СЕТИ СВЯЗИ МОБИЛЬНЫХ АБОНЕНТОВ

3.1. Историческая справка

Имеется много радиосистем связи. Наиболее известные из них:

1. Радиотелефоны стандарта **DECT** (**D**igital **E**nhanced **C**ordless **T**elecommunications). Обеспечивают беспроводную связь между телефонным аппаратом и базовой станцией на расстоянии 20-100 метров.

2. Беспроводный абонентский доступ **Wi-Fi** (**Wi**reless **Fi**delity). Обеспечивает беспроводную связь между компьютером и локальной сетью (Local Area Network, LAN) на расстоянии до 200 метров на скорости до 20 Мбит/с.

3. Спутниковые сети связи мобильных абонентов (**M**obile **S**atellite **S**ystems, **MSS**). Обеспечивают беспроводную связь между абонентами в пределах планеты за счет космических аппаратов.

4. Наземная сеть связи мобильных абонентов (**P**ublic **L**and **M**obile **N**etworks, **PLMN**). Обеспечивают беспроводную связь между абонентами в пределах планеты за счет наземных средств.

Первые разработки (генерация) аналоговых наземных сетей связи мобильных абонентов (PLMN) появились в конце 1970/начале 1980 годов, когда ограничение диапазона радиочастот было преодолено использованием одного и того же диапазона радиочастот в различных разнесенных сотах. В 1979 году коммерческая наземная сеть связи мобильных абонентов была введена в США (AMPS, Advanced Mobile Phone Service) и в Японии (Nippon Telegraph & Telephone Co., NTT-MTS). Позже сотовые сети связи появились в скандинавских странах, Англии, Германии и в других странах. Однако вскоре стали очевидны следующие недостатки аналоговых систем:

– мощность аналоговых сигналов не могла покрыть все возрастающее число мобильных пользователей;

– с увеличением расстояния между мобильной станцией и базовой станцией качество передачи катастрофически ухудшалось;

– слабая защита радиоканала позволяла легко перехватывать информацию посторонним лицам;

– каждая из стран использовала свои стандарты сетей, что затрудняло использование мобильной станции за пределами домашней сети (роуминг).

– слабая защита радиоканала позволяла легко перехватывать информацию посторонним лицам.

Архитектура последующих версий PLMN логически разделяется на две части: ядро сети (Core Network, CN) и сеть доступа (Access Network, AN). В свою очередь в зависимости от технологии коммутации ядро сети может быть с коммутацией каналов (Circuit Switched domain, CS domain) либо с коммутацией пакетов (Packet Switched domain, PS domain). Сети доступа в зависимости от способа построения радиоканалов разделяются на GERAN (**G**SM **E**DGE **R**adio **A**ccess **N**etwork), UTRAN (**U**niversal **T**errestrial **R**adio **A**ccess **N**etwork) и E-UTRAN (Evolved UTRAN).

В 1988 году был образован Европейский институт телекоммуникационных стандартов (**E**uropean **T**elecommunication **S**tandards **I**nstitute, **ETSI**), одной из главных целей которого стало разработка стандартов сети связи мобильных абонентов. В 1990 году были выпущены первые стандарты (Рекомендации) GSM, которые уже к 1998 году де-факто стали мировым стандартом. Эти Рекомендации объединены в 12 серий, отражающих различные аспекты описания структуры и интерфейсов.

Вначале 1990-х произошла вторая генерация (2G) сотовых наземных сетей связи мобильных абонентов (**G**lobal **S**ystem for **M**obile Communications, **GSM**), которые использовали цифровые методы передачи и коммутации. Это позволило значительно увеличить абонентскую емкость сети и повысить качество связи. Вместе с тем, разработка мобильных портативных устройств и аккумуляторов сделали мобильную связь необычайно популярной.

Стандарт GSM900 предусматривает использование радио полосы 35 МГц в диапазоне 880-915 МГц в направлении пользователь-сеть (Uplink) и 35 МГц в диапазоне 925-960 МГц в направлении сеть-пользователь (Downlink). Число полос в каждом направлении – 174, радиус соты – до 35 км.

Стандарт GSM1800 предусматривает использование радио полосы 75 МГц в диапазоне 1710-1785 МГц в направлении пользователь-сеть (Uplink) и 75 МГц в диапазоне 1805-1880 МГц в направлении сеть-пользователь (Downlink). Число полос в каждом направлении – 374, радиус соты – до 8 км.

Стандарт GSM предусматривает передачу речи и данных, но их темпы роста различны. Если в 1996 году объем трафика данных составлял всего 3%, то к 2007 году он достиг 50% и сравнялся с объемом трафика речи. Стандарт GSM, использующий сеть радиодоступа GERAN плохо приспособлен для передачи данных по нескольким причинам.

1. Взрывной характер трафика данных в некоторые короткие промежутки времени требует высокую скорость передачи, а в другие промежутки времени трафик отсутствует совсем. Это плохо сочетается с выделенной постоянной полосой передачи со скоростью 9,6 Кбит/с.

2. Соединения в IP-сеть пролегают через PSTN/ISDN, где принят повременный учет стоимости и низкая скорость установления соединения.

3. Длина коротких сообщений (SMS) ограничена 160 символами.

4. Одинаковая скорость передачи в направлениях пользователь-сеть и сеть-пользователь.

В результате длительной эволюции GSM, состоящей из трех фаз (GSM1, GSM2, GSM2+) произошли следующие изменения.

1. Добавлены все дополнительные виды обслуживания (Supplementary services), применяемые в цифровых сетях интегрального обслуживания.

2. Проведена интеграция услуг с интеллектуальной сетью связи (**C**ustomized **A**pplications for **M**obile network **E**nhanced **L**ogic, **CAMEL**).

3. Добавлена подсистема пакетной радиосвязи общего пользования (**G**eneral **P**acket **R**adio **S**ervice, **GPRS**), позволяющая резко увеличить скорость передачи данных.

Концепция GPRS изложена в Рекомендациях GSM 02.60 (Общие положения), 03.60 (Описание системы и архитектуры), 02.60 (Описание радио подсистемы).

В результате эволюции теоретическая скорость передачи данных возросла до 171,2 Кбит/с. Эти изменения в совокупности позволили вплотную приблизиться к стандарту 3-го поколения – Универсальной Мобильной Телекоммуникационной Системе (**U**niversal **M**obile **T**elecommunications **S**ystem, **UMT**S).

В 1998 году был создан консорциум 3GPP (**3**rd **G**eneration **P**artnership **P**roject, **3GPP**), в который вошли European Telecommunications Standards Institute, Association of Radio Industries and Businesses/Telecommunication Technology Committee (ARIB/TTC) (Япония), China Communications Standards Association (Китай), Alliance for Telecommunications Industry Solutions (Северная Америка) и Telecommunications Technology Association (Южная Корея). Консорциум объединил усилия ведущих телекоммуникационных компаний для выработки и принятия стандартов для сетей третьего поколения (3G), а также для стандартизации архитектуры сетей и сервисов.

Свои Рекомендации консорциум оформляет в виде технических спецификаций (Technical Specification) вида 3GPP TS 23.002: "Network Architecture".

Стандарт 3-го поколения 3G использует на радиоканале сеть UTRAN множественного доступа с кодовым разделением (**C**ode **D**ivision **M**ultiple **A**ccess, **CDMA**), обеспечивающий типовую скорость передачи данных 384 Кбит/с.

Дальнейшее увеличение скорости в направлении сеть-абонент достигается применением технологии высокоскоростной пакетной передаче данных от базовой станции к мобильному телефону (**H**igh-**S**peed **P**acket **A**ccess, **HSPA**), предусматривающей объединение нескольких кодов (до 15) и использование специального типа модуляции в радиоканале. В зависимости от категории мобильного терминала теоретически скорость передачи может достигать 14 Мбит/с на прием и 5.76 Мбит/с на передачу. Мощность излучения мобильного терминала 3-го поколения на порядок меньше мощности излучения терминала 2-го поколения.

Начиная с 8-ой версии (Release 8) развитие PLMN четвёртого поколения (4G) идёт путём эволюционного совершенствования существующей сети и получило название **L**ong **T**erm **E**volution (**LTE**). Стандартами сети четвёртого поколения занимается консорциум 3GPP. Эти усовершенствования направлены на повышение скорости, снижение издержек, расширения и улучшения уже оказываемых услуг.

Скорость передачи данных по стандарту 3GPP LTE в теории достигает 326,4 Мбит/с на приём (*download*) и 172,8 Мбит/с на передачу (*upload*); в стандарте определены скорости 173 Мбит/с на приём и 58 Мбит/с на передачу.

ВОПРОСЫ К РАЗДЕЛУ 3.1

1. Перечислите поколения наземных сетей связи мобильных абонентов (PLMN) и их основные признаки.

Ответ. 1G – использование на радиоканале частотного уплотнения аналоговых сигналов, 2G (GSM) – использование на радиоканале временного уплотнения цифровых сигналов, 3G (UMTS) – использование на радиоканале множественного доступа с кодовым разделением, 4G (LTE) – эволюционный переход к сетям пакетной коммутации.

2. Назовите организацию по разработке стандартов сети связи мобильных абонентов второго поколения.

Ответ. Европейский институт телекоммуникационных стандартов (ETSI).

3. Назовите организацию по разработке стандартов сети связи мобильных абонентов третьего поколения.

Ответ. Консорциум 3GPP.

4. Какова максимальная скорость передачи данных в подсистеме GSM?

Ответ. 9,6 Кбит/с.

5. Какова максимальная скорость передачи данных в подсистеме GPRS?

Ответ. 171,2 Кбит/с.

6. Какова теоретическая максимальная скорость передачи данных в стандарте UMTS?

Ответ. 80 Мбит/с.

7. Какова максимальная скорость передачи данных в стандарте LTE?

Ответ. 326,4 Мбит/с.

3.2. Сотовая наземная сеть связи мобильных абонентов второго поколения. Стандарт GSM

Наземные сети связи мобильных абонентов (**P**ublic **L**and **M**obile **N**etworks, **PLMN**) создаются национальными операторами для обеспечения связью мобильных абонентов, они дополняют и взаимодействуют с телефонными сетями общего пользования (**P**ublic **S**witched **T**elephone **N**etwork, **PSTN**), цифровыми сетями интегрального обслуживания (**I**ntegrated **S**ervices **D**igital **N**etwork, **ISDN**), сетями передачи данных (**P**acket **D**ata **N**etwork, **PDN**). Под последними обычно понимается Internet.

3.2.1. Сетевые элементы

Наземная сеть связи мобильных абонентов второго поколения (**GSM-PLMN**) состоит (рис. 3.1) из радио подсистемы (**R**adio **S**ubsystem – **RSS**), сетевой подсистемы (**N**etwork **S**witching **S**ubsystem, **NSS)** и подсистемы технического обслуживания и эксплуатации (**O**peration **S**ubsystem, **OSS**).

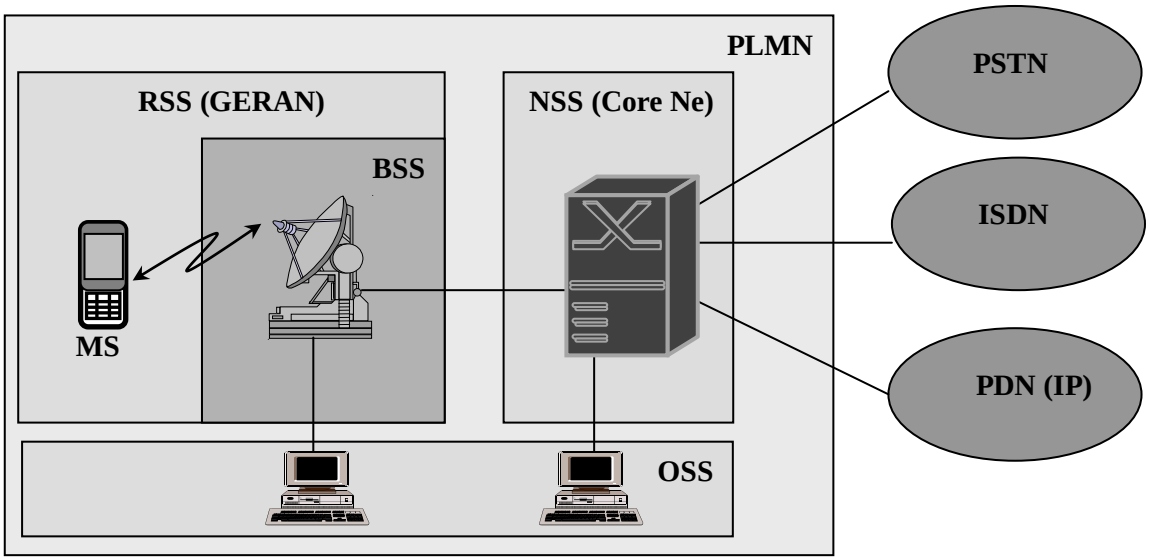

Рис.3.1. Подсистемы наземной сети связи мобильных абонентов

Радио подсистема включает в себя мобильные станции абонентов (**M**obile **S**tation, **MS**) и подсистему базовых станций (**B**ase **S**tation **S**ystem, **BSS**).

Компонентами мобильной станции (**M**obile **S**tation, **MS**) являются мобильное оборудование (**M**obile **E**quipment, **ME**) и модуль идентификации абонента (**S**ubscriber **I**dentification **M**odule, **SIM**). Посредством сменяемого мобильного оборудования пользователь осуществляет сеансы связи, а идентификация пользователя осуществляется посредством данных, хранящихся в модуле идентификации абонента (SIM-карте). Эти данные записываются в SIM-карту оператором сети при заключении контракта на обслуживание абонента и содержат в себе сетевой номер (MS ISDN), международный идентификатор мобильного абонента (International Mobil Subscriber Identity – IMSI), временный идентификатор подвижного абонента (Temporary Mobile Subscriber Identity, TMSI), алгоритмы идентификации и шифрования информации и др.

В подсистему базовых станций (BSS) входят следующие основные сетевые элементы (рис. 3.2):

– базовые приемопередающие станции (**B**ase **T**ransceiver **S**tation, **BTS**), обеспечивающие соединения между мобильной станцией и сетью по радио интерфейсу Um;

– контроллеры базовых станций (**B**ase **S**tation **C**ontroller, **BSC**), каждый из которых осуществляет управление радо ресурсами одной или нескольких базовых станций по A-bis интерфейсу;

– транскодеры (**T**ranscoding and **R**ate **A**daptation **U**nit, **TRAU**) обеспечивают перекодирование полосы передачи пользователя 64 Кбит/с, поступающей от сетевой подсистемы, в пониженную полосу передачи 13 Кбит/с, используемую на радо интерфейсе. Реально 13 Кбит/с помещается в канал со скоростью 16 Кбит/с.

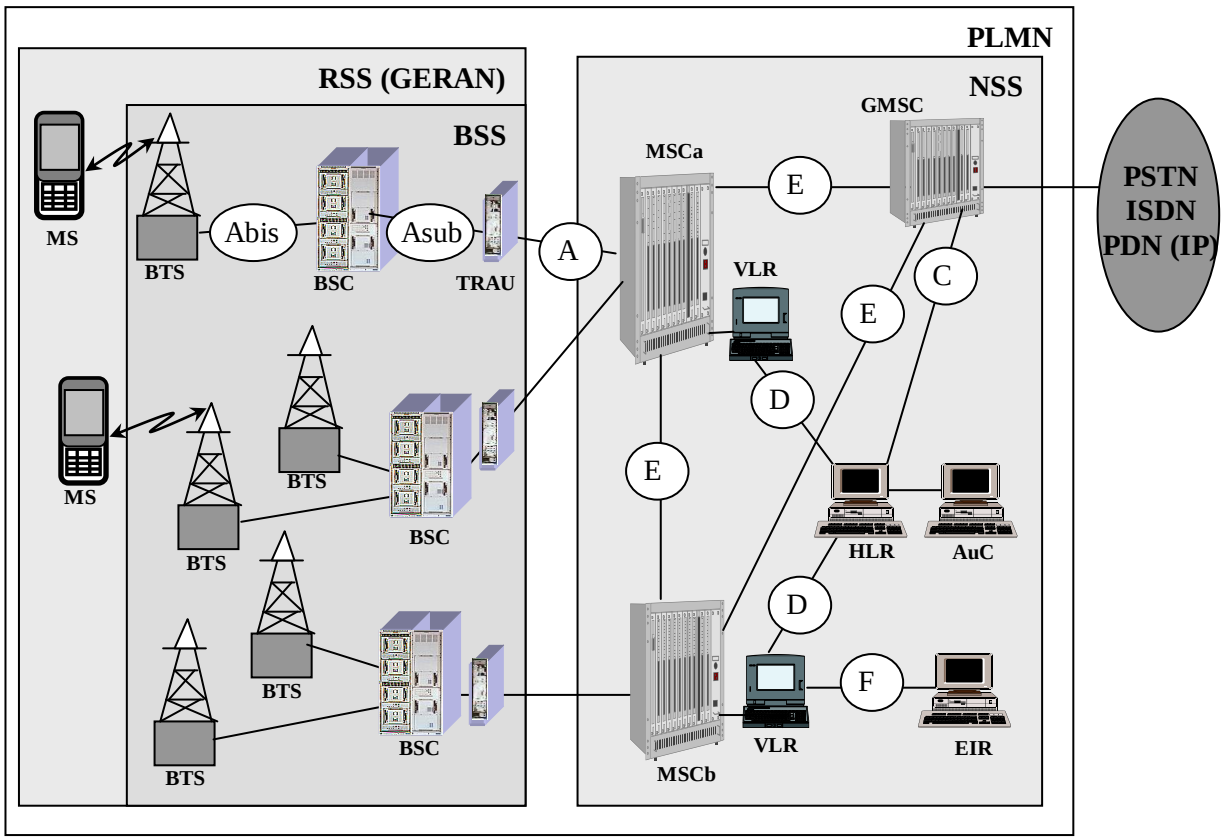

Рис.3.2. Сетевые элементы подсистем

Сетевая подсистема (NSS) состоит из следующих основных сетевых элементов (рис. 3.2):

– центров коммутации мобильных абонентов (**M**obile services **S**witching **C**enter, **MSC**), обеспечивающих соединения между мобильными станциями в пределах радио покрытия своей зоны по А-интерфейсу. Является основным элементом сети и выполняет функции аналогичные системам коммутации в сети стационарных абонентов. Те MSC, которые имеют соединение с другими сетями, называются шлюзовыми центрами коммутации мобильных абонентов (**G**ateway **M**obile services **S**witching **C**enter, **GMSC**). Они, как правило, не подключены к сети базовых станций BSS;

– гостевые регистры (**V**isitor **L**ocation **R**egister, **VLR**), каждый из которых однозначно ассоциирован с одним MSC внутренним В-интерфейсом и хранит базу данных мобильных абонентов, которые временно прибывают в зоне обслуживания

MSC. Практически часто реализуются в виде единого устройства с MSC и обозначаются как MSC/VLR;

– домашний регистр (**H**ome **L**ocation **R**egister, **HLR**), является постоянным хранилищем базы данных мобильных абонентов PLMN своего оператора и высылает ее по D-интерфейсу по запросу VLR или по C-интерфейсу по запросу GMSC;

– центр аутентификации (**A**uthentication **C**enter – **AuC**) однозначно ассоциирован с HLR и содержит данные о секретных ключах и алгоритмах шифрования. При каждом сеансе связи мобильный абонент должен пройти процедуру идентификации, Параметры идентификации генерируются AC и высылаются в VLR по его запросу.

– регистр идентификации оборудования (**E**quipment **I**dentity **R**egister, **EIR**) хранит базу данных о заводских номерах мобильной станции (мобильного телефона), что позволяет выявлять похищенное оборудование. Практически используется редко.

Частотные диапазоны для соты стандарта GSM900 предусматривают использование радио полосы диапазоне 880-915 МГц в направлении пользователь-сеть (Uplink) и в диапазоне 925-960 МГц в направлении сеть-пользователь (Downlink), число полос в каждом направлении – 174. Стандарт GSM1800 предусматривает использование радио полосы 1710-1785 МГц в направлении пользователь-сеть (Uplink) и в диапазоне 1805-1880 МГц в направлении сеть-пользователь (Downlink), число полос в каждом направлении – 374. В обоих случаях используется принцип частотно-временного уплотнения, при котором в каждой из 174/374 частотных полос шириной 200 КГц размещается 8 временных интервалов (рис. 3.3). Число каналов пользователей равно 174x8=1392 или 374x8=2992, соответственно, если канал занимается полностью (Full Rate Speech, FR) или в два раза больше, если занимается половина канала (Half Rate Speech, HR). Максимальная скорость передачи данных – 9,6 Кбит/с.

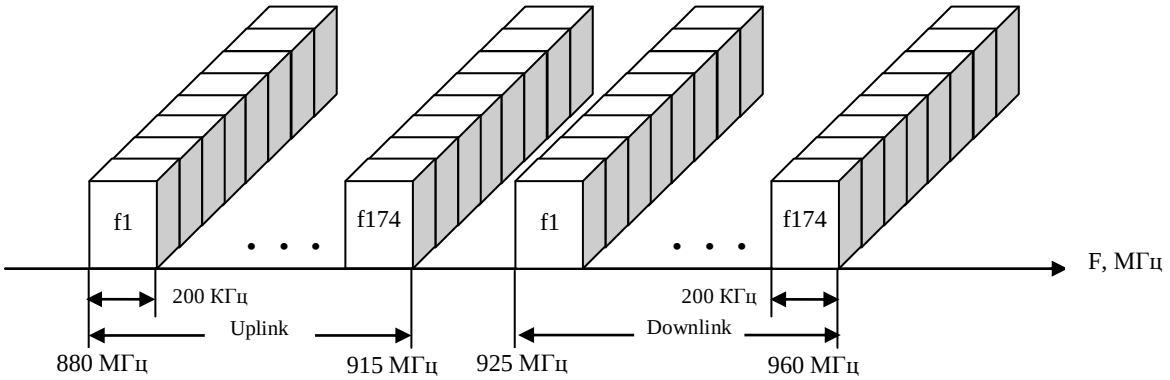

Рис. 3.3. Размещение радиоканалов в стандарте GSM900

3.2.2. Зона обслуживания центра коммутации

Зона обслуживания центра коммутации представляет собой множество ячеек (Cells), в каждой из которых устанавливается BTS (рис. 3.4а). Ячейка (сота) является минимальной зоной обслуживания и обычно использует антенну с круговым покрытием радиусом до 35 километров. Контроллер базовых станций управляет BSC несколькими ячейками (рис. 3.4б).

Зоны обслуживания соседних ячеек частично перекрываются, и для избегания интерференции каждая из ячеек использует только часть возможных общих радиоканалов (полос), остальные радиоканалы (полосы) размещаются в соседних ячейках на других частотах. Одни и те же каналы могут быть использованы в разных ячейках, которые удалены друг от друга на 2 промежуточные ячейки. При низкой плотности абонентов размер ячейки (мощность приемопередатчика BTS) увеличивают,

при высокой плотности – уменьшают. Еще одним способом увеличения зоны обслуживания ячейки является применение в BTS секционных антенн с углами излучения 180 или 120 градусов.

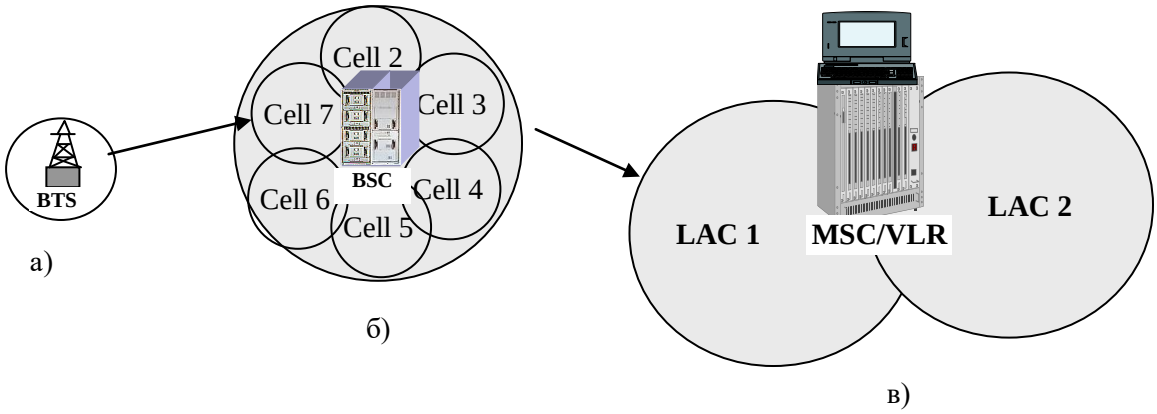

Рис.3.4. Зона обслуживания
а) ячейки, б) контроллера, в)центра коммутации

Совокупность ячеек, подсоединенных к BSC (или к нескольким BSC), образуют локальную зону (Local Area), идентифицируемой в MSC уникальным двухбайтным кодом зоны (**L**ocal **A**rea **C**ode, **LAC**).

Совокупность локальных зон, подсоединенных к MSC, образуют зону обслуживания центра коммутации. Каждая из BTS в своей ячейке излучает в эфир идентификатор (код) зоны (**L**ocation **A**rea **I**dentity, **LAI**), по которому мобильная станция распознает, в зоне обслуживания какого LAC она находится. Идентификатор зоны представляется в виде кода страны (MCC), кода сети мобильных абонентов (MNC), кода локальной зоны (LAC), т.е. LAI = MCC + MNC + LAC.

3.2.3. Идентификация и адресация в сети 2G

В сети связи стационарных абонентов последние постоянно подключены к фиксированному порту узла, в котором находится его база данных. Поэтому местоположение абонента и местонахождение его базы данных совпадают. База данных абонента содержит сведения о привязке сетевого номера к порту абонента, а также способах его обслуживания (состоянии его расчетного счета, оплаченных дополнительных услугах и т.д.). Специфика наземной сети мобильных абонентов состоит в том, что местоположение абонента и местонахождение его базы данных не совпадают.

Для установления соединения (адресации к абоненту) в ISDN и PSTN используется план нумерации согласно ***Рекомендации ITU-T E.164.*** Рекомендация ITU-T E.164 предлагает три принципа плана нумерации – географический (зоновый), глобальный и сетевой. Все три плана имеют максимальную длину номера 15 десятичных цифр без учета префикса выхода на выбранный план нумерации. В сети связи стационарных абонентов для установления соединения используется зоновый план нумерации, приспособленный к использованию географически связанных абонентов страны или стран. Формирование сетевого международного номера мобильного абонента (**M**obile **S**ubscriber International **ISDN** Number, **MSISDN**) для установления соединения происходит по схеме (рис. 3.5).

Так, для Германии код страны принимает значение CC=49, для Руанды – CC=250, для Реюньона (остров в Индийском океане, в группе Маскаренских островов) – 262, для Казахстана, России и Таджикистана – CC=7 и т.д.

Код страны (Country Code) CC= 1-3 знака (для России CC = ”7”)	Национальный код пункта назначения (National Destination Code) NDC	Номер абонента (Subscriber Number) SN

← Max (NDC+SN) = (15 – CC) знаков →

Рис.3.5. План нумерации по Рекомендации Е-164

В России национальный код пункта назначения для Москвы принимает значение NDC=495, национальный код пункта назначения для С-Петербурга принимает значение NDC=812 и т.д.

В наземной сети связи мобильных абонентов для установления соединения также используется зоновый план нумерации. Центр коммутации, в зоне обслуживания которого находится мобильный абонент, должен иметь его базу данных. База данных мобильного абонента фиксировано располагается в специальном устройстве – домашнем регистре (**H**ome **L**ocation **R**egister, **HLR**) и географически никак не связана с текущим местоположением мобильного абонента. Поэтому для запроса базы данных мобильного абонента MSC/VLR требуется еще дополнительный номер, адресуемый к HLR. Этим номером является международный идентификатор мобильного абонента (**I**nternational **M**obile **S**ubscriber **I**dentity, **IMSI**). Поскольку адресное пространство по Рекомендации Е.164 практически исчерпано, то для запроса удаленной базы данных мобильного абонента используется другой план нумерации согласно ***Рекомендации ITU-T E.212.*** Формирование адреса базы данных мобильного абонента по IMSI происходит по схеме (рис. 3.6).

Код страны (Mobile Country Code) MCC=3 знака (для России MCC = ”250”)	Код сети мобильных абонентов (Mobile Network Code) MNC=2-3 знака	Мобильный идентификатор абонента (Mobile Subscriber Identification Number) MSIN=10 знаков

Рис.3.6. План нумерации по Рекомендации Е-212

Так, для Германии код страны принимает значение MCC=262 (совпадает с кодом Реюньона по плану нумерации Е.164), для России – MCC=250 (совпадает с кодом Руанды по плану нумерации Е.164) и т.д.

В России код сети мобильных абонентов для оператора МТС принимает значение MNC=01, код сети мобильных абонентов для оператора Мегафон принимает значение MNC=02, и т.д.

Сетевые элементы при взаимодействии между собой используют различные протоколы: **M**obile **A**pplication **P**art (**MAP**), **C**amel **A**pplication **P**art (**CAP**), ISDN User Part (ISUP). Взаимодействие происходит через существующую сеть ISDN, которая использует план нумерации Е.164, поэтому для запроса данных приходится пересчитывать IMSI в адрес плана Е.164, а сам IMSI помещать в поле данных. Например, IMSI=250 01 1234567890 пересчитывается в номер 7 911 x567890, где x принимает значение 1, если устанавливается соединение к HLR или принимает значение 2, если соединение устанавливается к VLR. Правила пересчета содержатся в Рекомендации Е.214, а процедура пересчета называется трансляцией глобального заголовка (**G**lobal **T**itle **T**ranslation, **GTT**).

3.2.4. Способы учета стоимости соединений

Имеется два вида оплаты телекоммуникационных услуг мобильным абонентом: в кредит (postpaid) и с предоплатой (prepaid).

При *оплате в кредит* абонент пользуется телекоммуникационными услугами в долг. Оператор сети устанавливает предел кредита, абонент должен оплачивать услуги не дожидаясь его превышения. Если предел кредита будет достигнут, то обслуживание абонента прерывается. Баланс абонента всегда отрицательный, такой способ оплаты обычно применяется для корпоративных пользователей.

Предоплата подразумевает оплату пользователем телекоммуникационных услуг заранее, путем внесения определенной суммы на свой счет. В процессе обслуживания сеть вычитает из этой суммы плату за услугу. Если на счету отсутствуют средства для оплаты, то обслуживание абонента прерывается. Баланс абонента всегда положительный, такой способ оплаты обычно применяется для обычных пользователей.

Поскольку мобильный абонент постоянно не привязан к определенному узлу сети, то информация о счете абонента хранится в специальном сетевом элементе интеллектуальной сети – узле управления услугами (Service Control Point (SCP)/**C**AMEL **S**ervice **E**nvironment (**CSE**)). При расчете оплаты за соединение в сети мобильных абонентов справедливо правило ”каждый пользователь отвечает только за свои действия”. В отличие сети связи стационарных абонентов, где оплату за соединение производит вызывающий абонент, это правило влияет на начисление оплаты не только на вызывающего, но и на вызываемого абонента. Например, пусть оба абонента прописаны в сети С-Петербурга и имеют сетевые номера вида A=+7911xxxxxxx и B=+7911yyyyyyy. Допустим, что B-абонент уехал во Францию (находится в роуминге). Пусть A-абонент устанавливает с ним соединение набором его сетевого номера B=+7911yyyyyyy. В этом случае A-абонент оплачивает соединение только внутри домашней сети, т.е. внутри С-Петербурга (действие A-абонента – набор номера B-абонента), ибо он набрал номер домашней сети абонента B и может быть не осведомлен, где в действительности находится B-абонент. B-абонент будет оплачивать соединение от домашней сети до места его дислокации, т.е. от С-Петербурга до Франции (действие B-абонента – роуминг во Францию).

Учет стоимости соединения рассматриваемого случая схематично изображен на рис. 3.7. Подробно описаны только сообщения, относящиеся к учету стоимости.

1. При поступлении заявки на соединение от домашнего абонента с предоплатой HMSC/VLR по протоколу CAMEL Application Part сообщением CAP: Message Type=Begin, Operation Code=Initial Detection Point (CAP: MT=Begin, OP=IDP) открывает диалог с CSE, в котором описывает параметры инициатора соединения (A-абонента):

– вид запрашиваемой услуги (Service Key);
– номер вызывающего абонента (Calling Party Number);
– свой сетевой номер (MSC Address);
– номер вызываемого абонента (Called Party Number);
– текущее дата/время вызова (Time And Timezone).

2. При наличии у A-абонента достаточных средств для оплаты исходящего соединения CSE в ответном сообщении (CAP: MT=Continue, Operation Code=Request Report BCSMEvent) просит HMSC/VLR информировать его о прохождении соединения:

– отсутствии пути (RouteSelectFailure);
– занятости абонента (oCalledPartyBusy);
– ответе абонента (oAnswer);
. . .
– отбое абонента (oDisconnect).

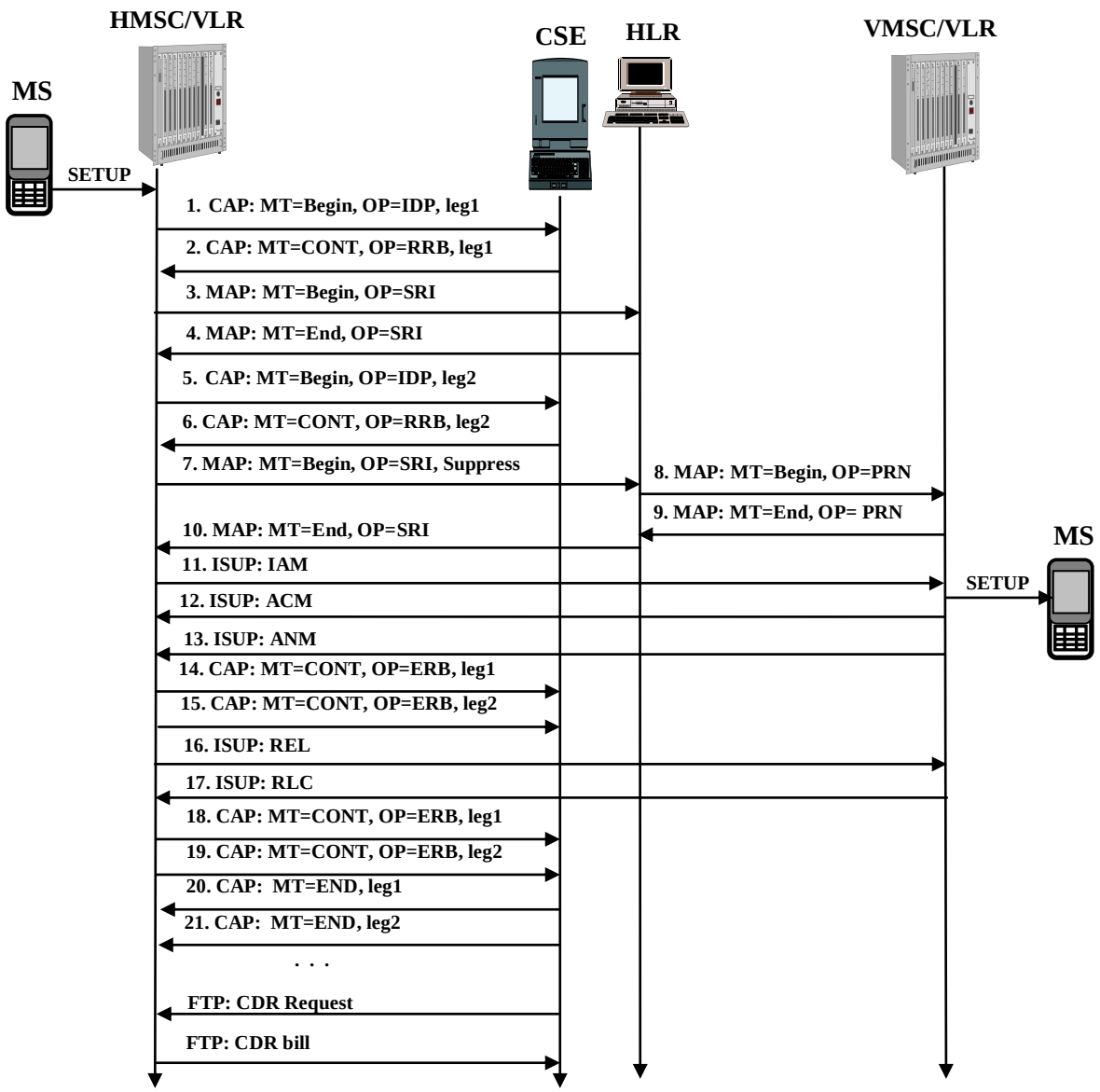

Рис. 3.7. Процедура начисления стоимости

3. Поскольку B-номер принадлежит домашней сети, то HMSC/VLR по протоколу Mobile Application Part сообщением MAP: Message Type=Begin, Operation Code=sendRoutingInfo (MAP: MT=Begin, OP=SRI) открывает диалог с HLR с запросом о текущем местоположении B-абонента, в котором содержится:

– номер вызываемого абонента (MS ISDN Address Signals);

– свой сетевой номер (GMSC Address Signals).

4. HLR в ответном сообщении высылает профайл B-абонента, в котором содержится указание на то, что B-абонент с предоплатой и закрывает диалог.

5. HMSC/VLR по протоколу CAMEL Application Part открывает новый диалог (CAP: Message Type=Begin, Operation Code=Initial Detection Point) с CSE, в котором описывает параметры исходящего соединения (на B-абонента):

– вид запрашиваемой услуги (Service Key);

– номер вызывающего абонента (Calling Party Number);

– свой сетевой номер (MSC Address);

– номер вызываемого абонента (Called Party Number);

– текущее дата/время вызова (Time And Timezone).

6. При наличии у B-абонента достаточных средств для оплаты входящего соединения CSE в ответном сообщении (CAP: MT=Continue, Operation Code=Request Report BCSMEvent) просит HMSC/VLR информировать его о прохождении соединения:

– отсутствии пути (RouteSelectFailure);

– занятости абонента (oCalledPartyBusy);

– ответе абонента (oAnswer);

. . .

– отбое абонента (oDisconnect).

7. HMSC/VLR по протоколу Mobile Application Part сообщением MAP: Message Type=Begin, Operation Code=sendRoutingInfo (MAP: MT=Begin, OP=SRI) снова открывает диалог с HLR о текущем местоположении B-абонента, в котором содержится:

– номер вызываемого абонента (MS ISDN Address Signals);

– свой сетевой номер (GMSC Address Signals),

– указание о прохождении взаимодействия с CSE (Suppress).

8. HLR сообщением MAP: Message Type=Begin, Operation Code= provideRoamingNumber (MAP: MT=Begin, OP=PRN) инициирует диалог с VMSC/VLR, где зарегистрировался B-абонент, в котором содержится:

– IMSI A-абонента (MCC + MNC + MSIN);

– свой сетевой номер (MSC Address Signals);

– номер вызываемого абонента (MS ISDN Address Signals).

9. VMSC/VLR роумингового B-абонента возвращает временный сетевой номер (Mobile Station Roaming Number, MSRN) для установления соединения (MAP: Message Type=End, Operation Code= provideRoamingNumber) и закрывает диалог. MSRN имеет структуру плана нумерации E.164.

10. HLR закрывает диалог пересылкой MSRN в HMSC/VLR, где находится A-абонент.

11. Используя MSRN, HMSC/VLR A-абонента по протоколу ISDN User Part устанавливает сетевое соединение к VMSC/VLR B-абонента (сообщение ISUP: IAM).

12. A-абонент извещается о поступлении вызова B-абоненту (сообщение ISUP: ACM).

13. B-абонент ответил (сообщение ISUP: ANM).

14. HMSC/VLR извещает CSE об установленном соединении A-абонентом (CAP: MT=Continue, Operation Code=Event Report BCSM, Event Type Bcsm=oAnswer. С этого момента начинается начисление оплаты на A-абонента на участке от мобильной станции до домашней сети (MS-HPLMN).

15. HMSC/VLR извещает CSE об установленном соединении B-абонентом (CAP: MT=Continue, Operation Code=Event Report BCSM, Event Type Bcsm=oAnswer. С этого момента начинается начисление оплаты на B-абонента на участке от домашней сети до гостевой сети (HPLMN-VPLMN).

16. A-абонент завершает соединение (сообщение ISUP: REL).

17. MSC/VLR B-абонента подтверждает окончание соединения (ISUP: RLC).

18. HMSC/VLR извещает CSE об окончании соединения A-абонентом (CAP: MT=Continue, Operation Code=Event Report BCSM, Event Type Bcsm=oDisconnect). CSE вычисляет плату A-абоненту за состоявшее соединение.

19. HMSC/VLR извещает CSE об окончании соединения B-абонентом (CAP: MT=Continue, Operation Code=Event Report BCSM, Event Type Bcsm=tDisconnect). CSE вычисляет плату B-абоненту за состоявшее соединение.

20. CSE уведомляет HMSC/VLR о завершении сеанса связи для A-абонента (CAP: MT=End).

21. CSE уведомляет HMSC/VLR о завершении сеанса связи для B-абонента (CAP: MT=End).

Понятно, что сведения о платёжеспособности абонента находятся в CSE, а сведения об израсходованных средствах в HMSC/VLR. Израсходованные средства периодически “выкачиваются” из HMSC/VLR центром оплаты (Billing Center) в виде Call Data Record (CDR) для контроля и разрешения возможных конфликтов с абонентами (сообщения FTP: CDR). CDR (bill) содержит подробную информацию о каждом разговоре: дате, продолжительности, номерах участников связи, тарифе и сумме к оплате.

На рис. 3.7 центр оплаты географически совмещен с интеллектуальной платформой, что не обязательно.

ВОПРОСЫ К РАЗДЕЛУ 3.2

1. Перечислите основные интерфейсы сети наземной связи мобильных абонентов.

Ответ. A-интерфейс соединяет RSS и NSS. B-интерфейс является внутренним между MSC и VLR. C-интерфейс соединяет GMSC и HLR. D-интерфейс соединяет VLR и HLR. E-интерфейс соединяет два MSC.

2. Назовите основную функцию центра коммутации мобильных абонентов (MSC).

Ответ. MSC обеспечивает соединения между мобильными станциями в пределах радио покрытия своей зоны.

3. Назовите основную функцию гостевого регистра (VLR).

Ответ. VLR хранит базу данных мобильных абонентов, которые временно прибывают в зоне обслуживания MSC.

4. Назовите основную функцию домашнего регистра (HLR).

Ответ. HLR хранит данные о местоположении (номере локальной зоны) абонента при входящей связи (выдает по C-интерфейсу по запросу GMSC) и его правах (выдает по D-интерфейсу по запросу VLR).

5. Назовите основную функцию центра аутентификации (AuC).

Ответ. AuC содержит данные о секретных ключах и алгоритмах шифрования.

6. Какие сетевые элементы обслуживают а)ячейку, б)локальную зону, в)несколько локальных зон?

Ответ. а)BTS, б)BSC, в)MSC.

7. Что излучает базовая приемопередающая станция в радиоканал соты?

Ответ. Код страны, код сети мобильных абонентов, код локальной зоны, т.е. LAI = MCC + MNC + LAC.

8. Какой план нумерации используется в сети связи стационарных абонентов?

Ответ. Согласно Рекомендации ITU-T E.164.

9. Какой план нумерации используется для идентификации мобильного абонента?

Ответ. Согласно Рекомендации ITU-T E.212.

10. Какова процедура пересчета идентификатора мобильного абонента в адрес сети связи стационарных абонентов?

Ответ. Согласно Рекомендации ITU-T E.214.

11. Перечислите протоколы, используемые в сети связи мобильных абонентов.

Ответ: Mobile Application Part (MAP), Camel Application Part (CAP), ISDN Application Part (ISUP).

12. Где хранится оригинальная база данных пользователя?

Ответ: В домашнем регистре (HLR).

13. Что храниться в гостевом регистре (VLR)?

Ответ: Копия базы данных из домашнего регистра (HLR).

14. Какой идентификатор использует пользователь для установления соединения к абоненту (пользователю)?

Ответ: Международный номер мобильного абонента (MSISDN).

15. Какой идентификатор использует VLR для запроса данных из HLR?

Ответ: Международный идентификатор мобильного абонента (IMSI).

16. Какой протокол используется при взаимодействии VLR и HLR?

Ответ: MAP.

17. Кто из участников соединения в сети мобильных абонентов оплачивает его стоимость?

Ответ. Абонент-инициатор оплачивает соединение от места своего местоположения до домашней сети абонента-получателя. Абонент-получатель оплачивает соединение от своей домашней сети до места своего местоположения.

18. Каким образом оконечная станция определяет номер инициатора мобильной связи?

Ответ. Запросом международного идентификатора мобильного абонента (International Mobile Subscriber Identity – IMSI).

19. В каком сетевом элементе хранятся данные о платежеспособности мобильного абонента?

Ответ. В специальном сетевом элементе интеллектуальной сети – узле управления услугами (Service Control Point (SCP)/CAMEL Service Environment (CSE)).

3.3. Процессы в сети связи мобильных абонентов второго поколения. Стандарт GSM

Центр коммутации мобильных абонентов (MSC) осуществляет следующие виды связи (рис. 3.8).

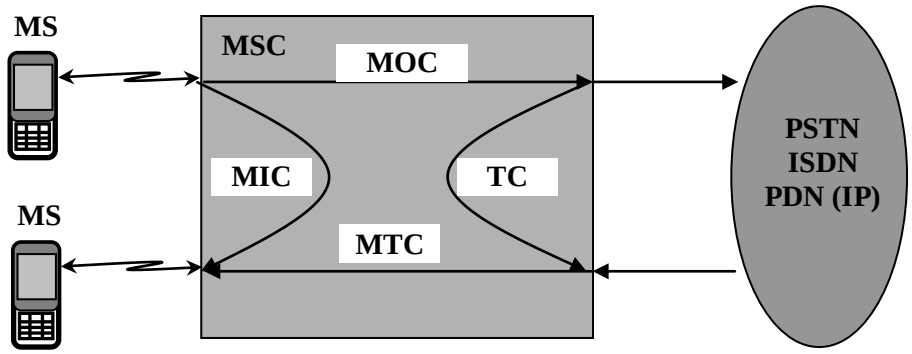

Рис. 3.8. Виды связи в центре коммутации

Исходящая связь (**M**obile **O**riginating **C**all, **MOC**) инициируется мобильной станцией и требуется соединение с абонентом другой сети (другого оператора).

Входящая связь (**M**obile **T**erminating **C**all, **MTC**) инициируется абонентом другой сети и требуется соединение с мобильной станцией в этой сети.

Внутренняя связь (**M**obile **I**nternal **C**all, **MIC**) инициируется мобильной станцией и требуется соединение с другой мобильной станцией в этой же сети.

Транзитная связь (**T**ransit **C**all, **TC**) инициируется абонентом другой сети и требуется соединение с абонентом другой сети.

3.3.1. Обеспечение безопасности сети

Под безопасностью сети связи мобильных абонентов понимается контроль посторонними лицами местоположения мобильных абонентов, угроза несанкционированного доступа к ресурсам сети, перехват/прослушивание передаваемых данных. Доступ посторонних лиц к линейно-кабельным сооружениям и коммутационному оборудованию затруднен, слабым местом сети является радиоканал.

Для предотвращения этих угроз на радиоканале принимаются специальные меры, главными из которых являются:

– сокрытие адресатов соединения, для предотвращения локации мобильных абонентов;

– аутентификация – установление легитимности участников связи для предотвращения несанкционированного доступа к ресурсам сети;

– шифрование – преобразование исходных данных, передаваемых по радиоканалу, в “нечитаемый” для посторонних лиц текст, предотвращающее доступ к чтению передаваемых данных.

Классическая модель криптосистемы приведена на рис. 3.9. В модели присутствуют три участника: два легальных пользователя (MS и BSS) и злоумышленник. Задача злоумышленника заключается в контроле местоположения абонента и перехвате передаваемых им сообщений. При этом предполагается, что злоумышленник имеет возможность подключения к радиоканалу связи и ему доступны

1. Открытые тексты передаваемых сообщений.
2. Алгоритм шифрования/дешифрования передаваемых сообщений.

Рис. 3.9. Классическая модель криптосистемы

Сокрытие местоположения (идентификатора) абонента производится следующим образом.

При первом сеансе связи абонент использует IMSI, который может быть известен злоумышленнику. При смене зоны обслуживания (LAC) MSC/VLR (командой TMSI Reallocation Command – TMSI_REAL_CMD) назначает абоненту псевдоним (**T**emporary **M**obile **S**ubscriber **I**dentity, **TMSI**), который запоминается в VLR и SIM-карте и используется как идентификатор абонента при следующем сеансе связи. TMSI имеет структуру вида TMSI = LAI + TIC, где TIC выбирается из пула (хранилища) VLR и имеет длину 4 байта.

Для аутентификации и шифрования используются три параметра:

– международный идентификатор мобильного абонента (IMSI);
– секретный ключ Ki (Individual Subscriber Authentication Key);
– алгоритмы кодирования A3 и A8.

Эти параметры имеются в центре аутентификации и SIM-карте и используются для вычисления триплетов (Triples). Триплет представляет собой 1)случайное число (RAND – 16 байт); 2)цифровая подпись (SRES – 4 байта), полученная перемешиванием случайного числа RAND с секретным ключом Ki (16 байт) по алгоритму A3; 3)ключ шифрования (Kc – 8 байт), полученный перемешиванием случайного числа RAND с секретным ключом Ki по алгоритму A8.

Процедура аутентификации и установка режима шифрования состоит в следующем (рис. 3.10).

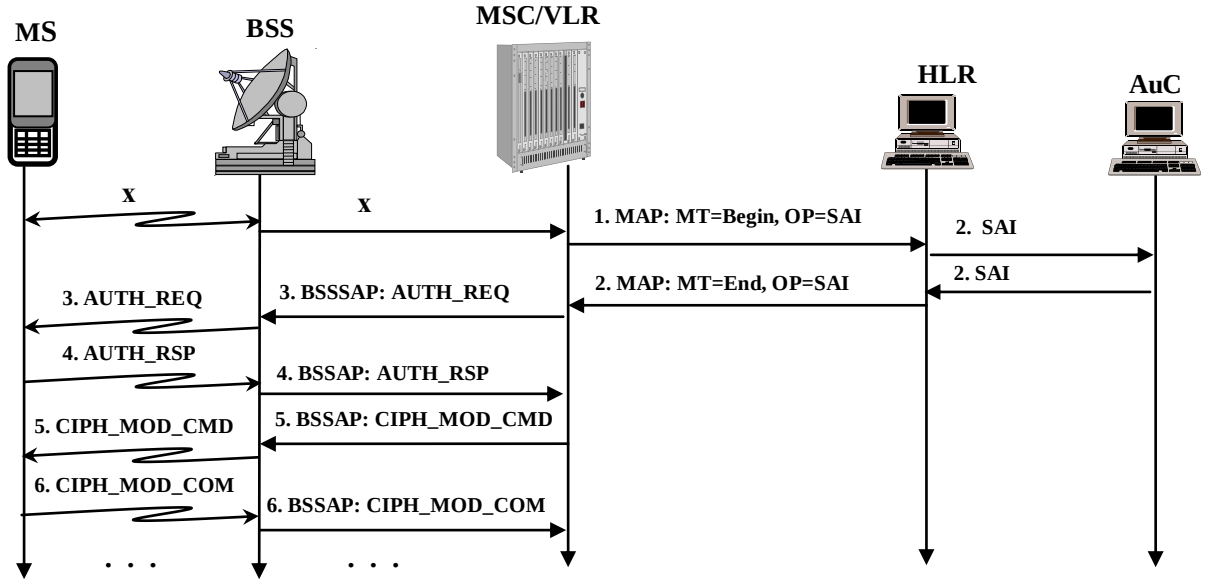

Рис. 3.10. Процедура аутентификации и установка режима шифрования

1. При первом запросе на осуществлении связи VLR по протоколу MAP открывает диалог сообщением MAP: Message Type=Begin, Operation Code=sendAuthenticationInfo (MAP: MT=Begin, OP=SAI), в котором запрашивает у HLR (или у предыдущего VLR) идентификационные параметры (триплеты).

2. HLR по внутреннему протоколу оператора запрашивает триплеты у AuC, получает несколько триплетов (обычно 5), отсылает их в MSC/VLR и закрывает диалог (MAP: MT=End, OP=SAI).

3. VLR выбирает один из триплетов и по протоколу BSS Application Part (BSSAP) посылает его случайное число RAND мобильной станции (команда Authentication Request – BSSAP: AUTH_REQ). Оставшиеся триплеты сохраняются для следующих сеансов связи. Если остался последний неиспользованный триплет, то MSC/VLR сообщением sendAuthenticationInfo запрашивает у HLR новую партию триплетов. При выходе из стоя HLR/AuC последний триплет используется до момента восстановления HLR/AuC.

4. Мобильная станция перемешивает случайное число RAND с секретным ключом Ki по алгоритму A3, получая цифровую подпись – SRES. Эту цифровую подпись мобильная станция возвращает MSC/VLR (сообщение Authentication Response – BSSAP: AUTH_RSP). VLR сравнивает SRES, полученную от абонента со SRES, полученной от HLR. При их совпадении процедура аутентификации считается успешной, в противном случае MS высылается сообщение Authentication Reject – AUTH_REJ.

5. VLR командой Ciphering Mode Command (BSSAP: CIPH_MOD_CMD) посылает BSS ключ шифрования Кс и алгоритм шифрования A5/x. BSS пересылает мобильной станции только алгоритм шифрования A5/x, ключ шифрования Кс мобильная станция вычисляет самостоятельно.

6. MS подтверждает установку режима шифрования (Ciphering Mode Complete – BSSAP: CIPH_MOD_COM).

Процедура шифрования (Ciphering) передаваемых сообщений (речи, данных) состоит в следующем.

При любом запросе на осуществлении связи MS высылает сети (сообщение Class Mark Update – CLS_MRK_UPD)список поддерживаемых алгоритмов шифрования A5/x. MSC/VLR командой Ciphering Mode Command (CIPH_MOD_CMD) извещает MS о переходе в режим шифрования с указанием конкретного алгоритма A5/x (алгоритм A5/0 означает отсутствие шифрования). MS отвечает подтверждением Ciphering Mode Complete (CIPH_MOD_COM). С этого момента обе стороны (MS и BSS) вычисляют шифрующую последовательность CS длинной 114 бит с использованием ключа шифрования Кс и алгоритма шифрования A5/x. Используется симметричный алгоритм шифрования с секретными ключами, при котором пара пользователей имеет один и тот секретный же ключ (шифрующую последовательность). Принцип симметричного алгоритма шифрования с секретными ключами изображен на рис. 3.11.

1. На передаче исходный открытый текст (PT) складывается по модулю 2 с шифрующей последовательностью CS. Шифрованный текст (CT) передается в канал связи.

2. На приеме шифрованный текст (CT) снова складывается по модулю 2 с той же шифрующей последовательностью CS, результатом является исходный открытый текст.

В обратном направлении шифрование происходит таким же образом.

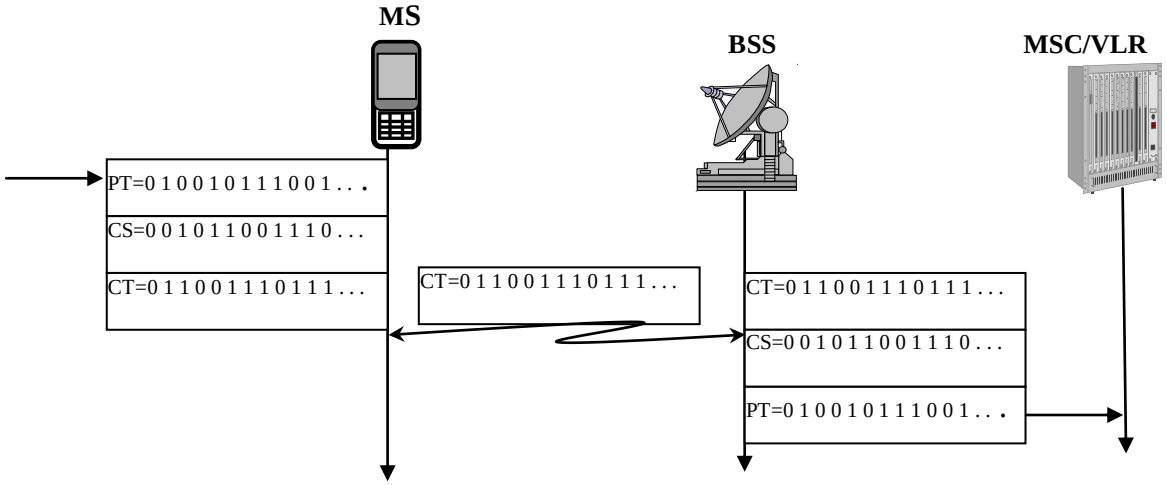

Рис. 3.11. Процедура шифрования

3.3.2. Регистрация мобильных абонентов

До установления любого соединения мобильная станция должна пройти процедуру регистрации.

Различают несколько видов регистрации.

Начальная регистрация (IMSI Attach) используется мобильной станцией при первоначальном включении или прибытии из сети другого оператора. В любом случае SIM-карта содержит в LAI код MCC, отличающийся от принимаемого кода MCC из радиоканала. Происходят следующие события (рис. 3.12).

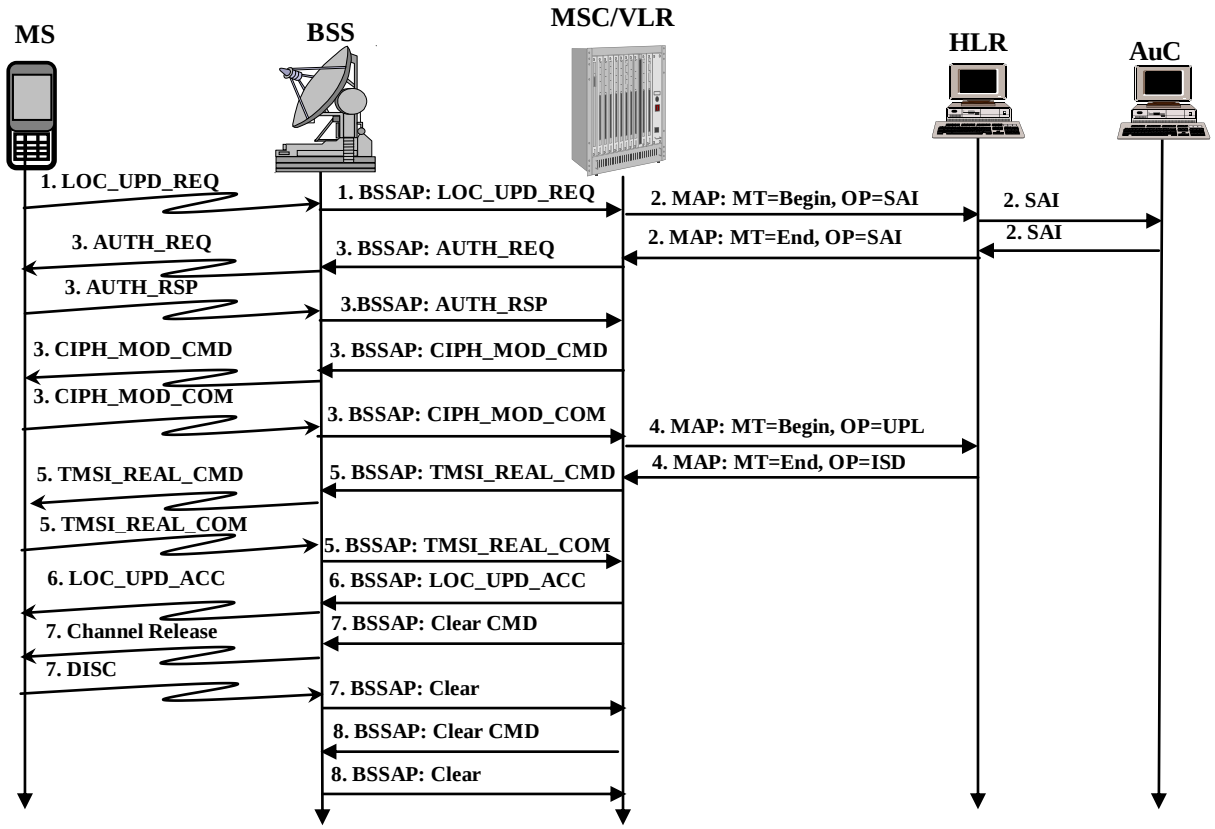

Рис. 3.12. Начальная регистрация (IMSI Attach)

1. Мобильная станция посылкой сообщения Location Update Request (LOC_UPD_REQ) инициирует в MSC/VLR запрос на регистрацию. В качестве собственного идентификатора MS использует IMSI.

2. VLR по адресу IMSI адресуется в HLR (MAP: MT=Begin, OP=SAI) и запрашивает у него идентификационные параметры (триплеты). В качестве своего идентификатора VLR использует сетевой номер (VLR number). HLR запрашивает триплеты у AuC, получает несколько триплетов (обычно 5) и отсылает их VLR.

3. VLR выбирает один из триплетов и инициирует процедуру аутентификации и шифрования.

4. При успешном исходе аутентификации и шифрования VLR сообщением MAP: Message Type=Begin, Operation Code=updateLocation (MAP: MT=Begin, OP=UPL) запрашивает у HLR базу данных (профайл) абонента. В ответ HLR высылает запрошенные данные (MAP: MT=End, OP=insertSubscriberData) и запоминает номер VLR. С этого момента HLR известно местоположение собственного мобильного абонента.

5. VLR запоминает абонентские данные, присваивает TMSI взамен IMSI, отсылает TMSI мобильной станции.

6. VLR завершает регистрацию (Location Update Accept – LOC_UPD_ACC). Мобильная станция записывает TMSI и LAI в SIM-карту.

7. MSC/VLR высылает команду об освобождении радиоканала, мобильная станция подтверждает освобождение.

8. MSC/VLR высылает команду о завершении сеанса связи с BSS и получает подтверждение.

Если мобильный абонент сменил свое местоположение, то MS обнаружит это сравнением старого LAI, записанным в SIM-карте, с новым LAI, принятому из радиоканала. В этом случае необходима *перерегистрация* (Location Update).

1. Мобильная станция посылкой сообщения LOC_UPD_REQ инициирует в MSC/VLR запрос на перерегистрацию (рис. 3.13). В качестве собственного идентификатора используется ранее присвоенный TMSI, а также старый LAI, новый LAI.

2. Новый VLR, обнаружив TMSI чужого VLR, использует старый LAI для запроса у старого (соседнего) VLR неиспользованных триплетов и IMSI (сообщение MAP: MT=Begin, OP=sendIdentificationInfo). Если в базе данных нового VLR не имеется сведений о старом VLR, то новый VLR запрашивает у MS (команда Identity request) IMSI и инициирует начальную регистрацию.

3. Новый VLR инициирует процедуру аутентификации и шифрования.

4. При успешном исходе аутентификации и шифрования новый VLR по адресу IMSI адресуется в HLR и запрашивает у него базу данных (профайл) абонента (сообщение MAP: MT=Begin, OP=UPL). База данных содержит MSISDN, разрешенные дополнительные услуги и т.д. В ответ HLR высылает запрошенные данные (сообщение MAP: MT=End, OP=ISD) и запоминает номер нового VLR. С этого момента HLR известно местоположение собственного мобильного абонента. Если же в запросе на перерегистрацию произошла смена LAI, принадлежащего тому же VLR, то обращение к HLR не происходит.

5. VLR запоминает абонентские данные, присваивает TMSI взамен IMSI, отсылает TMSI мобильной станции.

6. VLR завершает регистрацию (Location Update Accept – LOC_UPD_ACC). Мобильная станция записывает TMSI и LAI в SIM-карту.

7. HLR сообщением MAP: MT=Begin, Operation Code=cancelLocation (MAP: MT=Begin, OP=CANL) извещает старый VLR об уничтожении данных мобильного абонента).

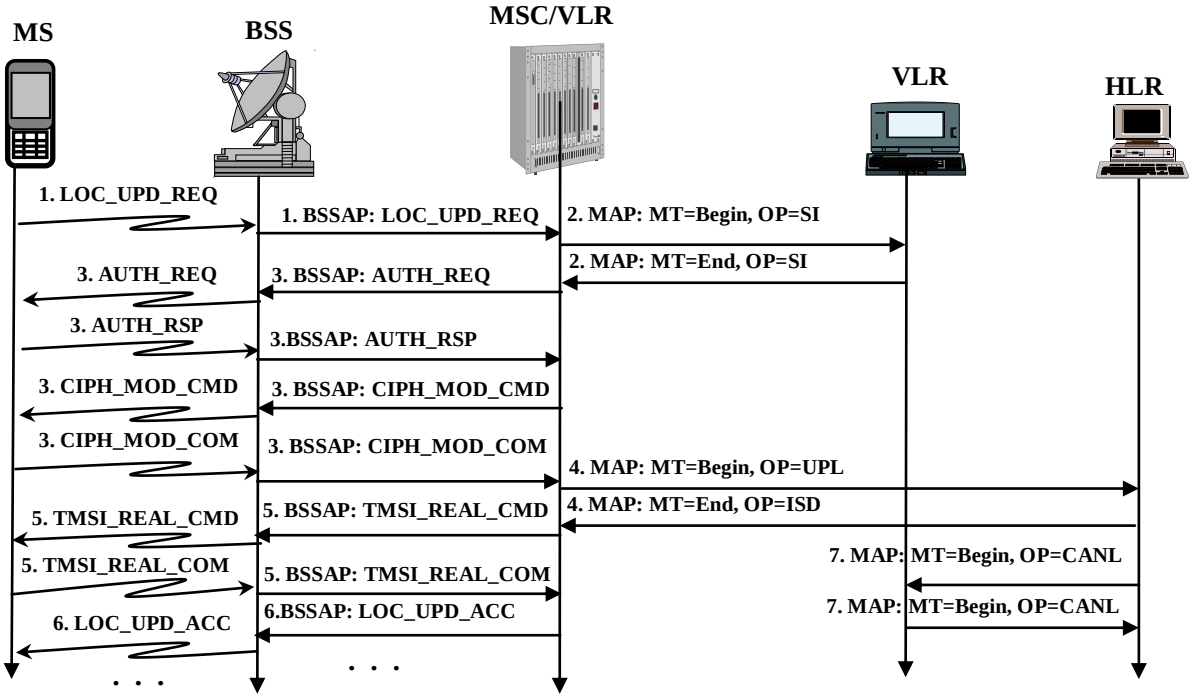

Рис. 3.13. Перерегистрация (Location Update)

В дальнейшем мобильная станция обязана производить *периодическую регистрацию* (период устанавливается оператором в диапазоне 6 – 480 минут), подтверждая свое присутствие в сети. В этом случае VLR производит те же операции перерегистрации, кроме пункта 4, т.е. не обращается к HLR.

Если в течение определенного времени (обычно 120 часов) мобильная станция не проявляет никакой активности (перерегистрации, инициирования и прием вызовов), то VLR производит удаление такой записи (Purging) с извещением HLR, который отмечает недоступность абонента. Это предохраняет VLR от переполнения памяти, а HLR – от неправильной регистрации. Удаление записей наиболее неактивных абонентов VLR также производит при заполнении 80% своей памяти. Для восстановления записи абоненту необходимо пройти начальную регистрацию.

При выключении MS посылает VLR сообщение (IMSI Detach – IMSI_DET), VLR извещает об этом HLR. Все это приводит к невозможности установления входящего соединения. Когда мобильная станция вновь подключается к сети, она вновь регистрируется в VLR (сообщение LOC_UPD_REQ с указанием причины – IMSI_ATT). VLR извещает об этом HLR, входящая связь снова становится возможна.

3.3.3. Установление исходящего соединения

Исходящая связь (**M**obile **O**riginating **C**all, **MOC**) инициируется мобильной станцией и требуется соединение с абонентом другой сети (оператора). Другая сеть может быть либо сетью связи стационарных абонентов, либо наземной сетью связи мобильных абонентов другого оператора. В любом случае в базе данных MSC сведения о порядке обслуживания вызываемого абонента отсутствуют, но в MSC прописан маршрут, устанавливающий соответствие между набранными абонентом цифрами номера и интерфейсом к другой сети. MSC устанавливает соединение через требуемый интерфейс. Дальнейшее обслуживание абонента продолжается другой сетью.

Происходят следующие действия (рис. 3.14, без сообщений учета стоимости).

1. Абонент делает запрос на установление исходящего соединения (сообщение CM Service Request – CM_SERV_REQ), в качестве своего идентификатора он использует TMSI.

2. VLR производит аутентификацию и с получением корректного SRES убеждается в легитимности абонента.

3. MS извещает MSC о поддерживаемой версии шифрования информации (сообщение Classmark update – CLS_MRK_UPD).

4. MSC выдает команду на переход в режим шифрования (команда Cipher Mode Command – CIPHER_MODE_CMD) и получает подтверждение (сообщение Cipher Mode Complete – CIPHER_MODE_COM).

5. MSC присваивает новый TMSI (TMSI_REAL_CMD и TMSI_REAL_COM).

6. MSC выдает команды BTS на резервирование радиоканала (команда Assignment Request – ASS_REQ) и получает подтверждение (Assignment Complete – ASS_COM).

7. MS передает набранные цифры номера (сообщение SETUP), а MSC в соответствии с набранными абонентом цифрами номера устанавливает исходящее соединение в другую сеть (сообщение Initial Address Message – IAM).

Дальнейшее установление исходящего соединения через ISDN ничем не отличается от установления соединения в сети связи со стационарными абонентами (сообщения ACM, ANM, . . .).

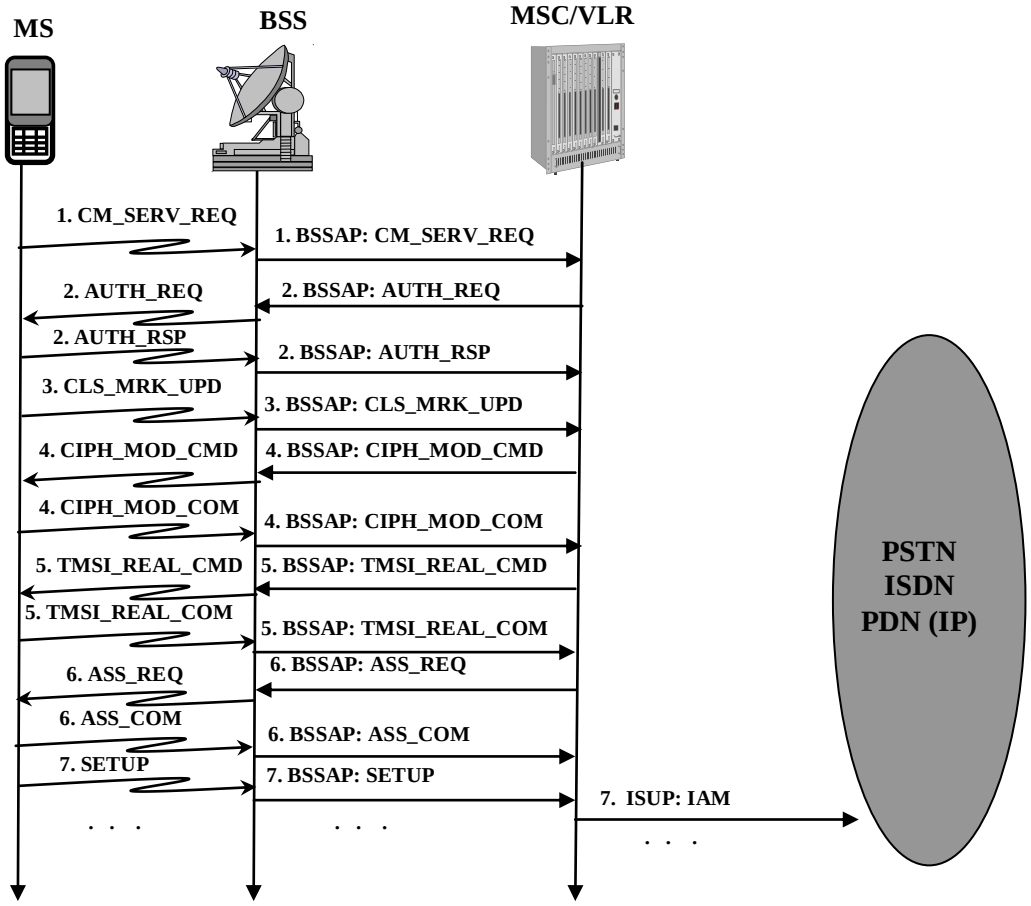

Рис. 3.14. Установление исходящего соединения

3.3.4. Установление входящего соединения

Входящая связь (**M**obile **T**erminating **C**all, **MTC**) инициируется абонентом другой сети и требуется соединение с мобильной станцией в этой сети.

Происходят следующие действия (рис. 3.15, без сообщений учета стоимости).

1. Соединение начинается в другой сети и поступает виде запроса на соединение (Initial Address Message – IAM) на шлюзовой центр коммутации (GMSC). Адресация на шлюзовой центр коммутации станцией другой сети происходит на основе MSISDN через ISDN.

2. GMSC не известно местоположение мобильного абонента, поэтому он обращается к HLR, где должен быть зарегистрирован мобильный абонент с домашним IMSI (сообщение sendRoutingInfo - SRI). При отсутствии регистрации HLR посылает GMSC отказ и соединение разрушается. Если абонент зарегистрирован, то HLR запрашивает маршрутный номер мобильного абонента (**M**obile **S**tation **R**oaming **N**umber – **MSRN**) у VLR (сообщение provideRoamingNumber – PRN), где зарегистрирован мобильный абонент, имеющий домашний IMSI. MSRN имеет структуру плана нумерации E.164.

3. VLR выдает из своего пула один из свободных MSRN, а HLR транслирует его GMSC.

4. GMSC, используя MSRN, обычным образом устанавливает соединение с гостевым MSC/VLR. По прибытии IAM на MSC использованный MSRN возвращается обратно в пул VLR и может быть использован для другого соединения.

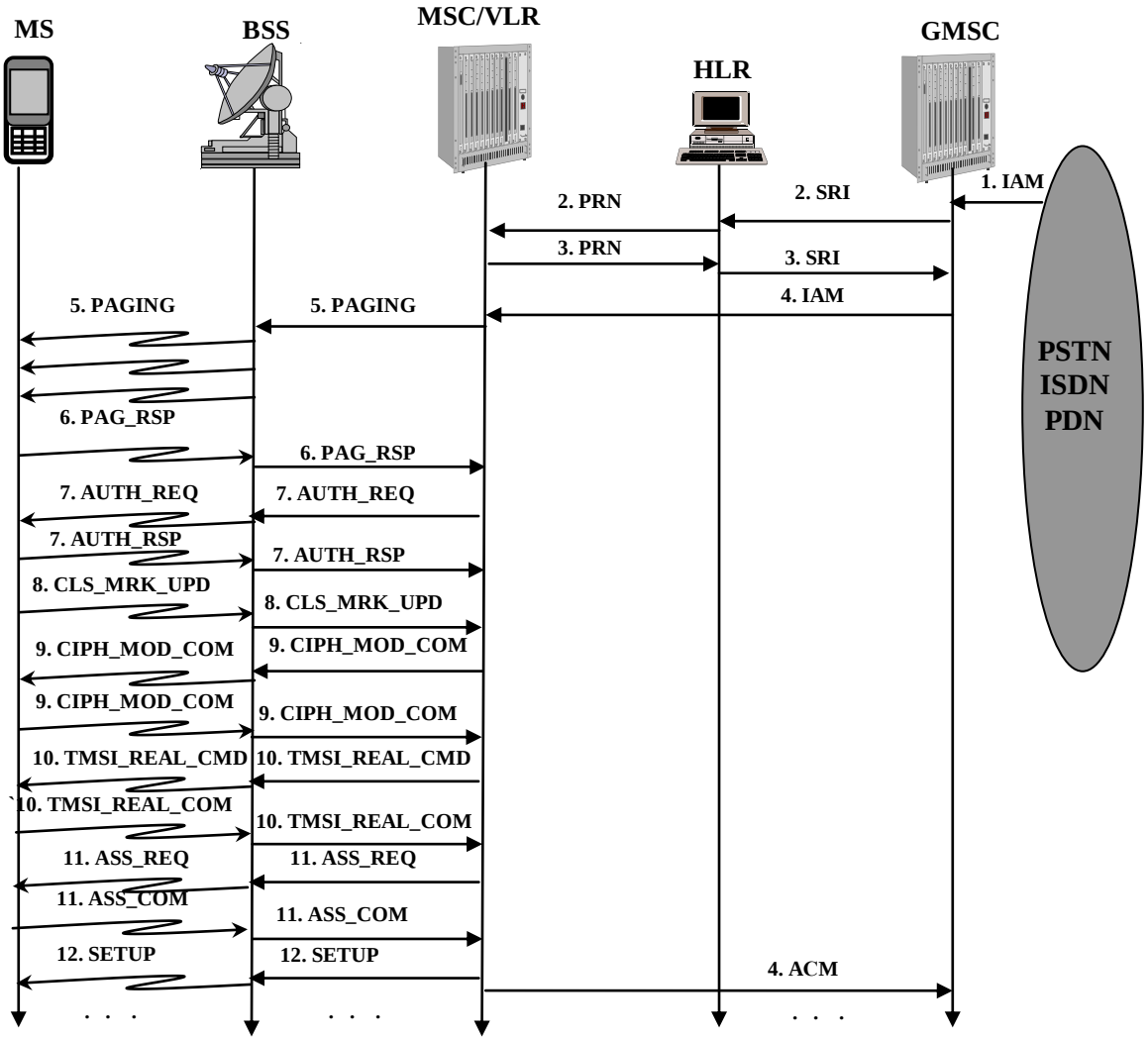

Рис. 3.15. Установление входящего соединения

5. MSC известна локальная зона нахождения абонента, но неизвестна ячейка. Поэтому MSC производит широковещательный поисковый вызов (PAGING) во все BTS, принадлежащие этой зоне.

6. Мобильная станция отвечает на поисковый вызов (сообщение Paging Response – PAG_RSP). MSC фиксирует конкретную BTS, где находится MS.

7-11. MS и MSC/VLR производят все операции (аутентификацию, шифрование, назначение нового TMSI, резервирование радиоканала), которые применяются при установлении исходящего соединения.

12. MSC инициирует посылку вызова мобильному абоненту (сообщение SETUP). Дальнейшее установление исходящего соединения ничем не отличается от установления входящего соединения в сети связи со стационарными абонентами.

3.3.5. Установление внутреннего соединения

Внутренняя связь (**M**obile **I**nternal **C**all, **MIC**) инициируется мобильной станцией и требуется соединение с другой мобильной станцией в этой же сети. Осуществляется путем двух соединений MOC-MTC через петлевое устройство внутри MSC.

3.3.6. Установление транзитного соединения

Транзитная связь (**T**ransit **C**all, **TC**) инициируется абонентом другой сети и требуется соединение с абонентом другой сети. Процедура установления соединения полностью аналогична процедуре установления транзитного соединения в сети связи стационарных абонентов и обычно используется для предоставления транспортной среды другим операторам.

3.3.7. Эстафетная передача соединения

Если мобильный абонент сменил свое местоположение в свободном состоянии (не в состоянии разговора), то MS инициирует перерегистрацию, как описано в 3.3.2. Если же смена местоположения происходит во время сеанса связи (разговора), то в этом случае производится эстафетная передача соединения (Handover). Возможно 2 случая: лучшая сота находится в своей зоне обслуживания и лучшая сота находится в зоне обслуживания другого MSC. Рассмотрим второй как более сложный случай.

Предположим, что соединение установлено между мобильным абонентом и сетью связи стационарных абонентов по цепи PSTN – MSC_A – BSC_A – MS (рис. 3. 16).

1. MS постоянно отслеживает мощность радиосигнала, поступающего от якорной радио подсистемы (BSC_A). При перемещении MS в другую ячейку (соту), обслуживаемую BSC_B, мощность радиосигнала от BSC_A уменьшается (Bad Measurement), а от BSC_B увеличивается (Good Measurement). BSC_A информирует об этом MSC_A сообщением HO_Required, в котором содержится номер соты текущего расположения MS (A-сота) и номер соты лучшего приема (B-сота).

2. В случае устойчивого ухудшения приема, т.е. получения 4-х сообщений HO_Required подряд, MSC_A принимает решение об эстафетной передаче соединения. В своей базе данных MSC_A по номеру B-соты находит сетевой номер MSC, который обслуживает эту соту и отправляет сообщение MAP: prepareHandover.

3. MSC_B по номеру B-соты обращается к соответствующему BSC_B о резервировании радиоканала (сообщение BSSAP: HO Request).

4. При наличии свободного радиоканала BSC_B резервирует его и высылает подтверждение (сообщение BSSAP: HO Request Ack).

5. Подтверждение наличия свободного радиоканала и возможности эстафетной передачи соединения MSC_B высылает MSC_A (сообщение MAP: prepareHandover).

6. MSC_A по сети ISDN высылает заявку на установление проводного соединения к MSC_B (сообщение ISUP: IAM).

7. MSC_B сообщением ISUP: ACM уведомляет, что заявка на установление проводного соединения принята.

8. MSC_A через BSC_A высылает команду MS на переключение в новую B-соту (BSSAP: HO Command) и MS сигнализирует BSC_B об инициализации переключения.

9. MSC_B устанавливает радиоконтакт с MS по новой B-соте (сообщение BSSAP: HO Detected).

10. MSC_B извещает MSC_A об установлении радиоконтакта с MS по новой B-соте (сообщение MAP: processAccSignaling).

11. MSC_B извещает об соединении проводного канала с радиоканалом (сообщение ISUP: ANM).

12. MS извещает о завершении переключения на новую B-соту (сообщение BSSAP: HO Complete).

13. MSC_B извещает MSC_A о завершении переключения на новую B-соту (сообщение MAP: sendEndSignal).

14. MSC_A выдает команду BSC_A об освобождении A_соты.

Регистрацию в новой соте абонент производит после завершения соединения.

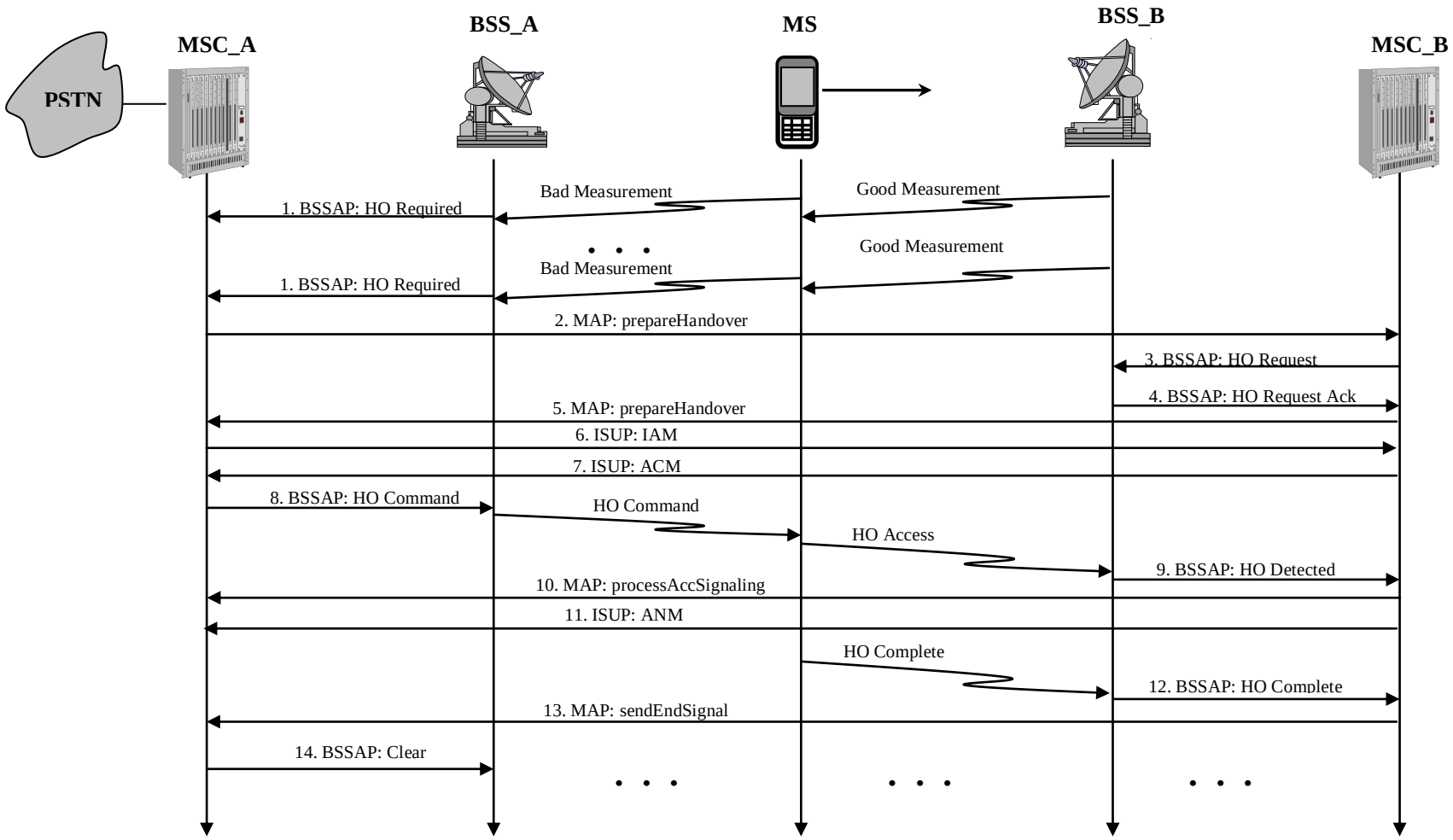

Рис. 3.16. Эстафетная передача соединения

3.3.8. Доставка коротких сообщений

Для реализации услуги доставки коротких сообщений (Short Message, SM) используется дополнительный сетевой элемент – сервисный центр коротких сообщений (SMSC). На участке MSC-SMSC используется протокол MAP, а на участке MS-MSC используется протокол DTAP, являющийся подпротоколом BSSAP. Основная идея реализации услуги состоит в использовании SMSC как пересылочного пункта, когда на первом этапе SM доставляется от пользователя к SMSC, а на втором этапе – от SMSC к MS. Эти две сетевые процедуры получили название MO-SM и MO-TM, соответственно.

Процедура доставки короткого сообщения от мобильной станции к сервисному центру коротких сообщений приведена на рис. 3.17.

1. Абонент MS1 делает запрос на передачу короткого сообщения (сообщение CM Service Request – CM_SERV_REQ), в качестве своего идентификатора он использует TMSI.

2 – 4. MSC/VLR производит аутентификацию и устанавливает режим шифрования.

5. MS1 передает короткое сообщение в MSC/VLR (CP-DATA(RP-DATA)), в котором указан адреса SMSC и абонента получателя MS2. BSC/BTS прозрачно транслирует сообщение в MSC/VLR. Последний подтверждает получение короткого сообщения (CP-ACK).

6. MSC/VLR открывает диалог с SMSC, в который вкладывает короткое сообщение (MAP: MT=Begin, OP=MO_ForwardSM). SMSC высылает подтверждение о получении короткого сообщения и закрывает диалог (MAP: MT=End, OP=MO_ForwardSM).

7. MSC/VLR извещает MS1 о доставке короткого сообщения в SMSC.

8. MSC/VLR высылает команду об освобождении радиоканала, мобильная станция MS1 подтверждает освобождение.

9. MSC/VLR высылает команду о завершении сеанса связи с BSS и получает подтверждение. Указанные сообщения относятся к процедуре к MO-SM.

10. Процедура MT-SM начинается с того, что SMSC высылает запрос в HLR о местоположении получателя короткого сообщения и в ответ получает адрес MSC/VLR, где находится получатель MS2.

11. По адресу, полученному от HLR, SMSC открывает диалог с MSC/VLR (MAP: MT=Begin, OP=MO_ForwardSM).

12 – 15. MSC/VLR производит поиск, аутентификацию и устанавливает режим шифрования с абонентом получателем MS2.

16. MSC/VLR доставляет короткое сообщение MS2 и получает подтверждение.

17. MSC/VLR уведомляет SMSC о доставке короткого сообщения и закрывает диалог (MAP: MT=End, OP=MO_ForwardSM).

18. MS2 уведомляет MSC/VLR об окончании сеанса связи.

19. MSC/VLR выдает команду (Clear CMD) BSC/BTS об освобождении радиоканала, BSC/BTS информирует (Channel Release) MS об освобождении радиоканала. MS подтверждает освобождение радиоканала (DISC). BSC/BTS подтверждает освобождение радиоканала (Clear COM).

20. MSC/VLR и BSC/BTS обмениваются сообщениями о завершении сеанса связи.

Если B-абонент в момент доставки SMS отсутствует, то HLR в ответ на запрос MSC/VLR информирует его об отсутствии абонента. Появление абонента в сети происходит по цепи входящий MSC/VLR-HLR-SMSC.

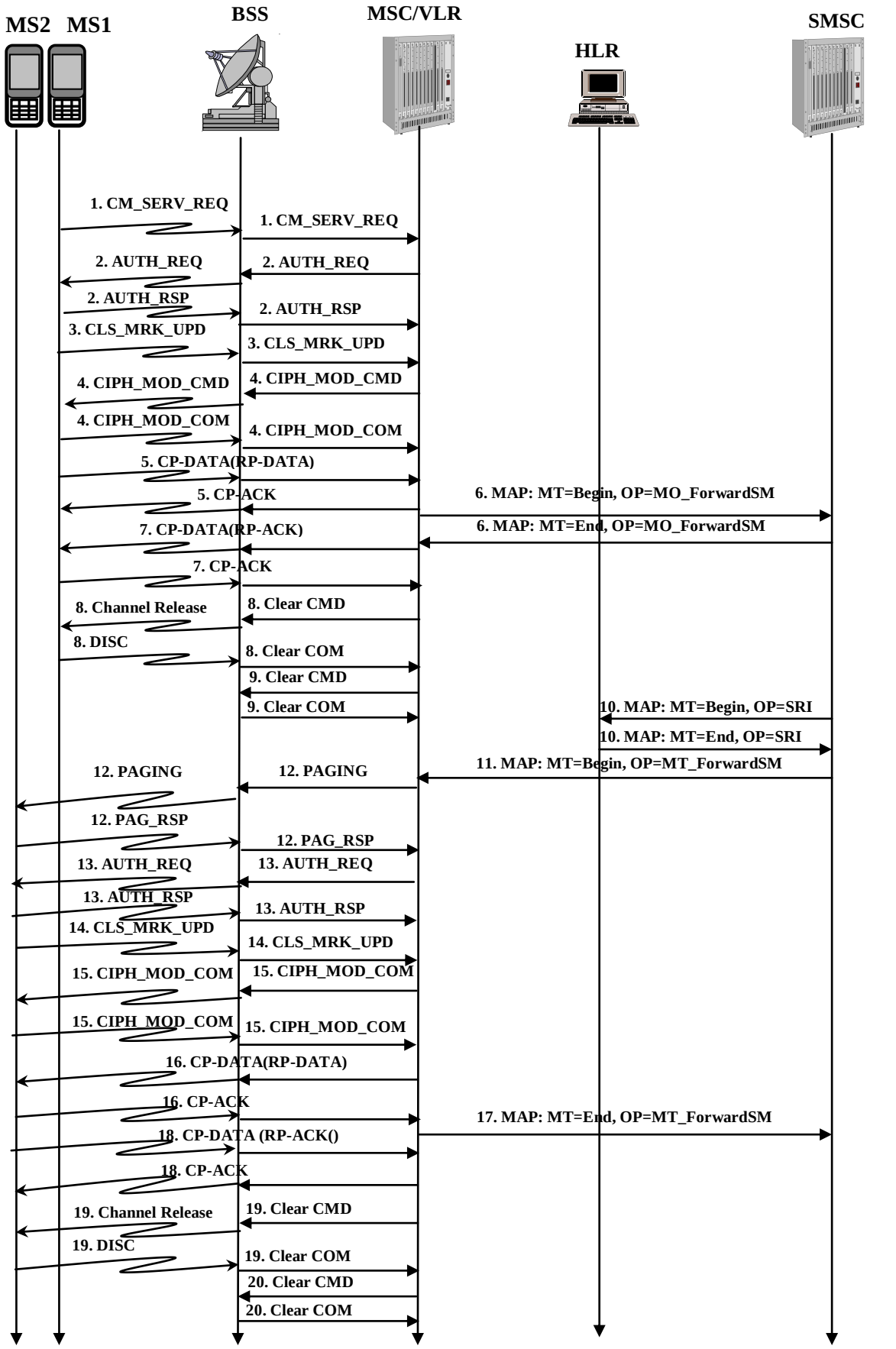

Рис. 3.17. Доставка коротких сообщений

ВОПРОСЫ К РАЗДЕЛУ 3.3

1. Какой участок сети наземной связи мобильных абонентов является наиболее уязвимым с точки зрения безопасности сети?

Ответ. Радиоканал на участке MS-BTS.

2. Как осуществляется сокрытие местоположения мобильного абонента?

Ответ. Присвоением ему переменного временного идентификатора (TMSI) при каждом новом сеансе связи.

3. Что такое триплет?

Ответ. Совокупность трех параметров: 1)случайного числа (RAND), 2)цифровой подписи (SRES), 3)ключа шифрования (Кс).

4. Какова цель аутентификации?

Ответ. Выяснение легитимности абонента, т.е. права абонента на осуществление связи.

5. Как осуществляется аутентификация?

Ответ. Абоненту посылается случайное число; это число и секретный ключ используется для формирования цифровой подписи.

6. Какова цель шифрования?

Ответ. Сокрытия передаваемой информации.

7. Как осуществляется шифрование информации?

Ответ. Сложением по модулю два передаваемой информации с шифрующей последовательностью.

8. Как осуществляется дешифрование информации?

Ответ. Сложением по модулю два принимаемой информации с шифрующей последовательностью.

9. В каких случаях мобильный абонент осуществляет регистрацию?

Ответ. При первоначальном включении MS, при смене своего местоположения (LAC), периодически.

10. Может ли абонент иметь сетевой номер (MSISDN), совпадающий с маршрутным номером мобильного абонента (MSRN)?

Ответ. Нет.

11. Поясните назначение широковещательного поискового вызова (Paging).

Ответ. Определение номера ячейки в локальной зоне, где находится мобильный абонент.

12. Какой сетевой элемент инициирует эстафетную передачу соединения (Handover)?

Ответ. Мобильная станция (MS).

13. Что является причиной эстафетной передачи соединения?

Ответ. Лучший прием радиосигнала от соседней ячейки (соты).

14. Что происходит с SMS при временном отсутствии абонента-получателя?

Ответ. SMSC высылает в HLR запрос о местоположении получателя SMS и в ответ получает отказ доставки. SMS продолжает храниться в SMSC.

15. Что происходит с SMS при появлении в сети абонента-получателя?

Ответ. Входящий MSC/VLR информирует HLR о появлении абонента. HLR информирует SMSC о появлении абонента. SMSC доставляет SMS абоненту-получателю.

16. Что происходит с SMS при постоянном отсутствии абонента-получателя?

Ответ. По истечении тайм-аута (обычно 120 часов) SMSC уничтожает SMS.

3.4. Надстройка сети связи мобильных абонентов второго поколения. Пакетная радиосвязь общего пользования

Стандарт GSM версии 2 предусматривает передачу речи и данных в режиме коммутации каналов. Речевая информация, поступающая из MSC в BSC со скоростью 64 Кбит/с, сжимается до 13 Кбит/с (Full Rate) и совместно с защитными битами излучается в радиоканал со скоростью 22,8 Кбит/с. Данные размещаются в разговорном канале и передаются со скоростью 9,6 Кбит/с. Передача данных в стандарте GSM версии 2 изображена на рис. 3.18.

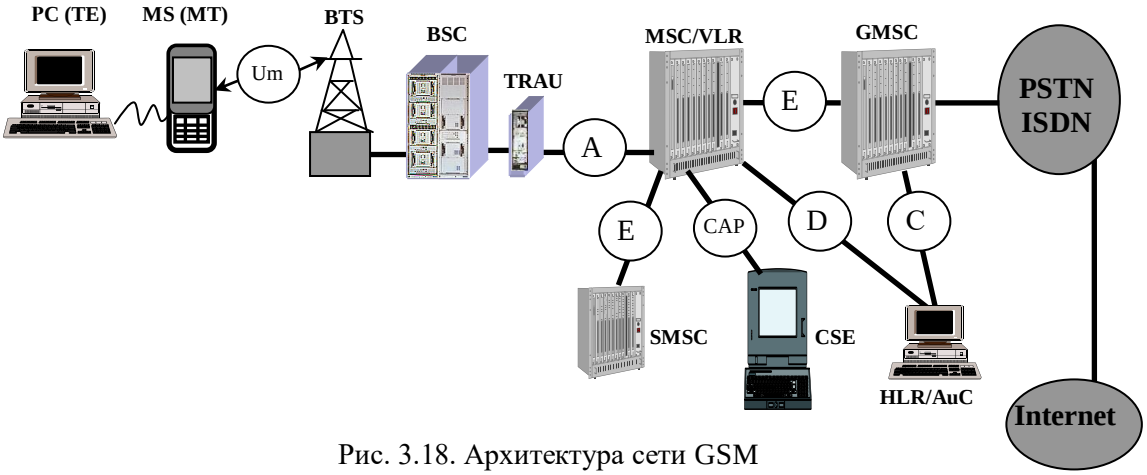

Рис. 3.18. Архитектура сети GSM

Такое решение, использующее MS как модем (MT), плохо приспособлено для передачи данных по нескольким причинам:

– взрывной характер трафика данных в некоторые короткие промежутки времени требует высокую скорость передачи, а в другие промежутки времени трафик отсутствует совсем. Это плохо сочетается с выделенной постоянной полосой передачи со скоростью 9,6 Кбит/с в режиме коммутации каналов и гораздо ниже скорости в ISDN (64 Кбит/с);

– соединения в IP-сеть пролегают через PSTN/ISDN, где принят повременный учет стоимости и низкая скорость установления соединения;

– длина коротких сообщений (SMS) ограничена 160 символами;

– одинаковая скорость передачи в направлениях пользователь-сеть и сеть-пользователь.

Существующее решение для высокоскоростной передачи данных (**H**igh **S**peed **C**ircuit **S**witched **D**ata, **HSCSD**) подразумевает объединение 4-х радиоканалов со скоростью передачи 14,4 Кбит/с каждый. Это позволяет достигнуть скорости 14,4x4=57,6 Кбит/с, что сравнимо со скоростью передачи в ISDN, но повременный учет стоимости делает это решение малопривлекательным.

3.4.1. Сетевые элементы

Указанные недостатки были устранены в стандарте GSM версии 2+ добавлением специальной подсистемы – пакетной радиосвязи общего пользования (**G**eneral **P**acket **R**adio **S**ervice, **GPRS**).

Имеется три класса оконечных устройств MS для GPRS:

класс A автоматически регистрируется в 2-х доменах и имеет возможность одновременного соединения речи (подсистема GSM) и данных (подсистема GPRS);

класс B автоматически регистрируется в 2-х доменах и имеет возможность попеременного соединения речи (подсистема GSM) или данных (подсистема GPRS);

класс С вручную регистрируется только в одном из 2-х доменов и имеет возможность соединения либо речи (GSM), либо данных (подсистема GPRS).

Для обеспечения функций передачи данных произошли следующие изменения (рис. 3.19).

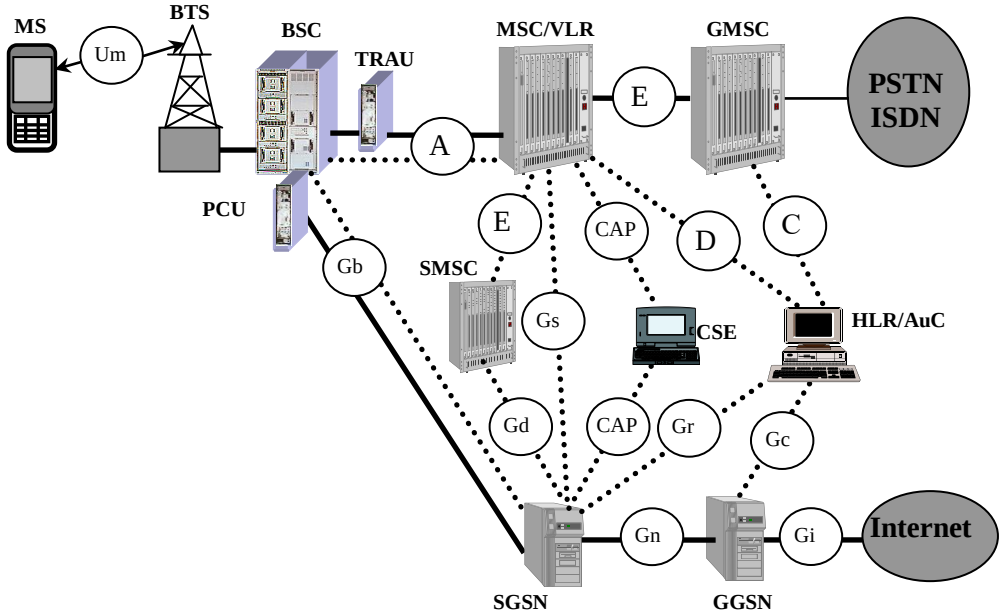

Рис. 3.19. Архитектура сети GSM/GPRS

- служебные сообщения (Control Plane)

- трафик пользователя (User Plane)

1. В подсистему BSS добавлен блок управления пакетами (Packet Control Unit, PCU) и дополнительные логические каналы для обслуживания трафика данных.

2. Применены 4-е новые схемы кодирования данных на радио интерфейсе:

CS-1 со скоростью передачи данных 9,05 Кбит/с и коррекцией ошибок;

CS-2 со скоростью передачи данных 13,4 Кбит/с и коррекцией ошибок;

CS-3 со скоростью передачи данных 15,6 Кбит/с и коррекцией ошибок;

CS-4 со скоростью передачи данных 21,4 Кбит/с без коррекции ошибок.

3. Добавлены устройства:

сервисный узел поддержки (**S**erving **G**PRS **S**upport **N**ode, **SGSN**) с функциями схожими с MSC/VLR, но для пакетного трафика;

шлюз с внешними сетями (**G**ateway **G**PRS **S**upport **N**ode, **GGSN**) с функциями схожими с GMSC, но для пакетного трафика;

сервер доменных имен DNS устанавливается на интерфейсе Gn (на рисунке не показан).

4. Добавлены интерфейсы, которые занимаются только при передаче данных:

Gb – между SGSN и BSC;

Gd – между SGSN и SMSC;

Gn – между SGSN и GGSN;

Gr – между SGSN и HLR;

Gs – между SGSN и MSC/VLR;

Gc – между GGSN и HLR;

Gi – между GGSN и Internet.

5. Модифицировано сетевое устройство HLR для хранения местоположения абонента и профайла абонента с данными для его обслуживания в подсистеме GPRS.

В результате в узле коммутации мобильных абонентов образовалось два независимых домена: домен, осуществляющий коммутацию каналов (Circuit Switched domain, CS-домен) и домен, осуществляющий коммутацию пакетов (Packet Switched domain, PS-домен).

SGSN выполняет функции аналогичные функциям MSC/VLR: регистрацию, аутентификацию, шифрование, широковещательный поиск, установление соединений для передачи/приема данных.

GGSN выполняет функции аналогичные функциям GMSC, взаимодействие по Gn и Gi интерфейсам происходит на основе IP-протоколов.

Пути прохождения трафика речи данных различны: речевой трафик проходит по цепочке BTS-BSC-TRAU-MSC/VLR-GMSC-ISDN, а данные (Packet Data Unit, PDU) проходят по цепочке BTS-BSC-PCU-SGSN-GGSN-Internet. Теоретически объединением 8-и радиоканалов скорость передачи данных возрастает до 21,4x8=171,2 Кбит/с. Однако, большинство современных телефонов поддерживают объединение только 4-х радиоканалов, что снижает скорость до 85,6 Кбит/с.

Для передачи речи и данных используются одни и те же радиоканалы, но речевой трафик имеет абсолютный приоритет перед трафиком данных, поэтому при передаче данных возможно возникновение очереди.

Оконечное устройство с функциями GPRS и SGSN могут находиться в одном из трех состояний (***3GPP TS 23.060*** [89]): СВОБОДНО (IDLE), ГОТОВНОСТЬ (READY) и ОЖИДАНИЕ (STANDBY). Диаграмма переходов состояний приведена на рис. 3.20.

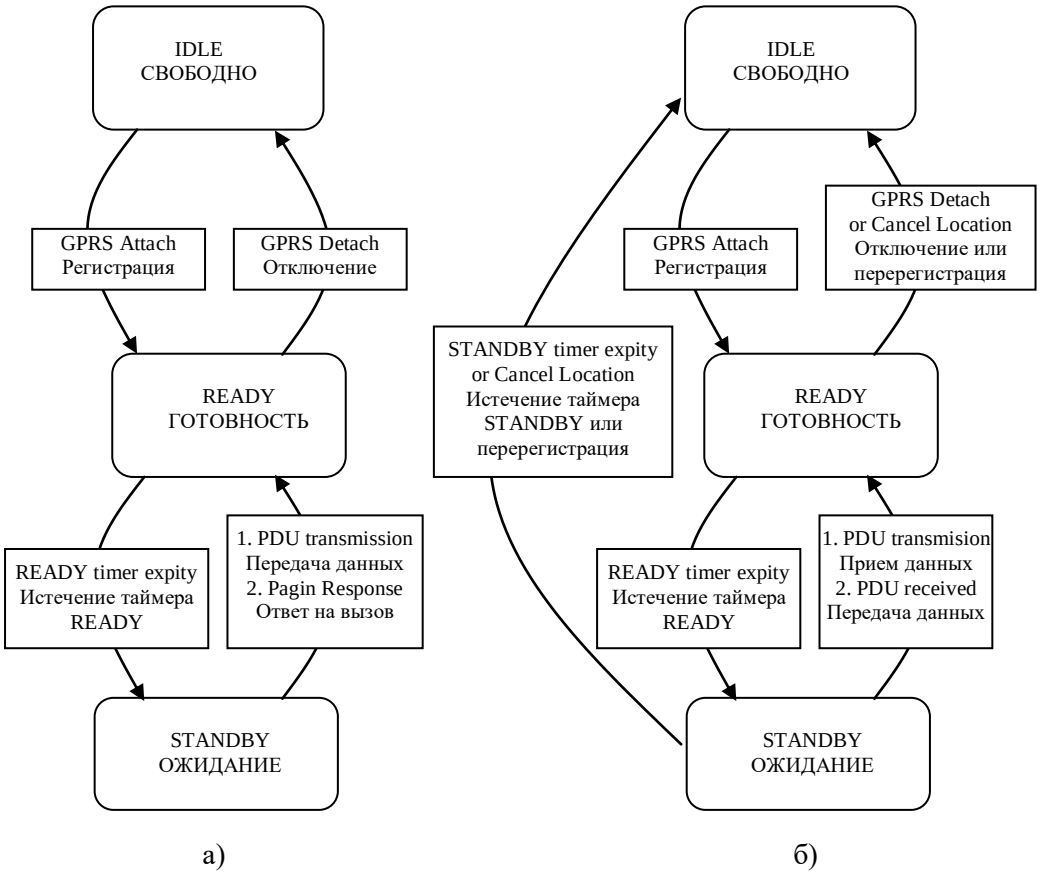

Рис.3.20. Диаграмма переходов состояний
а)GPRS_MS, б)SGSN

В состоянии СВОБОДНО подсистеме GPRS ничего не известно о MS. Передача и прием данных невозможны. Для осуществления связи MS должна пройти процедуру регистрации (GPRS Attach). В результате регистрации HLR становится известен номер SGSN, где находится мобильный абонент.

В состоянии ГОТОВНОСТЬ оконечное устройство имеет активный PDP-контекст, позволяющий осуществлять прием/передачу данных. PDP-контекст содержит IP-адрес мобильного абонента, параметры качества обслуживания (QoS профайл), параметры ограничения связи, IP-адрес GGSN.

В состоянии ОЖИДАНИЕ SGSN известно местоположение мобильного абонента. Оконечное устройство и GGSN не имеют активный PDP-контекст, не может передавать данные, может принимать широковещательный поиск с последующей активацией PDP-контекста для приема данных.

3.4.2. Обеспечение качества обслуживания

В GPRS определены 4 параметра для управления качеством обслуживания (Quality of Service, QoS) мобильного абонента (***3GPP TS 22.060*** [85]): приоритет обслуживания, надежность доставки, задержку доставки, скорость передачи.

Приоритеты имеют три класса: высокий, нормальный и низкий. При перегрузке сети пакеты с более низким приоритетом могут быть отброшены.

- Пакеты с высоким приоритетом имеют преимущество над всеми другими пакетами.
- Пакеты с нормальным приоритетом имеют преимущество перед пакетами с низким приоритетом.
- Пакеты с низким приоритетом обслуживаются после пакетов с высоким и нормальным приоритетами.

Надежность доставки разделяется на три класса в зависимости от заданной вероятности потери пакета, вероятности нарушения очередности доставки, вероятности повреждения пакета. Для первого класса вероятность равна E-9, а для третьего класса вероятность равна E-2.

Задержка доставки измеряется на участке между MS и Gi-интерфейсом. Значения задержек приведены в табл. 3.1.

Табл. 3.1. Значения задержек в GPRS

Класс задержки	Максимальное значение задержки (в секундах)			
	Длина пакета до 128 байт		Длина пакета до 1024 байт	
	Среднее значение	С вероятностью 0.95	Среднее значение	С вероятностью 0.95
1	< 0.5	< 1.5	< 2	< 7
2	< 5	< 25	< 15	< 75
3	< 50	< 250	< 75	< 375
4	Не определено			

Передача данных в GPRS происходит только при наличии свободных от речи каналов и зависит от загрузки радиоканалов трафиком речи и данных. По этой причине скорость передачи данных может варьироваться в широких пределах.

ВОПРОСЫ К РАЗДЕЛУ 3.4

1. Какая максимальная скорость передачи данных в подсистеме GSM?

Ответ. 9,6 Кбит/с.

2. Назовите способ увеличения скорости передачи данных на одном радиоканале в подсистеме GPRS.

Ответ. Применение новых способов кодирования CS-2, CS-3, CS-4.

3. Назовите способ увеличения скорости передачи данных в подсистеме GPRS.

Ответ. Предоставление пользователю на время сеанса связи нескольких (до 8) радиоканалов.

4. Назовите основные устройства подсистемы GPRS.

Ответ. Сервисный узел поддержки SGSN, шлюз с внешними сетями GGSN.

5. Назовите интерфейсы подсистемы GPRS.

Ответ. Gb – между SGSN и BSC, Gd – между SGSN и SMSC, Gn – между SGSN и GGSN, Gr – между SGSN и HLR, Gs – между SGSN и MSC/VLR, Gc – между GGSN и HLR, Gi – между GGSN и Internet.

6. Где хранится профайл пользователя?

Ответ. В HLR.

7. Что содержится в профайле пользователя?

Ответ. Данные о местоположении мобильного абонента и PDP-контекст.

8. Что содержится в PDP-контексте пользователя?

Ответ. Тип запрашиваемого IP-адреса, значение IP-адреса, параметры качества обслуживания, IP-адрес GGSN.

9. Назовите основную функцию Gs интерфейса.

Ответ. Gs интерфейс используется для синхронизации данных между MSC/VLR и SGSN о местоположении мобильной станции MS.

10. Какое устройство инициирует активацию PDP-контекста при исходящем соединении?

Ответ. Оконечное устройство MS.

11. Какое устройство инициирует активацию PDP-контекста при входящем соединении?

Ответ. Сеть (GGSN).

12. Как называется радио интерфейс между MS и BTS в сети связи второго поколения (2G)?

Ответ. Um.

13. Какая максимальная скорость передачи данных в подсистеме GPRS?

Ответ. 171,2 Кбит/с.

3.5. Сотовая наземная сеть связи мобильных абонентов третьего поколения. Стандарт UMTS

Все возрастающие запросы мобильных пользователей и популярность Internet требуют все большей скорости обмена информацией. Наиболее узким местом является скорость обмена на радио интерфейсе. Поэтому дальнейшее развитие сети связи мобильных абонентов идет в направлении поиска повышения скорости обмена на радио интерфейсе, обеспечивающей более высокую скорость, чем позволяет подсистема GPRS (171,2 Кбит/с). Это достигнуто в сети третьего поколения (3G) – Универсальной Мобильной Телекоммуникационной Системе (**U**niversal **M**obile **T**elecommunications **S**ystem, **UMTS**), которая на сети радиодоступа (**U**niversal **T**errestrial **R**adio **A**ccess **N**etwork, **UTRAN**) использует множественный доступ с кодовым разделением (**C**ode **D**ivision **M**ultiple **A**ccess, **CDMA**).

3.5.1. Структура сети 3G

Подсистема UMTS должна быть обратно совместима с уже существующими подсистемами GSM и GPRS. Для обеспечения новых функций в узле коммутации произошли следующие изменения (рис. 3.21).

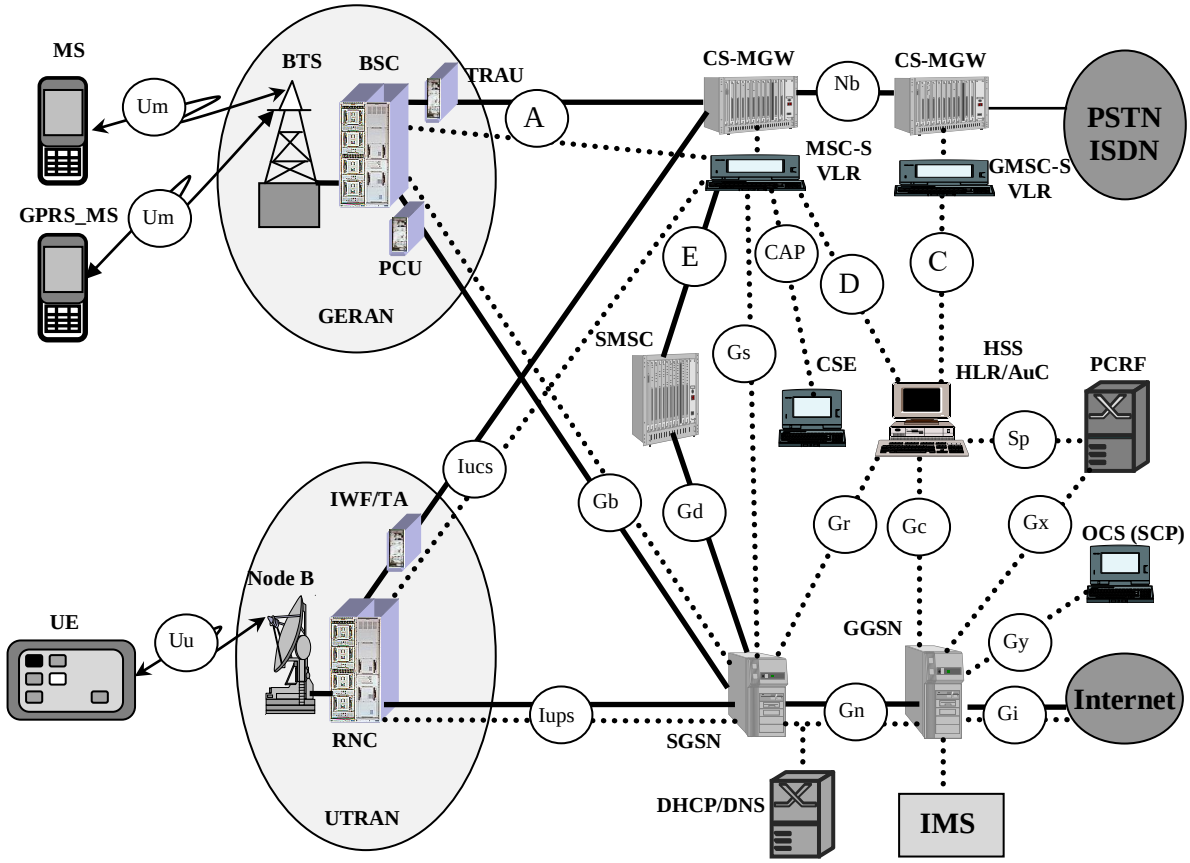

Рис. 3.21. Архитектура сети UMTS

- служебные сообщения (Control Plane)

- трафик пользователя (User Plane)

1. Добавлена новая радио подсистема **UTRAN**, включающая в себя

радио приемо/передатчики Node B с радио интерфейсом Uu и функциями аналогичными BTS;

контроллеры радио приемо/передатчиков (**R**adio **N**etwork **C**ontroller, **RNC**), с функциями аналогичными BSC;

транскодеры (Interworking Function/Transcoder IWF/TA), с функциями аналогичными TRAU и PCU.

2. Произошла модификация и объединение подсистем HLR и AuC в единую подсистему HSS (**H**ome **S**ubscriber **S**erver, HSS).

3. В CS-домене:

произошло разделение MSC/VLR на подсистему коммутации каналов (Cirquit Switching Media Gateway, CS-MGW) и подсистему управления (Mobile Switching Center Server/Visitor Location Register, MSC-S/VLR) с Mc-интерфейсом между ними.

4. В PS-домене:

добавлен интерфейс Iucs (GTP-U/RANAP) между RNC и CS-MGW/MSC-S для взаимодействия радио подсистемы UMTC с CS-доменом коммутации каналов (Circuit Switched Domain, CS-domain);

добавлен интерфейс Iups (GTP-U/RANAP) между RNC и SGSN для взаимодействия радио подсистемы UMTC с PS-доменом коммутации пакетов (Packet Switched Domain, PS-domain);

добавлена подсистема политики и начисления стоимости (Policy and Charging Rules Function, PCRF), которая по интерфейсу Gx управляет устройством реализации начисления стоимости (Policy and Charging Enforcement Function, PCEF), расположенным в GGSN;

добавлена подсистема состояния счета пользователей (Online Charging System, OCS), аналогичная CSE в CS-домене;

добавлен сервер динамической конфигурации мобильного оборудования (DHCP) и сервер доменных имен (DNS);

добавлена подсистема передачи мультимедийной информации на основе IP-протокола (**I**P **M**ultimedia Core Network **S**ubsystem, **IMS**).

В UMTS оконечное оборудование пользователя (**U**ser **E**quipment, **UE**) состоит из двух отдельных частей — мобильного оборудования (**M**obile **E**quipment, **ME**) и универсальной интегральной карты (**U**niversal **I**ntegrated **C**ircuit **C**ard, **UICC**). Мобильное оборудование ME состоит из мобильного окончания (MT) для взаимодействия по радио интерфейсу и терминального окончания TE для отображения информации на дисплее. Универсальная интегральная карта UICC содержит идентификационную абонентскую SIM-карту (**U**MTS **S**ervice **I**dentity **M**odule, **USIM**) и опционально идентификационный модуль интернет-услуг (**IMS I**dentity **M**odule, **ISIM**). В ISIM хранятся закрытый (Private User Identity, IMPI) и открытый (Public User Identity, IMPU) идентфикаторы пользователя.

В UMTS допустимо вместо обозначения UE использовать MS, а вместо HSS – HLR.

3.5.2. Сеть радиодоступа UTRAN

Все предыдущие методы использования радиоканалов сводились к предоставлению пользователю ограниченного (одного или нескольких) временных интервалов (тайм слотов), иначе говоря, части скорости радио интерфейса. В UMTS используется новая сеть радиодоступа (**U**niversal **T**errestrial **R**adio **A**ccess **N**etwork, **UTRAN**) использующая множественный доступ с кодовым разделением (**C**ode **D**ivision **M**ultiple **A**ccess, **CDMA**).

Идеология множественного доступа с кодовым разделением предполагает предоставление одновременно многим пользователям всю скорость радио интерфейса. Существо состоит в следующем (рис. 3.22).

Каждому пользователю на время сеанса связи выделяется уникальный код, например, 10101100. Каждый передаваемый в радиоканал бит складывается по модулю 2 (операция XOR) с уникальным кодом. На приеме каждый принимаемый из радиоканала бит складывается по модулю 2 (операция XOR) с тем же уникальным кодом. Правило сложения по модулю 2: $0 \oplus 0=0$, $0 \oplus 1=1$, $1 \oplus 0=1$, $1 \oplus 1=0$. Если бит пользователя имеет значение “1” (рис. 3.22а), а уникальный код имеет значение 10101100 (3.22б,г), то в канал будет передана последовательность 01010011 (рис. 3.22в) и прийта “1” (рис. 3.22д). Если бит имеет значение “0”, то имеет место рис. 3.22е-к.

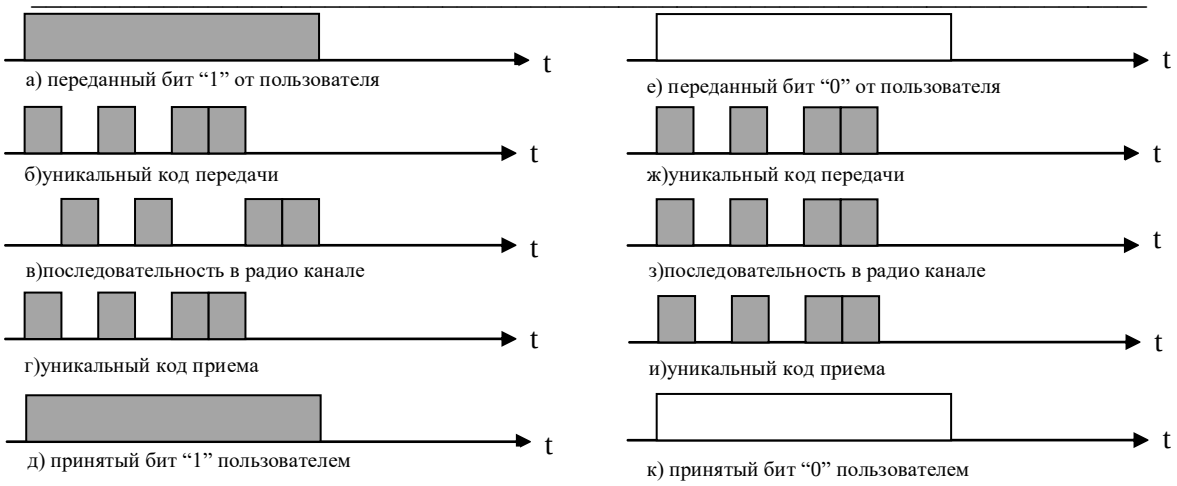

Рис. 3.22. Кодирование информации пользователя в радиоканале

Таким образом, 1 бит пользователя в нашем случае передается 8-ю битами в радиоканале. Если в цикле содержится 16 тайм слотов по 8 бит каждый, то каждый из 16-и пользователей в подсистеме GSM/GPRS получит только 8 бит на передачу. В подсистеме UMTS при уникальном коде из 8-и бит каждый из 16-и пользователей получит все 16 тайм слотов, т.е. 16 бит, что в два раза больше. Однако есть нюансы.

Предположим, что сеанс связи ведут два пользователя (рис.3.23).

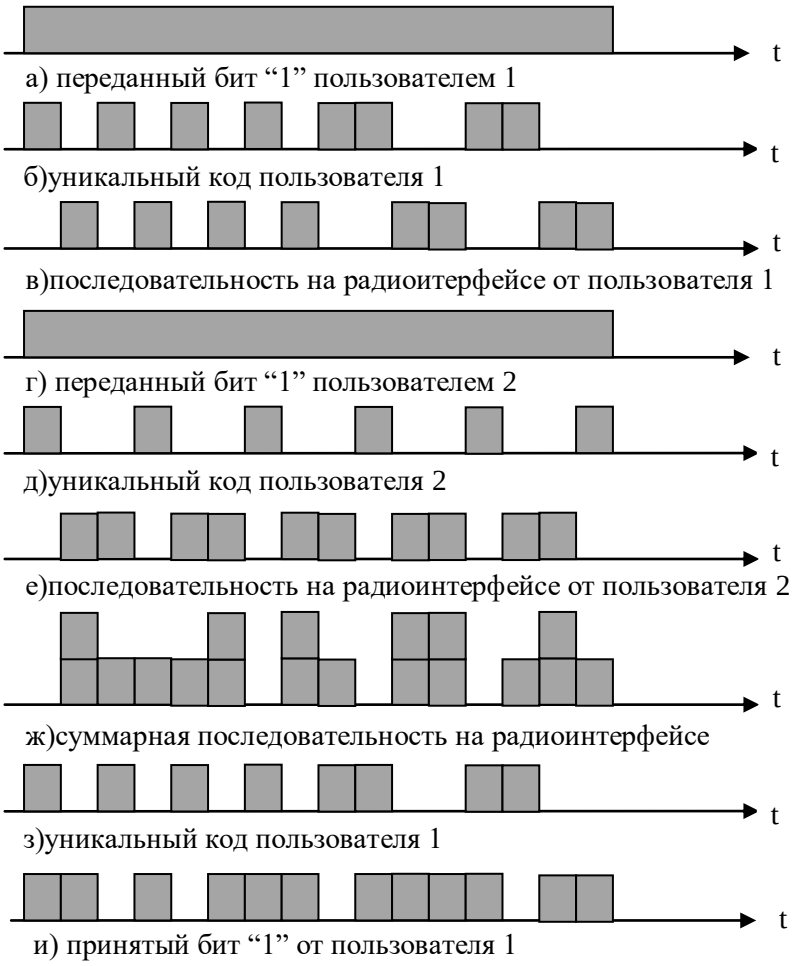

Рис. 3.23. Искажения принимаемого сигнала

Оба пользователя передают бит со значением “1”, первый пользователь имеет уникальный код 1010101011001100, второй пользователь имеет уникальный код 1001001001001001. Используется простая амплитудная модуляция. На рис. 3.23 показаны сигналы на радио интерфейсе от каждого пользователя (рис. 3.23в,е) и суммарный радиосигнал (рис. 3.23ж). Видно, что принятый от пользователя 1 бит “1” (рис. 3.23и) искажен из-за помех от второго пользователя, но из-за преобладания единиц распознается как “1”. Следовательно, для устойчивой работы с CDMA необходимо: иметь сильно отличающиеся друг от друга “длинные” уникальные коды; ограничивать мощность радиоизлучения; совершенствовать способы модуляции.

К настоящему времени разработаны способы модуляции, минимизирующие влияние помех пользователей друг на друга. Типовая скорость в подсистеме UMTS составляет 384 Кбит/с. Технология высокоскоростной пакетной передачи данных от базовой станции к пользователю (**H**igh-**S**peed **D**ownlink **P**acket **A**ccess, **HSDPA**) предусматривает выделение пользователю нескольких уникальных кодов, что позволило к настоящему времени теоретически повысить скорость передачи до 14 Мбит/с. Оконечные устройства третьего поколения характеризуется максимальным числом одновременно используемых кодов и типом модуляции в радиоканале. Последние версии реализации (Release) используют квадратурную амплитудную модуляцию (Quadrature Amplitude Modulation, QAM) и используют до 15 уникальных кодов.

3.5.3. Идентификация и адресация в сети 3G

В сети UMTS используется ряд необходимых идентификаторов (***3GPP TS 23.003*** [88]).

Для первоначальной идентификации абонента сети мобильной связи используется международный идентификатор мобильного абонента (**I**nternational **M**obile **S**ubscriber **I**dentity, **IMSI**):

$$IMSI = MCC + MNC + MSIN,$$

где MCC – код страны, MNC – код сети мобильных абонентов, MSIN – мобильный идентификатор абонента. IMSI хранится в USIM и HSS и используется для вычисления адреса к базе данных абонента (HSS), где хранится профайл абонента.

Для конфиденциальности идентификатора IMSI при каждом последующем сеансе связи используются временные идентификаторы (**T**emporary **M**obile **S**ubscriber **I**dentity, **TMSI**) в CS-домене и **P-TMSI** в PS-домене:

$$TMSI = LAI + TIC, \qquad P\text{-}TMSI = RAI + TIC,$$

где LAI – код зоны, RAI – код зоны маршрутизации, TIC – выбирается из пула (хранилища) VLR и имеет длину 4 байта. Хранится в USIM и VLR.

Для установления соединения к абоненту сети мобильной связи через CS-домен используется международный номер мобильного абонента (**M**obile **S**ubscriber International **ISDN** Number, **MSISDN**):

$$MSISDN = CC + NDC + SN,$$

где CC – код страны, NDC – национальный код пункта назначения, SN – номер абонента. Для разделения услуг пользователя используются различные MSISDN, один MSISDN для телефонии, второй – для факса, третий – для передачи данных и т.д. Хранится в USIM и HLR.

Для установления соединения к абоненту сети мобильной связи через PS-домен используется адрес PDP-контекста, который представляет собой IP-адрес мобильного абонента и обычно хранится в HLR.

Для идентификации мобильного оборудования применяется международный идентификатор мобильного оборудования (**I**nternational **M**obile **E**quipment **I**dentity,

IMEI), который из-за частой смены пользователями мобильных устройств применяется редко.

Для определения местоположения пользователя используется идентификатор зоны (**L**ocation **A**rea **I**dentity, **LAI**):

LAI = MCC + MNC + LAC

где MCC – код страны, MNC – код сети мобильных абонентов, LAC – код зоны.

В IMS используется адресация, принятая в IP-сети вида *username@realm*. Имя домена домашней сети *realm*, где находится HSS, хранится в ISIM или вычисляется USIM из IMSI в виде:

realm=ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org,

где MCC – 3-х значный код страны, MNC – 3-х значный код сети мобильных абонентов. Например, если IMSI=234150999999999, то доменное имя домашней сети ims.mnc015.mcc234.3gppnetwork.org.

Закрытый идентификатор пользователя (IP Multimedia Privite Identity, IMPI) используется для регистрации, авторизации и учета стоимости услуг. Если пользователь не имеет ISIM, то он вычисляется USIM из IMSI в виде:

<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org,

где MCC – 3-х значный код страны, MNC – 3-х значный код сети мобильных абонентов. Например, если IMSI=234150999999999, то закрытый идентификатор пользователя 234150999999999@ims.mnc015.mcc234.3gppnetwork.org.

Открытый идентификатор пользователя (IP Multimedia Public Identity, IMPU) используется для адресации (установления соединения) к пользователю. Если пользователь не имеет ISIM, то он вычисляется USIM из IMSI в виде:

sip:<IMSI>@ims.mnc<MNC>.mcc<MCC>.3gppnetwork.org,

где MCC – 3-х значный код страны, MNC – 3-х значный код сети мобильных абонентов. Например, если IMSI=234150999999999, то закрытый идентификатор пользователя sip:234150999999999@ims.mnc015.mcc234.3gppnetwork.org.

3.5.4. Обеспечение безопасности сети

Для повышения уровня безопасности на радиоканале вместо триплетов, используемых в 2G-сети, используются квинтеты (векторы аутентификации). Квинтет состоит из пяти параметров (***3GPP TS 33.102*** [90]):

- случайного числа RAND (128 бит);
- ожидаемого ответа XRES, полученного перемешиванием случайного числа RAND с секретным ключом K (128 бит) по алгоритму f2. Значение ключа никогда не передается по сети и неизвестно пользователю;
- ключа шифрования CK (128 бит), полученного перемешиванием случайного числа RAND с секретным ключом K по алгоритму f3, который используется для шифрования информации пользователя в радиоканале;
- ключа целостности IK (128 бит), полученного перемешиванием случайного числа RAND с секретным ключом K по алгоритму f4, который используется для шифрования сигнальных сообщений в радиоканале;
- анонимного ключа AUTH, полученного перемешиванием административной функцией AMF, порядкового номерам SQN, случайного числа RAND с секретным ключом K по алгоритму f5.

Выбор алгоритмов f1-f5 осуществляется оператором домашней сети и используются в HSS и в модуле USIM.

Безопасность на радио интерфейсе сети UMTS без подсистемы IMS во многом аналогична процедуре в сети GSM, и обеспечивается процедурой аутентификации и согласования ключей (**A**uthentication and **k**ey **A**greement, **AK**A), которая состоит в следующем (рис.3.24).

SGSN инициирует функции безопасности (Security function) используя процедуру AKA:

1. SGSN вычисляет из IMSI адрес HSS и запрашивает у него аутентификационные вектора (квинтеты).

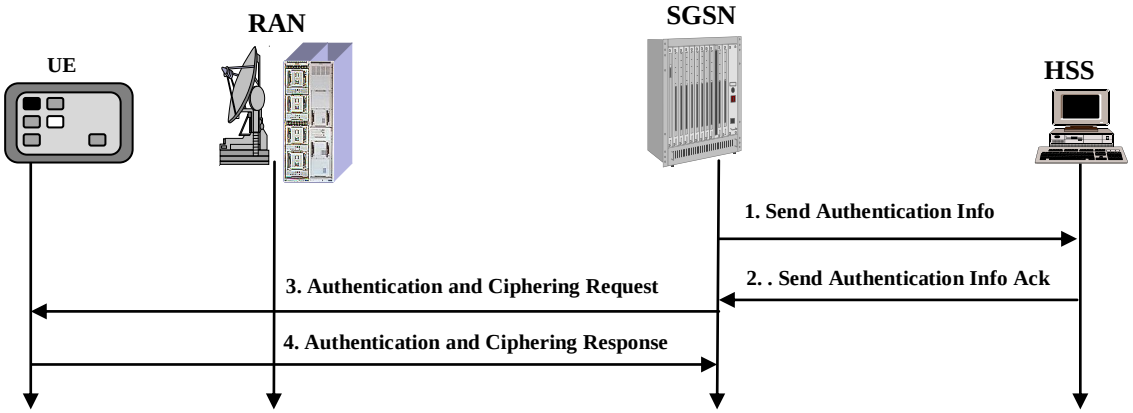

Рис. 3.24. Процедура AKA

2. При получении запроса (Send Authentication Info) HSS генерирует несколько (обычно 5) квинтетов и высылает их SGSN (Send Authentication Info Ack). Каждый квинтет содержит RAND, XRES, AUTN, CK и IK.

3. SGSN сохраняет ключ шифрования CK и ключ целостности IK у себя, а случайное число RAND и анонимный ключ AUTH прозрачно через радио подсистему RAN посылает в UE.

4. При получении сообщения Authentication and Ciphering Request (RAND, AUTN) UE извлекает SQN из AUTH и проверяет его корректное значение; используя RAND вычисляет значение XRES; высылает ответ Authentication and Ciphering Response (IMSI, XRES) SGSN. SGSN производит сравнение XRES, полученного от UE со значением XRES, полученного от HSS. При их совпадении регистрация считается успешной. UE также вычисляет новые значения CK и IK, которые будут использованы до следующей процедуры AKA.

Безопасность в IP-сети обеспечивается протоколами AH и IPsec подробно рассмотренными в разделе 2.6.

3.5.5. Регистрация мобильных абонентов

Аналогично абоненту GSM мобильная станция UE должна пройти регистрацию (***3GPP TS 23.060*** [89]). *Комбинированная регистрация* (Combined GPRS/IMSI Attach) происходит с точностью до зоны маршрутизации (Routeing Area Identity, RAI), состоящей из кода зоны LAI и кода нескольких близлежащих сот в зоне (Routeing Area Code, RAC). При регистрации используются только сигнальные сообщения, прозрачно проходящие через RAN. Для оконечного устройства класса A или B происходят следующие события (рис. 3.25).

1. UE находится в состоянии СВОБОДНО и посылает запрос на регистрацию. В запросе указывается:

- IMSI (при начальной регистрации) или P-TMSI при перерегистрации. В последнем случае MS присылает RAI предыдущего местоположения;
- Classmark – возможности MS по количеству объединения радиоканалов, способы шифрования;
- тип регистрации – в подсистеме GPRS или в GPRS/GSM.

2. В случае перерегистрации новый (текущий) SGSN запрашивает оставшиеся квинтеты у старого (прежнего) SGSN. Адрес старого SGSN новый SGSN высчитывает через P-TMSI.

3. Если SGSN неизвестен P-TMSI, то SGSN запрашивает у UE IMSI и получает его.

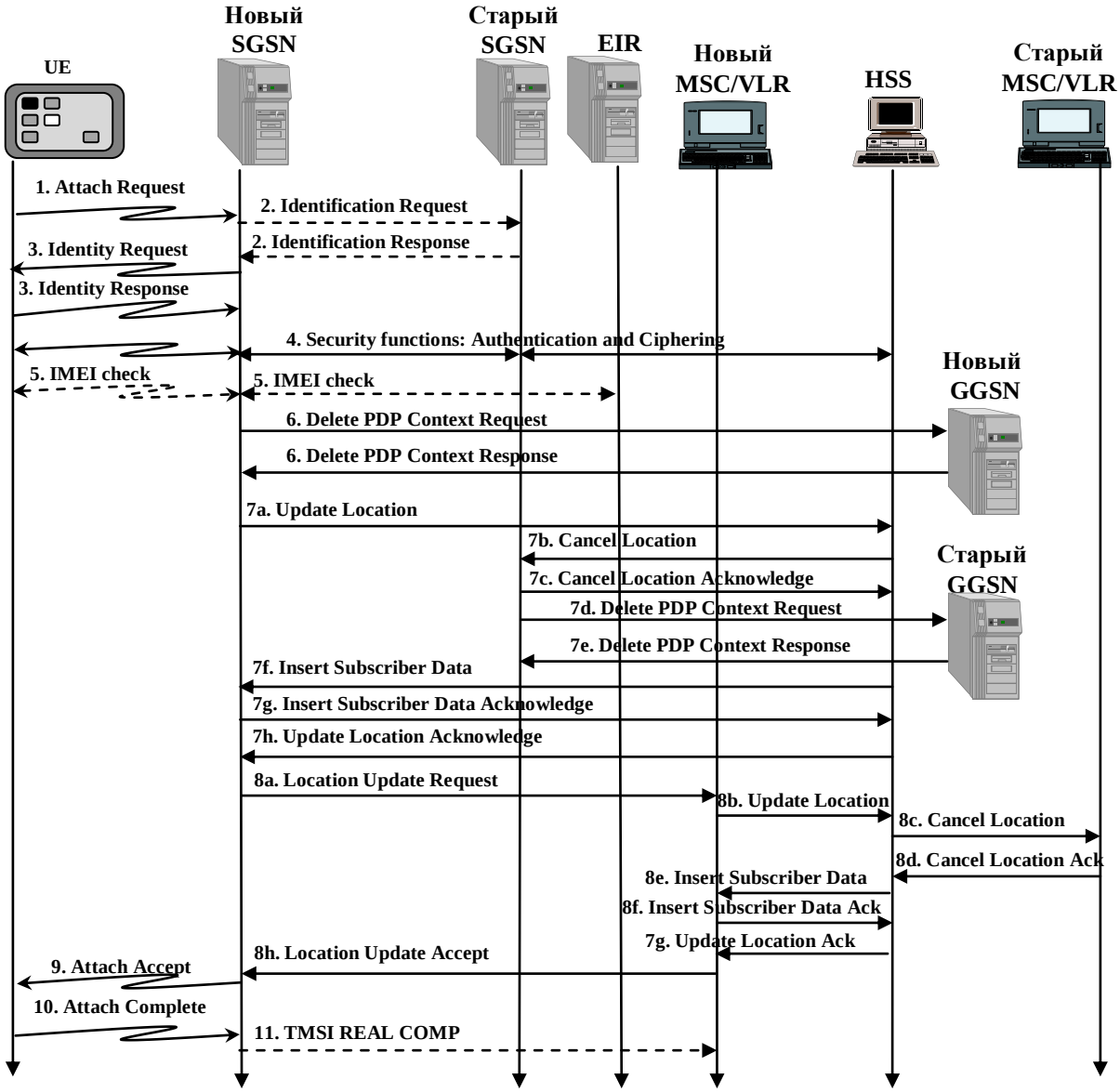

Рис. 3.25. Регистрация UE

4. SGSN инициирует функции безопасности (процедуру AKA, рис. 3.24).

5. Опционально SGSN может проверить не внесен ли MS в “черный список” в регистре идентификации мобильного оборудования (Equipment Identity Register, EIR). EIR хранит записи, например, похищенных UE в виде международных идентификаторов мобильного устройства (International Mobile Equipment Identity, IMEI).

6. Если у нового SGSN имеется сохраненный ранее активный PDP-контекст, то он инициализирует его уничтожение в GGSN.

7. SGSN инициирует регистрацию мобильной станции:

7a. Высылает заявку в HSS на регистрацию с указанием своего номера, адреса и IMSI мобильной станции.

7b. HSS извещает старый SGSN об уничтожении профайла мобильного абонента.

7c. HSS получает подтверждение об уничтожении профайла мобильного абонента.

7d. Если у старого SGSN имеется сохраненный ранее активный PDP-контекст, то он инициализирует его уничтожение в GGSN.

7e. Старый GGSN подтверждает уничтожение PDP-контекста.

7f. HSS высылает профайл абонента с PDP-контекстом новому SGSN.

7g. SGSN подтверждает получение данных.

7f. HSS завершает сеанс связи с SGSN.

8. SGSN по Gs интерфейсу извещает VLR о необходимости регистрации UE. Для вычисления адреса VLR новый SGSN использует RAI. Следуют события:

8a. SGSN высылает VLR новый LAI, свой номер, свой адрес и IMSI мобильной станции.

8b. VLR инициирует регистрацию UE в HSS.

8c. HSS извещает старый VLR об уничтожении данных мобильного абонента.

8d. HSS получает подтверждение об уничтожении данных мобильного абонента.

8e. HSS высылает данные абонента новому VLR.

8f. VLR подтверждает получение данных.

8g. HSS завершает сеанс связи с VLR.

8h. Новый VLR завершает сеанс связи с SGSN присвоением TMSI (VLR TMSI).

9. SGSN посылает UE подтверждение регистрации (P-TMSI, VLR TMSI).

10. UE подтверждает получение (P-TMSI, VLR TMSI).

11. SGSN уведомляет VLR, если VLR TMSI был изменен.

UE и SGSN переходят в состояние ГОТОВНОСТЬ. Теперь UE может активировать PDP-контекст. Если в течение таймаута READY (обычно несколько минут) UE не проявит никакой активности (инициализацию передачи данных), то UE и SGSN переходят в состояние ОЖИДАНИЕ, не активные PDP-контексты имеют UE, SGSN и GGSN.

3.5.6. Установление исходящего соединения в UMTS

Установление исходящего соединения данных приведено на рис. 3.26 (***3GPP TS 23.060*** [89]). UE и SGSN находятся в состоянии ОЖИДАНИЕ и не имеют активных PDP-контекстов.

1. UE посылает запрос на установление радиоконтакта (Radio Resource Control, RRC) и получает ответ.

2. UE посылает запрос на обслуживание (Service Request). Запрос содержит:

- временный идентификатор P-TMSI;
- код зоны маршрутизации RAI;
- тип запрашиваемой услуги (Service Type). В случае запроса передачи данных в запросе содержится информация о PDP-контексте на стороне UE.

3. SGSN инициирует функцию безопасности.

4. UE посылает SGSN запрос на активацию PDP-контекста. Запрос содержит:

- тип запрашиваемого адреса (PDP Type) – IP-адрес версии 4 или 6;
- значение адреса (PDP-address) – пустое поле, заполняемое GGSN;
- профайл качества обслуживания (QoS Profile) – приоритет обслуживания, задержку обслуживания, вероятность потерь, пиковую скорость передачи, среднюю скорость передачи.

5. SGSN анализирует поступившую информацию, пересылает запрос в GGSN и получает подтверждение.

6. SGSN высылает RNC запрос на выделение радио ресурса (Radio Access Bearer Assignment Request). Запрос содержит описание запрашиваемых параметров PDP-контекста. RNC прозрачно транслирует запрос UE.

7. UE принимает и возвращает SGSN реально возможные параметры на радио интерфейсе и устанавливает тоннель между UE и SGSN. Если от RNC получен отрицательный ответ, то SGSN может повторить запрос на выделение радио ресурса (пункт 5) с другим QoS-профайлом (по усмотрению оператора).

8. Установленный QoS-профайл UE высылает SGSN.

9. Если первоначальные параметры PDP-контекста были изменены, то SGSN извещает об этом GGSN.

10. SGSN подтверждает UE активизацию PDP-контекста. UE и SGSN переходят в состояние ГОТОВНОСТЬ.

11. UE посылает пакет данных в IP-сеть.

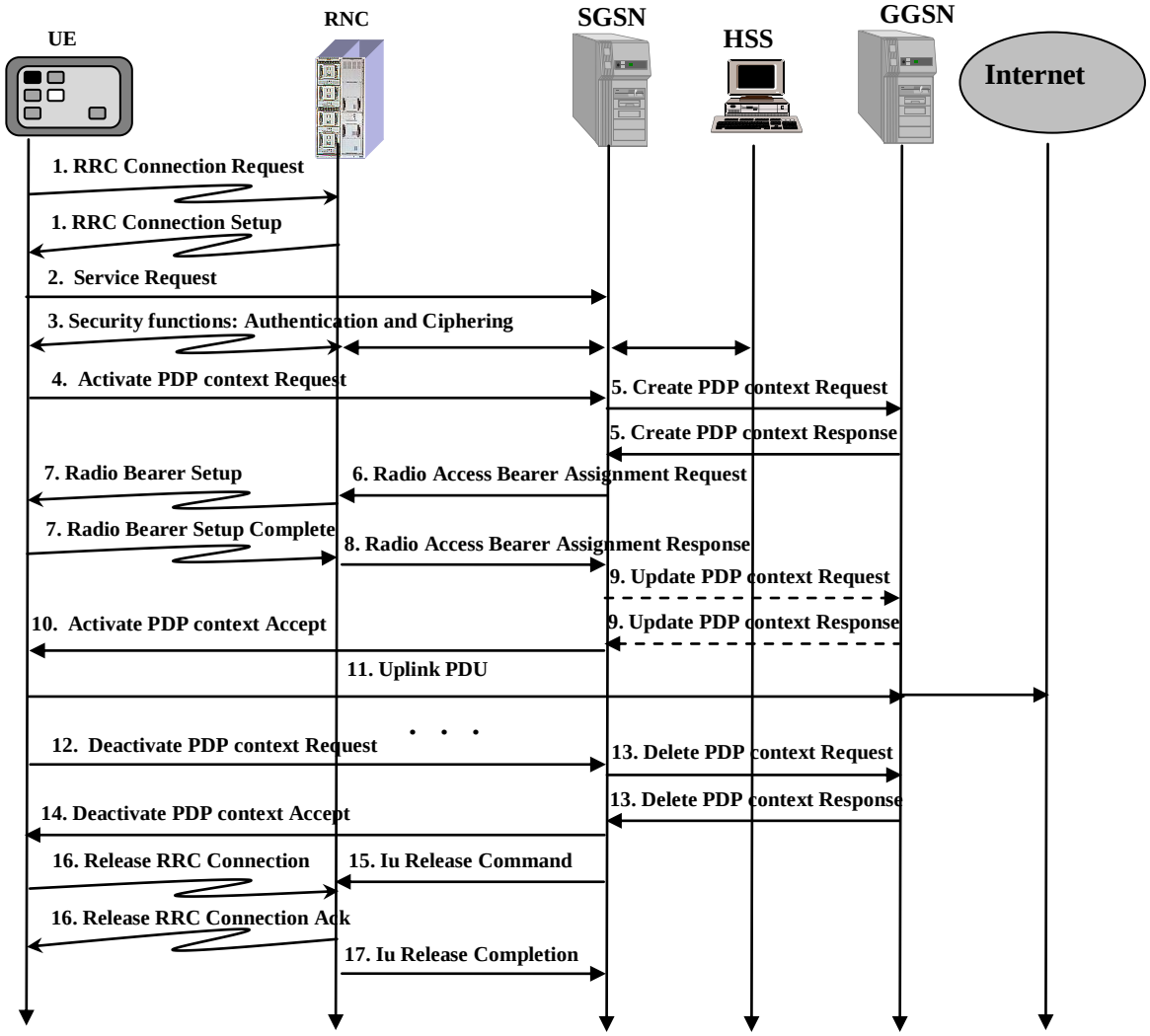

Рис. 3.26. Исходящее соединение

12. При окончании сеанса связи UE посылает SGSN запрос на дезактивацию PDP-контекста (Deactivate PDP context Request). Запрос может инициировать и RNC в случае длительной неактивности пользователя.

13. SGSN пересылает запрос в GGSN и получает подтверждение.

14. SGSN подтверждает дезактивацию PDP-контекста UE.

15-17. SGSN инициирует разрушение радиосоединения.

3.5.7. Установление входящего соединения в UMTS

Установление входящего соединения данных приведено на рис. 3.27. UE и SGSN находятся в состоянии ОЖИДАНИЕ и не имеют активных PDP-контекстов.

1. Из Internet поступает пакет данных в GGSN.

2. GGSN обращается к HSS за маршрутной информацией (sendRoutingInfo). В запросе содержатся (IMSI, адрес SGSN, доступность UE). HSS возвращает запрошенную информацию.

3. GGSN по полученному адресу SGSN рассылает широковещательный поиск UE с точностью до зоны маршрутизации (RAI). В сообщении Paging присутствует выделенный для UE IP-адрес и тип услуги (Service Type). SGSN прозрачно через радио подсистему пересылает уведомление UE.

4-13. Происходят действия аналогичные процессу установления исходящего соединения с п.1 – 10.

14. GGSN посылает пакет данных в UE.

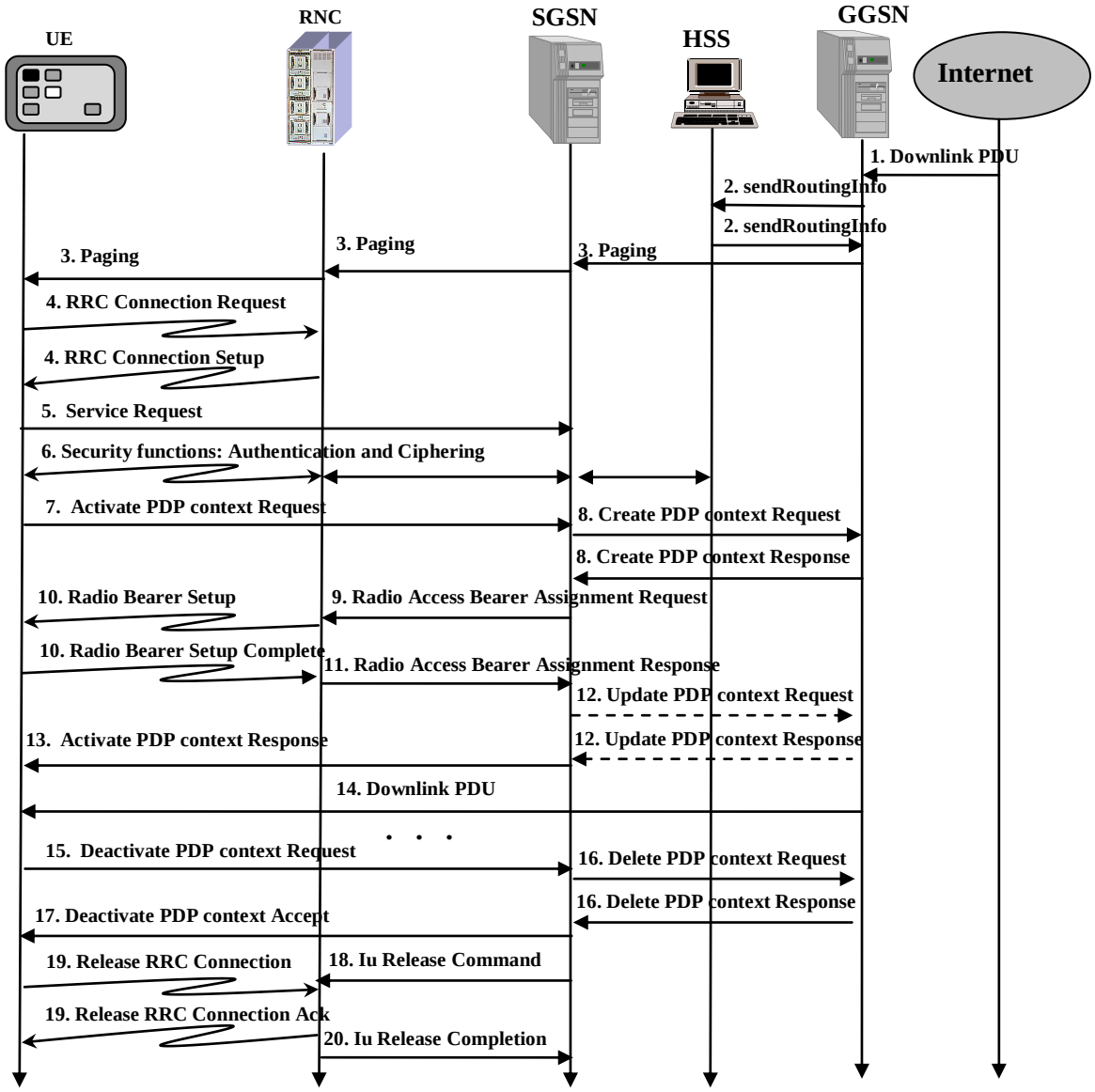

Рис. 3.28. Входящее соединение

15-20. Завершение входящего соединения аналогично процессам, рассмотренным при установлении исходящего соединения.

ВОПРОСЫ К РАЗДЕЛУ 3.5

1. В чем существо множественного доступа с кодовым разделением (CDMA)?

Ответ. Предоставление всем пользователям всю скорость радио интерфейса.

2. Назовите причину различных скоростей в восходящем (Uplink) и нисходящем (Downlink) направлениях.

Ответ. Запрос (Uplink) обычно содержит гораздо меньше информации (бит), чем ответ (Downlink).

3. Назовите технологию увеличения скорости в нисходящем (Downlink) направлении в подсистеме UMTS.

Ответ. Технология высокоскоростной пакетной передачи данных от базовой станции к пользователю (High-Speed Downlink Packet Access, HSDPA).

4. Поясните принцип технологии высокоскоростной пакетной передачи данных (HSDPA) в UMTS.

Ответ. Предоставление пользователю нескольких уникальных кодов.

5. Назовите интерфейсы радио подсистемы UMTS.

Ответ. Iucs между RNC и IWF/TA для взаимодействия радио подсистемы UMTC с доменом коммутации каналов (CS-Domain) и Iups между RNC и SGSN для взаимодействия радио подсистемы UMTC с доменом коммутации пакетов (PS-Domain).

6. Какова типовая скорость передачи в подсистеме UMTS?

Ответ. 384 Кбит/с.

7. Какова теоретически максимальная скорость передачи в подсистеме UMTS?

Ответ. 21 Мбит/с.

11. Как называется радио интерфейс между MS и RNC в сети связи третьего поколения (3G)?

Ответ. Uu.

12. Назовите состав вектора аутентификации.

Ответ. Случайное число RAND, ожидаемый ответ XRES, ключа шифрования информации пользователя в радиоканале CK, ключа целостности для шифрования сигнальных сообщений в радиоканале IK, анонимного ключа AUTH,

13. Что содержится в профайле качества обслуживания (QoS Profile)?

Ответ. Приоритет обслуживания, задержку обслуживания, вероятность потерь, пиковую скорость передачи, среднюю скорость передачи.

14. Из чего состоит код зоны маршрутизации

Ответ. Из кода зоны LAI и кода нескольких близлежащих сот в зоне (Routeing Area Code, RAC).

3.6. Подсистема IMS

Подсистема IMS предназначена для предоставления пользователю всех мультимедийных услуг через подсистему GPRS с использованием протоколов Internet, в частности SIP. Подсистема IMS позволяет реализовать (***3GPP TS 22.173*** [86])

услуги по качественной передаче как речи, так и речи в сочетании с другими компонентами (текст, видео);

дополнительные виды обслуживания, существующие в ISDN.

Подсистема IMS содержит следующие части (рис. 3.29).

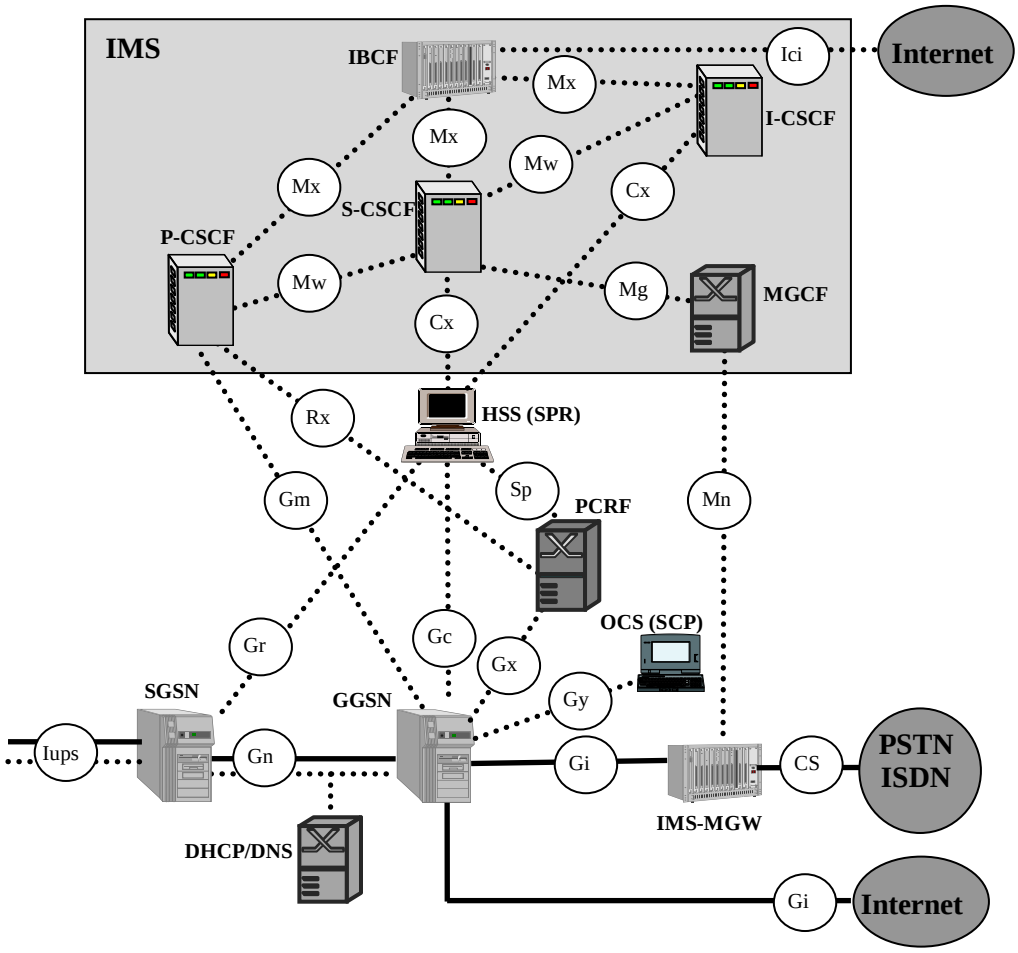

Рис. 3.29. Архитектура подсистемы IMS

- служебные сообщения (Control Plane)

- трафик пользователя (User Plane)

• Контроллер медиашлюза (**M**edia **G**ateway **C**ontrol **F**unction, **MGCF**) по интерфейсу Mn и протоколу H.248 управляет параметрами передачи информации пользователя через шлюз IMS-MGW.

• Граничный контроллер (**I**nterconnection **B**order **C**ontrol **F**unction, IBCF) обеспечивает взаимодействие по SIP между различными IP-сетями.

• Сервер управления сеансом связи (**C**all **S**ession **C**ontrol **F**unction, **CSCF**), который функционально состоит из сервера посредника абонента (P-CSCF), сервера-справочника (I-CSCF) и сервера-обслуживания (S-CSCF).

• Сервер-посредник абонента P-CSCF обрабатывает весь входящий и исходящий трафик от абонента по протоколу SIP. Он выполняет четыре функции:

- сжатие сообщений SIP на интерфейсе Gm. Сообщения SIP используют текстовый формат и занимают гораздо больший размер, чем сообщения в двоичной (формализованной) кодировке. Поэтому сжатие (компрессия) сообщений SIP в двоичный код приводит к резкому сокращению длины сообщений и к уменьшению времени их передачи;

- процедуру функции безопасности;

- обеспечение установочных параметров качества обслуживания:

- обслуживание экстренных вызовов.

- Сервер-справочник I-CSCF выполняет три функции:

- по интерфейсу Cx запрашивает у HSS адрес S-CSCF при входящих вызовах;
- назначает абоненту (P-CSCF) сервер-обслуживания (S-CSCF)
- ретранслирует телефонный номер в формат адресации SIP.

- Сервер-обслуживания S-CSCF выполняет три основные функции:

- хранит информацию о регистрации, полученной от HSS;
- устанавливает и разрушает соединения по протоколу SIP.

3.6.1. Регистрация мобильных абонентов в IMS

Перед тем, как пользователь начнет пользоваться услугами IMS, он должен получить конфигурационные параметры, в частности, IP-адрес сервера-посредника абонента P-CSCF. Этот процесс изображен на рис. 3.30 (***3GPP TS 23.228*** [92]).

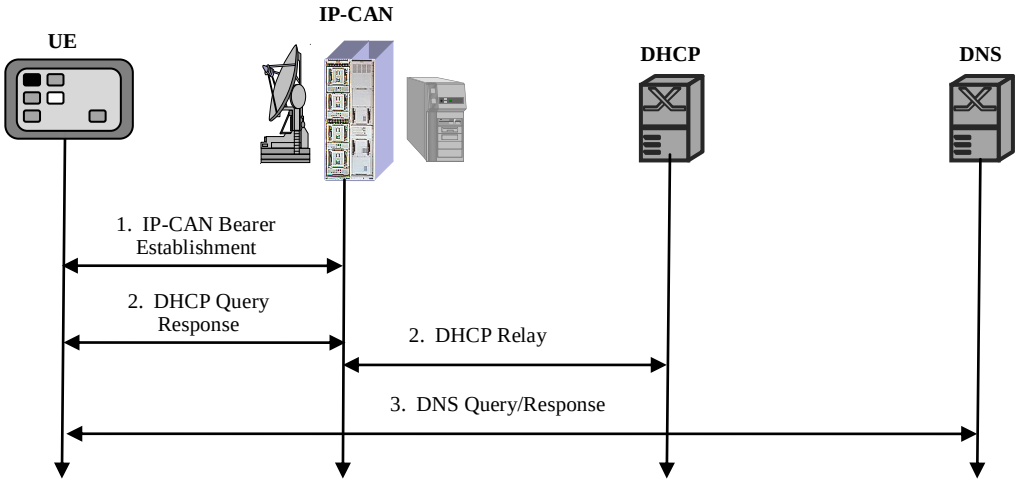

Рис. 3.30. Конфигурирование UE

1. Устанавливается соединение через сеть доступа (IP-Connectivity Access Network, IP-CAN) к GGSN.

2. UE запрашивает DHCP сервер доменное имя сервера-посредника P-CSCF и IP-адрес DNS сервера.

3. UE производит запрос DNS сервера об IP-адресе сервера-посредника P-CSCF. С этого момента UE может осуществлять сеансы связи через IMS, используя сервер-посредник P-CSCF.

Для установления соединения через IMS пользователь должен иметь открытый идентификатор пользователя IMPU, который он получает после аутентификации закрытого идентификатора пользователя IMPI.

Процедура аутентификации IMS AKA происходит между идентификационным модулем интернет-услуг ISIM и домашней сетью. Начальным идентификатором является закрытый идентификатор пользователя IMPI. Домашняя сеть выбирает параметры AKA для их транспортиования через UMTS по протоколу SIP.

Генерация вектора аутентификации (RAND, XRES, CK, IK, AUTH) производится в HSS, ISIM и HSS независимо друг от друга контролируют соответствие порядковых номеров SQN. При инициализации любого сеанса связи используются новые значения векторов аутентификации (AV) между UE и P-CSCF. Пользователь может иметь несколько IMPU, соответствующих одному IMPI. В зависимости от запрошенной услуги HSS выбирает соответствующий профайл.

Сценарий регистрации одинаков для домашних и роуминговых пользователей (рис. 3.31). Первое сообщение процесса регистрации – SIP REGISTER (***3GPP TS 33.203*** [94]).

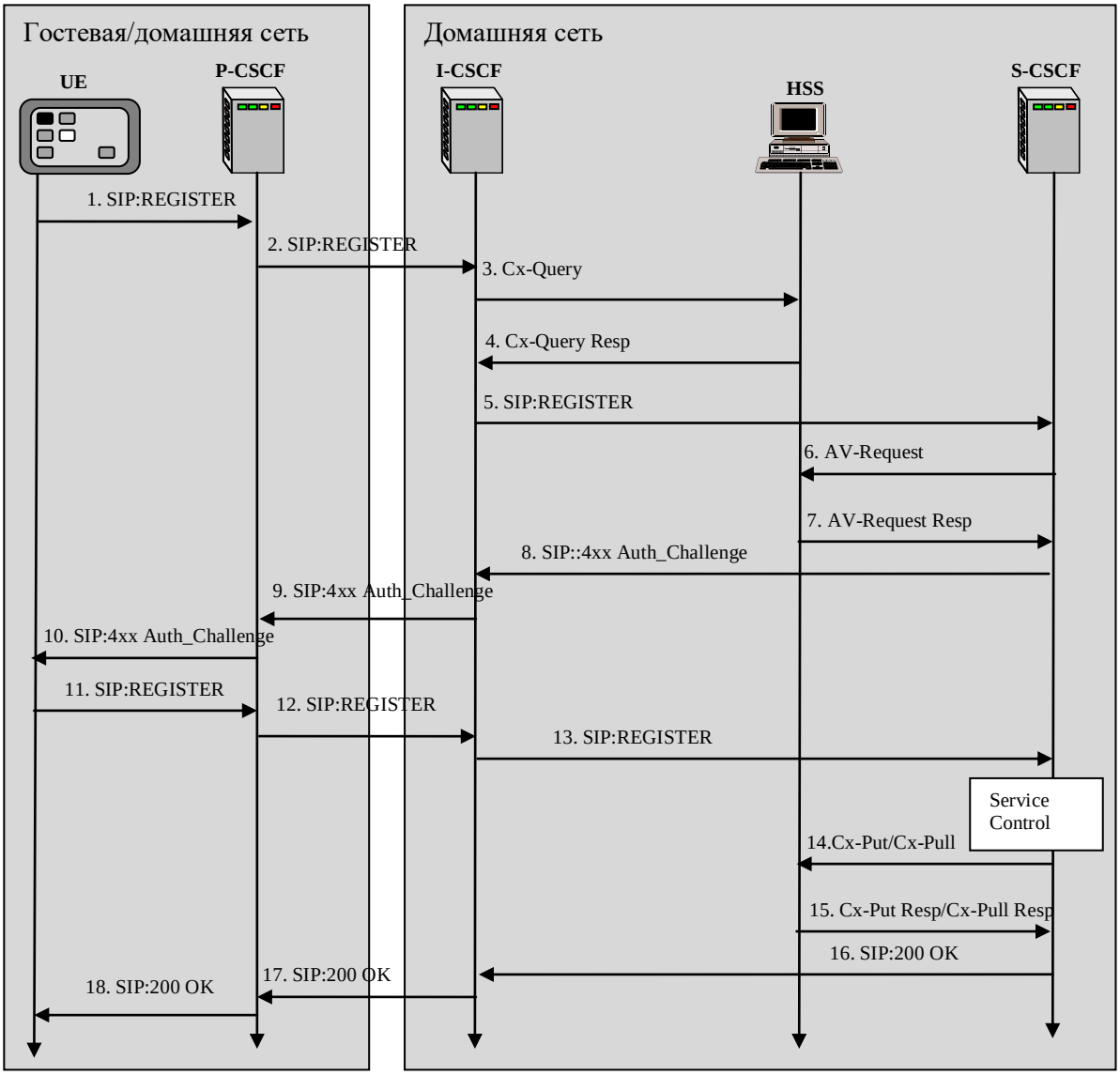

Рис. 3.31. Регистрация пользователя в IMS

1. После установления соединение через сеть доступа UE посылает сообщение Register к P-CSCF. Сообщение содержит идентификаторы IMPI, IMPU, доменное имя домашней сети, IP-адрес UE.

2. P-CSCF анализирует домашнее доменное имя UE для отправки сообщения в соответствующий домашний сервер-справочник I-CSCF.

3. I-CSCF посылает запрос Cx-Query (IMPI, IMPU, адрес P-CSCF) к HSS. HSS проверяет имеется ли запрошенный пользователь в базе данных и в каком S-CSCF он зарегистрирован/будет зарегистрирован.

4. HSS возвращает доменное имя S-CSCF к I-CSCF. При отсутствии данных посылается отказ в регистрации.

5. I-CSCF, используя DNS, определяет адрес S-CSCF и отсылает ему информацию о регистрации (адрес P-CSCF, IMPI, IMPU, IP-адрес UE).

6. Получив сообщение SIP:REGISTER S-CSCF должен начать процедуру аутентификации, используя очередной вектор (AV) для аутентификации. При их исчерпании S-CSCF запрашивает их очередную порцию (обычно 5) у HSS.

7. S-CSCF получает очередную порцию векторов (AV: RAND, XRES, CK, IK, AUTH) для аутентификации.

8. S-CSCF выбирает один из векторов и в сообщении SIP 4xx Auth_Challenge пересылает I-CSCF: IMPI, RAND, AUTN, CK, IK.

9. I-CSCF прозрачно пересылает их P-CSCF.

10. P-CSCF сохраняет ключ шифрования CK, ключ целостности IK у себя, а случайное число RAND и анонимный ключ AUTH посылает UE: IMPI, RAND, AUTN.

11. При получении сообщения SIP 4xx Auth_Challenge (IMPI, RAND, AUTN) UE извлекает SQN из AUTH и проверяет его корректное значение; используя RAND вычисляет значение XRES; высылает ответ SIP:REGISTER (IMPI, XRES) P-CSCF.

12. P-CSCF прозрачно пересылает ответ I-CSCF.

13. I-CSCF прозрачно пересылает ответ S-CSCF.

14. S-CSCF производит сравнение XRES, полученного от UE со значением XRES, полученного от HSS. При их совпадении регистрация считается успешной. S-CSCF посылает HSS сообщение Cx-Put/Cx-Put об успешной регистрации.

15. HSS устанавливает флаг о регистрации IMPI, IMPU.

16-18. UE уведомляется об успешной регистрации.

3.6.2. Установление соединения в IMS

На рис. 3.32 изображен процесс установления соединения абонента домашней сети с абонентом другого оператора (***3GPP TS 23.228*** [92]).

1. UE (А-абонент) через P-CSCF1 устанавливает исходящее соединение посылкой запроса в S-CSCF1 на открытие сеанса связи. Запрос SIP INVITE содержит описание начальных параметров медиа-связи (тип возможных кодеков, номер порта, …) в протоколе SDP.

2. S-CSCF1 определяет какой тип услуги содержит запрос.

3. S-CSCF1 анализирует адрес доставки, определяет сеть оператора, которому принадлежит адрес доставки и перенаправляет запрос в I-CSCF2 домашней сети вызываемого абонента (В-абонента).

4. I-CSCF2 запрашивает информацию у HSS2 о текущем местоположении В-абонента.

5. HSS2 возвращает адрес текущего местоположении В-абонента и адрес S-CSCF2, который займется установлением входящего соединения.

6. I-CSCF2 перенаправляет запрос INVITE в S-CSCF2.

7. S-CSCF2 определяет какой тип услуги содержит запрос.

8. S-CSCF2 отсылает запрос SIP INVITE (возможно через IP-сеть, если В-абонент находится в роуминге) с описанием параметров медиа-связи (тип возможных кодеков, номер порта, …) по адресу текущего местоположении В-абонента.

9. Вызываемый UE (В-абонент) высылает свои параметры медиа-связи (тип возможных кодеков, номер порта, …).

10. Вызываемый UE (В-абонент) высылает свои параметры медиа-связи (тип возможных кодеков, номер порта, …).

10-12. Параметры медиа-связи В-абонента доставляются А-абоненту.

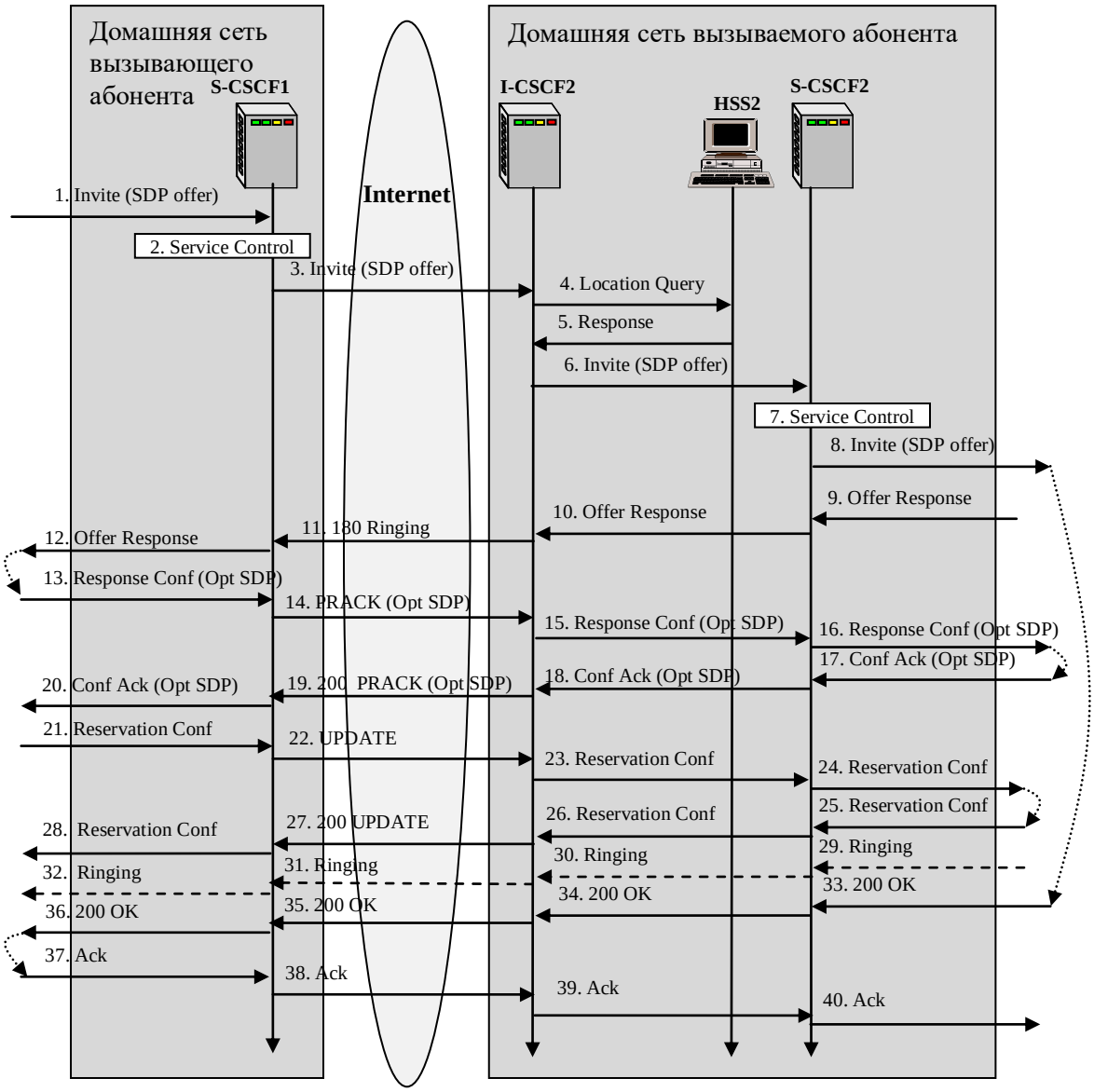

Рис. 3.32. Установление соединения в IMS

13-16. А-абонент высылает выбранные параметры медиа-связи (тип совместного кодека) В-абоненту.

17-20. В-абонент окончательно подтверждает использование параметров медиа-связи.

21-24. А-абонент высылает уведомление о резервировании ресурсов (в том числе на радиоканале).

25-28. В-абонент высылает уведомление о резервировании ресурсов.

29-32. В-абоненту высылается сигнал вызова, а от В-абонента к А-абоненту начинают поступать RTP/RTCP-пакеты (акустический сигнал “Контроль посылки вызова”).

33-36. Вызываемый абонент ответил (200 OK). От А-абонента к В-абоненту начинают поступать RTP/RTCP-пакеты.

37-40. Вызывающий А-абонент подтверждает установление связи.

ВОПРОСЫ К РАЗДЕЛУ 3.6

1. Поясните назначение подсистемы IMS.

Ответ. Предоставление пользователям мультимедийных услуг, существующих в ISDN.

2. Какой протокол использует подсистема IMS для установления мультимедийных соединений?

Ответ. Протокол инициирования сеанса связи (Session Initiation Protocol, SIP).

3. Какой протокол используется в IP-сети для переноса информации пользователя?

Ответ. Транспортный протокол реального времени (Real time Transport Protocol, RTP).

4. Назовите состав сервера управления сеансом связи (Call Session Control Function, CSCF).

Ответ. Сервер посредника абонента (P-CSCF), сервер-справочник (I-CSCF) и сервер-обслуживания (S-CSCF).

5. Какой идентификатор в IMS используется для идентификации пользователя?

Ответ. Закрытый идентификатор пользователя IMPI.

6. Какой идентификатор в IMS используется для установления связи к пользователю?

Ответ. Открытый идентификатор пользователя IMPU.

7. В чем смысл процедуры регистрации?

Ответ. Заявление IP-адреса текущего местоположения мобильного абонента.

8. В каком начальном сообщении передаются параметры медиа-связи?

Ответ. Параметры медиа-связи (IP-адрес отправителя, типы используемых кодеков, номер порта медиа связи) передаются в протоколе описания сеансов связи (Session Description Protocol, SDP), который вкладывается в SIP.

9. Какой протокол используется для контроля качества медиа-связи?

Ответ. Протокол управления протоколом реального времени (Real time Control Protocol, RTCP).

3.7. Сотовая наземная сеть связи мобильных абонентов четвертого поколения. Стандарт LTE

3.7.1. Архитектура сети

Целью сети четвертого поколения (4G) являются:

создание нового радио интерфейса с гораздо более высокой скоростью передачи;

разделение функций управления трафиком и самого трафика;

упрощение архитектуры системы, которая будет полностью основана на IP.

Этот проект консорциума 3GPP направлен на эволюционное совершенствование существующей сети связи мобильных абонентов и с 8-ой версии получил название **L**ong **T**erm **E**volution (**LTE**).

В результате исследований было принято решение о построении сети радиодоступа на базе мультиплексирования с ортогональным частотным разделением каналов (**O**rthogonal **F**requency-**D**ivision **M**ultiplexing, **OFDM**). Это роднит LTE с WiMAX, который также использует OFDM. Реализация предполагает использование специальных базовых станций eNodeB с радио интерфейсом LTE-Uu, являющейся аналогом NodeB+RNC для сети UMTS и BTS+BSC для сети GSM. Эстафетная передача соединения (Handover) между соседними сотами eNodeB производит самостоятельно по X2-интерфейсу.

Архитектура эволюционной сети (**E**volved **P**acket **S**ystem, **EPS**), состоящая из радиосети доступа (**E**volved **U**niversal **T**errestrial **R**adio **A**ccess **N**etwork, **E-UTRAN**) и ядра сети (**E**volved **P**acket **C**ore, **EPC**), приведена на рис. 3.33. Весь трафик (в том числе голосовой) обрабатывается как трафик данных.

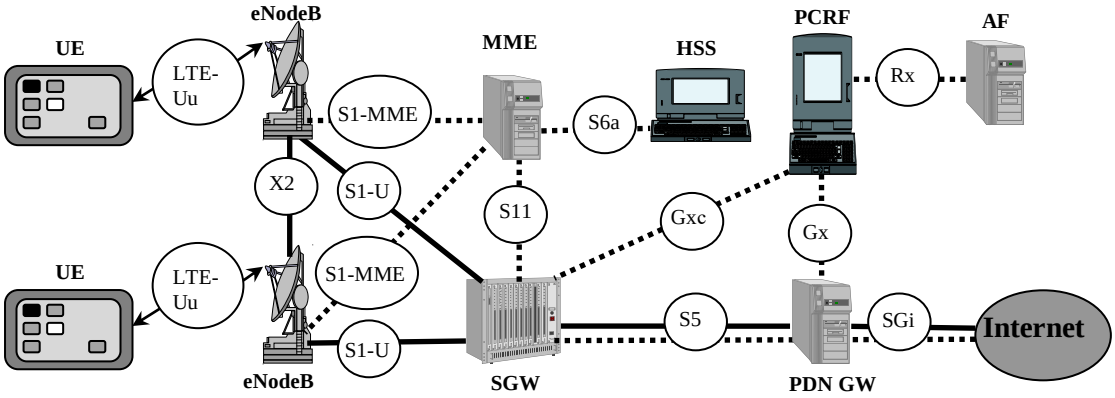

Рис. 3.33. Архитектура эволюционной сети (EPS) без IMS

- сигнальные сообщения

- трафик пользователя

Ядро сети EPC является аналогом подсистемы UMTS состоит из следующих сетевых элементов (***3GPP TS 23.002*** [87]).

Узел управления мобильностью (**M**obility **M**anagement **E**ntity, **MME**) является основным управляющим модулем LTE и обеспечивает

- отслеживание мобильности пользователя (интерфейс S1-MME);
- сигнализацию на радиоканале и функции безопасности (интерфейс S1-MME);
- ведение таблиц зон обслуживания;
- выбор и управление обслуживающего шлюза (SGW) для трафика пользователя (интерфейс S11);
- управление эстафетной передачи соединения в смежные сети 2G/3G;
- аутентификацию и авторизацию пользовательского устройства UE (интерфейсы S1-MME и S6a).

Обслуживающий шлюз (**S**erving **G**ateway, **SG**) предназначен для обработки и маршрутизации пакетных данных, поступающих из/в подсистему базовых станций eNodeB. Основными функциями являются

- буферизация данных из/в подсистему базовых станций eNodeB (интерфейс S1U);
- маршрутизацию пакетного трафика (интерфейс S1U);
- маркировку и обслуживание трафика в соответствии с классом качества обслуживания (**Q**oS **C**lass **I**dentifier, **QCI**);
- извещение о событиях в узел политики и оплаты PCRF (интерфейс GxC);
- выставление параметров нисходящего и восходящего каналов по умолчанию.

Домашний сервер абонента (**H**ome **S**ubscriber **S**erver, HSS) хранит базу данных абонентов.

Сервер приложений (**A**pplication **F**unction, **AF**) централизовано хранит данные политики обслуживания (QoS-профайлы) и форму оплаты счетов за пользование ресурсами сети связи. Он предоставляет эти данные нескольким PCRF по их запросу (интерфейс Rx).

Узел политики и оплаты (**P**olicy and **C**harging **R**ules **F**unction, **PCRF**) хранит копии данных политики обслуживания (QoS-профайлы) и форму оплаты счетов за пользование ресурсами сети связи во время сеанса связи.

Пакетный шлюз (**P**acket **D**ata **N**etwork **G**ate**w**ay, **PDN-GW**) обеспечивает

- фильтрацию (детальное обследование) пакетов (интерфейсы S5 и SGi);
- назначение IP-адресов пользовательским устройствам UE (интерфейс S5);
- установку кодов дифференцированного обслуживания (DSCP) пользовательского трафика (интерфейсы S5 и SGi), основываясь на указаниях от узла политики и оплаты PCRF (интерфейс Gx);
- формирование отчета в узел политики и оплаты PCRF об использовании трафика (интерфейс Gx);
- функции севера загрузки конфигурационных параметров DHCPv4/DHCPv6 в пользовательские устройства UE (интерфейс S5);
- реализация указаний PCRF (QoS-профайлов) при помощи устройства реализации политики и оплаты (**P**olicy and **C**harging **E**nforcement **F**unction, **PCEF**).

3.7.2. Взаимодействие с другими сетями

В настоящее время разработка сети LTE далека от завершения. До конца не решены вопросы качества обслуживания речевых сообщений, сопоставимые с GSM. Передача речи остается основной услугой в сети LTE. Как временное решение в настоящее время имеется две основные опции для качественной передачи речи:

- *возврат в домен коммутации каналов* (Circuit Switched Fallback, CS Fallback) (***3GPP TS 23.272*** [93]). Эта опция используется когда передача речи через подсистему IMS не поддерживается UE или оператором связи;
- *продолжение обслуживания одиночного речевого вызова* (Single Radio Voice Call Continuity, SRVCC) (***3GPP TS 23.216*** [91]). Эта опция используется когда передача речи через подсистему IMS поддерживается UE и оператором связи.

Опция CS Fallback предусматривает возможность UE поддерживать радио интерфейсы в UTRAN/EPC (LTE-Uu) и в GERAN (Um), а также установку дополнительного сигнального интерфейса SGs между MME и MSC (рис. 3.34).

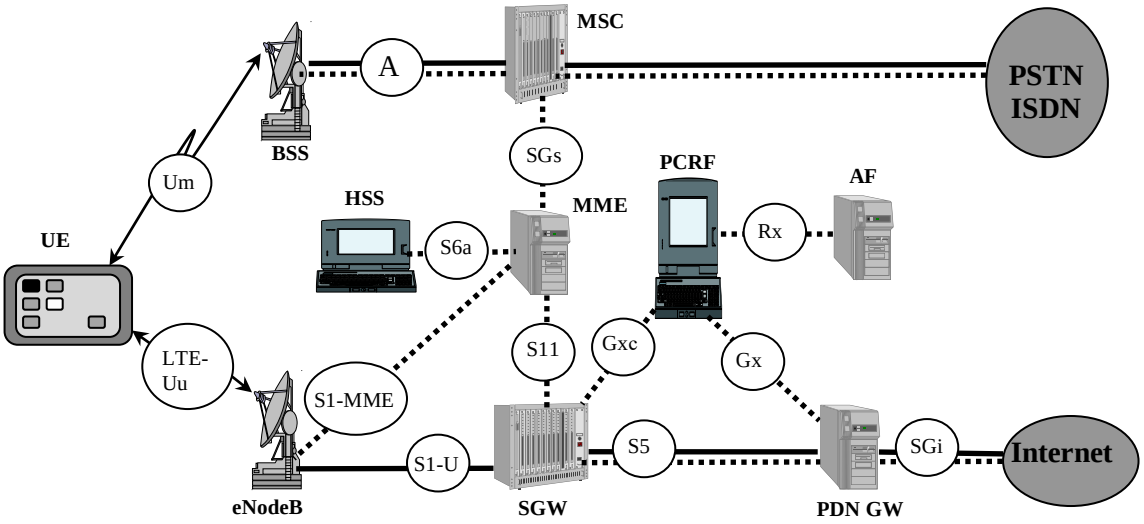

Рис. 3.34. Архитектура опции CS Fallback

..... - сигнальные сообщения

——— - трафик пользователя

Пример использования опции CS Fallback при установления исходящего соединения приведен на рис. 3.35.

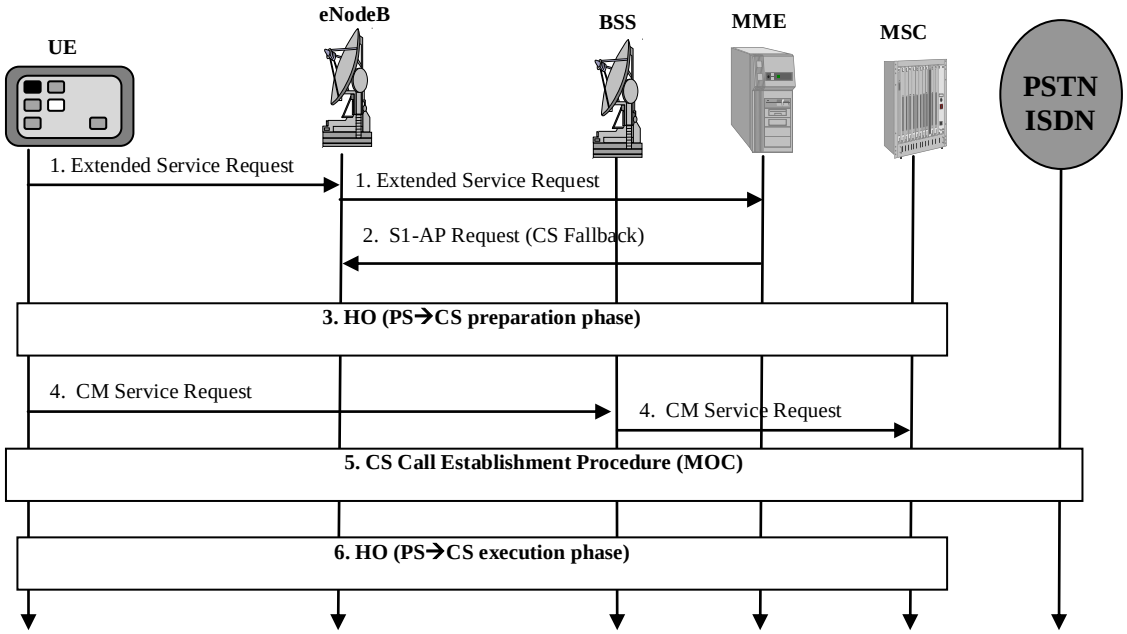

Рис. 3.35. Исходящее соединение с опцией CS Fallback

1. UE зарегистрирован в LTE-домене и имеет с ним радиоконтакт. UE посылает запрос (Extended Service Request) на соединение. Запрос содержит индикатор поддержки CS-домена и индикатор отсутствия регистрации в IMS.

2. MME анализирует запрос и возвращает запрос eNodeB на эстафетную передачу соединения (Handover).

3. UE инициирует эстафетную передачу соединения посылкой запроса HO_Required в MME с параметрами требуемой ячейки GERAN.

4. UE осуществляет запрос BSS на соединение в сеть GSM, генерируя запрос (CM Service Request). BSS транслирует запрос MSC.

5. MSC нормально устанавливает исходящее соединение по цепи UE – BSS – MSC – PSTN/ISDN.

6. MSC извещает MME об успешном установлении соединения, MME дает команду eNodeB на разрушение радиоканала.

Ограниченное радио покрытие сетей LTE на ранних стадиях внедрения вынуждает использовать ее только для передачи данных. Чтобы обеспечить непрерывную связь в районе отсутствия покрытия сети LTE, но при наличии покрытия сетью GSM и использовании подсистемы IMS предполагается использовать опцию продолжение обслуживания одиночного речевого вызова (Single Radio Voice Call Continuity, SRVCC).

Опция SRVCC рассматривается как более перспективное решение и предусматривает (рис. 3.36):

- возможность UE поддерживать радио интерфейсы в UTRAN/EPC (LTE-Uu) и в GERAN (Um);
- наличие в UE приложения SIP-клиента и модуля интернет-услуг (**I**MS **I**dentity **M**odule, **ISIM**). В ISIM хранятся закрытый (Private User Identity, IMPI) и открытый (Public User Identity, IMPU) идентификаторы пользователя;
- наличие в сети подсистемы IMS;

- установку вспомогательного оборудования (Interworking Function Solution) для связи MME с множеством MSC по сигнальному интерфейсу S102.

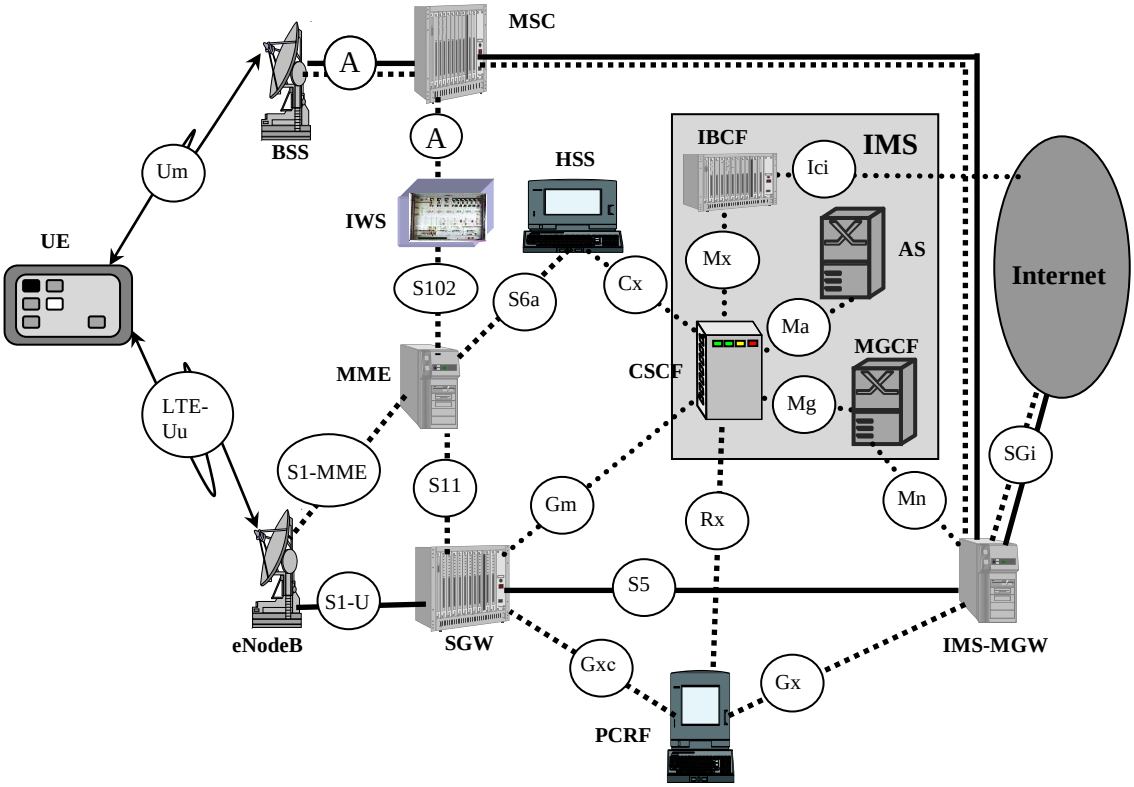

Рис. 3.36. Архитектура опции SRVCC

..... - сигнальные сообщения

——— - трафик пользователя

Пример использования опции SRVCC при установленном исходящем соединении в LTE-домене приведен на рис. 3.37.

1. Установлено соединение в LTE-домене по цепи UE – eNodeB – SGW – IMS-MGW - Internet. Процедура установления исходящего вызова в подсистеме IMS рассмотрена в п.3.6.2.
2. UE мигрирует в зону покрытия GSM и обнаруживает лучшее покрытие в GSM-домене, о чем рапортует eNodeB (Measurement Report).
3. eNodeB принимает решение о продолжении обслуживания одиночного речевого вызова в GSM-домене.
4. eNodeB посылает UE сообщение HO Preparation Request, которое UE воспринимает как запрос о параметрах эстафетной передачи.
5. UE высылает eNodeB код ячейки (CellID), имеющей хорошее радио покрытие.
6. eNodeB пересылает сообщение MME.
7. MME определяет IWS, для пересылки данных эстафетной передачи в требуемый MSC (сообщение Air Interface Signalling по интерфейсу S102). IWS прозрачно пересылает сообщение в MSC.
8. MSC резервирует радиоканалы в GSM (сообщения HO Request и HO Request Ack).
9. Сообщение об успешном резервировании радиоканала в сообщении HO Direction доставляется UE.
10. UE переключает радиоканал в сеть GSM.
11. UE извещает BSS об успешном подключении к GSM.

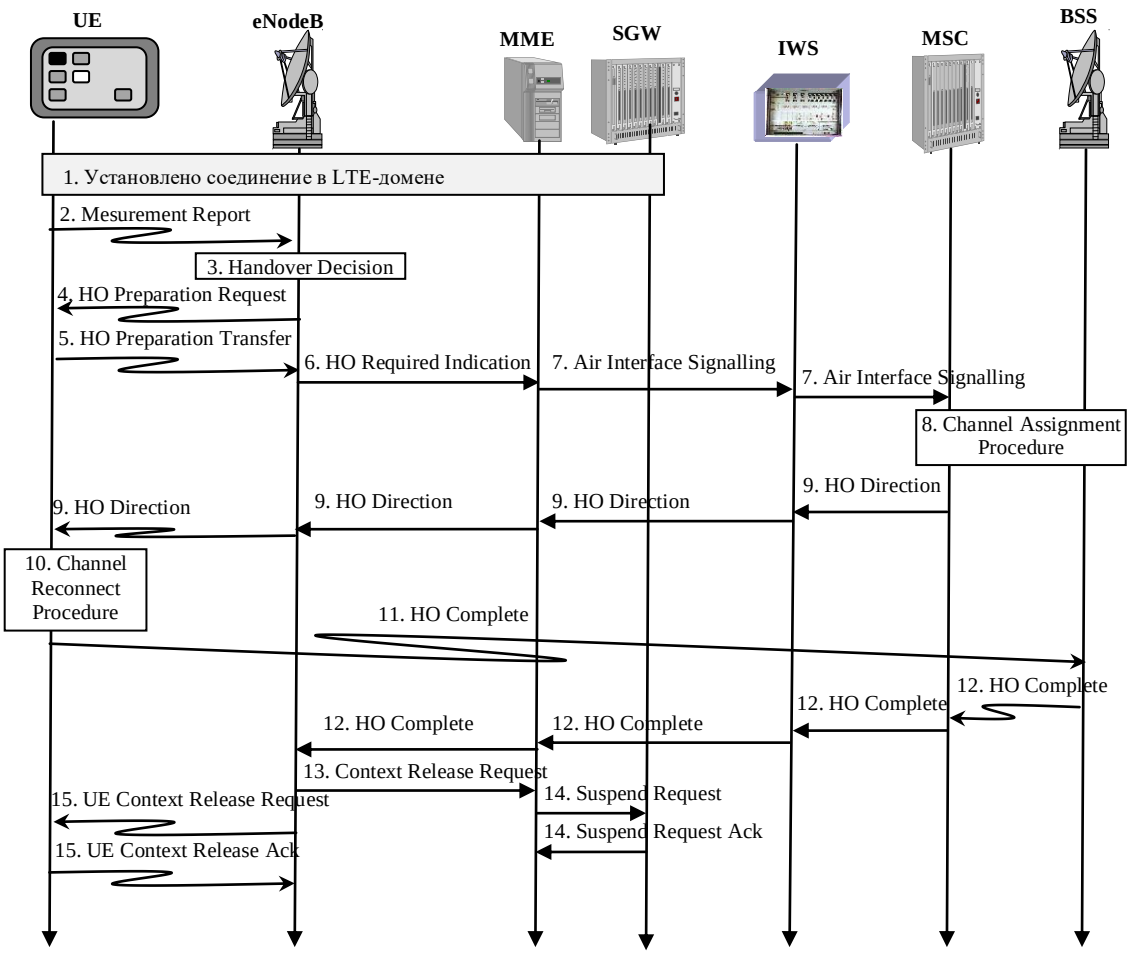

Рис. 3.37. Использование опции SRVCC

12. BSS оповещает MSC, MME и eNodeB об успешном подключении к GSM.
13. eNodeB запрашивает MME об уничтожении PDP-контекста.
14. MME контролирует уничтожение PDP-контекста в SGW.
15. eNodeB контролирует уничтожение PDP-контекста в UE.

Установлено новое соединение в GSM-домене по цепи UE – BSS – MSC – IMS-MGW - Internet.

ВОПРОСЫ К РАЗДЕЛУ 3.7

1. Перечислите состав ядра сети LTE.

Ответ. Узел управления мобильностью (Mobility Management Entity, MME), обслуживающий шлюз (Serving Gateway, SG), пакетный шлюз (Packet Data Network Gateway, PDN-GW), узел политики и оплаты (Policy and Charging Rules Function, PCRF), домашний сервер абонента (Home Subscriber Server, HSS).

2. В каком сетевом элементе EPC без IMS постоянно хранятся QoS-профайлы?

Ответ. В Сервере приложений (Application Function, AF).

3. В каком сетевом элементе EPC хранятся QoS-профайлы на время сеанса связи?

Ответ. В Узеле политики и оплаты (Policy and Charging Rules Function, PCRF).

4. В каком сетевом элементе EPC без IMS реализуются QoS-профайлы на время сеанса связи?

Ответ. В пакетном шлюзе (Packet Data Network Gateway, PDN-GW).

5. В каком сетевом элементе EPC с IMS реализуются QoS-профайлы на время сеанса связи?

Ответ. В пакетном шлюзе IMS (IMS-MGW).

6. Поясните существо опции CS Fallback.

Ответ. При поступлении исходящего или входящего вызова от/на абонента в LTE-домене обслуживание вызова переводится в GSM-домен с прохождением соединения через PSTN/ISDN-сеть.

7. Поясните существо опции SRVCC.

Ответ. При установленном исходящем или входящем соединении в LTE-домене в IP-сеть производится эстафетная передача соединения в GSM-домен с прохождением соединения через IP-сеть.