщения передаются узлу, который инициировал соединение в подтверждение того, что соединение установлено. Когда SCCP-узел, инициировавший соединение, получает СС-сообщение, то он завершает процедуру установления сигнального соединения.

**Отклонение соединения CREF**

Во время установления соединения используются **CREF**-сообщения. Отправитель или получатель сообщения передает этот сигнал для отклонения соединения. CREF-сообщение используется для отрицательного ответа на CR-сообщение.

В сотовых GSM-сетях CREF-сообщение может отправляться центром MSC контроллеру BSC (или наоборот) для отклонения запрашиваемого сигнального соединения по причине неспособности одной из сторон его обеспечить.

**Завершение соединения RLSD**

В процессе выполнения фазы завершения соединения используются **RLSD**-сообщения. Такие сообщения отправляются одним из узлов для уведомления другого узла о том, что сигнальное соединение будет разорвано.

В сотовых GSM-сетях для завершения SCCP-соединения и освобождения занятых им ресурсов, центром MSC отправляется RLSD-сообщение контроллеру BSC или наоборот.

**Соединение завершено RLC**

В фазе завершения соединения используются RLC-сообщения. Такие сообщения отправляются в ответ на RLSD-сообщения для выполнения соответствующих действий.

Не следует путать SCCP RLC-сообщения и RLC-сообщения подсистемы ISUP. **Первые не имеют никакого отношения к схемам освобождения звукового канала**. Эти сообщения принадлежат к различным пользовательским подсистемам, а также отличаются параметрами SIO.

**Форма данных 1 DT1**

DT1-сообщения используются только протоколами класса 2 с установлением соединения во время выполнения фазы передачи данных. Оба участника соединения используют эти сообщения для передачи пользовательских данных между двумя SCCP-узлами.

Сообщения DT1 в сотовых сетях используются для передачи данных между контроллерами BSC и центрами MSC после того, как при помощи CR- и СС-сообщений устанавливается соединение. Все данные между узлами MSC и BSC передаются при помощи сообщений DT1. DТ2-сообщения не используются в системе GSM.

**Компонент данных UDT**

Сообщения UDT используются для передачи данных в режиме без установления соединения с использованием протокола класса 0 или 1.

UDT-сообщения обычно используются для ТСАР-коммуникаций в IN-службах. В сотовых сетях GSM UDT-сообщения используются протоколом МАР для передачи его сообщений.

Управляющие SCCP-сообщения передаются при помощи UDT-сообщений.

**Служба компонентов данных (UDTS)**

Сообщения UDTS используются в протоколах класса 0 и 1 без установления соединения. Они предназначены для индикации того, что UDT-сообщения не могут быть доставлены получателю. UDTS-сообщения отправляются только в том случае, если в полученном UDT-сообщении было установлено необязательное поле уведомления об ошибке.

Сообщения UDTS, LUDTS и XUDTS означают, что соответствующие сообщения (UDT, LUDT и XUDT соответственно) не могут быть доставлены получателям.

##### **Управление маршрутизацией SCCP (SCRC)**

Подсистема SCCP обеспечивает следующие функции:

* маршрутизация сообщений, отправленных подсистемой МТР соответствующим локальным подсистемам;
* маршрутизация сообщений, отправленных локальными подсистемами другим локальным подсистемам;
* маршрутизация сообщений локальных подсистем, предназначенных для подсистем на удаленных узлах, с помощью транспортной службы МТР. Получатель задается в части CdPA параметра адреса, который назначается подсистемой. Адрес может содержать комбинацию кодов, системных номеров и глобальных заголовков.

Адресация подсистемы SCCP намного более гибкая в сравнении с адресацией в подсистеме передачи сообщений МТР 3, поэтому возможности механизма адресации несколько затруднены и к тому же возникает несколько различных комбинаций параметров маршрутизации.

Подсистема SCCP обеспечивает функцию маршрутизации, которая позволяет доставить сигнальные сообщения к заданному пункту исходя, например, из набранных цифр. Эта функция известна под названием **GTT** (Global Title Translation — трансляция глобального заголовка); она транслирует глобальный заголовок (например, набранные цифры бесплатного номера) в код сигнального пункта и номер подсистемы для корректной обработки такой информации приложением.

Итак, подсистема SCCP поддерживает такие типы сетевой адресации:

* маршрутизация по кодам пунктов (**Point Code — PC**);
* маршрутизация по номерам подсистем (**Subsystem Number — SSN**);
* маршрутизация по глобальным заголовкам (**Global Title**).

На уровне подсистемы МТР может использоваться **только** маршрутизация по кодам пунктов.

Используя маршрутизацию по кодам пунктов сигнализации подсистемы МТР, единицы MTU передаются через пункт передачи сигнала STP к узлам SP с требуемым кодом пункта-получателя DPC.

##### **Маршрутизация по номерам подсистем SSN**

Под подсистемой понимается имя, присвоенное приложению, которое использует систему SCCP. В рассматриваемой системе к приложениям относятся управляемые базы данных, а также подсистема ISUP, на основе которой реализован ограниченный набор дополнительных служб и система BSSAP (для радиосвязи в стандарте GSM). Код SSN используется для идентификации SCCP-пользователя способом, аналогичным службе идентификации пользователей подсистемы МТРЗ.

Вполне очевидно, что передача сигнальной информации, не связанной с каналом (non circuit-related signaling), например, транзакции базы данных для поддержки интеллектуальной сети, сотовой связи и т.п., задействует два удаленных приложения (подсистемы), которые обмениваются информацией. Для идентификации приложения используется номер подсистемы SSN.

Если маршрутизация SSN не используется, то SSN-номер размещен внутри CdPA-параметра. Подсистема SCCP использует SSN-номер для отправки SCCP-сообщений определенной подсистеме (приложению). Номер SSN также включается в параметр CgPA (Calling Party Address — адрес вызывающей стороны) для идентификации подсистемы, которая отправила SCCP-сообщение.

**Не следует путать** параметры **CgPA** (адрес вызывающей стороны) и **CdPA** (адрес вызываемой стороны) подсистемы SCCP и параметры Calling Party Number (адрес вызывающей стороны) и Called Party Number (адрес вызываемой стороны) подсистемы **ISUP**.

##### **Маршрутизация по этикеткам маршрутизации (OPC, DPC) и по GT (Global Title)**

Сообщение «приходящие» от уровня SCCP, на приемной стороне должны обрабатываться также уровнем SCCP. Например, если сообщение содержит только этикетку маршрутизации (OPC, DPC), то уровень SCCP не будет предпринимать никаких действий по обработке этого сообщения, а успешно передаст его для маршрутизации на нижний уровень MTP3 (см. схему ниже – маршрут от подсистемы CAP). Это тип роутинга называют роутинг по этикеткам маршрутизации – SCCP routing on label. С другой стороны, если сообщение будет содержать адрес сетевого элемента (GT) вместо этикетки маршрутизации, то уровень SCCP будет использовать этот адрес для роутинга сообщения. В этом случае роутинг будет осуществляться по GT – SCCP routing on Global Title.

Глобальный заголовок (**GT — Global Title**) является телефонным адресом. Таким образом, глобальный заголовок должен быть преобразован в сетевой адрес ОКС-7 (код DPC+SSN) перед его использованием. Глобальный заголовок размещается в параметрах GTAI полей CgPA и CdPA. Global Title — это адрес, который используется для определения получателя сигнального сообщения, при этом GT определяется на уровне приложения, а анализируется на уровне SCCP.

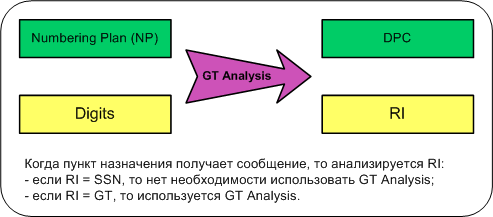
Большинство GT представляются в виде E.164 плана нумерации, но также могут быть представлены в виде E.212. По определению ITU-T глобальный заголовок представляет собой адрес, похожий на адрес из набираемых цифр номера, он не содержит явной информации о маршруте к узлу в ОКС-7-ceти.

Маршрутизация по глобальным заголовкам часто используется в сетях с фиксированными линиями связи для проверки телефонных карточек и в службах, обеспечивающих номера для телемаркетинга. Она используется в сотовых сетях для обмена сообщениями, когда реестры HLR и VLR принадлежат разным сетям или, когда между ними находятся несколько сигнальных пунктов.

Адрес вызывающей стороны (**CgPA**) содержит информацию, по которой можно идентифицировать отправителя SCCP-сообщения. Аналогично, адрес вызываемой стороны (**CdPA**) содержит информацию, по которой можно идентифицировать получателя SCCP-сообщения.



Для определения корректного адреса сетевого элемента, которому нужно передать сообщение, применяется GT Analysis, т.к. уровень SCCP использует нижние уровни MTP, то одним результатом GT Analysis будет DPC сетевого элемента, а вторым Routing Indicator (RI), который используется для указания следующему сетевому элементу, о необходимости проводить GT Analysis для полученного сообщения или нет (см. схему ниже)

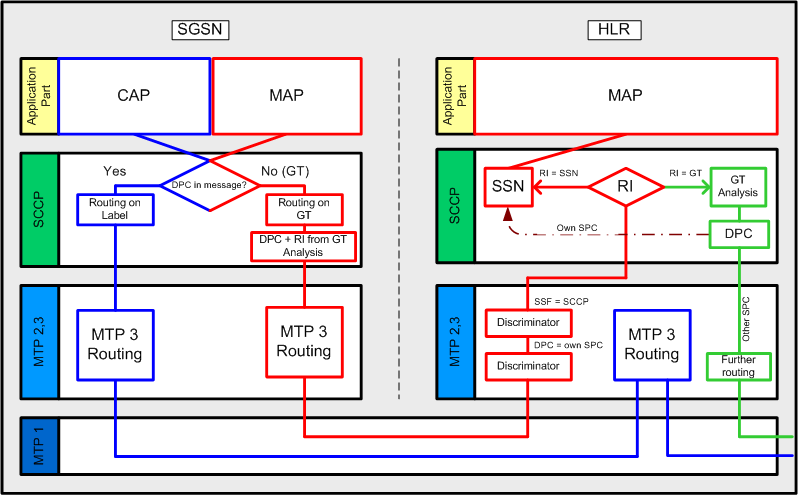


Рассмотрим пример:

Если SGSN еще не получал ни каких данных от абонента, то он может располагать только IMSI абонента. Чтобы определить расположение HLR абонента и выполнить запрос данных об абоненте, SGSN должен произвести IMSI Analysis. В этом случае “ответственной” за запрос Update Location будет подсистема MAP-HLR, которая воспользуется уровнем SCCP с **Connectionless** (не ориентированным на соединение) подключением.

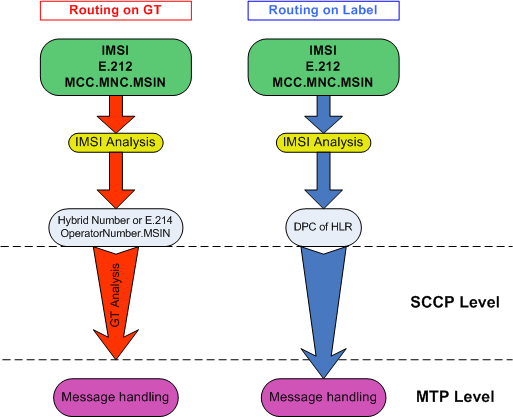
Как мы уже знаем на уровне SCCP существует два типа маршрутизации:

* по этикетке маршрутизации (SCCP routing on label);
* по GT (SCCP routing on GT).



Выбор типа маршрутизации будет зависеть от того где находиться абонент, в домашней сети либо в гостевой сети (т.е. в роуминге).

В случае, когда абонент находиться в роуминге, SGSN не знает DPC домашнего HLR абонента, поэтому SGSN будет использовать IMSI Analysis (см. рисунок ниже), чтобы транслировать IMSI из E.212 в E.214 (Hybrid Numbers) и маршрутизация будет естественно осуществляется по GT.



Затем транслированный в E.214 номер абонента, пройдет через GT Analysis, результатом которого обычно является DPC Gateway, которому отправляется сообщения для доставки в домашнюю сеть абонента, а также RI, который будет указывать нужен ли GT Analysis (в случае если RI = GT) на следующем сетевом элементе или нет (в случае если RI = SSN).

Если же абонент находиться в домашней сети, то использование IMSI Analysis основанного на роутинге по этикеткам маршрутизации или роутинге по GT будет зависеть от того, знает ли SGSN DPC HLR абонента. Если SGSN знает (имеет запись в своей таблице о DPC «домашних» HLR) DPC HLR, то будет использоваться роутинг по этикеткам маршрутизации, в противном случае (SGSN не знает DPC HLR), будет использоваться роутинг по GT.

## Подсистема TCAP

Основным назначением **ТСАР** (Transaction Capabilities Application Part) является предоставление возможностей передачи информации между сетевыми узлами и предоставление набора специальных услуг для приложений, независимо от типа приложений. ТСАР - это общая платформа для различных приложений (пользователей ТСАР), организующая с ними стандартный интерфейс. Пользователями ТСАР в GSM являются подсистемы МАР и САР.

Подсистема ТСАР обеспечивает общую базу для выполнения удаленных операций в сетевой среде ОКС 7, которая может использоваться для поддержания ряда услуг. Таким образом, использование ТСАР позволяет избежать разработки процедур, выполняющих данные функции для каждого приложения. ТСАР может быть использован распределенным приложением в одном узле для вызова или выполнения операции в другом узле.

ТСАР выполняет общие для различных приложений функции:

* кодирование/декодирование;
* упаковку/распаковку;
* отправку/прием информации пользователей ТСАР.

Эти общие функции были извлечены из каждого приложения и включены в ТСАР.

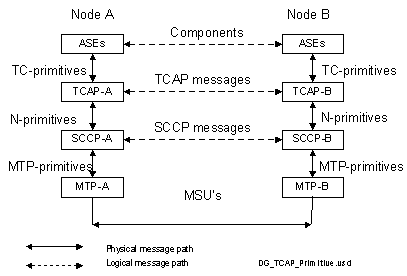
Из названия ясно, что ТСАР - протокол, ориентированный на транзакции. Транзакция представляет собой не связанное с каналом (виртуальное) соединение, которое используется для обмена информацией посредством сообщений ТСАР.

Это касается и диалогов пользователей, которые на уровне ТСАР называют транзакциями. Например, одна транзакция ТСАР соответствует одному диалогу МАР. ТСАР позволяет организовать выполнение множества диалогов одновременно. Каждый пользовательский диалог обозначается ТСАР идентификатором транзакции (Transaction ID), а каждый диалог в свою очередь идентифицируется значением Dialog ID.

**Transaction ID** - это идентификатор, независимо назначаемый каждым из двух узлов, взаимодействующих при помощи транзакций, позволяющий уникально определять каждую транзакцию и ассоциировать с ней содержимое сообщения. Существует два типа идентификаторов транзакций:

* *Originating* Transaction ID, назначается узлом, посылающим сообщение, и используется для определения транзакции до окончания диалога;
* *Destination* Transaction ID, назначается узлом, принимающим сообщение, и используется для определения транзакции до окончания диалога.

ТСАР кодирует и запаковывает компоненты операций пользователей в сообщения ТСАР, которые передаются в SCCP и МТР для передачи. На противоположной стороне ТСАР принимает сообщения, распаковывает и декодирует их для пользователя (МАР, САР). Подсистема ТСАР не имеет своей собственной системы маршрутизации. Сообщения ТСАР маршрутизируются средствами SCCP - МТР.



Различаются два типа диалогов:

* cтруктурированный.
* неструктурированный.

Структурированный диалог позволяет пользователю ТСАР начать диалог, обменяться контекстом (Application Context) и пользовательской информацией, обменяться компонентами диалога, завершить или аварийно прервать диалог. Структурированные диалоги используются, когда после доставки данных от получателя ожидается какая-либо реакция: подтверждение или ответ.

Неструктурированный диалог не имеет начала и завершения обмена данных. Он обеспечивает возможность только запроса на передачу одного или нескольких компонентов операции или уведомления об ошибках запросов.

Пользователи ТСАР в GSM используют исключительно структурированные диалоги.

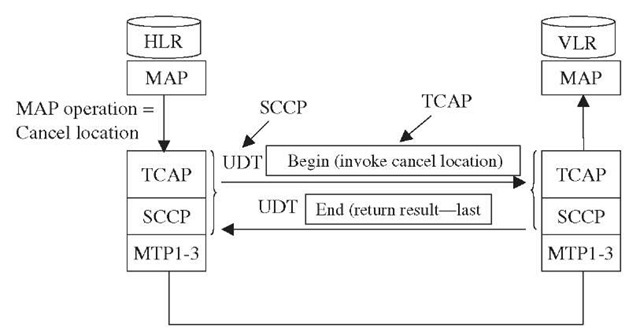
Структура TCAP

ТСАР структурно делится на два подуровня:

* подуровень компонент, который обеспечивает формирование компонент - порций данных прикладных протоколов, в которых передаются операции;
* подуровень транзакций, который обеспечивает обмен сообщениями, содержащими компоненты.

Взаимодействие между ТСАР и его пользователем основано на обмене примитивами. Для ТСАР определено 2 типа примитивов:

* примитивы диалога;
* примитивы компонент.

Примитивы диалога используются для инициирования, поддержания и окончания структурированного диалога пользователя (МАР, САР). Использование этих примитивов может быть сравнено с ориентированным на соединение обменом SCCP сообщений. Примитив BEGIN соответствует фазе установления вызова. На этом этапе выделяются ресурсы для соединения, в данном случае - идентификатор транзакции (Transaction ID). Примитив CONTINUE соответствует фазе передачи данных, а примитив END фазе освобождения ресурсов.

**Сообщения TCAP**

Информация, содержащаяся в примитивах, оформляется в виде сообщений TCAP, подлежащих передаче к системе-партнёру. Существуют сообщения пяти типов:

|  |  |
| --- | --- |
| **Unidirectional** (однонаправленное) | передаёт содержание примитивов **TR-UNI**. |
| **Begin** (начало) | передаёт содержание примитивов **TR-BEGIN**. |
| **Continue** (продолжение) | передаёт содержание примитивов **TR-CONTINUE**. |
| **End** (окончание) | передаёт содержание примитивов **TR-END**. |
| **Abort** (непредвиденное окончание) | передаёт содержание примитивов **TR-P-ABORT** и **TR-U-ABORT**. |

Для переноса сообщений через сеть ОКС, TCAP обращается к услугам подсистемы [SCCP](https://ru.wikipedia.org/wiki/Signalling_Connection_Control_Part).

Примитивы компонентов обрабатывают запросы на операции и ответы.

1. Связанные с содержанием компонентов — компонентные примитивы.

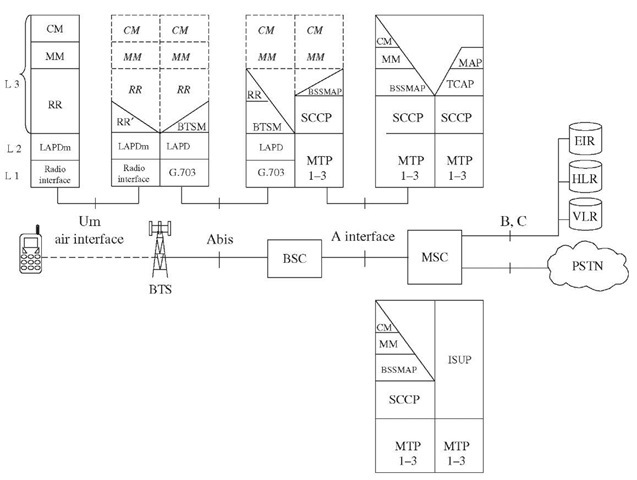
|  |  |  |
| --- | --- | --- |
| **Общее имя** | **Тип** | **Параметры** |
| **TC-INVOKE** (обращение к операции) | Запрос, Индикация | ID диалога, Класс, ID обращения, ID связанного обращения, Операция, Параметры, Последний компонент, Выдержка времени |
| **TC-RESUL-L** (результат успешной операции — последняя или единственная часть) | Запрос, Индикация | ID диалога, ID обращения, Параметры, Последний компонент |
| **TC-RESUL-NL** (результат успешной операции — не последняя часть) | Запрос, Индикация | ID диалога, ID обращения, Параметры, Последний компонент |
| **TC-U-ERROR** (отклик на обращение к операции, указывающий на неуспех) | Запрос, Индикация | ID диалога, ID обращения, Ошибка, Параметры, Последний компонент |
| **TC-L-CANCEL** (уведомление «своего» пользователя об отмене операции по тайм-ауту) | Индикация | ID диалога, ID обращения |
| **TC-U-CANCEL** (отмена операции по решению «своего» пользователя) | Запрос | ID диалога, ID обращения |
| **TC-L-REJECT** (отказ «своему» пользователю из-за неверного компонента) | Индикация | ID диалога, ID обращения, Код причины, Последний компонент |
| **TC-R-REJECT** (отказ пользователю со стороны партнера) | Индикация | ID диалога, ID обращения, Код причины, Последний компонент |
| **TC-U-REJECT** (отказ от компонента со стороны пользователя) | Запрос, Индикация | ID диалога, ID обращения, Код причины, Последний компонент |

2. Связанные с сопровождением диалога — диалоговые примитивы.

|  |  |  |
| --- | --- | --- |
| **Общее имя** | **Тип** | **Параметры** |
| **TC-UNI** (запрос/индикация неструктурированного диалога) | Запрос, Индикация | Качество обслуживания, Адрес получателя, Адрес отправителя, ID диалога, Наличие компонентов |
| **TC-BEGIN** (начало диалога) | Запрос, Индикация | Качество обслуживания, Адрес получателя, Адрес отправителя, ID диалога, Наличие компонентов |
| **TC-CONTINUE** (продолжение диалога) | Запрос, Индикация | ID диалога, Наличие компонентов |
| **TC-END** (окончание диалога) | Запрос, Индикация | ID диалога, Наличие компонентов, Версия окончания |
| **TC-U-ABORT** (внезапное прекращение диалога пользователем) | Запрос, Индикация | ID диалога, Информация пользователя |
| **TC-P-ABORT** (внезапное прекращение диалога пользователем) | Запрос, Индикация | ID диалога, Информация пользователя |

## Подсистема BSSAP

Для того чтобы понять работу сети GSM необходимо рассмотреть набор протоколов, в соответствии с которым осуществляется взаимодействие.



Сигнализация на A-интерфейсе относится к межстанционной сигнализации, несмотря на то, что BSC не является коммутационной станцией. Однако, контроллеры выполняют функции коммутации и каждому из них назначается собственный код пункта сигнализации (SPC). Протокол, используемый на A-интерфейсе, называется **Base Station Application Part** (BSSAP). Передается он при помощи подсистем МТР и SCCP.

**A-Bis** интерфейс переносит трафиковые и сигнальные данные между BSC и присоединенными к нему BTS. В эти данные входят все сообщения третьего уровня, которые предназначены для непосредственного обмена между MS и MSC. Однако некоторые сообщения относятся непосредственно к радиооборудованию и выделены в отдельный протокол обмена между BTS и BSC, который получил название BTSM (Base Transiver Station Management). На втором уровне используется протокол, который предназначен для выявления и коррекции ошибок, деления потока данных на фреймы и управления этим потоком. Этот протокол получил название Link Access Procedure D-channel (LAPD).

##### **Радио интерфейс Um**

Это звено между мобильной станцией абонента и основной сетью. Он состоит из трех уровней, которые рассмотрены ниже.

Стек протоколов сигнализации на радиоинтерфейсе Um делится на 3 уровня:

* Уровень 3 (Mobile Network Service Layer) управляет всеми аспектами радиоуправления, мобильности и обслуживания мобильной станции в сети. 3-й уровень сигнализации используется для следующих системных процедур:
  + установление радио-соединения между мобильной станцией и сетью;
  + регистрация и обновления местоположения;
  + установления вызовов;
  + передача SMS сообщений;
  + обеспечение хэндоверов;
  + управление дополнительными услугами;
* Уровень 2 (Data Link Layer) обеспечивает различные функции, относящиеся к управлению передачей данных к/от мобильной станции. На этом уровне используется протокол LAPDm, который отслеживает такие моменты как: подтверждение или не подтверждение операций, сегментация длинных сообщений Layer3, управление потоком данных и т.д;
* Уровень 1 (Physical Layer) содержит спецификации функций для физической побитовой передачи данных на радио-интерфейс. Эти функции включают:
  + канальное кодирование информации;
  + интерливинг (Interleaving) - перемежение на уровне бит и фреймов;
  + шифрование (Ciphering) - кодирование передаваемой информации;
  + форматирование пакетов (Burst formatting);
  + модуляция.

Уровень 1 так же отвечает за другие функции, такие как распределение логических каналов по физическим каналам, управление мощностью мобильной и базовой станций, выбор сектора мобильной станцией, хендовер и мониторинг качества.

Наиболее важным с позиции сети является 3-й уровень стека протоколов радиоинтерфейса.

###### **Протоколы 3-го уровня**

Уровень 3 (L3) делится на 3 подуровня, каждый из которых представляет набор сигнальных сообщений, которые отвечают за определенные аспекты сетевого обслуживания. Протоколы L3 получили следующие названия:

* Connection Management (CM) - управление соединением;
* Mobility Management (MM) - управление мобильностью;
* Radio Resource Management (RR) - управление радио-ресурсами.

Структура подуровней подразумевает взаимодействие «провайдер-пользователь»: подуровень RR является провайдером услуг для ММ подуровня (для обеспечения функций мобильности сначала должно быть установлено радио соединение), в свою очередь ММ подуровень является провайдером услуг для СМ подуровня (возможности мобильной функциональности должны предшествовать предоставлению услуг мобильной связи).

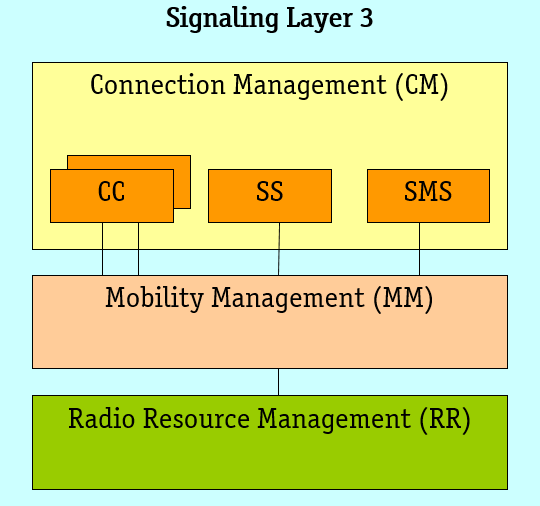
В то время как СМ и ММ функциональности принадлежат исключительно мобильной станции (MS) и MSC, функции RR распределены между MS, BTS, BSC и даже MSC. Однако BTS и MSC выполняют очень малую долю радио функций. Главным узлом, на котором завязано радиоуправление, является BSC.

###### **Управление соединением (СМ)**

Подуровень СМ имеет свою собственную структуру и делится на 3 функциональные части:

* СС (Call Control) - управление вызовом;
* SMS (Short Message Service - управление услугой коротких текстовых сообщений;
* SS (Supplementary Services) - управление дополнительными услугами.

Эти функциональные части равноправны и могут быть активированы одновременно в мобильной станции.



###### **Call Control (CC)**

Управление вызовом (CC) - содержит функции и процедуры для обеспечения ISDN вызова, модифицированные и адаптированные для использования в радио-среде. СС также обеспечивает функциями для управления дополнительными услугами, зависимыми от вызова, таких как ожидание вызова (CW) и удержание вызова (СН). Сообщения СС делятся на 5 групп:

* cообщения для установления вызова;
* сообщения информационной фазы вызова;
* сообщения для завершения вызова;
* сообщения для управления дополнительными услугами, зависимыми от вызова;
* другие сообщения.

###### **Short Messages Service support (SMS)**

Подуровень CM содержит в себе протокол для управления короткими сообщениями Short Message Control Protocol (SM-CP), который следит за передачей SMS между узлами управления короткими сообщениями (SMC), находящихся в MS и MSC соответственно. Эти узлы обслуживают уровень доставки коротких сообщений Short Messages Relay (SMR) используя протокол доставки коротких сообщений Short Messages Relay Protocol (SM-RP), ответственный за последовательную передачу содержимого SMS сообщений, так же, как и подтверждений и уведомлений между MS и SMS центром (SMSC). Протокол SM-CP состоит из 3-х сообщений: СР-Data, CP-Ack и CP-Error. Сообщения CP-Data переправляют содержимое SMS сообщений, в то время как CP-Ack и CP-Errors сообщения служат для подтверждения успешной доставки SMS и указания ошибки доставки соответственно.

Протокол SM-RP обеспечивает механизм уведомления сети о состоянии памяти MS.

###### **Supplementary Services management (SS)**

Абонент управляет дополнительными услугами с мобильной станции, выполняя процедуры интерфейса «человек-машина» (MMI). Это может быть достигнуто 2-мя путями: вводом последовательности цифр от 0 до 9 и символов # и \*, или используя пункты меню аппарата. Если MS находится в режиме idle, когда абонент инициирует процедуры управления SS, то в этом случае сигнального соединения еще нет. В этом случае соединение должно быть установлено специально для управления услугами. Этот процесс относится к управлению дополнительными услугами, независимыми от вызова.

Сообщения SS относятся к различным аспектам состояния услуг (регистрация, активация, просмотр и др.) Чаще всего узлы, связанные с управлением SS это MS и HLR. MSC выполняет роль посредника сигнальных сообщений между этими узлами, причем на этом этапе сообщения транслируются в операции протокола МАР.

Узлы SS создают ММ соединение из конца в конец. Следующие 3 сообщения могут быть переданы через это ММ соединение:

* Register;
* Facility;
* Release Complete.

Первое сообщение Register посылается для назначения нового идентификатора сигнальной процедуре, затем могут передаваться сообщения возможностей услуг Facility. По окончании процедуры передается сообщение Release Complete, освобождающее идентификатор. Все три сообщения содержат информационные элементы услуг, которые переносят запросы или подтверждения операций дополнительных услуг.

###### **Управление мобильностью (ММ)**

Подуровень ММ включает в себя всю функциональность, необходимую для управления мобильностью и безопасностью. Сообщения ММ делятся на 3 основные категории:

* сообщения регистрации (Registration);
* сообщения безопасности (Security);
* сообщения управления соединением (Connection management).

Первая группа включает сообщения для обновления местоположения (Location Update - LU) всех типов, а также процедура IMSI detach.

Вторая группа имеет дело с процедурами безопасности, такие как аутентификация мобильной станции, проверка идентификации (IMSI и IMEI), а также конфиденциальность идентификаторов абонентов, основанную на использовании номеров TMSI.

Третья группа содержит сообщения, предоставленные подуровнем СМ с возможностью использования ММ соединения для связи с оконечным узлом на удаленной стороне. Основное ММ сообщение в группе - CM Service Request, целью которого является указание сети типа запрашиваемой услуги.

###### **Управление радиоресурсами (RR)**

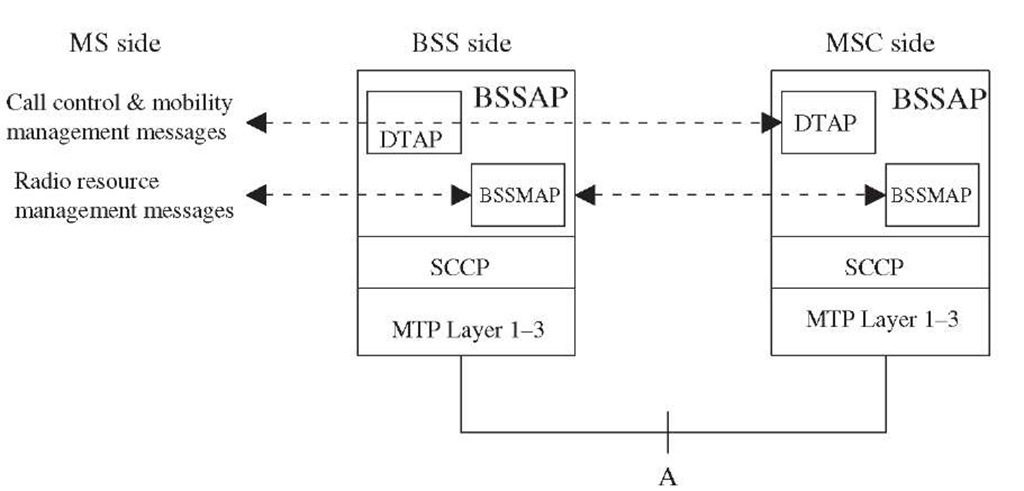
Подуровень управления радиоресурсами отвечает за выполнение всей радио-функциональности на сети GSM. Большинство RR сообщений передаются между MS и BSC. Однако некоторые процедуры, связанные с радиоинтерфейсом (радиозависимые) выполняются на интерфейсе между BTS и MSC. Например, для межкоммутаторного хендовера необходим обмен сообщениями RR 3-го уровня между контроллерами и коммутаторами, участвующими в этой процедуре, а также обмен МАР сообщениями между двумя коммутаторами.

К радиозависимым процедурам относятся: назначение и освобождение радиоканалов, шифрование, смена радиоканала в процессе разговора, хендоверы, передача системной информации, запрос данных об оборудовании MS и другие.

##### **A-интерфейс**

Сигнализация на А интерфейсе основана на сигнализации ОКС-7. Используются режимы СО (Connection Oriented) и CL (Connection Less) подсистемы SCCP. BSSAP - прикладная подсистема, которая используется между MSC и BSC. BSSAP выполняет 2 функции:

* DTAP (Direct Transfer Application sub-Part) - используется для передачи сообщений СМ и ММ с радио интерфейса между MS и MSC. Эти сообщения являются прозрачными для подсистемы BSS;
* BSSMAP (BSS Management Application sub-Part) - поддерживает другие процедуры между MSC и BSS, относящихся к MS (пейджинг, управление ресурсами, хендовер).

Сообщения BSSAP имеют следующий формат:

## Подсистема ISUP

Подсистема-пользователь стека ОКС7 — ISUP (ISDN User Part) выполняет функции сигнализации в цифровой сети интегрального обслуживания (ISDN) при установлении телефонных соединений, сеансов передачи данных, а также при предоставлении дополнительных услуг. ISUP используется также и для управления разговорными каналами в сетях подвижной связи, и в интеллектуальных сетях, и для связи с сетями VoIP.

Для переноса информации подсистема ISUP использует услуги, передаваемые подсистемой передачи сообщений MTP, и в некоторых случаях подсистемой управления сигнальными соединениями SCCP.

Сигнальный протокол подсистемы ISUP используется, прежде всего, для управления установлением соединения от станции вызывающего абонента до станции вызываемого абонента. Дополнительно к этому ISUP предоставляет средства для передачи информации, связанной с уже установленным соединением.

##### **Услуги**

Подсистема ISUP предусматривает два класса услуг: основные и дополнительные.

**Основные услуги**

Услуги доставки информации (bearer services), в частности:

* речь (с коммутацией каналов);
* аудиосигнал 3,1 кГц (с коммутацией каналов) – обеспечивает доставку нетелефонной информации, совместимой с речевым каналом;
* цифровая информация 64 кбит/сек без ограничений (с коммутацией каналов);
* пакетная информация — доставка данных в пакетном режиме по каналам B и D.

**Дополнительные услуги**

Набор дополнительных услуг содержит услуги как ориентированные, так и не ориентированные, на создание в сети ОКС7 сигнального соединения:

* идентификация номера: предоставление номера вызывающей стороны CLIP (calling line identification presentation); запрет предоставления номера вызывающей стороны CLIR (calling line identification restriction) и другие;
* предложение связи: переадресация связи ЕСТ (explicit call transfer); переадресация вызова при занятости вызываемого абонента CFB (call forwarding busy); переадресация вызова, если абонент не отвечает CFNR (call forwarding no reply); безусловное перенаправление вызова CFU (call forwarding unconditional) и другие;
* завершение установления соединения: вызов на ожидании CW (call waiting); удержание соединения HOLD (call hold); завершение создания соединения при занятости абонентов CCBS;
* многосторонняя связь: конференцсвязь CONF (conference call addon); трехсторонняя связь 3PTY (three party);
* для групп пользователей: замкнутая группа пользователей CUG (closed user group) и другие;
* начисление платы: извещение о стоимости (АОС, advice of charge),
* возможность относить начисление платы за связь на входящую сторону (REVC, reverse charging);
* перенос дополнительной информации: сигнализация пользователь-пользователь UUS (user-to-user signalling).

##### **Сообщения ISUP**

Для ISUP специфицировано около 40 типов сообщений и около 80 параметров. Они передаются посредством подсистемы MTP или, реже, SCCP. Вот некоторые примеры типов сообщений:

* Начальное адресное сообщение (**IAM** (Initial Address Message)) — первое сообщение, посылаемое для информирования другой АТС, что для конкретного CIC в данном сообщении запрашивается установление соединения. Обычно содержит номер вызываемого и вызывающего абонента, тип сервиса (голос, данные и т. д.) и многие другие опциональные параметры.
* Последующее адресное сообщение (**SAM** (Subsequent Address Message)) — в случае, если IAM не содержит полной адресной информации, одно или несколько сообщений SAM содержат дополнительные цифры номера.
* Сообщение о приёме полного номера (**ACM** (Address Complete Message)) — сообщение, передаваемое оконечной АТС, когда был найден вызываемый абонент и его телефонный аппарат начинает звонить.
* Сообщение ответа (**ANM** (Answer Message)) — отправляется, когда вызываемый абонент снял трубку. Начиная с этого момента стартует начисление платы.
* Запрос разъединения (**REL** (Release)) — отправляется для разрушения установленного соединения, например, когда абонент положил трубку.
* Подтверждение разъединения (**RLC** (Release complete)) — подтверждение разъединения, означает, что разговорный канал свободен и может быть снова использован для осуществления нового вызова.

##### **Пример установления соединения**

Ниже приведён один из базовых сценариев обмена сигнальными сообщениями ISUP при установлении соединения.

''' Абонент А АТС A АТС B Абонент B '''

Снятие трубки | |

Набор номера ---> | |

| -- IAM --> |

| |

| <-- ACM -- |

| | -Посылка вызова->

| <-- ANM -- |

-Снятие трубки

======================= РАЗГОВОР ======================

Трубка положена | |

| -- REL --> | Трубка положена

| <-- RLC -- |

## Подсистема MAP

##### **Предназначение MAP**

Для поддержания GSM сигнализации в коммутационных системах был разработан специальный протокол прикладной подсистемы подвижной связи (МАР - Mobile Application Part). Концепция GSM предполагает коммуникацию между узлами как внутри одной PLMN, так и между узлами различных PLMN. Использование МАР для этих целей предполагает использование подсистемы возможностей транзакций (ТСАР) и подсистемы управления сигнальными соединениями (SCCP). МАР использует не ориентированный на соединение тип SCCP.

Протокол МАР используется, например, в следующих случаях:

* Процедуры обработки вызовов;
* Межкоммутаторный хэндовер;
* Предоставление информации аутентификации;
* Обработка дополнительных услуг;
* Передача SMS сообщений.

В сущности, МАР сообщения - это операции, запрос которых инициируется в определенном узле коммутационных систем из другого узла. Во многих случаях операция, запрошенная в узле, может инициировать последовательность запросов операций в других узлах.

Например, при установлении входящего вызова GMSC запрашивает операцию sendRoutinglnfo в HLR, который в свою очередь запрашивает операцию provideRoamingNumber в определенном VLR.

##### **Прикладные объекты МАР**

Для поддержания различных типов операций в GSM архитектура МАР функционально разделена на так называемые «прикладные объекты» (АЕ -Application Entities). Они идентифицируются номерами подсистем SCCP (SSN):

* МАР-HLR, SSN=6;
* МАР-VLR, SSN=7;
* MAP-MSC, SSN=8;
* MAP-EIR, SSN=9;
* MAP-AUC, SSN=10.

Каждый АЕ также делится на определенное количество прикладных сервисных элементов (ASE - Application Service Elements). Каждый ASE состоит из одной или нескольких операций со своими параметрами. Каждая запрошенная операция, так же, как и ее результат передается между узлами в виде МАР-компоненты внутри ТСАР-сообщения. ТСАР считается общим ASE, который включен в каждый МАР-АЕ.

##### **Операции MAP**

Протокол МАР развивается с эволюцией системы GSM. С добавлением новых услуг получили развитие новые версии МАР. В настоящее время существует три версии протокола МАР:

* версия 1 МАР (МАР 1) - соответствующая фазе GSM 1;
* версия 2 МАР (МАР 2) - соответствующая фазе GSM 2/2+;
* версия 3 МАР (МАР 3) - соответствующая фазе GSM 2+.

В таблице показан набор операций МАР версии 2 с соответствующим кодом и интерфейсами, на которых они используются.

|  |  |  |
| --- | --- | --- |
| **Имя операции** | **Код операции** | **Интерфейс** |
| **Location registration:** | | |
| updateLocation | 2 | D |
| cancelLocation | 3 | D |
| purgeMS | 67 | D |
| sendldentification | 55 | D |
| **Call handling:** | | |
| sendRoutinglnfo | 22 | C |
| provideRoamingNumber | 4 | D |
| resumeCallHandling | 6 | E |
| **Handover:** | | |
| prepareHandover | 68 | E |
| sendEndSignal | 29 | E |
| processAccessSignalling | 33 | E |
| forwardAccessSignalling | 34 | E |
| prepareSubsequentHandover | 69 | E |
| **Authentication:** | | |
| sendAuthenticationInfo | 56 | D |
| **IMEI management:** | | |
| checkIMEI | 43 | F |
| **Operation and Maintenance:** | | |
| activateTraceMode | 50 | D |
| deactivateTraceMode | 51 | D |
| sendIMSI | 58 | D |
| **Supplementary Service handling:** | | |
| registerSS | 10 | B, D |
| eraseSS | 11 | B, D |
| activateSS | 12 | B, D |
| deactivateSS | 13 | B, D |
| nterrogateSS | 14 | B, D |
| processUSSD-Request | 59 | B, D |
| unstructuredSS-Request | 60 | B, D |
| unsIructuredSS-Notify | 61 | B, D |
| registerPassword | 17 | B, D |
| getPassword | 18 | B, D |
| **Short message service:** | | |
| sendRoutingInfoForSM | 45 | C |
| mo-forwardSM | 46 | E |
| mt-forwardSM | 44 | E |
| **Subscriber management:** | | |
| insertSubscriberData | 7 | D |
| deleteSubscriberData | 8 | D |
| reportSM-DeliveryStatus | 47 | С |
| informServiceCentre | 63 | С |
| alertServiceCentre | 64 | С |
| readyForSM | 66 | D |
| **Fault recovery:** | | |
| reset | 37 | D |
| forwardCheckSS-Indication | 38 | B, D |
| restoreData | 57 | D |

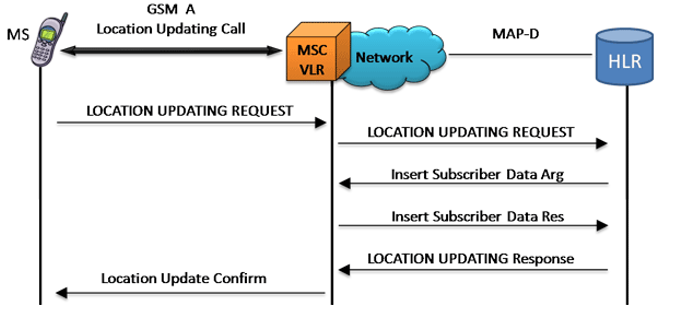
##### **Диалоги MAP**

Обмен операций МАР организован в форме диалогов. Простой диалог может содержать один «вопрос» и один «ответ», но существуют также длинные диалоги, которые содержат несколько вопросов и несколько ответов (это значит, что было запрошено несколько операций).

Имя МАР операций сохраняется (код операции один и тот же), не зависимо от того, запрос ли это с одной стороны или возврат результатов с другой. Определение того, запрос это или ответ закреплено за ТСАР.

Если используются разные версии МАР, удаленными узлами устанавливается соглашение об использовании общей версии. Это организовано при помощи параметров порции диалога сообщения ТСАР. Если одной из сторон отправляется отрицательный ответ в связи с отсутствием поддержки версии протокола, тогда другой стороной применяется процедура отката (fallback procedure) и понижение версии протокола на ступень. Каждый сигнальный узел коммутационной системы поддерживает протокол МАР версии 1. Однако, с понижением версии протокола, определенные операции, соответствующие новым системным возможностям, могут быть невозможны.

Пример диалога МАР на базе процедуры Location Update показан на рисунке:



##### **Услуги MAP**

Услуги МАР делятся на общие (common MAP services), которые доступны всем MAP-пользователям и специфические для пользователя (user specific services), которые доступны одному или нескольким, но не всем МАР-пользователям. Предоставление услуг обеспечивается посредством обмена примитивами. Используются все типы примитивов:

* Request (запрос);
* Indication (индикация);
* Response (ответ);
* Confirmation (подтверждение).

Если сервис не требует ответной посылки примитивов Response/Confirmation, то он называется сервисом без подтверждения (unconfirmed).

###### **Common MAP services**

Выполняет базовые функции уровня приложений:

* Установление и прекращение МАР-диалога;
* Доступ к функциям, поддерживаемым нижними уровнями;
* Информирование о сбойных ситуациях;
* Работа с различными версиями МАР;
* Проверка активности диалога на каждой из сторон;

При этом обеспечиваются следующие общие сервисы:

* MAP-OPEN - (сервис с подтверждением) с помощью этого примитива приложение запрашивает МАР установить диалог с другим приложением. Содержит спецификацию запрашиваемой транзакции (application context name);
* MAP-CLOSE - (сервис без подтверждения) используется для окончания существующего процесса;
* MAP-DELIMITER - (сервис без подтверждения) посылкой этого примитива приложение информирует, что пакет данных полный и готов к передаче через порт;
* MAP-U-ABORT - (user abort) (сервис без подтверждения) обозначает, что приложение намерено прервать диалог;
* MAP-P-ABORT - (service provider abort) (только примитив Indication) обозначает, что ТСАР намерено прервать или уже прервало диалог;
* MAP-NOTICE - (только примитив Indication) обеспечивает приложение информацией о проблемах со стороны порта.

###### **User specific services**

Выполняет конкретные функции по обработке событий пользовательских приложений. Имеются следующие группы:

* Mobility services;
* Operation and maintenance services;
* Call handling services;
* Supplementary services related services;
* SMS management services.

###### **Передача коротких сообщений (SMS)**

Служба коротких сообщений (SMS) предоставляет мобильным станциям возможность обмена текстовыми сообщениями, содержащими до 160 буквенноцифровых символов. Функции хранения и отправки сообщений выполняет SC (SMS Center).

Служба коротких сообщений (SMS) включает 3 основных процедуры:

1. Передача SM от MS на SC (Mobil Originated SM) и передача обратного рапорта на MS, содержащего результаты доставки на SC.
2. Прием SM от SC на MS (Mobil Terminated SM) и передача обратного рапорта на SC, содержащего результаты доставки на MS.
3. Передача Извещения (Alert). Данная процедура состоит из всех необходимых операций для HLR и VLR для инициирования передачи Извещения SC (Alert SC), информируя SC, что MS восстановила работоспособность.

Услуга передачи коротких сообщений предусматривает возможность информирования инициатора посылки SM об окончательном результате доставки сообщения адрессату (delivery report). Если сообщение не доставлено, то отчет должен содержать причину.

Протокол обмена короткими сообщениями подразделяется на соответствующие уровни. Верхний уровень - уровень приложения -обеспечивается в MS и SC. Уровень передачи - обеспечивает прохождение сообщения через отдельные элементы сети GSM. На уровне передачи имеется 6 типов PDU (Protocol Data Units):

* SMS-DELIVER - передает короткое сообщение от SC на MS;
* SMS-DELIVER-REPORT - передает:
  + причину ошибки (если необходимо);
  + информацию, как часть положительного или отрицательного подтверждения на SMS-DELIVER или SMS-STATUS-REPORT;
* SMS-SUBMIT - передает короткое сообщение от MS на SC;

SMS-SUBMIT-REPORT - передает

* + причину ошибки (если необходимо);
  + информацию, как часть положительного или отрицательного подтверждения на SMS-SUBMIT or SMS-COMMAND;
* SMS-STATUS-REPORT - передает отчет о состоянии от SC на MS;

SMS-COMMAND - передает команду от MS на SC.

При передаче и приеме SM MS может находиться в состоянии IDLE или BUSY. Пейджинг, установление управляющего сигнального канала SDCCH, аутентификация и т.д. требуется только в состоянии IDLE.

**Передача SM от MS на SC (Mobil Originated SM)**

Мобильная станция передает SM на SC, который, в свою очередь, информирует MS о доставке или недоставке сообщения.

1. MS устанавливает соединение с сетью, так же как при попытке установления голосового соединения. Если аутентификация прошла успешно, MS отправляет короткое сообщение (GSM 04.11).
2. MSC запрашивает VLR о возможности для данного абонента передачи короткого сообщения (MAP\_SEND\_INFO\_FOR\_MO\_SMS). 3. В ответном сообщении (MAP\_SEND\_INFO\_FOR\_MO\_SMS\_ACK) либо подтверждается успешное завершение операции MAP\_SEND\_INFO\_FOR\_MO\_SMS, либо выдается причина неуспешного завершения.
3. Если MSC не является шлюзом для взаимодействия с SC (IWMSC), то сообщение переправляется на IWMSC через операцию MAP\_MO\_FORWARD\_SHORT\_MESSAGE.
4. Короткое сообщение доставляется на SC с помощью протокола, который не является стандартным для сети. Алгоритм взаимодействия и формат обмена определен в GSM 03.40.
5. Алгоритм обмена предусматривает посылку ответного сообщения с указанием результата.
6. Осуществляется посылка результата выполнения операции (успешного или неуспешного) MAP\_MO\_FORWARD\_SHORT\_MESSAGE\_ACK.
7. MS получает информацию о результате выполнения операции доставки SMS.

При неуспешной попытке доставки сообщения, когда из HLR выдается отрицательное подтверждение, дополнительно из GMSC в HLR посылается сообщение MAP\_INFORM\_SERVICE\_CENTRE

**Прием SM от SC на MS (Mobile Terminated SM)**

Мобильный прием SMS - это возможность передачи коротких сообщений от SC на MS.

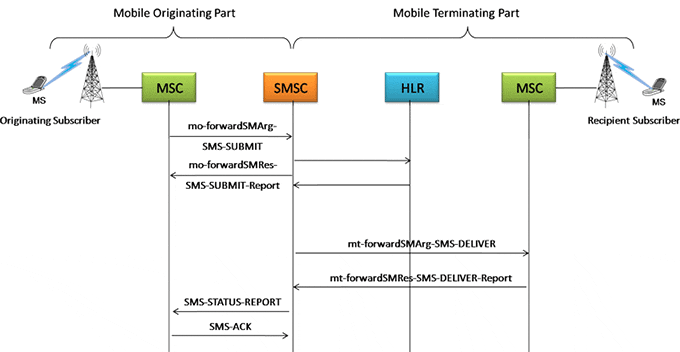
1. Сообщение, полученное от пользователя, отправляется с SC на соответствующий SMS-GMSC.
2. SMS-GMSC запрашивает в HLR информацию для маршрутизации сообщения (операция MAP\_SEND\_ROUTING\_INFO\_FOR\_SM).
3. HLR возвращает информацию о маршруте (номер MSC, обслуживающего абонента) и номер IMSI абонента на SMS-GMSC (операция MAP\_SEND\_ROUTING\_INFO\_FOR\_SM\_ACK).
4. SMS-GMSC отправляет сообщение на MSC, обслуживающий абонента (операция МAP\_MT\_FORWARD\_SHОRT\_MESSAGE).
5. MSC запрашивает VLR о возможности выполнения доставки короткого сообщения (операция MAP\_SEND\_INFO\_FOR\_MT\_SMS).
6. В случае успешного завершения операции (абонент доступен и для него возможна передача SMS) VLR запрашивает в MSC вызов абонента (MAP\_PAGE).
7. На MS поступает вызывной сигнал (в случае если MS в Idle).
8. Устанавливается соединение с сетью, так же как, для случая установления речевого соединения.
9. MSC подтверждает выполнение вызова абонента (MAP\_PROCESS\_ACCESS\_REQUEST).
10. От VLR поступает подтверждение на выполнение операции MAP\_SEND\_INFO\_FOR\_MT\_SMS (успешное или неуспешное).
11. MSC передает сообщение на MS, используя управляющий сигнальный канал SDCCH (или SACCH, если MS в состоянии Busy).
12. Завершение процесса передачи короткого сообщения на MS.
13. По окончании процесса передачи MSC информирует о результате SMS-GMSC (подтверждение).
14. SMS-GMSC передает результаты выполнения операции посылки короткого сообщения на SC (успешное и неуспешное). Если передача была успешной, то на этом процесс завершается. Если нет, то SMS-GMSC информирует об этом HLR (операция MAP\_REPORT\_SM\_DELEVERY\_STATUS).

Доставка короткого сообщения может окончится неуспешно по следующим причинам:

* Unknown subscriber (Р);
* Teleservice not provisioned (P);
* Illegal Subscriber (P);
* Call barred (T);
* Absent subscriber (T)
* Memory Capacity Exceeded (T).

Причины, отмеченные P (permanent) приводят к удалению сообщения.

В случае неуспешной доставки по причинам, отмеченным Т (temporary) сообщение сохраняется для осуществления повторной попытки доставки. В HLR устанавливается индикатор ожидания доставки SMS. Когда MS станет доступной или будет получена информация о наличии свободной памяти в MS, VLR проинформирует об этом HLR (операция MAP\_READY\_FOR\_SM), после чего будет инициирован процесс доставки короткого сообщения на MS. Для этого HLR запрашивает в IWMSC выполнение операции MAP\_ALERT\_SERVICE\_CENTRE.



## Протокол CAP

##### **Концепция интеллектуальной сети связи (Intelligent Network)**

Интеллектуальная сеть связи - это архитектурная концепция создания и предоставления новых услуг связи, которая обладает следующими характеристиками:

* использование современных методов обработки информации;
* эффективное использование сетевых ресурсов;
* модульность и многоцелевое назначение сетевых элементов;
* интегрированные возможности разработки и внедрения услуг;
* стандартизированное взаимодействие сетевых функций посредством независимых от услуг сетевых интерфейсов;
* возможность управления атрибутами услуг со стороны абонентов;
* стандартизованное управление логикой услуг.

Далее интеллектуальная сеть будет рассмотрена на примере технологии CAMEL - Customized Applications in Mobile Networks, Enchanced Logic.

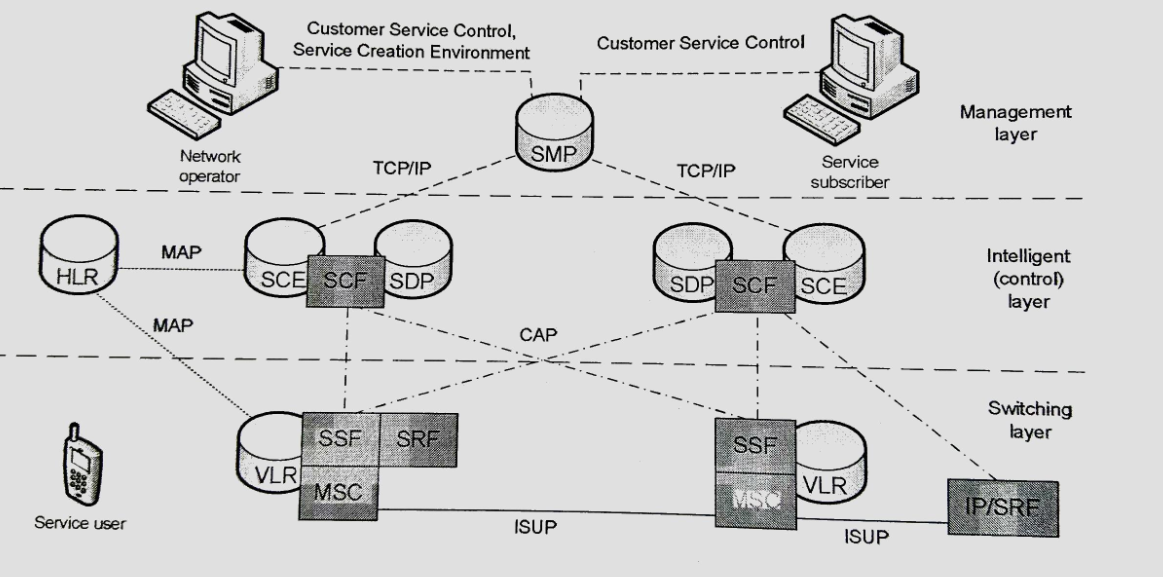
##### **Физическая структура**

Основная философия сети CAMEL - это введение уровня контроля, который будет содержать логику услуги и данные услуги в центральной точке, тем самым позволяя более эффективно обслуживать существующие и новые услуги. Кроме того, взаимодействие между узлами и идентификаторы услуг стандартизированы.

Для предоставления CAMEL услуг необходимы следующие компоненты:

* Мобильный центр коммутации услуг (service switching point SSP) формирует переход из базовой сети к узлу интеллектуальной сети. SSP распознает, должна ли услуга обрабатываться при помощи CSE, и, если да, запрашивает соответствующую информацию по услуге. В дополнении к функционалу доступа к CSE, SSP также имеет функционал MSC. Он может быть расположен в домашней или гостевой сети IN-абонента. Функционал SSP могут иметь как GSM MSC's, так и GPRS SGSN's.
* CAMEL-окружение (CAMEL service environment CSE) - узел IN, контролирующий услуги. CSE подключен к SSF посредством сигнальной сети ОКС7. CSE содержит пользовательские и сетевые данные, необходимые в процессе предоставления услуги. Он всегда расположен в домашней сети IN-абонента. IN услуги в сети GSM и в сети GPRS могут обслуживаться одним и тем же CSE.
* Центр управления услугами (service management point SMP) обеспечивает развертывание и предоставление CAMEL услуг. То есть, оператор сети имеет возможность создавать новые CAMEL услуги с помощью так называемого SCE (Service Creation Environment) и клиент или абонент услуги может администрировать и управлять некоторыми специфичными для услуги функциями при помощи CSC (Customer Service Control). В CSE будут загружены только услуги или модификации услуг, которые были успешно протестированы в SMP.
* Интеллектуальная периферия (intelligent periphery IP) - предоставляет ресурсы для пользовательского диалога (такие как автоответчики, прием набранных цифр, генераторы тонов).
* HLR, центральная абонентская база данных для GSM и GPRS, может иметь подключение к CSE посредством протокола МАР для возможности предоставления запроса "Any Time Interrogation" и для пересылки USSD кодов в CSE.
* Пользователи услуги (Service users) - это участники вызова, которые собственно и используют IN услугу. В случае, если предоставляется услуга CAMEL, пользователем всегда является мобильный абонент GSM и/или GPRS.
* Абоненты услуги (Service subscribers) платят за услуги, предоставленные оператором сети, для того, чтоб сделать услуги доступными пользователям услуги (к примеру, компания, предоставляющая услугу "бесплатный вызов"). Абоненты услуги имеют возможность модифицировать свои абонентские данные в базе данных IN. В некоторых случаях, при предоставлении услуги «Prepaid Service» пользователь услуги может также являться и абонентом услуги.

Схема базовой архитектуры сети **CAMEL** представлена ниже.

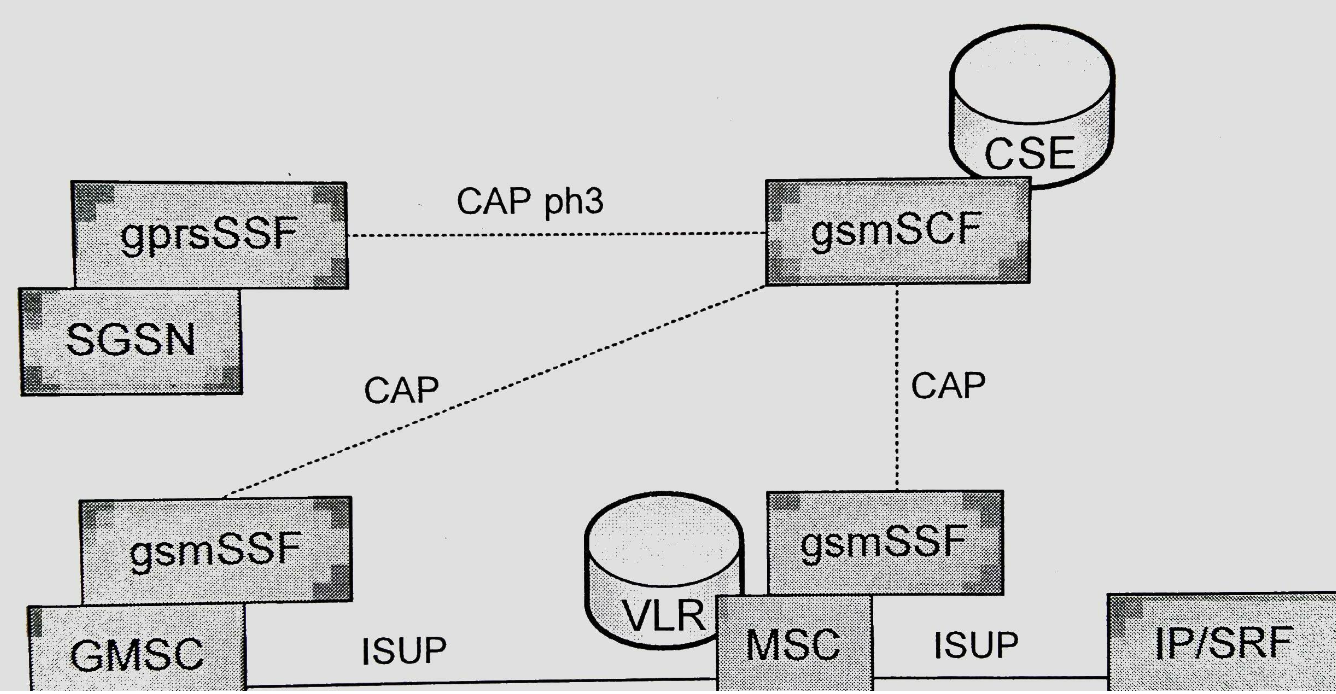


##### **Протоколы взаимодействия**

Взаимодействие между SSP и CAMEL IN осуществляется посредством стандартизированного протокола CAMEL Application Protocol (САР). Сам по себе САР является приложением стека протоколов ОКС7. Для процедур Any Time Interrogation и Supplementary Service Invocation Notification, связь c CSE осуществляется посредством сообщений протокола МАР версии 3. Между двумя SSP может происходить взаимодействие по протоколу ISUP - для процедур assist. Внутри IN, между CSE и SMP, взаимодействие происходит посредством протокола TCP/IP.

###### **Service Switching Point (SSP)**

Помимо обеспечения доступа пользователей в сеть и выполнения необходимых коммутационных функций, SSP обеспечивает доступ к набору возможностей CAP. SSP имеет функцию обнаружения запросов на услугу CAMEL. Также он имеет возможность взаимодействия с другими физическими, элементами, имеющими функцию управления услугой (service control function - gsmSCF), такими как service control point (CSE). Функционально SSP содержит в себе функцию контроля вызова (call control function -gsmCCF) и функцию коммутации услуги (service switching function - gsmSSF); в случае же SSP, включенного в состав SGSN, SSP содержит только gprsSSF.



###### **Intelligent Periphery (IP)**

IP предоставляет ресурсы, такие как стандартные и персонализированные голосовые автоответчики, распознавание голоса, прием набранных посредством DTMF (dual tone multi-frequencies) команд пользователя, и содержит коммутационное поле для проключения пользователей к данным ресурсам. IP поддерживает гибкий обмен информацией между пользователем и сетью - так называемый user interaction dialog. В существующих реализациях только MSC может быть оборудовано IP и только MSC может получать к ней доступ. Функционально IP контролируется функцией специализированных ресурсов (special resource function - gsmSRF). IP может быть подключена к одному или нескольким SSP.

CSE может запросить у SSP соединение с ресурсом, находящимся в IP, подключенном к тому SSP, на котором произошел запрос услуги пользователем. Кроме того, CSE может запросить соединение с ресурсом, находящимся в IP, подключенном к другому SSP (так называемая процедура assist или CAMEL-перемаршрутизация).

###### **CAMEL Service Environment**

CSE содержит программы логики услуг (service logic programs - SLP) и данные, которые используются для предоставления CAMEL услуг, такие как абонентские данные или распределение интеллектуальных периферий в сети. CSE полностью отвечает за обработку услуги. CSE также иногда называют Service Control Point (SCP). Он подключен к SSP посредством сети сигнализации ОКС7. Несколько CSE могут содержать одни и те же SLP для увеличения надежности и разделения нагрузки. Тем не менее, при обслуживании одного вызова всегда используется только один CSE. Функционально CSE содержит service control function (gsmSCF) и service data function (gsmSDF). GsmSCF также используется для обслуживания SLP GPRS.

CSE может быть подключено к SSP (опционально и к IP) посредством сигнальной сети. Также может CSE может подключаться к IP посредством функции передачи управления SSP (SSP relay function)

###### **The Service Data Point**

SDP содержит пользовательские и сетевые данные, используемые в процессе предоставления услуги. Функционально SDP содержит в себе функции gsmSDF. CSE может иметь доступ к данным SDP как через сигнальную сеть, так и напрямую. Обычно SDP и CSE объединены в один узел.

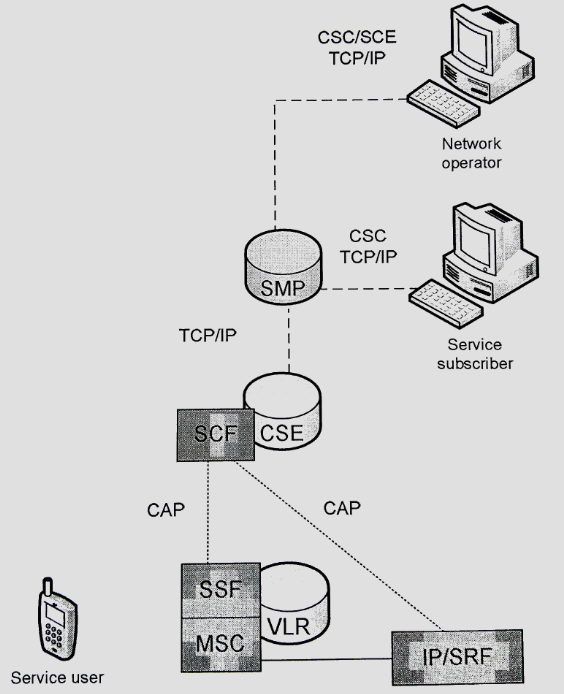
###### **Service Management Point**

Данный функционал позволяет развертывать и предоставлять новые CAMEL-услуги, а также оказывать последующую поддержку услуг.

Услуги создаются и тестируются в SMP сетевым оператором, используя SCE, прежде чем они загружаются в CSE. Также, когда абоненты услуги изменяют данные IN услуги посредством CSC, они изменяют базу данных, находящуюся в SMP и являющуюся зеркальным образом базы в CSE. Это делается чтоб избежать прямого доступа в CSE и облегчить внесение изменений в случае если на сети более одного CSE.

В **SMP** входят следующие компоненты:

* CSC - Customer Service Control (контроль пользователя услуги)
* SCE - Service Creation Enviroment (окружение для создания услуг).



##### **Абонентские данные для CAMEL**

Для указания на то, что при работе с данным абонентом используется обращение к функциям CAMEL, в абонентские данные включается специальная информация, которая называется CSI (CAMEL subscription information). Для одного абонента предусматривается несколько разновидностей CSI:

* для использования в исходящем соединении O-CSI;
* для использования во входящем соединении T-CSI;
* для использования при управлении дополнительными услугами SS-CSI и др.

CSI содержит следующую информацию:

* **TDP List** - список Detection Point, в которых будет срабатывать триггер.
* **Адрес SCP** (gsmSCF address) - фактически Global Title SCP. Пояснение, SCF - Service Control Function - так называется SCP на другом логическом уровне.
* **Service Key** - номер, указывающий на определённую логику, которую должен применить SCP.
* **Default Call Handling** - что делать со звонком в случае неответа SCP. Варианта два - продолжить или прекратить обработку.

CSI хранится вместе с остальными абонентскими данными в HLR. В процессе обработки вызова к моменту принятия решения об использовании интеллектуальных услуг (CAMEL) эта информация должна уже находиться в VLR (О-CSI) или в GMSC (T-CSI).

Информация О-CSI передается из HLR в VLR в процессе выполнения процедуры Location Update.

##### **Точки обнаружения**

Для внедрения в алгоритм обработки вызова функциональности взаимодействия с сетью IN (CAP) необходимо дополнение его механизмом работы с точками обнаружения (Detection Point - DP) и обеспечения возможности воздействия на обработку IN вызова логики IN услуг. Точки DP определяют точки PIC, в которых возможна передача управления. При достижении DP из SSF в SCF посылается операция (команда). Точки обнаружения делятся на TDP (триггерные точки обнаружения) и EDP (событийные точки обнаружения). Триггерные точки - это точки, в которых происходит первое обращение к логике IN.

Точки управления - управление SSP со стороны SCP (TDP-R, EDP-R). В точке управления процесс обработки вызова переходит в состояние ожидания.

Точки мониторинга - мониторинг SSP (TDP-N, EDP-N). В точке мониторинга процесс не останавливается.

Существует два вида точек обнаружения:

* Originating DP1 - DP10;
* Terminating DP12 - DP18.

Состояние точки может быть активным (armed) и неактивным (disarmed). Армирование и дизармирование точек может быть динамическим (EDP) в процессе обработки вызова, и статическим (TDP) в процессе создания и изменения услуги (от блока SMF).

Точки обнаружения для **исходящей** стороны:

* DP1 - Origination\_Attempt\_Authorized - исходящая попытка вызова;
* DP2 - Collected Information - собранная информация (достаточна для принятия решения об активации SSP);
* DP3 - Analysed\_Information - проанализированная информация (достаточна для принятия решения об активации SSP);
* DP4 - Route Select Failure - отказ выбранного маршрута;
* DP5 - O\_Called\_Party\_Busy - вызванная сторона занята, информация от исходящей стороны;
* DP6 - O\_No Answer - вызванная сторона не отвечает, информация от исходящей стороны;
* DP7 - O\_Answer - ответ, информация от исходящей стороны;
* DP9 - O\_Disconnect - разъединение, информация от исходящей стороны;
* DP10 - O\_Abandon - отказ с исходящей стороны.

Точки обнаружения для **входящей** стороны:

* DP12 - Terminating\_Attempt\_Authorized - входящая попытка вызова;
* DP13 - T\_Called\_Party\_Busy - вызванная сторона занята, информация от входящей стороны;
* DP14 - T\_No\_Answer - вызванная сторона не отвечает, информация от входящей стороны;
* DP15 - T\_Answer - ответ, информация от входящей стороны;
* DP17 - T\_Disconnect - разъединение, информация от входящей стороны;
* DP18 - T\_Abandon - отказ от входящей стороны.

##### **Модели вызова**

Теперь рассмотрим, как вызов выглядит с точки зрения сети SS7. Начнём с исходящего вызова.

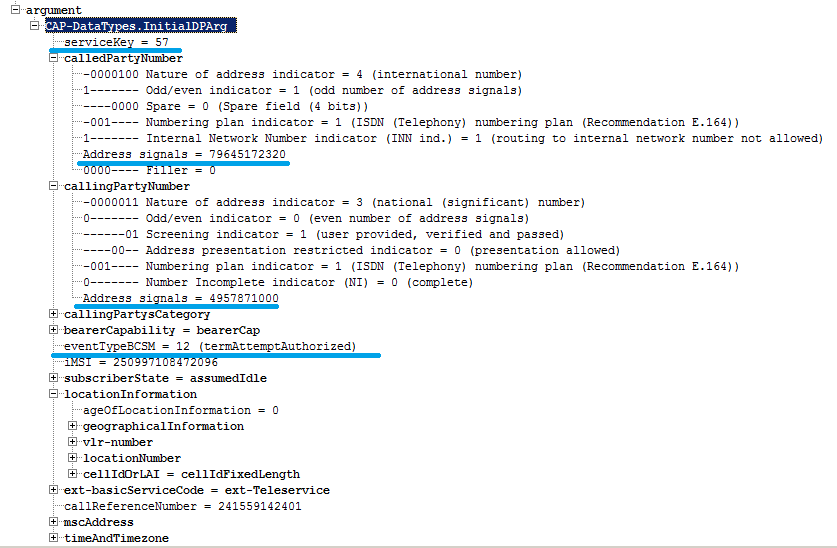
1. MSC при обработке исходящего вызова останавливается в DP2, потому что в профиле абонента "активирован" триггер для DP2.
2. SSP (MSC в терминологии CAMEL) инициирует CAMEL-запрос InitialDP на адрес SCP из профиля абонента с просьбой указать, что делать с этим вызовом.
3. SCP анализирует запрос, выполняет внутреннюю логику (например, определяет - есть ли деньги на счету абонента для выполнения вызова) и отвечает сообщением RequestReportBCSM (если есть необходимость "активировать" триггеры), за которым следует одно из сообщений: **Continue** (продолжить вызов с теми же параметрами), **Continue\_With\_Argument** (если несколько параметров в вызове надо изменить) или **Connect** (внутри этого сообщения содержится новый Б-номер с которым должен быть установлен вызов). Если же вызов не должен быть продолжен, то SCP отвечает сообщением **Release**.
4. SSP продолжает обработку вызова и если в профиле абонента или в RequestReportBCSM были активированы триггеры, то с помощью сообщения EventReportBCSM SCP информируется о срабатывании DP.

Теперь подробно о каждом из сообщений.

Сообщение **InitialDP** содержит такие важные поля:

* **serviceKey** - указатель на определённую логику в SCP. Например, SCP может предоставлять несколько разных услуг. Поле ServiceKey явно указывает какая именно CAMEL-услуга должна быть предоставлена для этого вызова.
* **callingPartyNumber** - номер вызывающего абонента (A-party number)
* **locationNumber** - номер MSC с которого происходит вызов
* **eventTypeBCSM** - описание триггера, который сработал. В нашем случае это DP2
* **locationInformation** - текущий VLR абонента и возраст этой информации
* **calledPartyBCDNumber** - вызываемый номер в BCD формате.
* **calledPartyNumber -** вызываемый номер при входящем вызове на CAMEL-пользователя.

Пример **InitialDP** при вызове абонента Облачной АТС:

Ответное сообщение **RequestReportBCSM** содержит список триггеров (**bcsmEvents**), которые необходимо установить в модели звонка. Для этого каждый триггер задаётся следующими параметрами:

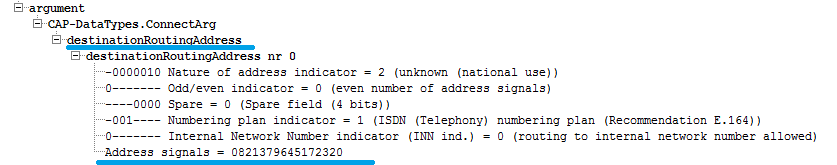
* **eventTypeBCSM** - DP, в котором необходимо активировать триггер
* **monitorMode** - что делать SSP в случае срабатывания триггера. Варианты такие: interrupted (EDP-R, останов и ожидание инструкции от SCP); notifyAndContinue (EDP-N, просто информирование SCP о наступлении события); transparent (не сообщать о наступлении события).
* **legID** - указатель на "часть вызова" от которой ожидается получить нотификацию. Вызов условно разделяется на Исходящую (Originating, legID 1) и Входящую (Terminating, legID 2) части. В каждой из этих частей будет, например, своё событие Disconnect. Указатель legID позволяет понять от какой из частей вызова пришло извещение о событии.
* **applicationTimer** - параметр, который определяет значение таймера No\_Answer для события No\_Answer (DP6/DP14). Если вызываемый номер не ответил в течении заданного времени, то SSP должен сообщить об этом на SCP. Тут есть один ньюанс, который мне доводилось видеть на практике - значение этого таймера должно быть меньше чем соответствующий таймер неответа на MSC. Иначе вместо события No\_Answer можно получить Busy.

|  |
| --- |
| **Обратите внимание:** при вызове абонента Облачной АТС и наоборот сообщения типа **RequestReportBCSM** не запрашиваются. |

Сообщение **Continue** особого интереса не представляет, поскольку не содержит никаких параметров - SCP просто указывает продолжить вызов.

**Continue\_With\_Argument** описано в спецификации, но в реальной жизни я этого сообщения никогда не видел. Поэтому писать о нём не будем.

**Connect**. Самый главный параметр в этом сообщении это **destinationRoutingAddress**. Фактически, это новый номер, на который должен пойти вызов. Пример, Вы пользователь услуги виртуальной АТС и позвонили на короткий номер Вашего коллеги - 777. SCP преобразует этот номер в "полный" MSISDN 79031234567 и отправит его в сообщении **Connect**.

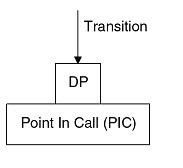
Пример сообщения **Connect** при вызове абонента Облачной АТС:

Есть ещё сообщение **ConnectToResource**, которое очень похоже на **Connect**, только позволяет совершить соединение с новым номером до соединения с набранным номером. Обычно в качестве нового номера выступает Intelligent Peripheral. Таким образом, например, Вас могут предупредить о том, что средства на счету или срок их действия истекают. После предупреждения вызов будет продолжен.

Если в сообщении **RequestReportBCSM** были активированы триггеры, то SSP информирует об их срабатывании с помощью сообщения EventReportBCSM. Это сообщение будет содержать тип события (DP), которое произошло, и дополнительную информацию по этому событию. Например, в случае события Busy будет указано точная причина занятости (Subscriber absent, User busy).

**Базовая модель состояния вызова (BCSM, Basic Call State Model)**

Для эффективного управления, вызов разбивается на отдельные элементы (состояния):

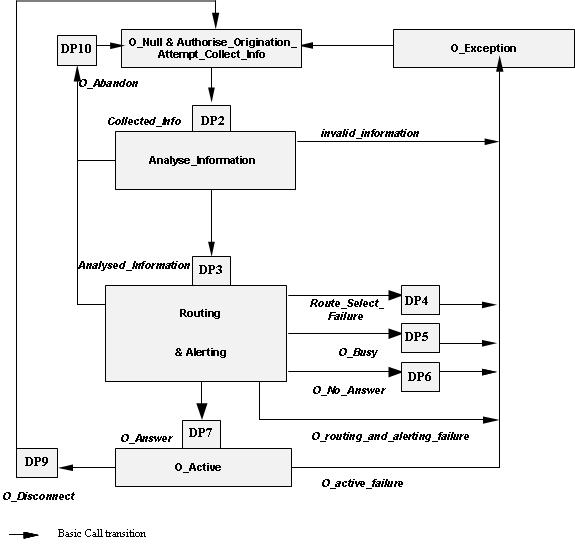


DP (**Detection Point**) это своеобразный указатель на текущее состояние. Например, DP2 (Collected Info) указывает на то, что это исходящий вызов в самом начале его обработки. Point In Call - это действия, которые выполняются в этом месте вызова. DP бывают 3-х типов:

1. Trigger Detection Point - Request (TDP-R). Это как раз тот триггер, о котором я уже упоминал. Устанавливается статически (до того, как начался вызов), создаёт CAMEL запрос на SCP и ждёт ответа. Обработка звонка при этом приостанавливается.
2. Event Detection Point - Request (EDP-R). Это динамический точка (устанавливается во время вызова по запросу от SCP). Обработка звонка приостанавливается и SSP ждёт инструкций от SCP.
3. Event Detection Point - Notification (EDP-N). Тоже динамическая точка. Отличие в том, что звонок не прерывается (хотя SCP информируется о достижении этой точки, как и в предыдущем случае).

##### **Модель исходящего вызова (Originating Basic Call State Model, O-BCSM)**

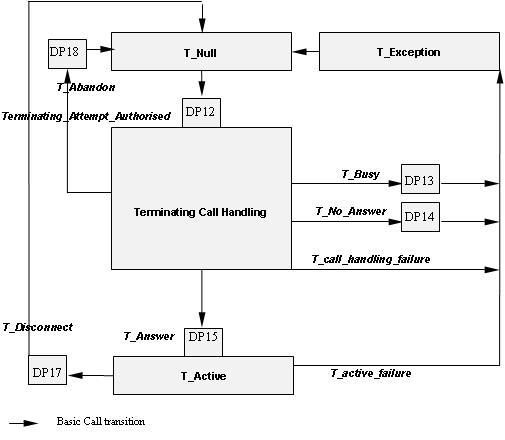
Обработка исходящего вызова происходит на Visitor MSC, т.е. на коммутаторе в котором абонент зарегистрирован в данный момент. VLR этого MSC уже содержит копию профиля абонента, а значит и **O-CSI** (если таковой у абонента имеется). В CAMELопределена такая модель исходящего вызова:



1. Вызов начинается с "**O\_Null & Authorise\_Origination\_Attempt\_Collect\_Info**". В этом месте (Point In Call) производится проверка запретов (пользовательских и со стороны оператора) на исходящие вызовы и анализ O-CSI.
2. В DP **Collected Info** у нас уже есть обработанная информация из O-CSI. Если в O-CSI, в поле TDP List содержится DP **Collected Info** (а для исходящих звонков там может быть только DP **Collected\_Info** и DP **Route\_Select\_Failure**), то инициируется запрос в SCP.
3. Далее вызов переходит в состояние "Analyse\_Information". На входе (в DP Collected Info) содержится обработанная информация из O-CSI, потом производится "разбор" вызываемого номера (например, определяется его тип -международный/национальный/неопределённый).
4. Предположим, что разбор номера произошёл успешно и вызов переходит в точку DP **Analysed\_Information**. На этом этапе тоже возможен запрос к SCP (хотя детали мне не известны).
5. Далее происходит переход в состояние "Routing & Alerting". Здесь нам доступна информация о вызываемом номере и его типе (Nature of address - национальный, международный, неопределённый). Происходит непосредственный вызов абонента Б, в телефоне звучит ответ от удалённого коммутатора (КПВ или мелодия сервиса RBT). Исключением является событие Route\_Select\_Failure с последующим вызовом DP4. Это происходит если на коммутаторе не нашлось подходящего маршрута для установления соединения (в результате т.н. B-number analysis).
6. Далее будет либо ответ вызываемой стороны (по ISUP мы получим ANM), а значит переход в DP7 O\_Answer, либо вызов будет неуспешным по одной из причин - занято (DP5), отсутствие ответа в течении заданного времени (DP6, время задаётся параметром в сообщении Request Report BCSM, но об этом позже), прерывание вызова А-абонентом (DP10).
7. Если ответа не было, то через PIC O\_Exception коммутатор освобождает все ресурсы и закрывает CAMEL диалоги. И мы возвращаемся в самое начало.
8. Если вызов успешный и у нас был ответ удалённой стороны, то рано или поздно вызов будет завершен (DP9) и мы снова вернёмся в начало.

##### **Модель входящего вызова (Terminating Basic Call State Model, T-BCSM)**

Перед тем, как начать рассматривать входящие вызовы, я напомню, что мы имеем дело с мобильной сетью. А значит местоположение Б-номера заранее неизвестно. Задача определения, текущего MSC вызываемого абонента в классической GSM сети (без **CAMEL**) была возложена на GMSC домашней сети. С введением **CAMEL**, именно на GMSC возложили задачу обработки **T-CSI** (Примечание. Согласно стандарту, возможен также **CAMEL**диалог между VMSC и SCP). Как происходит обработка вызова на GMSC показано на рисунке ниже:



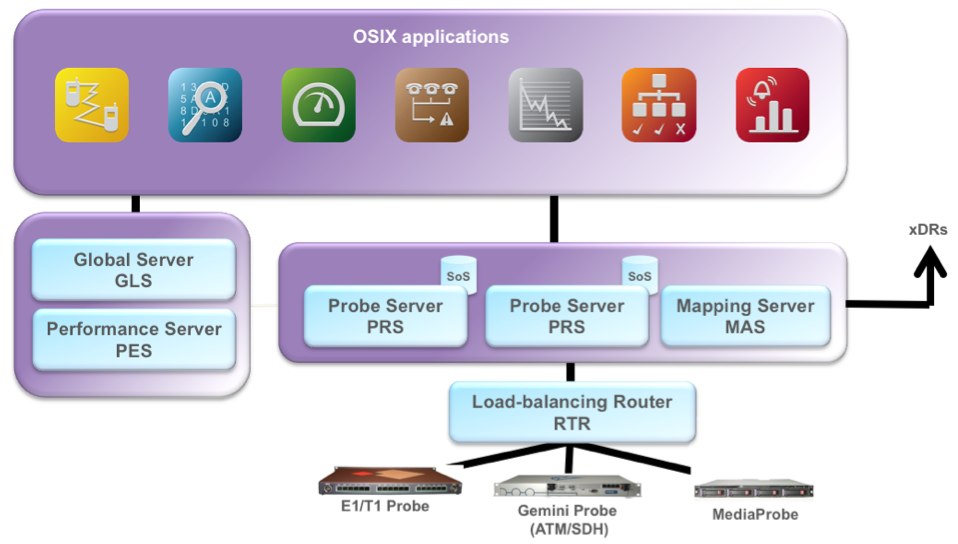
1. Вызов начинается с точки T\_Null. Входящий вызов поступает на GMSC для обработки (ISUP IAM). Поскольку GMSC ничего не знает о вызываемом абоненте и его местоположении, то он отправляет MAP SendRoutingInformation на HLR. В ответе на запрос содержится текущий MSC абонента, а также его профиль. Происходит проверка запретов на вызовы, а также анализ **CAMEL**подписки для входящих вызовов - **T-CSI**.
2. В DP12 Terminating\_Attempt\_Authorised у нас уже есть обработанная информация из **T-CSI**. Если в **T-CSI**, в поле TDP List содержится DP Terminating\_Attempt\_Authorised (а для входящих звонков там может быть только DP Terminating\_Attempt\_Authorised, DP T\_Busy, и DP T\_No\_Answer), то инициируется запрос в **SCP**.
3. Вызов переходит в PIC "Terminating Call Handling". В этом PIC осуществляется маршрутизация вызова и информирование Б-номера о поступлении вызова.
4. Далее будет либо ответ вызываемой стороны (по ISUP мы получим ANM), а значит переход в DP15 T\_Answer, либо вызов будет неуспешным по одной из причин - занято/абонент недоступен/ошибка установления соединения (DP13), отсутствие ответа в течении заданного времени (DP14), прерывание вызова А-абонентом (DP18).
5. Если ответа не было, то через PIC T\_Exception коммутатор освобождает все ресурсы и закрывает **CAMEL**диалоги. И мы возвращаемся в самое начало.
6. Если вызов успешный и у нас был ответ удалённой стороны, то рано или поздно вызов будет завершен (DP17) и мы снова вернёмся в начало.

## Работа с комплексом Polystar OSIX

##### **Введение**

Polystar OSIX является программно-аппаратным комплексом, структурно состоящим из следующих компонентов:

* датчики мониторинга сети **(Probe)** — аппаратный компонент, подключаемый к сети оператора для непосредственного съёма трафика. Поддерживаемые интерфейсы: E1 / T1 / J1, ATM, SDH/SONET, Ethernet 10/100/1000 **(MediaProbe)**;
* Маршрутизатор балансировки нагрузки **(Load-balancing Router)** - аппаратный компонент, распределяющий и балансирующий трафик от Probe к серверам, который этот трафик обрабатывают **(Probe Servers)**;
* **Probe Server** — программно-аппаратный компонент, который собирает, обрабатывает, хранит и выдаёт по запросу информацию о сети;
* **Mapping Server** — программно-аппаратный компонент, который хранит и обновляет информацию о соответствии IMSI и TMSI;
* **Performance Server** — программно-аппаратный компонент, используемый при анализе производительности сети оператора;
* Программные приложения OSIX **(OSIX Application)** — набор программных приложений для анализа полученных данных.

  
  
**Варианты применения:**

* Распределённый — Probe и Probe Server размещаются на каждом сайте и подключаются к сигнальным линкам своего сайта;
* Централизованный — все Probe и Probe Server размещаются на одном из сайтов (центральном сайте). Информация от сигнальных линков с каждого сайта передаётся на центральный сайт через **DXC (Digital Cross Connect)**.

**Области применения:**

* ТфОП (PSTN Networks)
  + ISUP, INAP, ISDN PRI, Parlay, BICC и т.д., + соответствующие протоколы нижних уровней;
* Сети мобильных операторов
  + MAP, IS-41, BSSMAP, GPRS, CAMEL, Parlay, MMS/WAP, SIGTRAN и т.д., + соответствующие протоколы нижних уровней;
* VoIP сети
  + SIP, H.323, MGCP, MEGACO, RTP, RTCP, SDP + соответствующие протоколы нижних уровней.

**Обработка собранных данных**

Собранные данные:

* могут быть обработаны программными приложениями мониторинга **(OSIX monitoring applications)**;
* cохранены в базе данных **SoS (OSIX Storage of Signals)** для дальнейшего использования;
* направлены к **xDR** приложению;
* направлены к внешним **OSS** приложениям;
* различные события могут генерировать **SNMP trap**, который может направляться к системам управления сторонних производителей.

**Программные приложения для мониторинга и обработки собранной информации:**

* **Call Trace** — мониторинг трасс вызовов с использованием различных видов фильтрации;
* **Protocol Analyzer** — анализатор протоколов с фильтрацией, возможностью просмотра в хронологическом порядке и на разных уровнях сетевой модели ISO OSI;
* **Performance Analyzer** — мониторинг сетевых параметров и контроль качества в соответствии с различными политиками: количество успешных, неуспешных и коротких вызовов, успешные SCCP/TCAP транзакции и т.п;
* **Mass Call** — мониторинг большого количества попыток вызова **(Call Attemps)** для исходящих/входящих номеров;
* **Real-Time Statistics** — статистика сетевых параметров в реальном времени с возможностью фильтрации по заданным условиям;
* **Network Status** — мониторинг аварийных сообщений MTP1,2,3 (ОКС-7), загрузки линков и линсетов в ОКС-7, а также SCTP-ассоциаций (SIGTRAN). Результаты могут отображаться в форме карты с нанесёнными линками;
* **Statistics Alarm** — Генерирование сообщений по определённым критериям: фильтр, протокол, сообщение протокола, звонок, транзакция.

##### **Подключение к OSIX и настройка полей поиска**

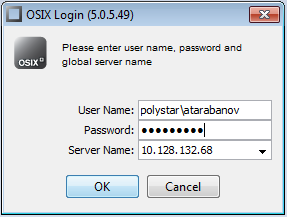
Для подключения к OSIX нужно предварительно поднять VPN до DCN (основной сервер 10.190.16.110, резервный сервер 10.190.16.109). Доступ к ИТ-услуге оформляется по заявке NS 31\_A - роль Штаб-квартира: доступ к транспортной и мобильной сети, **с ролью доступ к транспортной сети подключиться к OSIX нельзя.**

Далее запускаем OSIX. Запросят параметры для подключения.

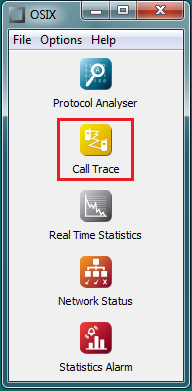
User Name: пишем префикс polystar\ **ваше доменное имя пользователя**

Password: пароль от доменной учетной записи

Server Name: 10.128.132.68

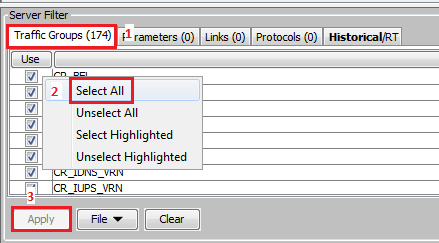
[](http://b2bts.vimpelcom.ru/w/images/1/1d/00_connect_osix.png)

Далее в окне OSIX выбираем иконку Call Trace:

[](http://b2bts.vimpelcom.ru/w/images/a/a6/01_select_ctrace.png)

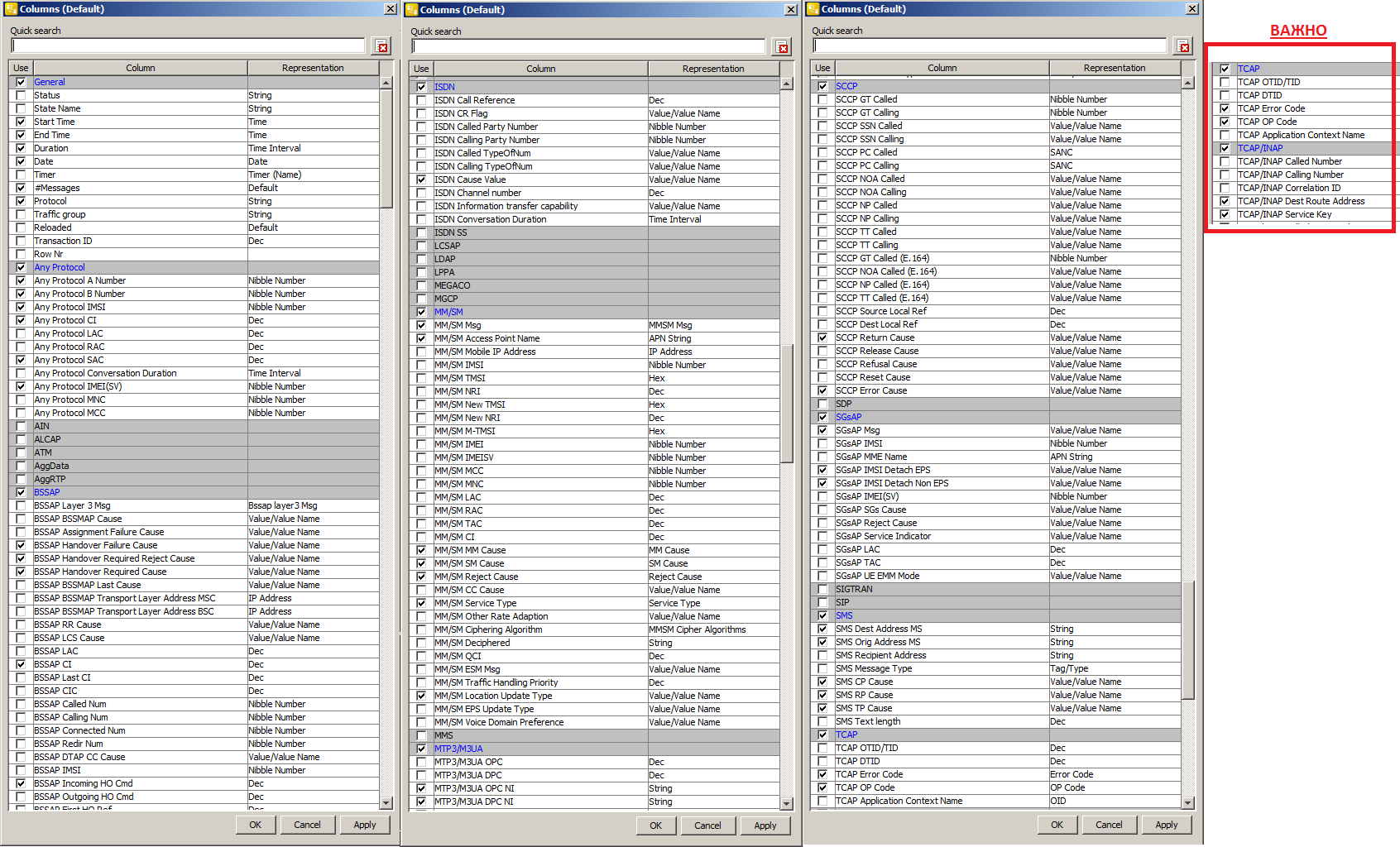
##### **Настройка рабочего пространства OSIX**

После открытия основного окна программы в левом нижнем углу выбираем вкладку Traffic Groups из раздела Server Filter, на колонке Use нажимаем правой клавишей мыши и выбираем Select All, далее нажимаем Apply.

[](http://b2bts.vimpelcom.ru/w/images/8/83/02_filter_1.png)

После этого в верхней части на панели меню выбираем **Options**, далее **Columns**... и расставляем галочки как указано ниже:

Рисунок нужно сохранить – будет полный размер.



Использование данных настроек покроет до 90% потребностей при решении клиентских проблем.

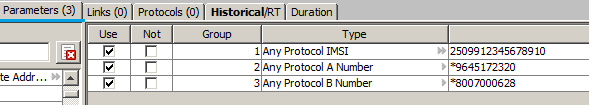
##### **Поиск трейсов**

Для того, чтобы найти трейсы по заранее известным параметрам, нам понадобится настроить временной интервал и параметры поиска.

|  |
| --- |
| Обращаю внимание, что возможность поиска по параметрам будет доступна только после добавления колонок из пункта выше.  После ввода параметров (отдельно на каждой вкладке) нажимаем «Apply» |

###### **Параметры**

Параметры указываются на вкладке **Parameters**:



Кратко по параметрам и когда какой из них выбирать:

**IMSI** – это, безусловно, сердце всего поиска, так как по данному параметру можно найти все необходимые операции, которые происходят на мобильной сети, а именно операции, которые используются в протоколах **MAP**, **RANAP**, **BSSAP**, **BSSGP**, **GTP** (обмен между MSC и VLR/HLR, обновления профиля на HLR, handover, регистрация в сети GSM и GPRS). Особенно важно указывать **IMSI** при поиске трейсов на радиосети, иначе ключевой информации о возможных сбоях на радио или информации о **реально** набранном номере просто не получите.

**Any protocol A/B number** – используя данный параметр, мы сможем найти обмен на таких протоколах как **ISUP**, **ISDN**, **SIP, MAP.** Важно, отметить, что именно на этих протоколах передается информация о вызове и о номерах A и B, в то время как на других протоколах мы можем увидеть лишь один из номеров, например, указав IMSI и MSISDN абонента B и номер абонента А - мы увидим входящий вызов по протоколу **BSSAP**, в котором будет видно лишь следующее:



Однако, при сохранении этих параметров, на протоколе **ISUP** мы увидим лишь номера абонентов A и B, но не увидим **IMSI**, так как он не используется на данном протоколе:



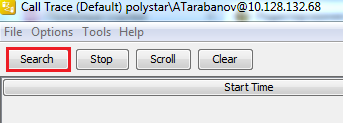
Остальные параметры **не** являются ключевыми для нашей работы, поэтому использовать поиск по ним рекомендуется только в случаях, когда нужна точечная диагностика.

Отмечу, что при указании **номера** **А** или **B** необходимо впереди номера ставить символ **\***, чтобы включить в наш поиск всевозможные префиксы, 7-ки или 8-ки впереди номера.

Параметр **IMSI** не является переменным, поэтому его указываем безо всяких символов.

Если необходимо искать значение, которое равно искомому, то \* ставить не нужно. Такой поиск полезен при поиске наборов на короткие номера в **Облачной** **АТС** или **FMTN**.

Для поиска по заданным параметрам в верхнем левом углу окна нажимаем кнопку «**Search»**:



**Где взять IMSI?**

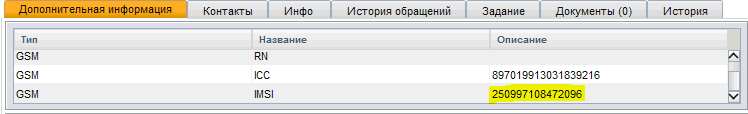
Данный параметр можно взять из базы **aCRM** или **CSM**

**aCRM**

1. В поле «Поиск CTN» пишем нужный номер 
2. Выбираем номер, который в статусе «Active»

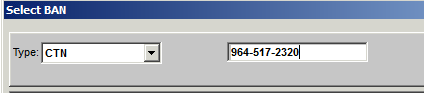


1. В представленной табличке скроллим вниз до нужного значения IMSI



**CSM**

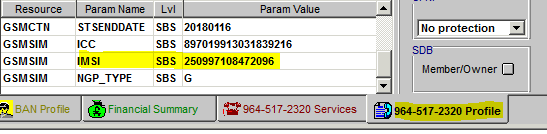
1. В запущенном CSM нажимаем F6 и в появившемся поле указываем номер:



1. Выбираем активный договор



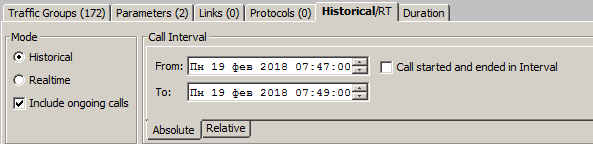
1. Переходим на вкладку «Profile» и смотрим значение:



###### **Искомый период**

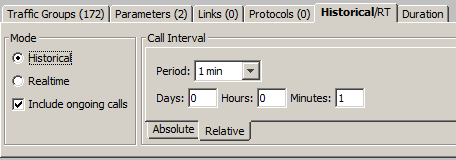
OSIX позволяет искать данные в режимах:

**Historical/Absolute** – в данном случае указывается искомый временной промежуток. Это полезно для поиска исторических событий, например, когда клиент сдает проблемные звонки, которые совершались 1-2 дня назад.



|  |
| --- |
| **Обращаю внимание на то, что актуальные данные в OSIX хранятся около 7 дней.**  **Обязательно учитывайте это при диагностике.** |

**Historical/Relative** – в данном случае указывается период равный с/до текущего времени. Например, вам известно, что клиент совершал набор не более 15 минут назад, следовательно, можно выставить такое значение и успешно найти трейсы. Период можно выбрать из предложенных, либо установить необходимый самостоятельно.

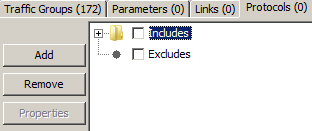


###### **Протоколы**

Полезной функцией программы является возможность выбора протоколов сигнальной сети. Это может быть полезно для того, чтобы искомые данные не сливались в общую кашу, так как на сигнальной сети может происходить многое, не связанное с конкретным поисковым запросом. Следовательно, исключив некоторые протоколы, мы не запутаемся при анализе.

Например, частым отвлекающим фактором, являются сообщения, связанные с протоколами пакетной передачи данных, которые могут появится, как и перед вызовом, так и после, так и во время него. Поэтому, если мы не анализируем проблему по пакетной передаче данных, то эти протоколы рекомендуется убрать.

Работает это так – на вкладке **Protocols** есть две категории: **Include** и **Exclude** (включать протокол и не включать соответственно).



В данных категориях действует принцип:

* **Include** *–* включать только то, что указано; остальное не выводить
* **Exclude** – выводить всё, кроме указанных.

Поэтому, если мы хотим исключить протоколы передачи данных, то следует указать так, добавив протоколы через кнопку **Add** и поставить галочку на **Excludes**:

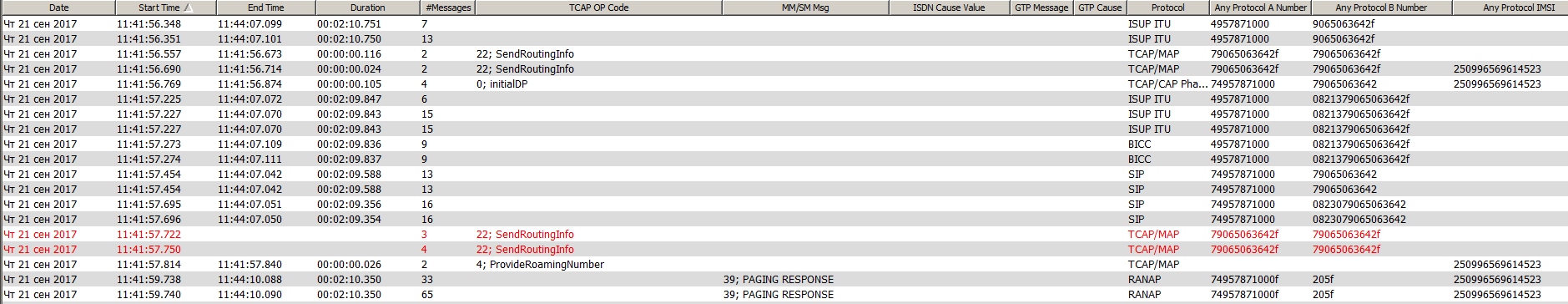


Аналогичный принцип может применяться и для остальных протоколов.

Остальные вкладки, которые есть в OSIX, нас не интересуют.

###### **Вывод трейсов**

На рисунке ниже отображен стандартный вывод трейса по искомым данным (в данном случае был **Any Protocol A, Any Protocol B, IMSI номера B**):



Обращаю внимание на то, что это вывод всех протоколов, которые были задействованы во время искомого вызова, а не вывод в каждой строке отдельного звонка. Открыв сообщение конкретного протокола, мы сможем увидеть, что происходило именно по нему, но всегда необходимо помнить, что это лишь часть вызова и некоторые важные события могут содержаться в других сообщениях.

В данном случае мы видим, что звонок зародился со стороны ТФоП (**ISUP**) и ушел в мобильную сеть на вызываемый номер (**PAGING RESPONSE**). Также видны протоколы **BICC** и **SIP**, которые участвуют в сигнальном обмене при использовании услуги **«Облачная АТС»**.

###### **Чтение трейсов**

Чтение трейсов и поиск неисправности по ним не должен вызывать проблем, если успешно освоены предыдущие [теоретические материалы](#_Система_сигнализации_ОКС). Но, естественно, необходимо отметить некоторые моменты, касаемые особенностей чтения.

Как было отмечено в разделе «Вывод трейсов», перед нами лишь набор протоколов, в которых содержаться параметры, которые мы указали, следовательно, чтобы получить целостный вызов, необходимо понимать откуда он начинается и где заканчивается.

В общем случае, следуя модели входящего вызова, он начинается на радиоинтерфейсе BSSAP или RANAP сообщением **CM Service Request** (запрос радиоресурсов), далее пойдут операции по поиску абонента в сети (**Send Routing Info**, **Provide Roaming Number**), далее возможны соединения по протоколу ISUP (**IAM**) (если вызов происходит между коммутаторами региона или страны), также возможна активация CAMEL подписки (**протокол TCAP/CAP**) – сообщения **initialDP** и взаимодействия по протоколам **SIP** и **BICC**, после этого вызов должен дойти до вызываемого абонента, то есть пойдет запрос на радиоинтерфейс **BSSAP**/**RANAP** (**Paging**) и до мобильной станции в случае её ответа (**Paging Response** ).

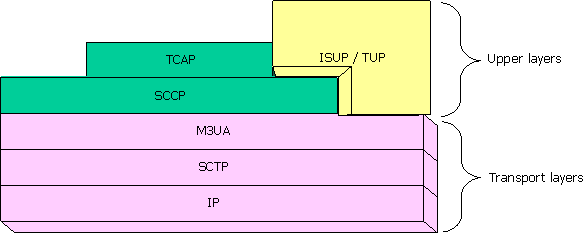
Зная это, мы можем «собрать» данный вызов в один, используя инструмент «**Correlation**». Для это необходимо выделить всё, что относится к вызову (по вашему мнению) и, нажав правой кнопкой мыши, выбрать пункт **«Correlate» > «Manual correlation»** и нам представится весь набор сообщений из всех выбранных протоколов, затем мы лишь выгрузим его в Call Flow (**View > Call Flow**) и перед нами предстанет весь обмен от и до. Очень полезная функция для анализа проблемы. Но высшим пилотажем будет являться умение находить «проблемные» протоколы в зависимости от типа проблемы, без привязки ко всему звонку, но это приходит только с практикой.

Теперь про сами **сообщения**. Открыв сообщение ОКС7 впервые, вы наверняка удивитесь обилию информации в нем, например,

* **Ethernet**
  + Destination address = 74:d0:dc:94:2f:86
  + Source address = 00:30:88:1d:94:a0
  + Frame type = 8100'H (802.1Q Virtual LAN)
  + IEEE 802.1Q, (VLAN Tagging)
    - 000----- Priority = 0
    - ---0---- CFI = 0
    - Id = 645
    - Frame type = 800'H (IPv4)
* **IP**
  + 0100---- Protocol version = 4 (IP version 4)
  + ----0101 Header length = 5 (20 bytes)
  + Differentiated Services Field
    - 000000-- Differentiated Services Codepoint = 0
    - ------0- ECN-Capable Transport (ECT) = 0
    - -------0 ECN-CE = 0
  + Packet length = 124
  + Identification = 25193
  + Flags
    - 0------- Reserved = 0 (Reserved)
    - -0------ DF = 0 (May Fragment)
    - --0----- MF = 0 (Last Fragment)
  + Fragment offset = 0
  + 00111111 Time to live = 63
  + 10000100 Protocol = 132 (Stream Control Transmission Protocol)
  + Header checksum = 8a09'H
  + Source IP address = 10.13.61.16
  + Destination IP address = 10.13.61.98
* **SCTP**
  + Common Header
    - Source Port Number = 9900 (Port Number)
    - Destination Port Number = 39520 (Port Number)
    - Verification Tag = 45f99027'H
    - Checksum = 9294622f'H
  + Chunk Field
    - 00000000 Chunk Type = 0 (Payload Data)
    - 00000--- Reserved = 0
    - -----1-- U-bit = 1
    - ------1- B-bit = 1
    - -------1 E-bit = 1
    - Length Field = 92
    - TSN = 37567953
    - Stream Identifier S = 1
    - Stream Sequence Number n = 0
    - Payload Protocol Identifier = 1 (IUA)
* **IUA**
  + 00000001 Version = 1 (Release 1.0)
  + 00000000 Spare = 0 (Spare field (8 bits))
  + 00000101 Message Class = 5 (Q.921/Q.931 Boundary Primitives Transport (QPTM) Messages)
  + 00000010 Message Type = 2 (Data Indication Message)
  + Length Field = 76
  + Interface Identifier (integer)
    - Tag = 1 (Interface Identifier)
    - Length Field = 8
    - Integer = 2721052
  + Data Link Connection Identifier
    - Tag = 5 (Data Link Connection Identifier)
    - Length Field = 8
    - -------0 0/1 ext = 0 (ExtBit)
    - ------0- SPR = 0
    - 000000-- SAPI = 0
    - -------1 0/1 ext = 1 (StopBit)
    - 0000000- TEI = 0
    - SpareBits16 = 0
  + Protocol Data
    - Tag = 14 (Protocol Data)
    - Length Field = 51
* **ISDN**
  + 00001000 Protocol discriminator = 8 (Q.931/I.451 user-network call control messages)
  + 0000---- Spare = 0 (Spare field (4 bits))
  + ----0010 Length Field = 2
  + 0------- Call reference flag = 0 (The origination side)
  + Call reference value = 2327
  + MSG: SETUP
    - 00000101 Tag = 5 (x05)
    - IE: Sending complete
      * 10100001 Tag = 161 (xA1)
    - IE: Bearer Capability
      * 00000100 Tag = 4 (x04)
      * 00000011 Length Field = 3
      * ---10000 Information transfer capability = 16 (3.1 kHz audio)
      * -00----- Coding standard = 0 (ITU-T standardized coding as described below)
      * 1------- 0/1 ext = 1 (StopBit)
      * ---10000 Information transfer rate = 16 (64 kbit/s)
      * -00----- Transfer mode = 0 (Circuit mode)
      * 1------- 0/1 ext = 1 (StopBit)
      * ---00011 User information layer 1 protoco = 3 (Recommendation G.711 A-law)
      * -01----- Layer 1 identity = 1
      * 1------- 0/1 ext = 1 (StopBit)
    - IE: Channel identification
      * 00011000 Tag = 24 (x18)
      * 00000011 Length Field = 3
      * ------01 Information channel selection = 1 (B1 channel (Basic), As indicated in following octets (Other interfaces))
      * -----0-- D-channel indicator = 0 (The channel identified is not the D-channel)
      * ----1--- Preferred/Exclusive = 1 (Exclusive; only the indicated channel is acceptable)
      * ---0---- Spare = 0 (Spare field (1 bit))
      * --1----- Interface type = 1 (Other interface e.g. primary rate)
      * -0------ Interface identifier present = 0 (Interface implicitly identified)
      * 1------- 0/1 ext = 1 (StopBit)
      * ----0011 Channel type/map element type = 3 (B-channel units)
      * ---0---- Number/map = 0 (Channel is indicated by the number in the following octet)
      * -00----- Coding standard = 0 (ITU-T standardized coding as described below)
      * 1------- 0/1 ext = 1 (StopBit)
      * -0010101 Channel number/Slot map = 21
      * 1------- 0/1 ext = 1 (stop bit)
    - IE: Progress indicator
      * 00011110 Tag = 30 (x1E)
      * 00000010 Length Field = 2
      * ----0001 Location = 1 (Private network serving the local user)
      * ---0---- Spare = 0 (Spare field (1 bit))
      * -00----- Coding standard = 0 (ITU-T standardized coding as described below)
      * 1------- 0/1 ext = 1 (StopBit)
      * -0000011 Progress description = 3 (Origination address is non-ISDN)
      * 1------- 0/1 ext = 1 (StopBit)
    - IE: Calling party number
      * 01101100 Tag = 108 (x6C)
      * 00001100 Length Field = 12
      * ----0001 Numbering plan (applies for type of number = 000, 001, 010 and 100) = 1 (ISDN/telephony numbering plan (Recommendation E.164 [19]))
      * -010---- Type of number = 2 (National number)
      * 0------- 0/1 ext = 0 (ExtBit)
      * ------00 Screening indicator = 0 (User-provided, not screened)
      * ---000-- Spare = 0 (Spare field (3 bits))
      * -00----- Presentation indicator = 0 (Presentation allowed)
      * 1------- 0/1 ext = 1 (StopBit)
      * Number Digits (IA5) = 9037030611
    - IE: Called party number
      * 01110000 Tag = 112 (x70)
      * 00001011 Length Field = 11
      * ----0001 Numbering plan (applies for type of number = 000, 001, 010 and 100) = 1 (ISDN/telephony numbering plan (Recommendation E.164 [19]))
      * -010---- Type of number = 2 (National number)
      * 1------- 0/1 ext = 1 (StopBit)
      * Number Digits (IA5) = 9683622348

Перед нами типичный вывод сообщения SETUP протокола ISDN, который в точности похож на ISUP.

Чтобы понять, что тут к чему, обратимся к иллюстрации:



На ней изображен стек протокола **SIGTRAN** + **ISUP**. Анализируя представленный выше трейс мы уже можем понять, что протоколы **IP**, **SCTP** и **M3UA** будут относится к транспорту, а **полезная** для нас информация будет лишь в протоколе **ISDN**, так как он является протоколом пользовательской части (содержательная часть). Отсюда вывод, что не стоит смотреть на трейс целиком, а необходимо разделять его на подуровни и сверяться с эталонным стеком модели ОКС 7 и уже понимать, где какую информацию смотреть. Однако, никто не спорит, что и на транспортном уровне тоже есть полезная информация, например, на подуровне **M3UA (или MTP)** мы можем посмотреть **OPC/DPC**, но, зачастую, они требуются лишь в некоторых случаях.

Итак, если мы «свернем» в OSIX все сообщения, то получится тот самый стек ОКС7:



Выходит, что нам необходимо лишь «прокрутить» вниз сообщение и смотреть на сообщение **IAM**. Аналогичную схему можно применить к любому сообщению.

В данной главе не будет разъяснений по поводу того, какие параметры передаются в каждом протоколе, так как так или иначе, в последующих разделах про это будет упоминаться.

Дополнительно, можно почитать материалы на <http://b2bts.vimpelcom.ru> (SS7) или в сети Интернет.