8. Процедуры уровня L3

8.1. Пейджинг

Процедура пейджинга приведена на рис. 8.1.

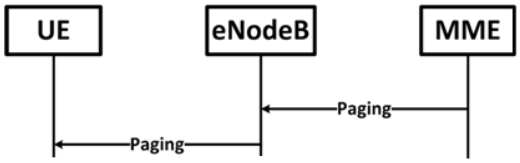


Рис. 8.1. Процедура пейджинга

Сообщения пейждинга относятся к сигнализации NAS и содержат S-TMSI или IMSI вызываемых абонентов. Пребывая в состоянии IDLE, UE обычно находится в режиме сна (DRX), но просыпается для прослушивания канала пейджинга. Общее число передаваемых сообщений пейджинга оператор устанавливает, передавая в SIB2 два параметра: *число кадров*, через которое UE прослушивает канал пейджинга в соте по умолчанию, *default-pagingCycle* = $T_{Cell\text{-}DRX\text{-}default}$, и параметр $nB = \{4T, 2T, T, T/2, T/4, T/8, T/16, T/32\}$ [36].По умолчанию $T = T_{Cell\text{-}DRX\text{-}default}$. Однако оператор может установить для конкретного UE $T < T_{Cell\text{-}DRX\text{-}default}$.

Число кадров, где за период T передают сообщения пейджинга,

$$N = min(T, nB), \tag{8.1}$$

а число субкадров, где в кадре могут передавать пейджинг,

$$N_S = max(1, nB/T) \tag{8.2}$$

Обычно $T_{Cell\text{-}DRX\text{-}default} = \{32, 64, 128, 256\}$. При $nB = \{4T, 2T, T\}$ сообщения пейджинга передают в каждом кадре, при $nB = T/2$ – через кадр, при $nB = T/4$ – через 4 кадра и т.д. При $nB \le T$ $N_s = 1$ и в кадре передают только один пакет пейджинга в одном субкадре; при $nB = 2T$ – 2 пакета пейджинга в двух разных субкадрах, при $nB = 4T$ – 4 пакета пейджинга в четырех разных субкадрах.

Номера кадров SFN для прослушивания канала пейджинга, UE определяют по формуле

$$\mathrm{SFN}(\mathrm{mod}T) = (T/N)(UE\_ID(\mathrm{mod}N)) \tag{8.3}$$

а номер субкадра из табл. 8.1 [36].

Таблица 8.1

Ns	Частотный дуплекс				Временной дуплекс			
	i_s=0	i_s=1	i_s=2	i_s=3	i_s=0	i_s=1	i_s=2	i_s=3
1	9	N/A	N/A	N/A	0	N/A	N/A	N/A
2	4	9	N/A	N/A	0	5	N/A	N/A
4	0	4	5	9	0	1	5	6

В формуле (8.3) *UE_ID* = IMSI(mod1024), где IMSI – системный номер абонента в десятичном формате. В табл. 8.1 $i\_s = \lfloor UE\_ID / N \rfloor \bmod N_S$, где знаком $\lfloor\ \rfloor$ обозначена целая часть числа.

Приведем пример расчета номеров кадров и определения субкадра, где абоненту с IMSI = 250022593191333 могут передавать пейджинг. Положим $T = T_{Cell\text{-}DRX\text{-}default} = 128$, $nB = T$, $N = T$, $N_S = 1$, сеть работает с частотным дуплексом.

UE_ID = IMSI(mod1024) = 421; $i\_s = \lfloor UE\_ID / N \rfloor \bmod N_S = 0$.

В соответствии с (8.3)

SFN(mod*T*) = (*T*/*T*)(421(mod128)) = 37

Таким образом, UE должен прослушивать канал пейджинга в субкадре 9 кадров с номерами SFN = 37, 165, 293 и далее.

8.2. Установление соединения с сетью

Процедура *RRC connection establishment* относится к протоколу RRC (рис. 8.2), описана в [11].

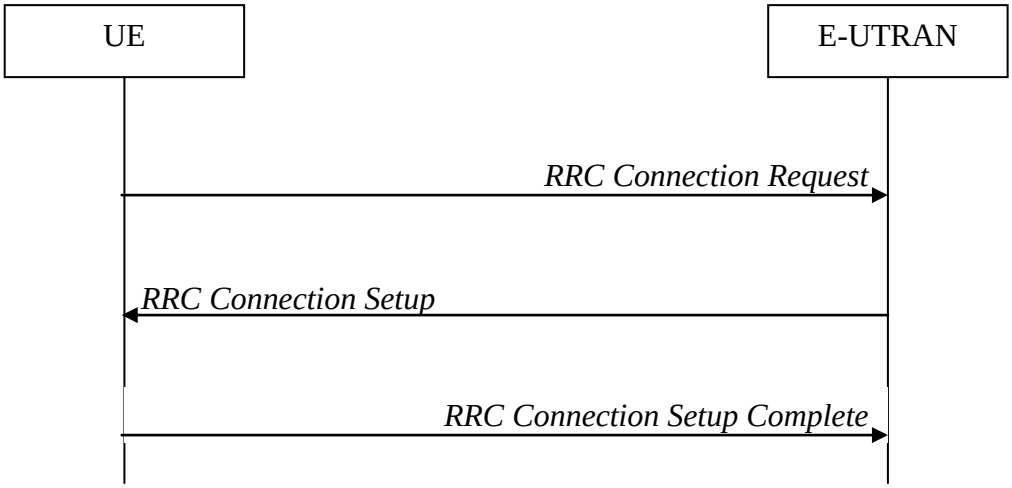


Рис. 8.2. Процедура RRC connection establishment

Процедура происходит при переходе UE в состояние *CONNECTED* из состояний *Detached* и *IDLE*. В результате процедуры устанавливается соединение по SRB1 (Signal Radio Bearer 1).

Согласно [23] передача сигнализации для каждого UE идет по организуемым SRB. SRB1 и SRB2 используют постоянно:

- SRB2 для сообщений NAS, DCCH на логическом уровне,

- SRB1 для остальных сигнальных сообщений логического уровня DCCH, в том числе и NAS до установки SRB2.

Существует также SRB0 для передачи сообщений канала CCCH в начале процедуры *RRC connection establishment* до установления SRB1.

Сообщение *RRC Connection Request* содержит:

- идентификатор UE (S-TMSI при пейджинге и при повторных запросах услуг),

- причину запроса соединения – срочный вызов (emergency), высокоприоритетный доступ (High Priority Access), доступ, инициируемый сетью (Mobile Terminating), передача данных, инициируемая UE (Mobile Originating), сигнализация, инициируемая UE (Mobile Originating).

Сообщение *RRC Connection Setup* устанавливает SRB1.

8.3. Процедура Attach

С процедуры *Attach* (подключения) начинается каждый сеанс связи. При этом происходит регистрация UE в сети, подсоединения UE к EPC для реализации услуг передачи пакетного трафика. Ядро сети организует сквозное соединение по протоколу IP: сквозной канал по умолчанию (default EPC bearer). После выполнения процедуры *Attach* могут быть добавлены один или несколько выделенных каналов (процедура *Dedicated Bearer Establishment*). При выполнении процедуры *Attach* происходит активизация или выделение абоненту IP-адреса.

Спецификациями [6] предусмотрены 3 варианта запуска процедуры:

- когда UE находится в режиме с коммутацией пакетов,

- когда UE находится в состоянии с коммутацией каналов/пакетов,

- при организации срочных вызовов (emergency). При этом возможна ситуация, когда MME (сеть) не поддерживает срочных вызовов. Существуют особенности процедуры *Attach* при межсистемных хэндоверах.

Алгоритм процедуры приведен на рис.8.3 [6]. Первое сообщение *Attach Request* (рис.8.3, п.1), которое UE посылает на eNB, содержит большое число параметров, в том числе:

- идентификатор абонента (IMSI или GUTI = GUMMEI + M-TMSI),

- идентификатор последней визитной зоны TAI (Tracking Area Identity),

- UE Core Network Capability (возможность работы в разных сетях, поддержка IMS и проч.),

- тип процедуры (*EPS Attach, Combined EPS/IMSI Attach, Emergency Attach*),

- параметры, необходимые для выполнения процедур безопасности, если они были установлены ранее, вместе с указанием выбранной сети обслуживания (оператора) и старым GUMMEI. При этом UE может защитить целостность передаваемого сообщения *Attach Request*. При положительном результате проверки целостности пришедшего сообщения *Attach Request* MME использует для выполнения защиты информации хранящиеся в базе данных абонента вектора аутентификации (п.3.3).

Attach Request также содержит указание требуемого типа пакетной сети (поддержка протоколов IPv4, IPv6 или IPv4/IPv6) и соответственный вариант IP-адреса. UE может установить прямой обмен параметрами с PDN GW посредством PCO (Protocol Configuration Options), в том числе в зашифрованном виде.[1] При этом UE передает на PDN GW имя точки доступа APN и совокупную максимальную скорость передачи в точке доступа APN-AMBR (Aggregated maximum Bit Rate).[2]

В п.2 eNB извлекает из *Attach Request*, переданного UE, идентификатор MME, который обслуживал UE в предыдущем сеансе связи. Если eNB не имеет выхода на этот MME, то он выбирает новый MME, который будет обслуживать абонента. В сообщение *Attach Request*, направленное обслуживающему MME, eNB дополнительно включает глобальный идентификатор зоны TAI и глобальный идентификатор соты ECGI (E-UTRAN Cell Global Identifier), откуда поступил запрос. TAI (Tracking Area Identity) состоит из кода страны, кода оператора и кода зоны TAC (Tracking Area Code – 16 бит). В ECGI в макро и микросетях идентификатор eNB определяют 20 бит, а в фемтосетях 28 бит являются кодом домашней базовой станции HeNB. [37]. Таким образом, уже на этапе подключения абонента к сети его можно локализовать с точностью до соты.

П.3. Если произошла смена MME после последнего сеанса связи, то новый MME (new MME) пересылает *Attach Request Message* на старый MME (old MME) для получения системного номера (IMSI) абонента. Старый MME проверяет целостность полученного сообщения *Attach Request* и отвечает сообщением *Identification Response*. Оно содержит IMSI абонента и его базу данных (*MM Context*), сохраненную с предыдущего сеанса связи. Если база абонента удалена или целостность сообщения *Attach Request* нарушена, то старый MME сообщает об ошибке и полностью производится процедура безопасности по протоколу MM (пп. 4 – 6).

П.4. Если идентификатор абонента IMSI не удалось определить, MME посылает запрос абоненту *Identity Request*. Ответ *Identity Response* содержит IMSI.

[1] Эти параметры передают прозрачно через MME и S-GW.

[2] При описании алгоритма процедуры Attach и следующих процедур в данном издании не рассмотрены особенности обслуживания абонентов выделенных групп пользователей в фемтосотах и при использовании LIPA. Детали соответствующих процедур изложены в [6] и в [26].

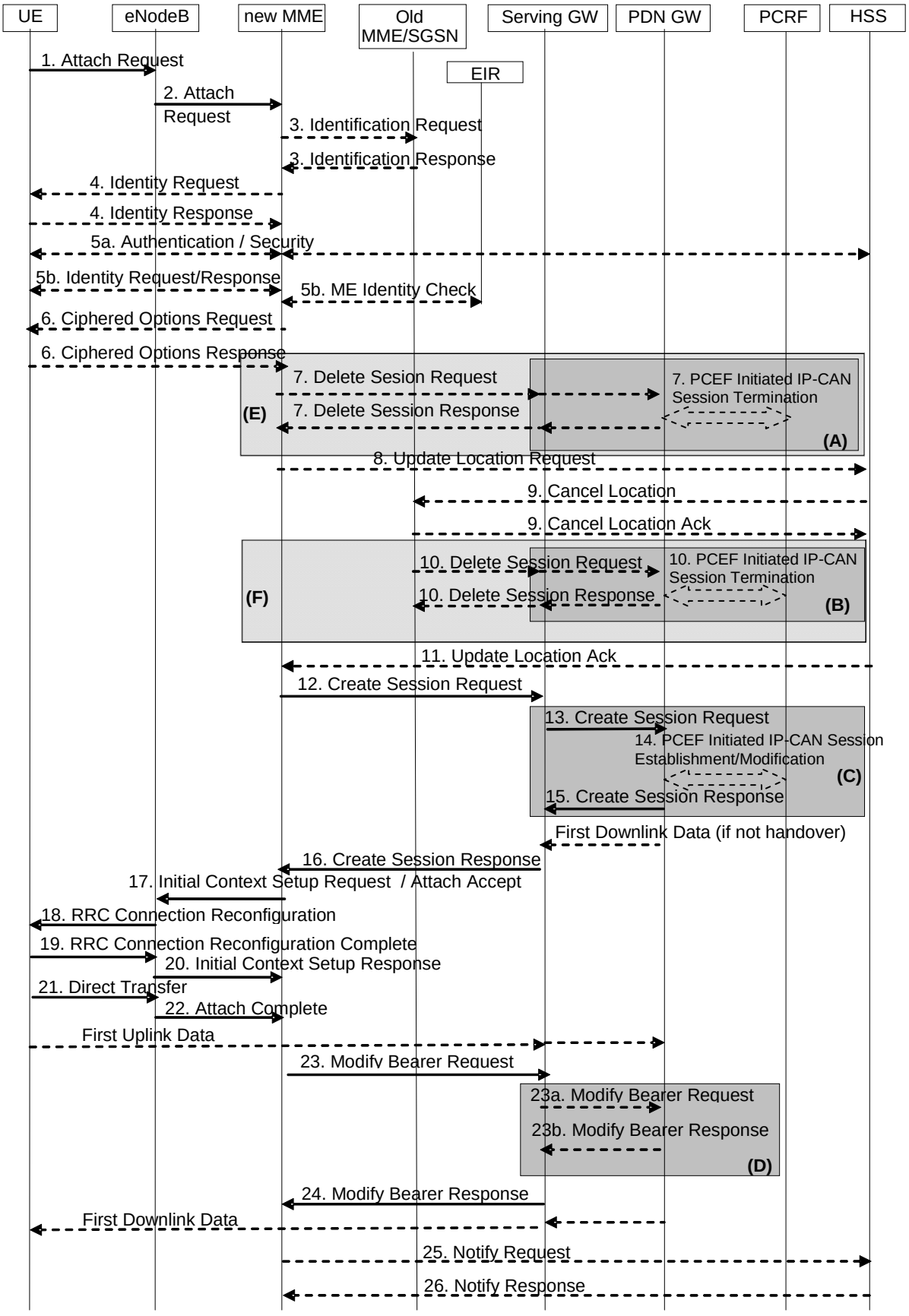


Рис. 8.3. Процедура Attach

П.5a – процедуры взаимной аутентификации и установления режима шифрации выполняют обязательно, если параметры безопасности определяют заново. Если можно использовать результаты предыдущего сеанса связи, то необходимость выполнения п.5a определяет оператор.

В п.5b осуществляют проверку мобильного терминала (IMEI – International Mobile Equipment Identity).

П.6 выполняют в том случае, когда UE просит организовать в PCO шифрацию при передаче параметров подключения к IP-сети в PDN GW (см. п.1).

П.7. Если при завершении предыдущего сеанса связи в контексте абонентских параметров, сохраненных в старом MME, не были удалены параметры организованных сквозных каналов (процедура завершения сеанса связи *Detach* не была выполнена полностью), новый MME удаляет эти каналы, посылая команду *Delete Session Request* в S-GW и PDN GW. PDN GW сообщает PCRF о завершении предыдущего сеанса связи и о высвобождении выделенного канального ресурса – блоки (E) – (A). Это же относится и к блокам (F) – (B) п.10, когда произошла замена MME.

П.8. Если произошла смена MME или база данных абонента в MME организуется заново, то новый MME направляет запрос *Update Location Request* в HSS. HSS фиксирует идентификатор обслуживающего абонента MME, даёт команду стереть базу данных абонента в старом MME (*Cancel Location*, п.9) и посылает сообщение *Update Location Ack*) в новый MME (п.11).

В команде *Update Location Ack* передают IMSI абонента и *Subscription Data* – параметры услуг (*PDN Subscription Context*), которые могут быть предоставлены абоненту. В *Subscription Data* записаны параметры одной или нескольких услуг (PDN) для APN. Каждая услуга в *PDN Subscription Context* содержит требования к качественным характеристикам: *EPS Subscription QoS Profile*. Новый MME проверяет возможность обслуживания абонента в новой зоне. Если абонент не имеет прав на обслуживание в данной зоне, тогда MME прерывает процедуру *Attach*, о чем UE получает соответствующее уведомление.

П.12. Команда *Create Session Request* содержит все данные, которые необходимы для организации сквозного канала по умолчанию. В большинстве случаев UE передаёт имя точки доступа APN, что определяет адрес PDN GW. Если APN неизвестен, то MME выделяет его по умолчанию.

MME выбирает S-GW и назначает идентификатор сквозного канала по умолчанию. В сообщении *Create Session Request* передают IMSI, MSISDN[3], IMEI, адрес PDN GW, параметры QoS организуемого канала, IP-

[3] Если он получен из HSS.

адрес абонента, тип протокола на интерфейсе S5/S8, ECGI, временной пояс, где находится абонент[4], APN-AMBR и ряд параметров, характеризующих сеть и особенности процедуры. *Create Session Request* также содержит идентификатор туннеля TEID на сигнальном интерфейсе S-11 в направлении S-GW → MME (рис. 1.1).

П.13. S-GW создаёт новую запись в таблице сквозных каналов и пересылает полученные от MME параметры, в том числе информацию о локализации абонента, на PDN GW по адресу, указанному в команде (п.12). Сообщение (п.13) *Create Session Request* также сдержит конечные точки TEID туннелей в плоскости трафика и сигнальной плоскости на интерфейсе S5/S8 в направлении PDN GW → S-GW. Теперь S-GW готов буферизировать пакеты, следующие вниз от PDN GW.

П.14. Получив сообщение *Create Session Request,* PDN GW осуществляет процедуру запуска сеанса связи *IP-CAN* (Connectivity Access Network) *Session Establishment* или его модификации (*Modification*) в случае хэндовера. Всю информацию об абоненте и организуемой услуге (IMSI, IP-адрес абонента, APN, сеть обслуживания, данные о локализации и др.) PDN GW направляет в PCRF, который может принять, а может и изменить параметры QoS организуемого сквозного канала. При назначении тарифа для оплаты услуг используют данные о локализации абонента и часовом поясе, где он находится.

П.15. PDN GW создаёт в базе данных сквозных каналов запись о новом канале и присваивает ему идентификатор для тарификации трафика (Charging Id). Теперь и в PDN GW, и в S-GW открыты базы данных абонента. Организуется сквозной канал для пакетного обмена между PDN GW и S-GW. Сообщение *Create Session Response* содержит все характеристики сквозного канала, в том числе варианты используемого протокола IP (IPv4 или IPv6). Активизируется PDN адрес абонента. Абонент может иметь статический или динамический адрес в домашней сети или получить динамический адрес в визитной сети. Выделение динамического адреса осуществляет DHCP (Domain Host Configuration Protocol). Для создания туннелей вверх на интерфейсе S5/S8 в *Create Session Response* передают TEID туннельных соединений в пользовательской и сигнальной плоскостях.

Теперь пришедшие ранее пакеты данных из PDN GW могут быть переданы в буфер S-GW.

П.16. Получив сообщение *Create Session Response,* S-GW заносит характеристики сквозного канала в базу данных и передаёт необходимые параметры в MME для организации сквозного канала на интерфейсе S1 м радиоинтерфейсе.

[4] Параметр NITZ (Network Identity and Time Zone) [38] нужен для тарификации услуг.

П.17. MME передает на eNB 2 сигнальных сообщения. Внутреннее сообщение *Attach Accept* содержит параметры организованного сквозного канала, номер сигнального сообщения NAS между UE и MME и новый GUTI, если абонента стал обслуживать новый MME. Сообщение *Attach Accept* в п. 18 будет далее переслано UE. В п.17 *Attach Accept* размещено в команде *Initial Context Setup Request*, где дополнительно для eNB передают параметры безопасности, а также сквозного канала на интерфейсе S1:, адрес S-GW и TEID туннеля вверх на S1.

П.18. eNB направляет UE сообщение *RRC Connection Reconfiguration*, содержащее *Attach Accept* и идентификатор сквозного канала на радиоинтерфейсе EPS Radio Bearer Identity. UE получает имя точки доступа APN и активизированный IP-адрес. В ответном сообщении *RRC Connection Reconfiguration Complete* (п.19) UE подтверждает получение необходимой информации.

П.20. Сообщение *Initial Context Setup Response* содержит адрес eNB и TEID сквозного канала вниз на интерфейсе S1.

П.21. В сообщении Direct Transfer UE передаёт команду *Attach Complete* (идентификатор сквозного канала, номер сообщения NAS), адресованную MME. eNB ретранслирует *Attach Complete* в MME (п.22). После этого UE может начать передачу пакетов вверх.

П.23. Сообщение *Modify Bearer Request* содержит идентификатор сквозного канала, адрес eNB, eNB TEID, что необходимо для организации на интерфейсе S1 туннеля вниз.

При межсистемном хэндовере в *Modify Bearer Request* передают индикатор хэндовера и далее выполняют команды 23a и 23b (блок D). S-GW информирует PDN GW о завершении организации сквозного канала на участке eNB – S-GW. Теперь пользовательские пакеты можно направлять на eNB по интерфейсу S1.

П.24. Команда *Modify Bearer Response* является подтверждением получения команды *Modify Bearer Request.* Теперь можно начать прямую передачу пользовательских пакетов вниз.

Сообщения пп.25 и 26 передают только в том случае, если MME назначил для сквозного канала PDN GW отличный от того, что прописан в базе данных абонента в HSS. MME информирует HSS о выбранном PDN GW и APN. HSS вносит их в базу данных абонента и отправляет в MME подтверждение.

8.4. Процедура локализации

Процедура локализации *TAU* (*Tracking Area Update*) происходит, когда UE, находящийся в состоянии *IDLE*, перемещается при движении або-

нента в соту, расположенную в зоне слежения, которая не указана в списке зон регистрации абонента. Напомним, что MME может регистрировать абонента в одной зоне слежения или в нескольких зонах. В этом случае UE при последней локализации получает от MME список зон, по которым будут передавать сигналы пейджинга. В сети также предусмотрена периодическая локализация, когда UE через определенное время запускает процедуру *TAU*, чтобы подтвердить свою доступность.

Когда UE зарегистрирован в сети и пребывает в состоянии *IDLE*, в MME, S-GW, PDN GW открыты базы данных абонента, сохраняются сигнальные туннели на S1, S5/S8 и туннели для сквозных каналов на S5/S8. Процедура *TAU* может происходить без замены MME, со сменой MME и со сменой S-GW. Алгоритм процедуры с заменой MME приведен на рис. 8.4 [6].

Процедуру запускает UE (п.1). После установления соединения с сетью следует сообщение *Tracking Area Update (TAU) Request* (п.2). Оно содержит идентификаторы и параметры обслуживающей абонента сети, GUTI, идентификатор последней зоны пребывания UE, параметры безопасности, порядковый номер передаваемого сообщения NAS. Эта команда должна быть защищена кодом целостности сообщения MAC (Message Authentication Code). [5]

П.3. Из полученного сообщения eNB извлекает старый GUMMEI и определяет сеть, в которой зарегистрирован абонент. eNB направляет запрос на локализацию в новый MME, дополняя его параметром TAI+ECGI, что позволяет локализовать абонента с точностью до соты.

П.4. MME определяет старый MME (old MME) и отправляет ему запрос *Context Request* для получения базы данных абонента. Это сообщение содержит *TAU Request*, чтобы старый MME мог проверить и подтвердить его целостность. Если *TAU Request* содержал параметры SGSN, то запрос направляют в SGSN.

П.5. Старый MME проверяет целостность сообщения *TAU Request* и если она подтверждена, то в сообщении *Context Response* пересылает базу данных абонента и UE: IMSI, MSISDN, параметры безопасности, контекст сквозных каналов, адрес и сигнальный TEID S-GW и т.д. Если целостность *TAU Request* нарушена или в старом MME нет базы данных абонента, то *Context Response* содержит информацию об ошибке. В этом случае обязателен к выполнению п.6. MME запускает в полном объеме процедуры безопасности: аутентификации и генерации ключей шифрации и целостности (п.3.3). При получении параметров безопасности в *Context Response* объем

[5] В сообщении *TAU Request* UE может вместо GUTI передавать параметры, относящиеся к пакетной сети GERAN/UMTS: к базе данных абонента в SGSN.

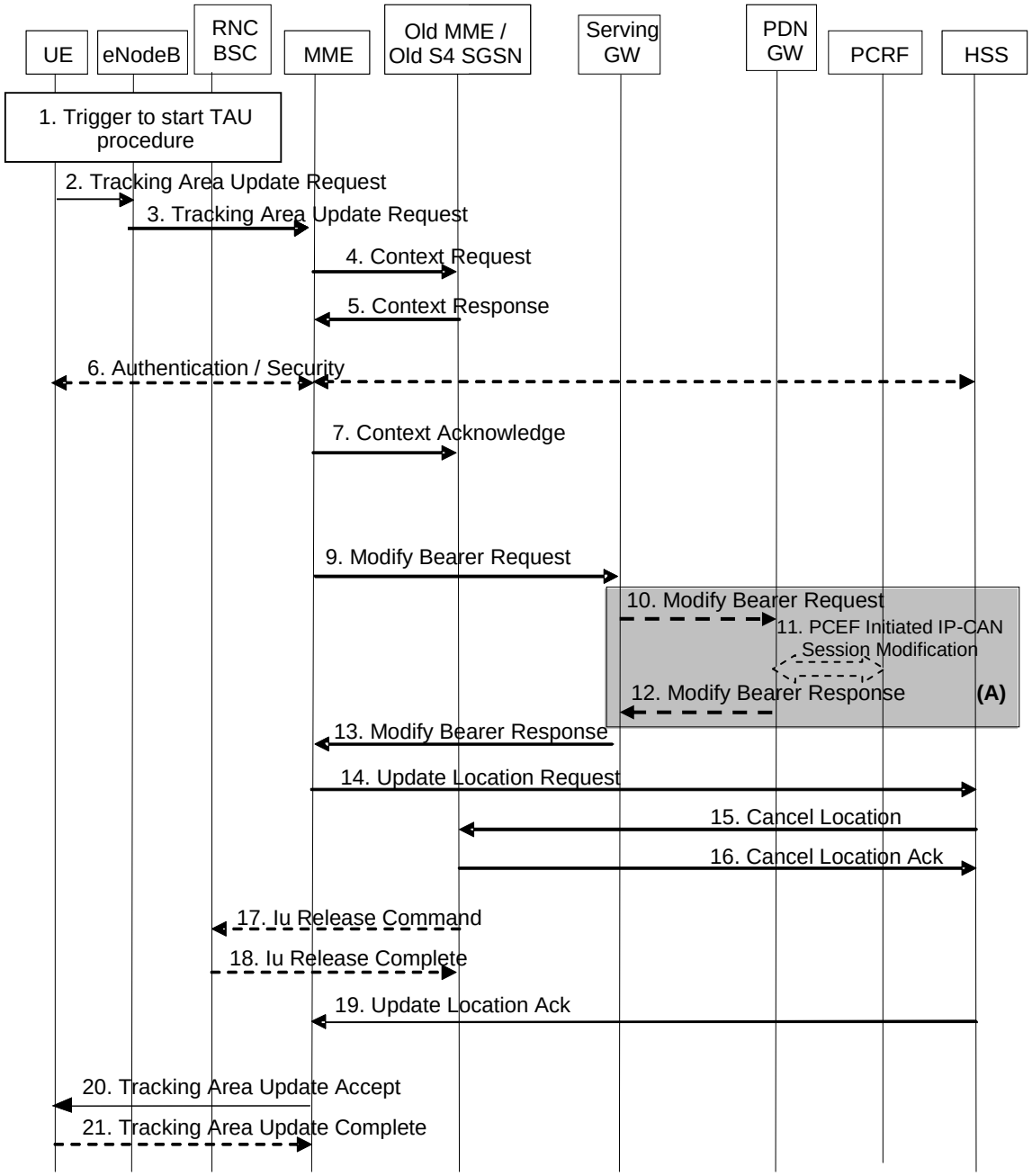


Рис. 8.4. Процедура TAU с заменой MME

выполнения п.6 определяет оператор. MME отправляет в старый MME подтверждение в получении базы данных абонента (*Context Acknowledge*, п.7).

П.9. Если произошла смена MME, новый MME создает базу данных абонента, устанавливая контекст его сквозных каналов, полученный из старого MME. При этом он проверяет возможность поддержки ранее организованных каналов и деактивирует те соединения, которые он поддерживать не может. Далее он организует сигнальное соединение на интерфейсе S11. Сообщение *Modify Bearer Request* содержит тип сети, адрес MME и TEID. Опционально MME может активизировать ISR. Из полученного контекста

сквозных каналов абонента MME определяет адрес S-GW и при смене сети передает в S-GW идентификатор новой сети, а также изменения часового пояса обслуживания абонента и его местоположения.

ПП. 10. 11, 12 (блок А) выполняют в случае, когда произошла смена сети обслуживания, часового пояса или локализации абонента, что связано с изменением тарифов услуг. S-GW передаёт необходимую информацию в PDN GW, а PDN GW запускает процедуру *IP-CAN Session Modification Procedure* [6].

П.13. S-GW обновляет базу данных абонента и направляет в MME сообщение *Modify Bearer Response*, содержащее адрес S-GW и TEID для передачи трафика вверх.

П.14. Новый MME проверяет наличие необходимых данных для UE и, если произошла смена MME, информирует об этом HSS (*Update Location Request*), сообщая свой адрес и возможности в обслуживании абонента. HSS посылает в старый MME команду *Cancel Location* (п.15). Старый MME может сразу удалить базу данных абонента или спустя некоторое время, запустив соответствующий таймер. В HSS он отсылает подтверждение *Cancel Location Ack.*

ПП.17 и 18 выполняют в том случае, когда для UE организован Iu интерфейс с контроллером сети GERAN/UTRAN.

П.19. HSS подтверждает получение сообщения от нового MME (*Update Location Ack)* и при необходимости передаёт в новый MME дополнительные данные об абоненте. MME: завершает формирование базы данных абонента. В сообщении *Tracking Area Update Accept* (п.20) абонент получает GUTI, список зон регистрации (TAI-list), статус сквозных каналов (часть прежних каналов может быть удалена). Если GUTI изменился, UE подтверждает получение сообщения *Tracking Area Update Accept* (п.21).

8.5. Перевод абонентской станции в состояние Idle

При переводе UE из состояния *CONNECTED* в состояние *IDLE* происходит разрыв сигнального соединения UE – MME и разрушение участков сквозных каналов трафика на радиоинтерфейсе и интерфейсе S1. eNB удаляет базу данных, относящуюся к UE. В спецификациях [6] – это *S1 Release Procedure* (рис. 8.5).

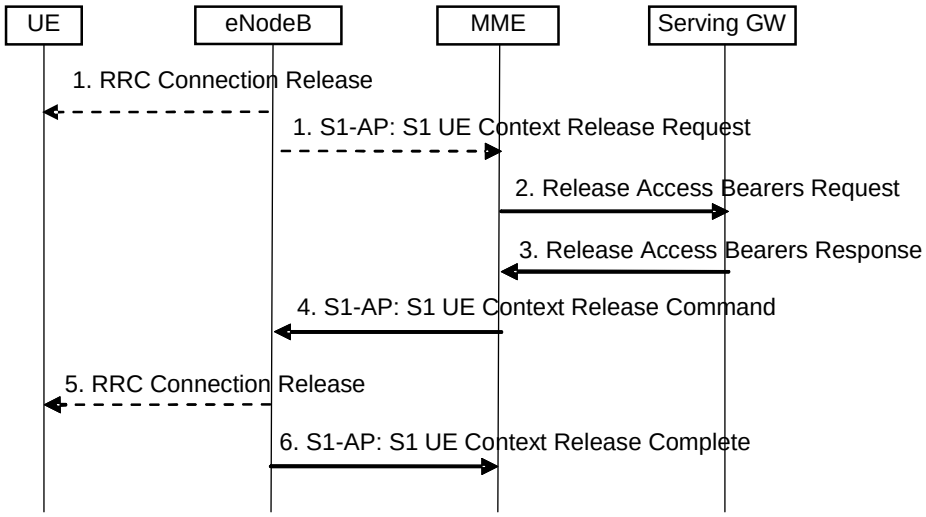


Рис. 8.5. Процедура освобождения интерфейса S1

Обычно эту процедуру запускает eNB (п.1), например, при срабатывании таймера неактивности абонента или разрыва с UE сигнального соединения, но её может инициировать и MME. Получив от eNB сообщение *S1-AP: S1 UE Context Release Request,* MME направляет в S-GW команду *Release Access Bearer Request* (п.2).

S-GW убирает из базы данных UE всё, что касается eNB (адрес и TEID по S1 вниз) и отвечает MME сообщением *Release Access Bearer Response* (п.3). Все остальные данные контекста UE S-GW сохраняет. Это параметры организованных ранее сквозных каналов данного абонента, в частности, туннелей на интерфейсе S5/S8, и их конфигурацию на S1-U. Сохраняются и TEID туннельных соединений вверх на S1-U и S11. Поэтому при поступлении пакетов входящего трафика, когда UE находится в состоянии *IDLE*, S-GW буферизирует эти пакеты и запускает процедуру *Service Request* (рис. 8.6).

П.4. MME освобождает интерфейс S1, отправляя eNB команду*S1-AP: S1 UE Context Release Command.* Если eNB ещё не разорвал соединения с UE по протоколу RRC, он передает UE сообщение *RRC Connection Release* (п.5), требуя подтверждения. В сообщении *S1-AP: S1 UE Context Release Complete* (п.6) eNB информирует MME об освобождении интерфейса S1 от сквозных каналов абонента. Получив от UE подтверждение получения сообщения (п.5), eNB удаляет базу данных UE.

MME из контекста UE стирает всю информацию, относящуюся к eNB (адрес, идентификаторы соединений), но остальные данные сохраняет для последующей процедуры *Service Request.*

8.6. Процедура Service Request

Service Request – процедура запроса услуги передачи данных по ранее организованному сквозному каналу. На интерфейсе S5/S8 существует тунель для пакетов трафика, а в PDN GW, S-GW и MME– параметры сквозного канала занесенные в соответствующие базы данных. Процедуру может инициировать как абонент, так и сеть (входящий вызов). Как правило, при этой процедуре станция переходит из состояния *IDLE* в состояние *CONNECTED*. Алгоритм процедуры *Service Request* при запуске со стороны абонента представлен на рис. 8.6 [6].

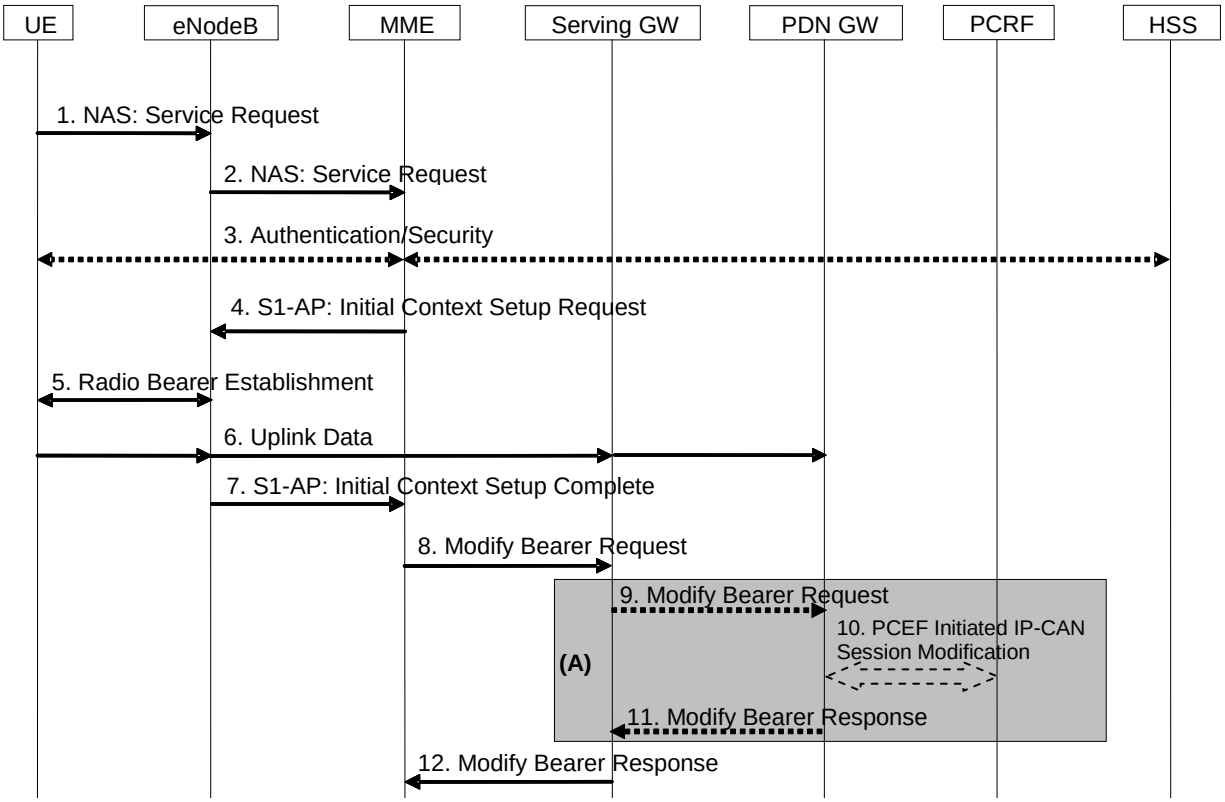


Рис.8.6. Процедура Service Request, запускаемая UE

UE посылает сообщение *NAS: Service Request* (п.1), которое eNB доставляет в MME, дополняя его идентификатором соты (TAI+ECGI) и временным идентификатором абонента S-TMSI. (п.2). MME может запустить процедуры аутентификации и генерации ключей безопасности или использовать данные, полученные ранее (п.3) (п.3.3).

MME направляет в eNB сообщение *S1-AP: Initial Context Setup Request* (п.4). Оно содержит адрес S-GW, TEID туннеля вверх на интерфейсе S1-U, параметры QoS организуемого сквозного канала, параметры безопасности, идентификатор сигнального соединения, список ограничений при хэндове-

ре[6]. eNB заполняет базу данных обслуживаемого абонента и организует канал трафика на радиоинтерфейсе, включая шифрацию пользовательской информации (п.5). Теперь UE может начать передачу пользовательских пакетов вверх *Uplink Data* (п.6).

П.7. eNB в сообщении *S1-AP: Initial Context Setup Complete,* передает MME свой адрес, список установленных (принятых) и удаленных сквозных каналов абонента, TEID туннеля вниз на интерфейсе S1-U.

П.8. MME отсылает S-GW сообщение *Modify Bearer Request* (адрес eNB, TEID туннеля вниз на интерфейсе S1-U, тип сети радиодоступа RAT). Теперь завершена организация туннельного соединения на интерфейсе S1-U. Если произошли изменения сети обслуживания абонента или часового пояса, то эту информацию MME также включает в данную команду.

ПП.9 – 11 (блок А) выполняют только при смене сети обслуживания абонента или часового пояса. Эти изменения должны быть учтены PCRF, в частности, в установлении тарифов.

Подтверждение S-GW о завершении организации сквозного канала (п.12 *Modify Bearer Response)* заканчивает процедуру.

Алгоритм процедуры *Service Request* при входящих вызовах (поступлении пакетов трафика со стороны сети) показан на рис. 8.7 [6].

Он представляет собой процедуру *Service Request*, рассмотренную ранее (в п.5 использован алгоритм на рис. 8.6), дополненную командами пейджинга абонентского терминала.

Пришедшие пакеты трафика PDN GW направляет в S-GW по существующему туннелю на интерфейсе S5/S8. S-GW их буферизирует. Передавать дальше он их не может, так как сквозной канал на участке UE – eNB – S-GW отсутствует. S-GW определяет, какой MME или SGSN ведет базу данных абонента и посылает туда уведомление (п.2a *Downlink Data Notification*). MME или SGSN подтверждают получение уведомления (п.2b *Downlink Data Notification Ack),* формируют сообщение пейджинга (3a,b), которое через eNB или RNC/BSC доставляют UE (4a,b).

Если UE находится в состоянии *IDLE*, то алгоритм (рис.8.6) выполняют полностью, начиная с первого сообщения *NAS:Service Request.* В том случае, когда между UE и MME существует сигнальное соединение (например, абонент получает трафик по другому сквозному каналу), но туннель на S1-U для данной услуги отсутствует, то алгоритм (рис. 8.6) запускают с п.4: MME посылает команду *S1-AP: Initial Context Setup Request* организовать сквозной канал на радиоинтерфейсе.

[6] В этом списке MME указывает сети, зоны, соты, в которые хэндовер невозможен.

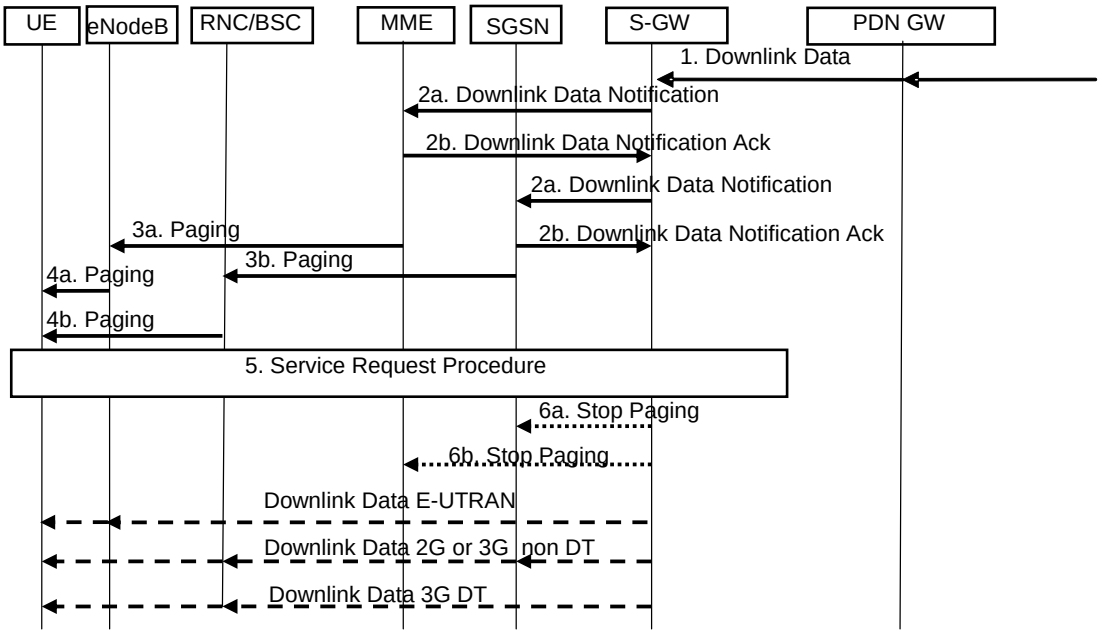


Рис.8.7. Процедура Service Request, запускаемая сетью

ПП.6a и 6b выполняют, когда активизирован ISR. Если S-GW получил информацию от MME об отправке сообщения пейджинга, он посылает SGSN команду *Stop Paging*. Наоборот, при отправке сообщения пейджинга из SGSN команду *Stop Paging* получает MME.

8.7. Процедура Detach

Процедуру *Detach* – отключение абонента от сети, может запускать как абонент, так и сеть, например, когда истекает время нахождения UE в состоянии *IDLE*. В этом случае процедуру инициирует MME.

На рис. 8.8 приведен протокол процедуры *Detach*, запускаемой UE [6].

UE посылает сообщение *Detach Request,* содержащее GUTI и Switch off (п.1). eNB, пересылая это сообщение в MME, добавляет к нему идентификатор соты, где находится абонент, TAI+ECGI.

Посылая сообщение *Delete Session Request* в S-GW (п.2), MME запускает процедуру деактивации сквозных каналов. S-GW стирает базу данных абонента и отправляет команду *Delete Session Request* в PDN GW деактивировать сквозные каналы на интерфейсе S5/S8 (п.6). PDN GW стирает базу данных абонента и запускает процедуру освобождения канального ресурса (завершения сеанса связи) *IP-CAN Session Termination Procedure* (п.8). О выполнении команд S-GW информирует MME (п.3), а PDN GW – S-GW (п.7).

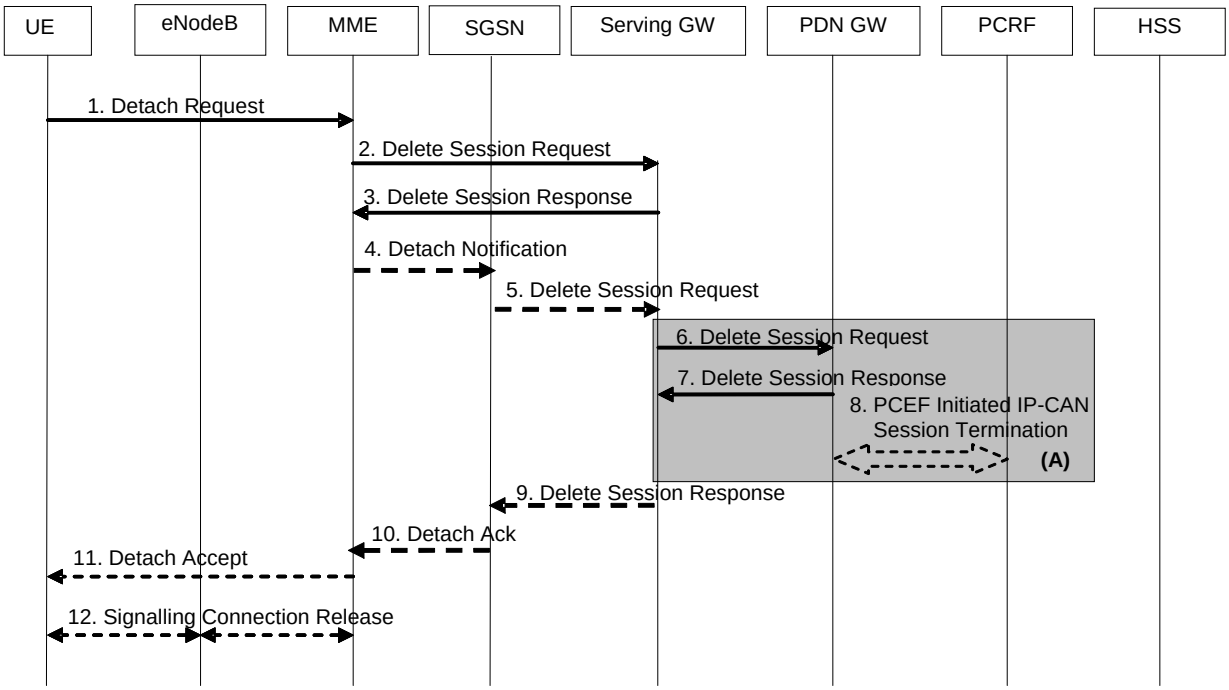


Рис.8.8. Процедура Detach

Если был активирован ISR, т.е. UE был параллельно подключен к сетям E-UTRAN и GERAN/UTRAN, MME командой *Detach Notification* (п.4) деактивирует базу данных абонента в SGSN, о чем тот информирует S-GW (п.5, *Delete Session Request*). В этом варианте процедуры команду (п.6) S-GW отсылает только после получения сообщения (п.5).

Сообщения (пп.9, 10, 11), подтверждающие выполнение соответствующих команд, опциональны. Командой *Signaling Connection Release* (п.12) MME освобождает сигнальное соединение на интерфейсе S1. Происходит стирание данных UE в eNB. MME сохраняет базу данных абонента в заблокированном состоянии.

8.8. Процедура активации (организации) сквозного канала

Основная часть алгоритма процедуры *Dedicated Bearer Activation* представлена на рис. 8.9 [6].

Параметры сквозного канала: возможность выделения необходимого канального ресурса, качественные характеристики канала QoS и тарифы обслуживания устанавливает PCRF. PDN GW использует полученные от PCRF параметры как основу при выполнении процедуры *Dedicated Bearer Activation* (п.1). Он генерирует идентификатор оплаты услуги (Charging Id) и отправляет в S-GW сообщение *Create Bearer Request* (п.2). Это сообщение содержит IMSI, параметры QoS, TEID на S5/S8, Charging Id и TFT. В *Create Bearer Request* также включен идентификатор сквозного канала по умолчанию для данного UE (LBI – Linked EPS Bearer Identity), организованного в результате выполнения процедуры Attach (см. 8.3). В случае, когда проце-

дуру *Dedicated Bearer Activation* запускает UE (см. далее 8.10), сообщение содержит идентификатор транзакции PTI (Procedure Transaction Id).

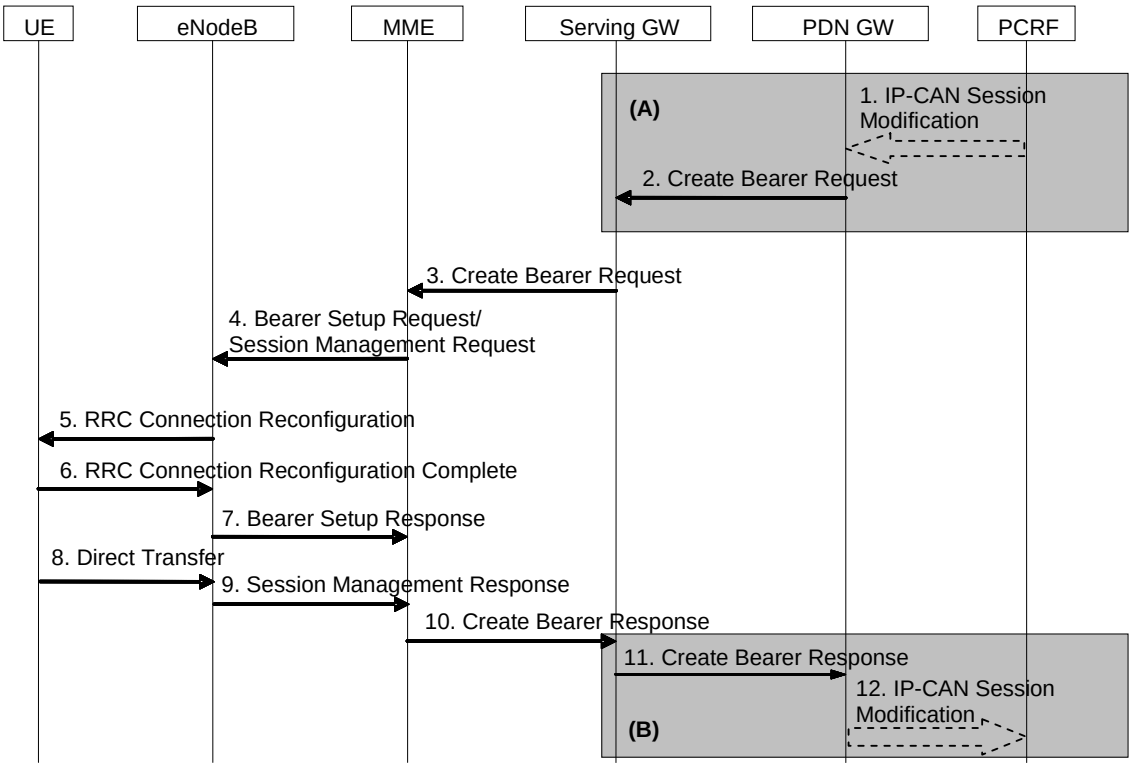


Рис.8.9. Процедура активации сквозного канала

П.3. S-GW посылает MME сообщение *Create Bearer Request*, содержащее IMSI, QoS сквозного канала, TFT, S1-TEID, LBI. Если UE находится в состоянии IDLE, то MME запустит процедуру *Service Request* (рис. 8.7), начиная с п.3. При этом пп.4–7 процедуры *Service Request* могут выполняться параллельно командами данной процедуры.

П.4. MME присваивает организуемому сквозному каналу новый идентификатор (EPS Bearer Identity) и включает его вместе с PTI, TFT, QoS сквозного канала, LBI в сообщение *Session Management Request*. Далее MME передаёт eNB команду *Bearer Setup Request*, содержащую идентификатор канала, сообщение *Session Management Request,* QoS сквозного канала, S1-TEID.

eNB устанавливает полученные QoS как директивные при организации канала на радиоинтерфейсе. Терминалу eNB отсылает команду *RRC Connection Reconfiguration* (QoS, *Session Management Request,* идентификатор сквозного канала на радиоинтерфейсе) (п.5). UE устанавливает полученный идентификатор канала, его QoS, LBI. UE использует пакетные

фильтры вверх (UL TFT) при передаче трафика данной услуги по организованному каналу.

П.6. Ответом *RRC Connection Reconfiguration Complete* UE подтверждает полученное сообщение.

П.7. eNB подтверждает завершение организации канала сообщением *Bearer Setup Response* (идентификатор канала, S1-TEID). В сообщении eNB указывает, может ли он активировать канал на радиоинтерфейсе с требуемым QoS или нет.

UE формирует сообщение NAS *Session Management Response* (п.9) для MME, которое передает через eNB командой *Direct Transfer* (п.8).

Получив подтверждения от UE (п.9) и eNB (п.7), MME подтверждает организацию сквозного канала, отсылая S-GW сообщение *Create Bearer Response* (идентификатор канала, S1-TEID) (п.10). S-GW отправляет подтверждение PDN GW *Create Bearer Response* (идентификатор канала, S5/S8 TEID) (п.11). В конце процедуры уведомление об организации сквозного канала с установленными параметрами QoS получает PCRF (п.12).

8.9. Процедура изменения параметров качества сквозного канала

Процедура *Bearer modification with bearer QoS update* позволяет изменить следующие его характеристики :

- класс услуг (QCI),

- гарантированную скорость передачи данных в канале (GBR),

- максимальную скорость передачи данных в канале (MBR – Maximum Bit Rate),

- TFT,

- приоритет в назначении и сохранении канала (ARP – Allocation and Retention Priority). Заметим, что ARP не передают UE и он не влияет на работу планировщиков в мобильном терминале и eNB,

- APN-AMBR – per APN Aggregate Maximum Bit Rate. Напомним, что на передачу по каналам с гарантированной скоростью APN-AMBR не влияет.

Отметим, что данная процедура может менять QCI и ARP сквозного канала по умолчанию, но не позволяет изменить тип канала GBR на Non-GBR и наоборот.

Алгоритм процедуры приведен на рис. 8.10 [6].

Сравнение алгоритмов данной процедуры (рис. 8.10) и процедуры *Dedicated Bearer Activation* (рис. 8.9) показывает их структурное родство. Различия состоят в назначении и содержании сообщений. В начале процедуры PCRF определяет политику в отношении изменений параметров QoS

сквозного канала, передавая сообщение *IP-CAN Session Modification* [19] о его модификации в PDN GW (п.1).

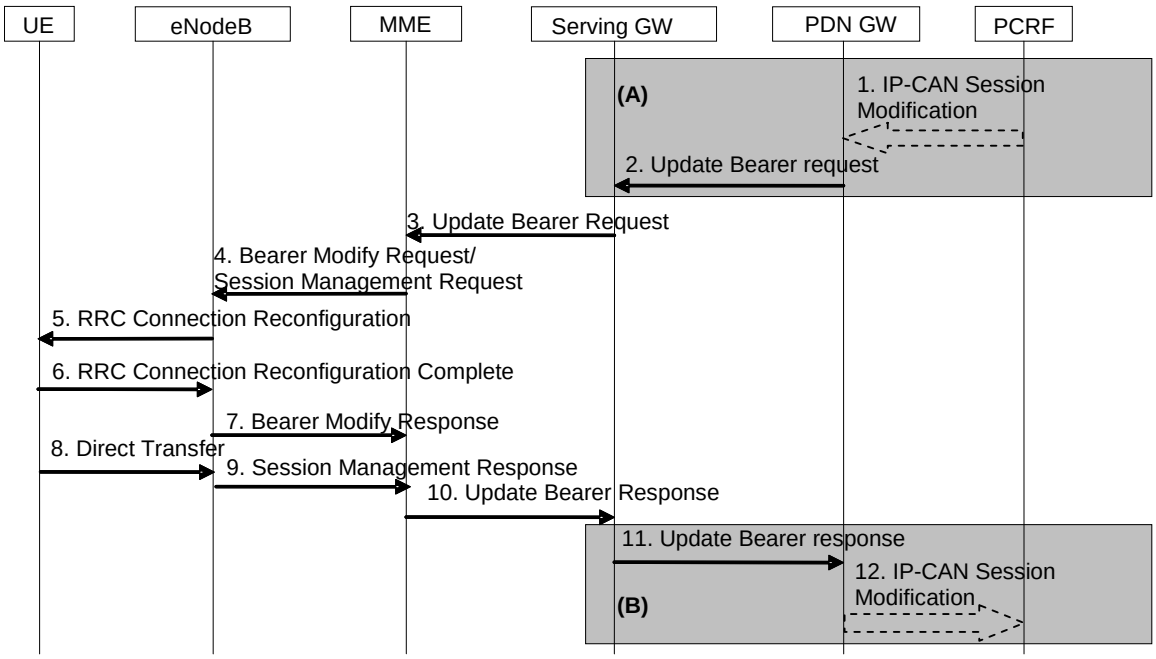


Рис.8.10. Процедура изменения параметров качества сквозного канала

П.2. PDN GW устанавливает, какие параметры QoS потока данных должны быть изменены или какие потоки должны быть объединены или удалены из активного сквозного канала. Далее он посылает S-GW сообщение *Update Bearer Request*, содержащее идентификатор канала, его QoS, APN-AMBR, TFT. Если процедуру инициировал UE, то в сообщение включают PTI. Параметр APN-AMBR относится только к каналам с негарантированной скоростью.

П.3. S-GW отправляет MME сообщение *Update Bearer Request*, содержащее все полученные им от PDN GW параметры канала. Если UE находится в состоянии *IDLE*, то MME запускает процедуру *Service Request* (рис. 8.7) с п.3. параллельно с выполнением данной процедуры. Если изменения касаются только APN-AMBR, а UE находится в состоянии *IDLE*, то запуска процедуры *Service Request* не происходит, а пп.4 – 9 данной процедуры пропускаются.

П.4. MME готовит сообщение *Session Management Request,* включая в него идентификатор канала, QoS канала, APN-AMBR, TFT и PTI. Если изменен APN-AMBR, то MME может изменить UE-AMBR. На eNB MME отправляет сообщение *Bearer Modify Request*, состоящее из идентификатора канала, его QoS, *Session Management Request,* UE-AMBR.

eNB устанавливает полученные QoS как директивные при организации канала на радиоинтерфейсе. Терминалу eNB отсылает команду *RRC Connection Reconfiguration* (QoS, *Session Management Request,* идентифика-

тор сквозного канала на радиоинтерфейсе) (п.5). Если изменен APN-AMBR, UE записывает его в базу данных и может изменить MBR PDP-контекста для каналов не с гарантированной скоростью. При передаче трафика по модифицированному каналу UE использует пакетные фильтры вверх (UL TFT).

В пп.6 – 12 процедуры передают подтверждения выполнения полученных команд, как и в алгоритме процедуры активации сквозного канала (рис. 8.9).

8.10. Процедура модификации сквозных каналов по запросам UE

UE может запросить организовать новый сквозной канал с определенным QoS для новой услуги, изменить пакетные фильтры существующего канала или запустить процедуру снятия (деактивации) канала (см. 8.11). При этом в сети должно существовать соединение по протоколу IP между UE и PDN GW. В запросе на изменение пакетных фильтров UE передает параметр TAD (Traffic Aggregate Description), содержащий идентификаторы фильтров и информацию о них.

Алгоритм процедуры показан на рис.8.11 [6].

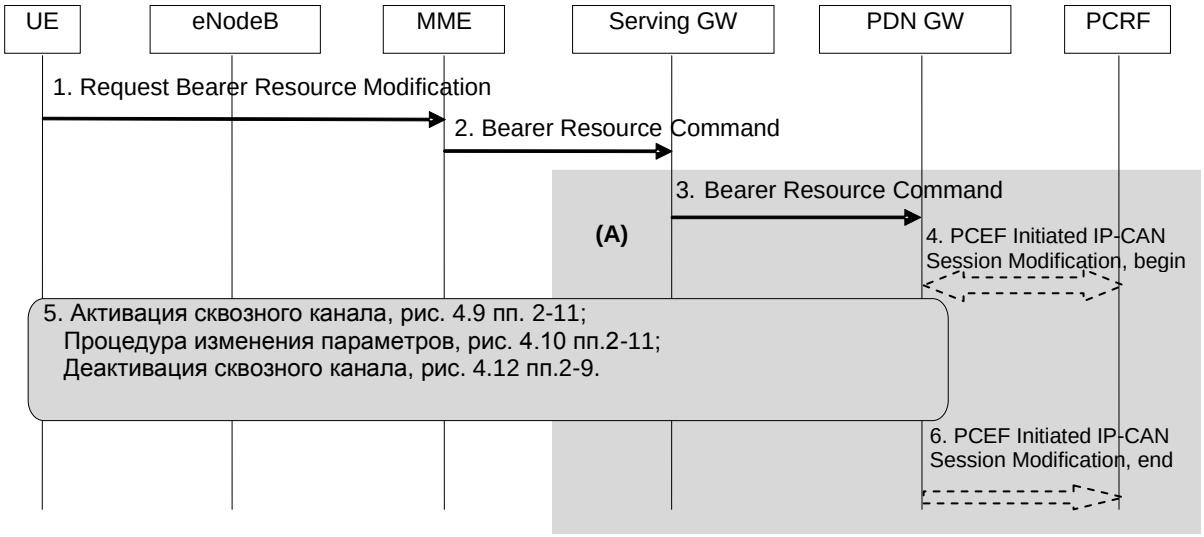


Рис.8.11. Процедура модификации сквозных каналов по запросам UE

Процедура начинается с запроса *Request Bearer Resource Modification* (п.1), в котором UE передает LBI, PTI, идентификатор сквозного канала, QoS, Protocol Configuration Options. MME по индикатору сквозного канала по умолчанию LBI проверяет действенность запроса и при его подтверждении направляет запрос далее в S-GW, откуда он следует в PDN GW и в PCRF (пп.2 – 4). Начиная с п.4 идет выполнение процедур активизации сквозного канала (рис. 8.9) или изменения его параметров (рис. 8.10).

8.11. Деактивация (снятие) сквозного канала

Процедуру *Dedicated Bearer Deactivation* (снятия сквозного канала) может запустить UE или MME. В любом случае запрос процедуры следует на PDN GW, PCRF и ее выполнении начинается с п.1 (рис. 8.12) [6]. PCRF посылает PDN GW команду снять сквозной канал в рамках микропроцедуры *IP-CAN Session Modification.*

PDN GW отправляет S-GW сообщение *Delete Bearer Request* (п.2), содержащее идентификатор удаляемого канала, причину его удаления, а также PTI, если инициатором деактивации канала был UE. S-GW пересылает сообщение *Delete Bearer Request* далее MME (п.3a) и SGSN (п.3b), когда активизирован ISR.

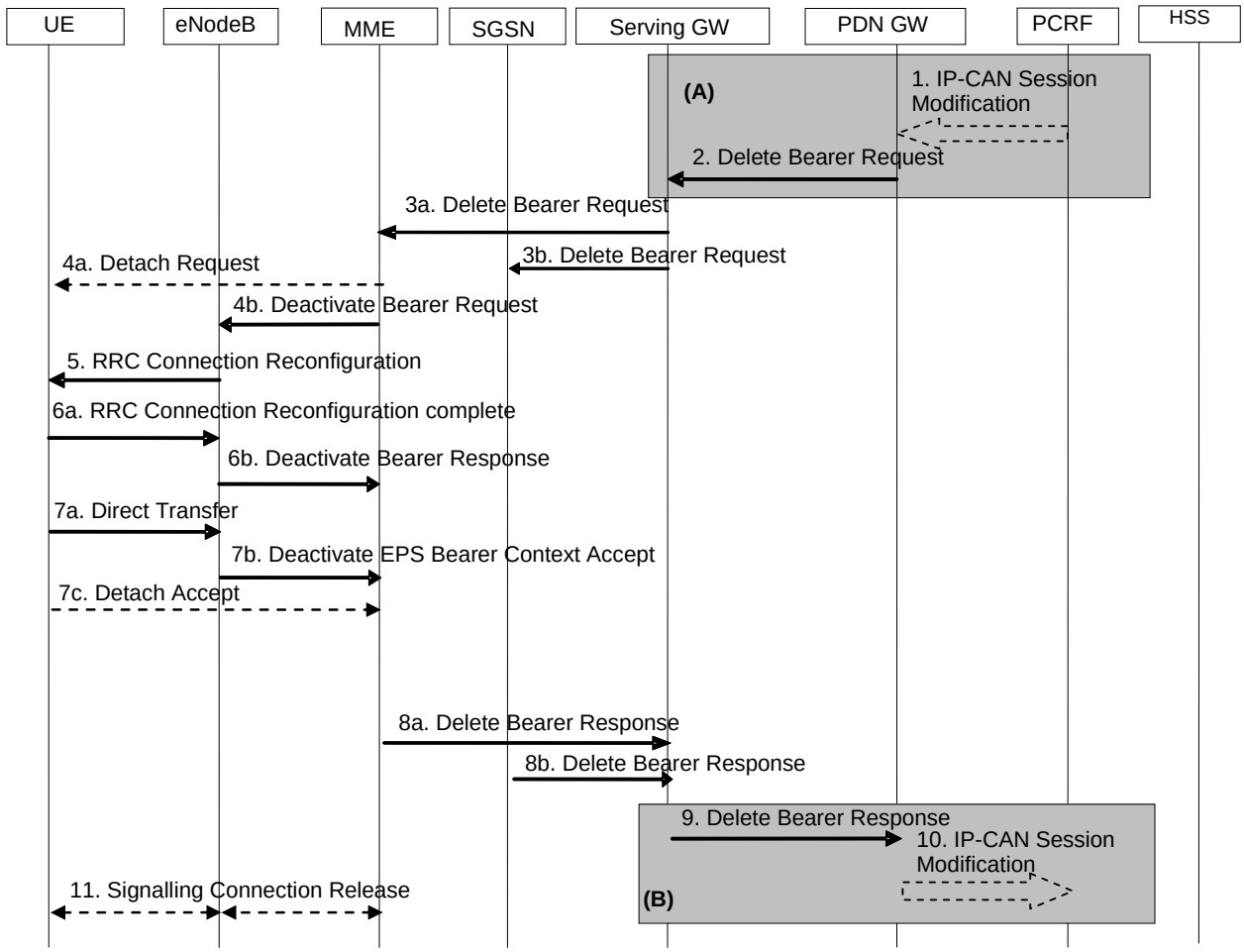


Рис.8.12. Процедура деактивации сквозного канала; UE в состоянии CONNECTED

Если удаляемый сквозной канал – последний, связывающий UE с сетью, то MME запускает процедуру отключения UE от сети командой *Detach Request* (п.4a). Если UE при этом пребывает в состоянии *IDLE*, MME

вызывает абонента, посылая ему сигнал пейджинга. В этом случае пп. 4b – 7b не выполняют и процедуру продолжают с п. 7c.

Если сквозной канал уже удален на радиоинтерфейсе и MME об этом информирован, то пп. 4 – 7 также пропускают. Если удаляемый канал не последний, связывающий UE с сетью, MME отправляет eNB сообщение *Deactivate Bearer Request* (п.4b). Внутри это сообщение содержит команду NAS для UE *Deactivate EPS Bearer Context Request*, где указан идентификатор удаляемого канала. Если запрос на удаление канала исходил от UE, то в команду включают PTI.

П.5. eNB отправляет сообщение *RRC Connection Reconfiguration*, содержащее идентификатор удаляемого радиоканала и команду *Deactivate EPS Bearer Context Request.* UE деактивирует радиоканал, указанный в сообщении (п.5), снимает TFT вверх удаленного канала и его идентификатор. Выполнив необходимые процедуры, UE отвечает сообщением *RRC Connection Reconfiguration Complete* (п.6a). eNB посылает MME подтверждение об удалении сквозного канала *Deactivate Bearer Response* (п.6b).

UE формирует сообщение NAS *Deactivate EPS Bearer Context Accept*, где указан идентификатор удаленного канала. Это сообщение для MME (п.7b) UE отправляет eNB посредством команды *Direct Transfer* (п.7a). Если UE получил от MME команду *Detach Request* (п.4a), то он отвечает подтверждением *Detach Accept* (п.7c).

П.8. После получения сообщений *Deactivate Bearer Response* и *Deactivate EPS Bearer Context Accept* MME удаляет контекст, относящийся к деактивируемому сквозному каналу и подтверждает выполнение процедуры, посылая S-GW *Delete Bearer Response.* При активизации ISR SGSN также удаляет PDP-контекст деактивированного канала, о чем отправляет подтверждение (п.8b).

Получив подтверждения, S-GW удаляет контекст деактивированного канала и уведомляет об этом PDN GW сообщением *Delete Bearer Response* (п.9). Теперь пришла очередь PDN GW удалить контекст деактивированного канала, после чего PDN GW информирует об освобождении канального ресурса PCRF. Команды (п.11) следуют в том случае, если происходит отключение UE от сети.

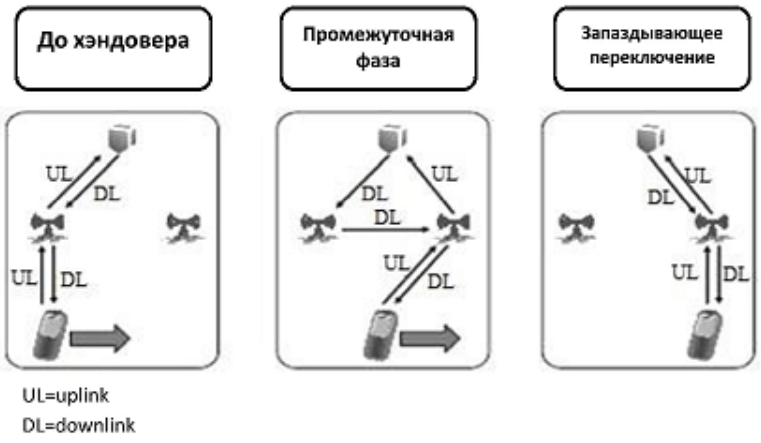
8.12. Внутрисистемный хэндовер с использованием интерфейса X2

Вопрос о хэндовере возникает при выполнении событий *Event A3* или *Event A5* (см. 5.1). Стандарт предусматривает 2 варианта хэндовера:

- с использованием интерфейса X2, напрямую связывающего обслуживающий (source) eNB и целевой (target) eNB, на который сеть переключает UE,
- без использования интерфейса X2, когда весь сигнальный обмен идет по интерфейсу S1-C (рис. 1.1).

- Хэндовер может происходить без смены S-GW и со сменой обслуживающего шлюза. Рассмотрим здесь протокол первого варианта хэндовера без смены S-GW. Хэндоверы со сменой S-GW и второй вариант описаны в [6].

- Процедура внутрисистемного хэндовера состоит из 3 этапов: подготовки к хэндоверу, собственно хэндовера и завершения хэндовера (запаздывающего переключения). До хэндовера трафик идет через обслуживающий eNB (рис. 8.13). После переключения UE на новый целевой eNB трафик вверх идет через него, а вниз через обслуживающий eNB, интерфейс X2 и целевой eNB. После 3-го этапа хэндовера, происходящего с участием MME и S-GW, происходит переключение трафика вниз на целевой eNB.



- Рис.8.13. Переключение сквозных каналов трафика при хэндовере

Алгоритм первых двух этапов процедуры представлен на рис.8.14 [16]. Сплошными линиями на рис.8.14 показаны сигнальные сообщения, пунктиром – передача пакетов трафика.

На первых двух этапах хэндовера использована сигнализация протокола RRC и интерфейса X2. На source eNB есть список eNB-кандидатов на хэндовер. При подготовке хэндовера source eNB дает UE команду произвести измерения сигналов конкретного eNB из этого списка для выбора его как целевого объекта (п.1). Для передачи результатов измерений UE получает дополнительный канальный ресурс вверх (UL allocation). UE передает запрошенные данные (п.2), на основе которых source eNB принимает решение о запуске процедуры хэндовера (п.3).

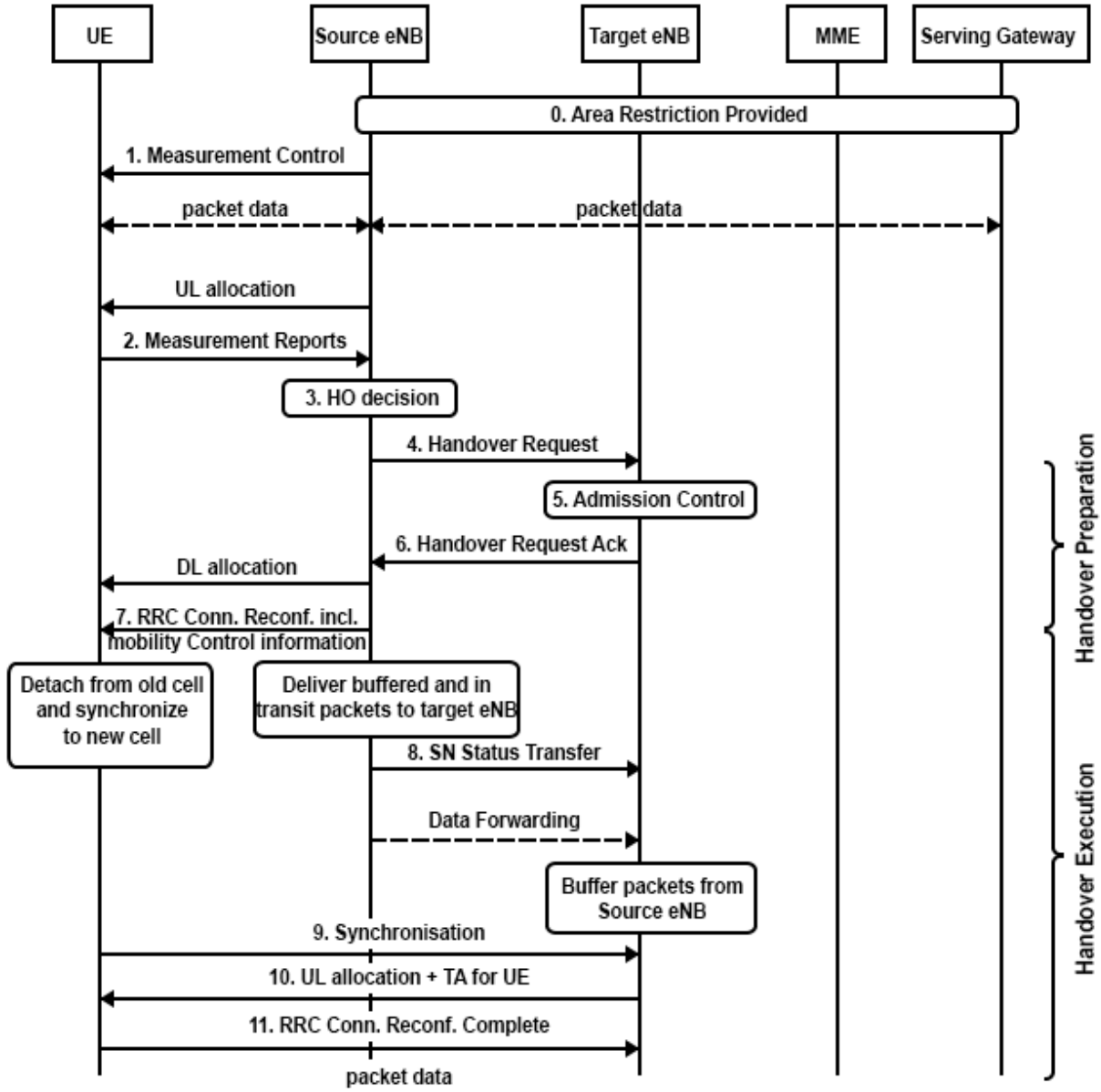


Рис. 8.14. Процедура внутрисистемного хэндовера (два первых этапа)

П.4. Обслуживающий eNB отправляет на целевой сообщение *Handover Request*. Оно содержит параметры сигнальных соединений UE на интерфейсах S1 и X2, идентификатор целевой соты, ключ k_{eNB} для выполнения процедур безопасности, контекст UE по протоколу RRC, включая идентификатор C-RNTI абонента в исходной соте, идентификатор исходного eNB, , информацию о поддерживаемых сквозных каналах, включая их идентификаторы и профили QoS.

П.5. Целевой eNB выполняет процедуру управления доступом (*Admission Control*), оценивая канальный ресурс, который он должен выделить для всех сквозных каналов абонента. Если ресурса достаточно, eNB дает согласие на хэндовер и подготавливает конфигурацию каналов управления на радиоинтерфейсе к подключаемому UE.

П.6. В сообщении *Handover Request Acknowledge* целевой eNB передает прозрачный контейнер параметров для UE. Среди этих параметров новый C-RNTI, идентификаторы алгоритмов безопасности, системная информация. Опционально может быть передан код преамбулы RACH для процедуры доступа UE к сети. По существу целевой eNB передает сообщение *RRCConnectionReconfiguration,* содержащее контейнер с *mobilityControlInformation.* Обслуживающий eNB шифрует это сообщение, защищает его целостность и транслирует UE (п.7). UE начинает выполнение операций хэндовера. В целях ускорения процедуры он не отправляет на обслуживающий eNB подтверждения полученной команды.

Начинается второй этап процедуры. Обслуживающий eNB отсылает целевому eNB сообщение *SN Status Transfer*, содержащее информацию о состоянии передачи SDU (Service Data Units), включая номера пакетов для повторной передачи (п.8). После этого по каналу трафика интерфейса X2 следует передача буфера данных.

П.9. UE синхронизируется с целевым eNB и, используя полученные в контейнере с *mobilityControlInformation* параметры, посылает преамбулу запроса на доступ к целевому eNB. Приняв запрос, целевой eNB выделяет UE канальный ресурс для передачи вверх и передает параметр TA (Timing Advance) (п.10). В ответ UE отсылает подтверждение завершения хэндовера *RRCConnectionReconfigurationComplete*, содержащее новый C-RNTI. Теперь передача трафика может возобновиться.

П.11. Процедура подключения UE к целевому eNB завершена. UE отправляет на новый обслуживающий его целевой eNB сообщение *RRCConnectionReconfigurationComplete* с новым C-RNTI вместе с сообщением о статусе его буфера. Начинается передача трафика в обоих направлениях. При этом в направлении вверх трафик идет по прямому маршруту UE → целевой eNB → S-GW, но в направлении вниз по-прежнему через обслуживающий его до хэндовера eNB: S-GW → исходный eNB, поскольку в S-GW TEID туннеля вниз на интерфейсе S1-U не переключен на новый целевой eNB. Поэтому в процедуре предусмотрен 3-й этап – запаздывающее переключение с целью организации туннеля вниз на S1-U: S-GW → целевой eNB.

Алгоритм этого этапа представлен на рис. 8.15 [6].

П.1. Целевой eNB отправляет MME сообщение *Path Switch Request,* содержащее TAI+ECGI соты, где находится абонент, и список сквозных каналов, которые следует переключить на данный eNB. MME по списку сквозных каналов проверяет, какие каналы были переключены на целевой eNB. Каналы, которые переключены не были, MME снимает с обслуживания.

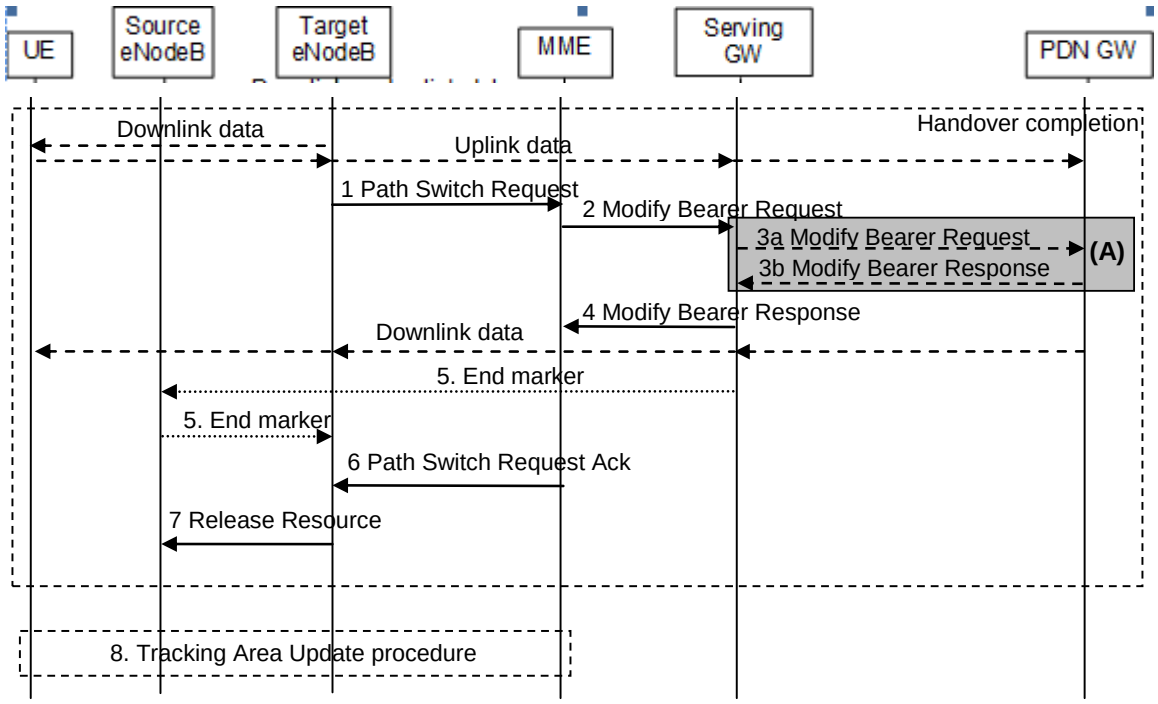


Рис 8.15. Процедура внутрисистемного хэндовера (третий этап)

П.2. MME посылает сообщение *Modify Bearer Request* (адрес визитного eNB, TEID для всех сквозных каналов вниз на S1-U). Если PDN GW запрашивает информацию о местоположении абонента, то MME включает ее в свое сообщение.

ПП.3a и 3b (блок A) опциональны и выполняются только в том случае, когда из-за изменения положения абонента меняется тарификация услуг.

S-GW посылает MME подтверждение *Modify Bearer Response* и начинает передачу пакетов вниз непосредственно целевому eNB по новому тунелю. Одновременно S-GW посылает исходному eNB специальные пакеты-маркеры (*End marker*) (п.5). Эти пакеты не содержат пользовательской информации, а то, что они маркерные, помечено в заголовке GTP. После передачи маркерных пакетов S-GW больше абонентских пакетов исходному eNB не шлет.

Исходный eNB пересылает маркерные пакты на целевой eNB и по интерфейсу X2 направляет полученные им из S-GW за время хэндовера пользовательские пакеты, которые он далее передает на UE.

П.6. Сообщением *Path Switch Request Ack* MME подтверждает сообщение (п.1). Если при хэндовере какие-либо сквозные каналы не были переключены на целевой eNB, то MME помечает их в *Path Switch Request Ack* с целью удаления в целевом eNB контекста этих каналов. Целевой eNB направляет исходному eNB сообщение *Release Resource* (п.7), информируя его

о завершении хэндовера и высвобождении им ресурса по обслуживанию данного UE.

Если в результате хэндовера UE вышел из предписанного списка зон слежения, то по завершении передачи трафика UE запускает процедуру локализации (п.8).

8.13. Процедура межсистемного хэндовера из E-UTRAN в UTRAN

Межсистемные хэндоверы UE возможны между сетями E-UTRAN (LTE)–UTRAN (UMTS), E-UTRAN–GERAN и E-UTRAN–CDMA2000. В этом и следующем параграфах будут рассмотрены хэндоверы E-UTRAN–UTRAN.

Процедура хэндовера из E-UTRAN в UTRAN состоит из двух фаз: подготовки хэндовера и выполнения хэндовера. До начала процедуры трафик идет через исходный eNB (Source eNB), исходный S-GW и PDN GW. Алгоритм подготовки хэндовера приведен на рис. 8.16 [6].

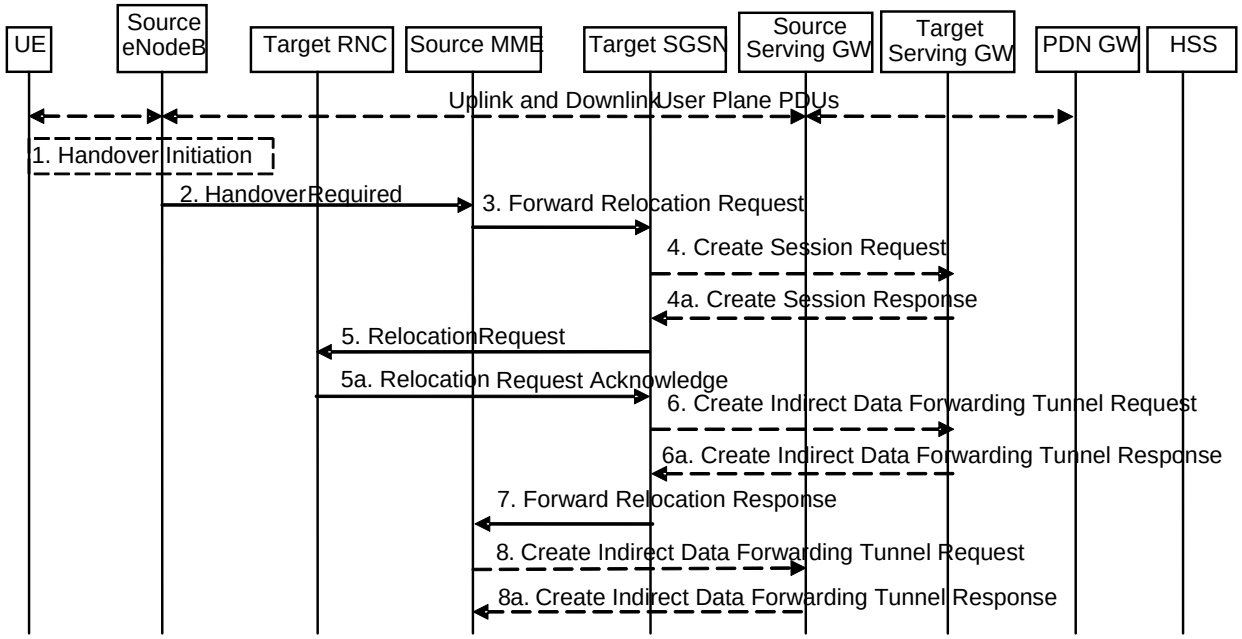


Рис.8.16. Подготовка хэндовера из E-UTRAN в UTRAN

П.2. Процедуру запускает исходный eNB (п.1). eNB посылает MME сообщение *Handover Required*, содержащее Cause[7], идентификатор целевого (target) RNC и контейнер данных для того, чтобы выделить необходимые ресурсы для обслуживания абонента в RNC, SGSN и S-GW. Далее в п.7

[7] Cause идентифицирует причину хэндовера [37].

SGSN идентифицирует сквозные каналы, которые надо будет организовать при переключении на сеть UMTS (UTRAN).

П.3. Из полученного сообщения MME определяет, что eNB запрашивает межсетевой хэндовер. MME определяет целевой (target) SGSN, который будет обслуживать абонента в сети UMTS. Если активизирован ISR, то приоритетным будет SGSN, где зарегистрирован абонент. MME отправляет SGSN сообщение *Forward Relocation Request* о выделении ресурсов для обслуживания абонента, включающее IMSI, идентификатор RNC, Cause, базу данных (контекст) по протоколу MM, идентификатор текущей сети обслуживания, адрес MME и TEID интерфейса для сигнализации, контейнер данных абонента, часовой пояс обслуживания абонента. В сообщении приведен контекст всех сквозных каналов, обслуживающих абонента, для каждого соединения указана точка доступа (APN), а также адрес исходного S-GW и его TEID на сигнальном туннеле вверх.

Получив сообщение *Forward Relocation Request*, целевой SGSN устанавливает PDP-контекст абонента и заносит в него параметры переключаемых сквозных каналов. База данных по протоколу MM обеспечивает выполнение процедур безопасности при обслуживании абонента в сети UMTS. SGSN определяет максимальную пропускную способность потоков данных абонента через точки доступа.

SGSN устанавливает контекст сквозных каналов для UE.

П.4. В случае смены сети обслуживания SGSN заменяет исходный S-GW на целевой (target) S-GW и направляет ему сообщение *Create Session Request*. Оно содержит IMSI, адрес SGSN и TEID для сигнального соединения, адреса PDN GW для пользовательских каналов и сигнальных соединений, PDN GW TEID туннелей вверх в пользовательской и сигнальной плоскостях, тип соединения на S5/S8 (IPv4 или IPv6). Требуемый тип протокола устанавливает S-GW.

Целевой S-GW выделяет ресурс для обслуживания абонента и отвечает сообщением *Create Session Response* (адреса S-GW в пользовательской и сигнальной плоскостях, TEID туннелей вверх в пользовательской и сигнальной плоскостях) – п.4а.

П.5. SGSN посылает запрос *Relocation Request* на целевой RNC для выделения канального ресурса и организации туннелей. Запрос содержит идентификатор UE, Cause, индикатор ядра сети, базу данных для выполнения процедур безопасности, список сквозных каналов с их параметрами , контейнер данных UE, информацию об ограничениях доступа абонента к ресурсам сети при хэндоверах. В запрос также включают адрес S-GW в пользовательской плоскости в случае прямого туннеля RNC ↔ S-GW или адрес SGSN при непрямом туннеле и соответствующие TEID для туннелей

вверх. RNC выделяет ресурсы для организации запрошенных сквозных каналов.

П.5а. В обратном сообщении *Relocation Request Acknowledge* RNC отправляет контейнер для eNB, список установленных сквозных каналов и, если есть таковые, список каналов, которые не установлены и чей контекст будет деактивирован. Теперь RNC готов принимать пакеты данных абонента в направлении вниз по организованным сквозным каналам.

П.6 выполняют в случае замены S-GW и создания обходного пути (*Indirect Forwarding*) для трафика вниз в процессе хэндовера. Если в UTRAN существует прямой туннель S-GW↔RNC (см.комментарий к рис.1.2), то в сообщении *Create Indirect Data Forwarding Tunnel Request* целевой S-GW получает адрес и TEID RNC. При использовании непрямого туннеля S-GW получает адрес и TEID SGSN. В обратном сообщении *Create Indirect Data Forwarding Tunnel Response* S-GW передает свой адрес и TEID (п.6а).

П.7. SGSN отправляет MME ответ *Forward Relocation Response* (Cause, адрес SGSN и TEID для сигнализации, контейнер для UE, индикатор замены S-GW, информация об организации сквозных каналов в сети UTRAN и параметры для организации промежуточных туннелей при передаче трафика вниз в процессе хэндовера).

Если не было замены S-GW или была замена, но существует прямое физическое соединение между исходным eNB и целевым RNC (*Direct Forwarding*), то сообщают адрес и TEID RNC для каналов трафика.

Если нет физического соединения между исходным eNB и целевым RNC (*Indirect Forwarding*) и произошла замена исходного S-GW на целевой, то сообщают адрес и TEID целевого S-GW.

Если замены S-GW не было, но при передаче вниз будут использованы *Indirect Forwarding* и непрямой туннель S-GW → SGSN, то сообщают адрес и TEID SGSN.

П.8 выполняют при организации *Indirect Forwarding*. MME направляет в S-GW, используемый при *Indirect Forwarding*, сообщение *Create Indirect Data Forwarding Tunnel Request,* содержащее идентификаторы сквозных каналов, адрес и TEID, полученные MME в п.7. Обычно этим S-GW является исходный S-GW, но может быть и другой обслуживающий шлюз. В ответном сообщении *Create Indirect Data Forwarding Tunnel Response* (п.8а) S-GW сообщает свой адрес и TEID для организации временного туннеля.

Алгоритм следующей фазы выполнения хэндовера показан на рис. 8.17.

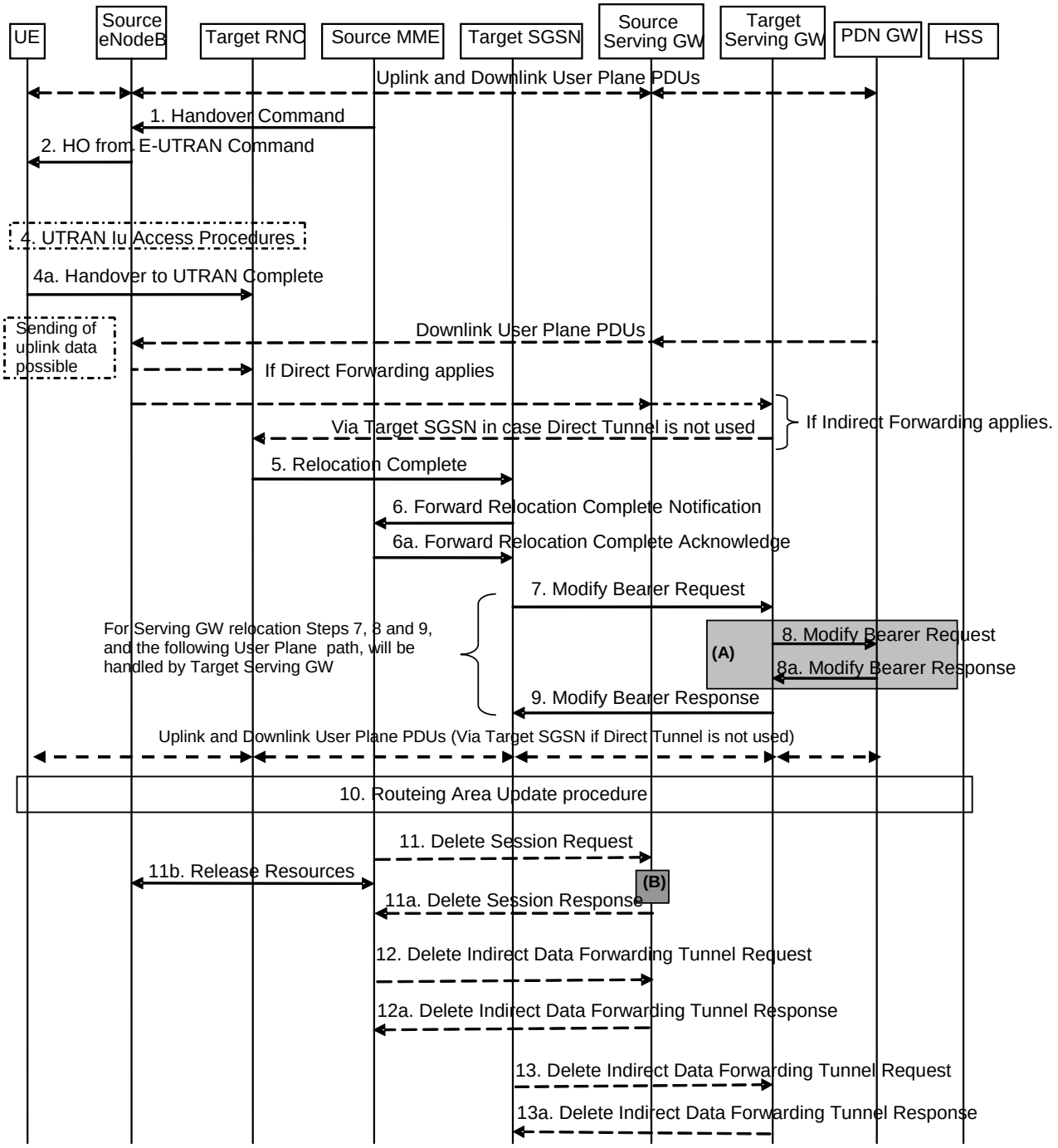


Рис.8.17. Выполнение хэндовера из E-UTRAN в UTRAN

П.1. MME завершает подготовку к хэндоверу, посылая eNB *Handover Command*, содержащую контейнер для eNB, список сквозных каналов, которые следует деактивировать, и каналов, которые надо организовать для временной передачи трафика вниз (Bearers Subject to Data forwarding list). Для организации этих каналов eNB получает адреса и TEID, которые были пересланы MME в пп. 7 при *Direct Forwarding* или 8a при *Indirect Forwarding* подготовительной фазы (рис. 8.16). В результате будет обеспечен либо прямой путь передачи данных eNB → RNC, либо обходной через исходный S-GW в зависимости от конфигурации сети.

П.2. eNB посылает UE команду выполнить хэндовер. В этой команде UE передают контейнер, содержащий необходимые для хэндовера параметры, которые RNC загрузил в контейнер в подготовительной фазе. Приняв команду, UE останавливает передачу трафика вверх, идентифицирует сквозные каналы в соответствии с протоколом доступа с коммутацией пакетов в UTRAN и выполняет процедуру хэндовера (п.4). По завершении хэндовера UE может начать передавать трафик вверх.

Что касается передачи трафика вниз, то при смене S-GW он попрежнему идет по маршруту PDN GW→исходный S-GW→eNB, поскольку не было переключения туннеля вниз от PDN GW на новый целевой S-GW. При наличии физического соединения eNB→ RNC используют вариант *Direct Forwarding*. Если такого соединения нет, то осуществляют *Indirect Forwarding* (пунктир на рис. 8.17). Переключение туннеля от PDN GW на целевой S-GW произойдет после выполнения пп.8–9.

П.5. RNC сообщением *Relocation Complete* информирует SGSN об успешном завершении процедуры подключения UE к сети UTRAN.

П.6. MME получает от SGSN уведомление *Forward Relocation Complete Notification* о том, что UE обслуживается сетью UTRAN. Если произошла замена S-GW, то SGSN сообщает об этом MME. Если замены не было, то SGSN может активировать ISR и известить об этом MME в уведомлении. В таком случае MME сохранит и будет вести параллельно с SGSN базу данных абонента. MME подтверждает получение уведомления (п.6a).

MME запускает таймер, по истечении которого будет удален контекст абонента в eNB и исходном S-GW, если он был заменен на целевой. Если трафик вниз идет по варианту *Indirect Forwarding*, то, получив от MME подтверждение (6a), SGSN также запускает таймер хранения ресурсов в целевом S-GW.

П.7. SGSN приступает к завершающей фазе хэндовера. Он отправляет обслуживающему S-GW сообщение *Modify Bearer Request*, содержащее адрес SGSN и TEID туннеля сигнализации, адрес SGSN и TEID туннеля трафика при непрямом соединении в UTRAN или адрес RNC и TEID туннеля трафика при прямом соединении (рис.1.2), а также NSAPI каналов трафика. Если PDN GW требует информацию о локализации абонента, то SGSN передает дополнительные параметры. Если хэндовер произошел без смены S-GW, то может быть активизирован ISR.

Все сквозные каналы, которые не были сохранены при хэдовере, SGSN деактивирует.

П.8 выполняют при замене S-GW, при смене сети радиодоступа или серьезных изменений в локализации абонента. Если заменен S-GW, то в сообщении *Modify Bearer Request* целевой S-GW передает PDN GW свой адрес

и TEID для организации туннеля вниз на интерфейсе S5/S8. При смене сети радиодоступа или локализации абонента возможны изменения тарифов обслуживания. PDN GW обязательно отвечает подтверждением *Modify Bearer Response* (п.8а).

П.9. S-GW в сообщении *Modify Bearer Response* подтверждает переключение соединения вниз (Cause, адрес S-GW и TEID для сигнализации). Теперь трафик вниз следует по маршруту PDN GW→ S-GW→(SGSN)→RNC. Если замены S-GW не было, то сразу после переключения каналов трафика S-GW передает несколько маркерных пакетов по старому пути, сигнализируя о завершении передачи

П.10 выполняется в том случае, когда UE по окончании передачи трафика находит, что он оказался в другой зоне маршрутизации или его временным номером остается GUTI. Тогда UE запускает процедуру *Routing Area Update*.

П.11. Когда срабатывает таймер, установленный в п.6, MME отправляет eNB команду *Release Resources* для стирания баз данных абонента в eNB.

Если произошла замена S-GW, то MME сообщением *Delete Session Request* дает команду исходному S-GW удалить контекст абонента. eNB и S-GW отвечают MME подтверждениями полученных команд.

ПП12 и 13 выполняют в том случае, если произошла замена S-GW и до переключения туннеля трафик вниз из PDN GW шел по варианту *Indirect Forwarding*. MME дает команду исходному S-GW, а SGSN – целевому S-GW освободить канальный ресурс, выделенный для организации временного туннеля между ними. Оба S-GW подтверждают получение команд.

8.14. Процедура межсистемного хэндовера из UTRAN в E-UTRAN

Эта процедура является зеркальной по отношению к хэндоверу, рассмотренному в предыдущем параграфе. Она также состоит из двух фаз: подготовки хэндовера и выполнения хэндовера. Алгоритм первой фазы приведен на рис. 8.18 [6].

Прохождение трафика до начала хэндовера показано на рис.8.18 пунктиром. Процедуру запускает контроллер сети UTRAN RNC (п.1). Он отправляет SGSN сообщение *Handover Required*, содержащее Cause, идентификатор eNB, идентификатор RNC, контейнер с параметрами UE для выделения ресурсов в eNB, MME и целевом S-GW (п.2). Далее в п.7 MME идентифицирует сквозные каналы, которые надо будет организовать при переключении UE на сеть E-UTRAN.

П.3. Из полученного сообщения SGSN заключает, что RNC запрашивает хэндовер в сеть E-UTRAN. SGSN отправляет MME сообщение *Forward*

Relocation Request о выделении ресурсов для обслуживания абонента, включающее IMSI,

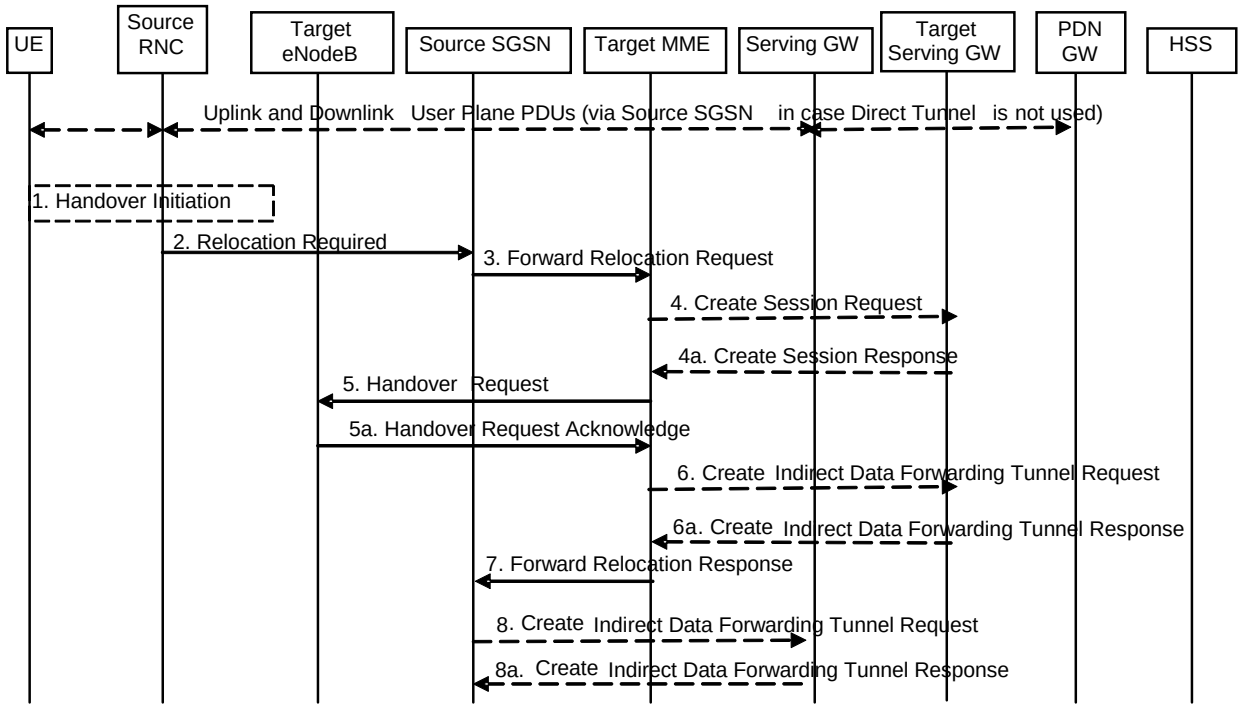


Рис.8.18. Подготовка хэндовера из UTRAN в E-UTRAN

идентификатор eNB, Cause, базу данных (контекст) по протоколу MM, идентификатор текущей сети обслуживания, адрес SGSN и TEID интерфейса для сигнализации, контейнер данных абонента, часовой пояс обслуживания абонента. Сообщение содержит контекст всех сквозных каналов, обслуживающих абонента с их точками доступа (APN), адреса и TEID туннелей вверх в исходном S-GW. Если активизирован ISR, то он сохраняется активированным и после хэндовера.

Получив сообщение *Forward Relocation Request*, целевой MME устанавливает сквозные каналы абонента в порядке приоритетов и определяет те каналы, которые сеть не сможет поддерживать. База данных по протоколу MM обеспечивает выполнение процедур безопасности при обслуживании абонента в сети E-UTRAN. MME определяет максимальную пропускную способность потоков данных абонента через точки доступа.

П.4. MME определяет, следует ли заменить S-GW. Если происходит замена S-GW, то MME направляет ему сообщение *Create Session Request*. Оно содержит IMSI, адрес MME и TEID для сигнального соединения, адреса PDN GW для пользовательских каналов и сигнальных соединений, PDN GW TEID туннелей вверх в пользовательской и сигнальной плоскостях, тип соединения на S5/S8 (IPv4 или IPv6). Требуемый тип протокола устанавливает S-GW.

S-GW выделяет ресурс для обслуживания абонента и отвечает сообщением *Create Session Response* (адреса S-GW в пользовательской и сигнальной плоскостях, TEID туннелей вверх в пользовательской и сигнальной плоскостях) – п.4а.

П.5. MME посылает запрос *Relocation Request* на целевой eNB для выделения канального ресурса и организации сквозных каналов В запросе передают идентификатор UE, Cause, базу данных для выполнения процедур безопасности, список сквозных каналов с их параметрами , контейнер данных UE, информацию об ограничениях доступа абонента к ресурсам сети при хэндоверах. В запрос также включают адрес S-GW в пользовательской плоскости и TEID для туннелей вверх. eNB выделяет ресурсы для организации запрошенных сквозных каналов.

П.5а. В обратном сообщении *Relocation Request Acknowledge* eNB отправляет контейнер для RNC, список установленных сквозных каналов и, если есть таковые, список каналов, которые не установлены и чей контекст будет деактивирован. Теперь eNB готов принимать пакеты данных абонента в направлении вниз по организованным сквозным каналам.

П.6 выполняют в случае замены S-GW и создания обходного пути (*Indirect Forwarding*) для трафика вниз в процессе хэндовера. В сообщении *Create Indirect Data Forwarding Tunnel Request* целевой S-GW получает адрес и TEID eNB. В обратном сообщении *Create Indirect Data Forwarding Tunnel Response* S-GW передает свой адрес и TEID (п.6а).

П.7. MME отправляет SGSN ответ *Forward Relocation Response* (Cause, адрес MME и TEID для сигнализации, контейнер для UE, индикатор замены S-GW, информация об организации сквозных каналов в сети E-UTRAN и параметры для организации промежуточных туннелей при передаче трафика вниз в процессе хэндовера).

Если не было замены S-GW или была замена, но существует прямое физическое соединение между исходным RNC и целевым eNB (*Direct Forwarding*), то сообщают адрес и TEID eNB для каналов трафика.

Если нет физического соединения между исходным RNC и целевым eNB (*Indirect Forwarding*) и произошла замена исходного S-GW на целевой, то сообщают адрес и TEID целевого S-GW.

П.8 выполняют при организации *Indirect Forwarding*. SGSN направляет в S-GW, используемый при *Indirect Forwarding*, сообщение *Create Indirect Data Forwarding Tunnel Request,* содержащее идентификаторы сквозных каналов, адрес и TEID, полученные SGSN в п.7. Обычно этим S-GW является исходный S-GW, но может быть и другой обслуживающий шлюз. В ответном сообщении *Create Indirect Data Forwarding Tunnel Response* (п.8а) S-GW сообщает свой адрес и TEID для организации временного туннеля.

Алгоритм следующей фазы выполнения хэндовера показан на рис. 8.19.

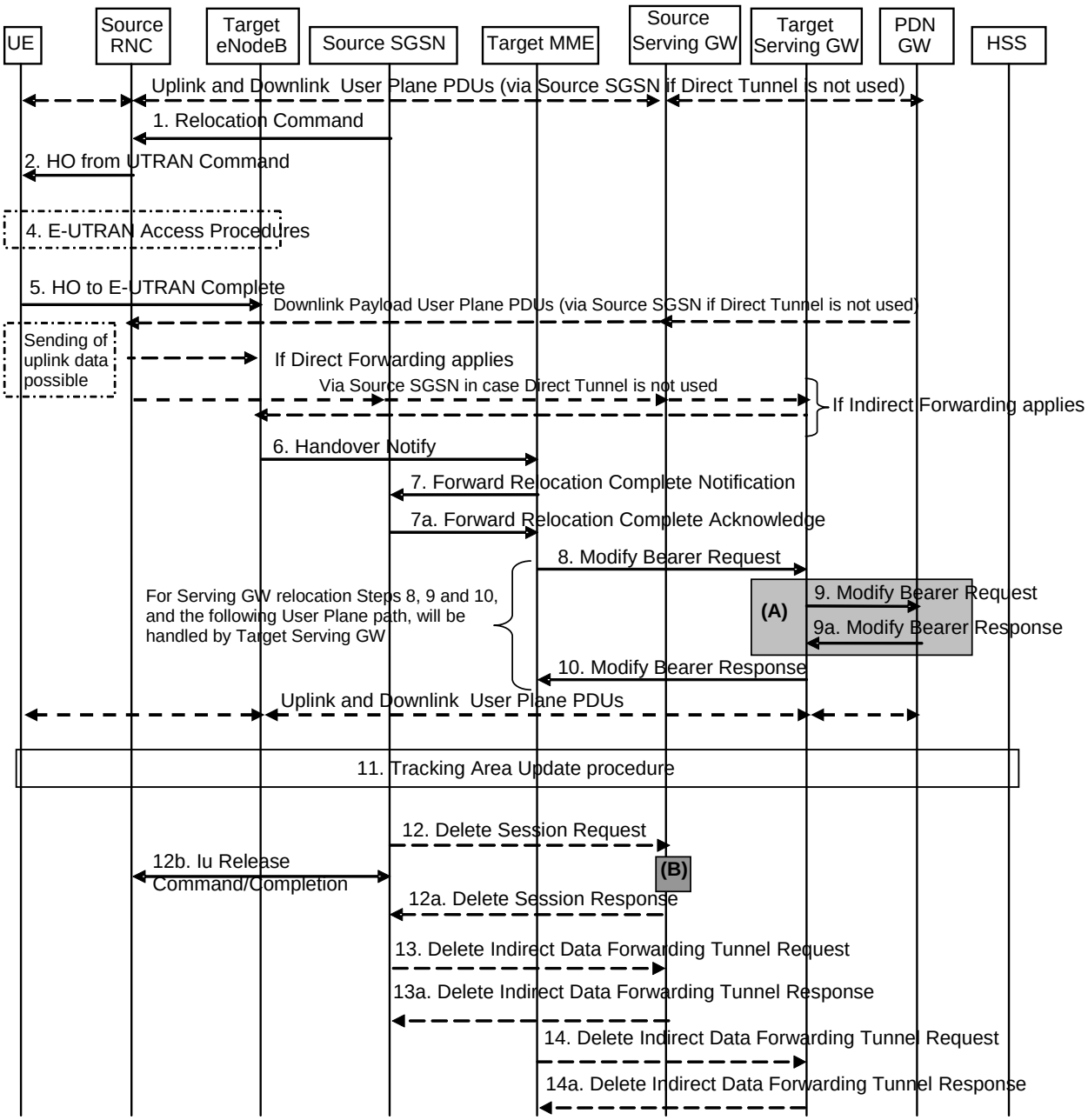


Рис.8.19. Выполнение хэндовера из UTRAN в E-UTRAN

П.1. SGSN завершает подготовку к хэндоверу, посылая RNC *Handover Command*, содержащую контейнер для RNC, список сквозных каналов, которые следует деактивировать, и каналов, которые надо организовать для временной передачи трафика вниз (RABs Subject to Data forwarding list). Для организации этих каналов eNB получает адреса и TEID, которые были пересланы SGSN в пп. 7 при *Direct Forwarding* или 8a при *Indirect Forwarding* подготовительной фазы (рис. 8.18). В результате будет обеспечен либо пря-

мой путь передачи данных RNC→eNB, либо обходной через исходный S-GW в зависимости от конфигурации сети. Если в сети UTRAN был непрямой туннель трафика (через SGSN), то при Indirect Forwarding RNC получает для обходного туннеля адрес и TEID SGSN.

П.2. RNC посылает UE команду выполнить хэндовер. В этой команде UE передают контейнер, содержащий необходимые для хэндовера параметры, которые eNB загрузил в контейнер в подготовительной фазе. Приняв команду, UE останавливает передачу трафика вверх, устанавливает соответствие идентифи каторов сквозных каналов в E-UTRAN с NSAPI каналов в UTRAN и выполняет процедуру доступа к сети E-UTRAN (п.4).

П.5. Получив доступ к eNB, UE отправляет ему сообщение *HO to E-UTRAN complete*.

П.6. Сообщением *Handover Notify* eNB информирует MME о завершении подключения UE к сети E-UTRAN.

П.7. SGSN получает от MME уведомление *Forward Relocation Complete Notification* о том, что UE обслуживается сетью UTRAN. Если произошла замена S-GW, то MME сообщает об этом SGSN. Если замены не было, то SGSN может активировать ISR и известить об этом MME в уведомлении. В таком случае SGSN сохранит и будет вести параллельно с MME базу данных абонента. SGSN подтверждает получение уведомления (п.7a).

SGSN запускает таймер, по истечении которого будет удален контекст абонента в RNC и исходном S-GW, если он был заменен на целевой. Если трафик вниз идет по варианту *Indirect Forwarding*, то, получив от SGSN подтверждение (7a), MME также запускает таймер хранения ресурсов в целевом S-GW.

П.8. MME приступает к завершающей фазе хэндовера. Он отправляет обслуживающему S-GW сообщение *Modify Bearer Request*, содержащее Cause, адрес MME и TEID туннеля сигнализации, адрес eNB и TEID туннеля трафика вниз, идентификаторы сквозных каналов. Если PDN GW требует информацию о локализации абонента, то MME передает дополнительные параметры. Если хэндовер произошел без смены S-GW, то может быть активизирован ISR.

Все сквозные каналы, которые не были сохранены при хэдовере, MME деактивирует.

П.9 выполняют при замене S-GW, при смене сети радиодоступа или серьезных изменений в локализации абонента. Если заменен S-GW, то в сообщении *Modify Bearer Request* целевой S-GW передает PDN GW свой адрес и TEID для организации туннеля вниз на интерфейсе S5/S8. При смене сети радиодоступа или локализации абонента возможны изменения тарифов об-

служивания. PDN GW обязательно отвечает подтверждением *Modify Bearer Response* (п.9а).

П.10. S-GW в сообщении *Modify Bearer Response* подтверждает переключение соединения вниз (Cause, адрес S-GW и TEID для сигнализации). Теперь трафик вниз следует по маршруту PDN GW→ S-GW→eNB. Если замены S-GW не было, то сразу после переключения каналов трафика S-GW передает несколько маркерных пакетов по старому пути, сигнализируя о завершении передачи

П.11 выполняется в том случае, когда UE по окончании передачи трафика находит, что необходимо запустить процедуру *Tracking Area Update*.

П.12. Когда срабатывает таймер, установленный в п.7, SGSN отправляет RNC *Release Command* для стирания в нем базы данных абонента. RNC отвечает подтверждением *Release Complete.*

Если произошла замена S-GW, то SGSN сообщением *Delete Session Request* дает команду исходному S-GW удалить контекст абонента. S-GW отвечают SGSN подтверждением полученной команды.

ПП13 и 14 выполняют в том случае, если произошла замена S-GW и до переключения туннеля трафик вниз из PDN GW шел по варианту *Indirect Forwarding.* SGSN дает команду исходному S-GW, а MME – целевому S-GW освободить канальный ресурс, выделенный для организации временного туннеля между ними. Оба S-GW подтверждают получение команд.

8.15. Процедуры в подсистеме PCC

PCC (Policy and Charging Control) – подсистема управления качеством обслуживания и тарификацией. В ней используют PPC-правила (Rules), исходя из которых, принимаются PCC-решения. Центральным элементом принятия PCC-решений в сетях 3GPP является элемент PCRF [31]. Логические структуры PCC для Rel.12.4.0 приведены на рис. 8.20 при обслуживании абонента в домашней сети и на рис. 8.21 при обслуживании абонента в визитной сети.

Задачи PCC:

- установка и управление качественными показателями сквозных каналов,

- установка тарифов организуемых услуг,

- подготовка данных для генерации учетных записей CDR (Charging Data Records).

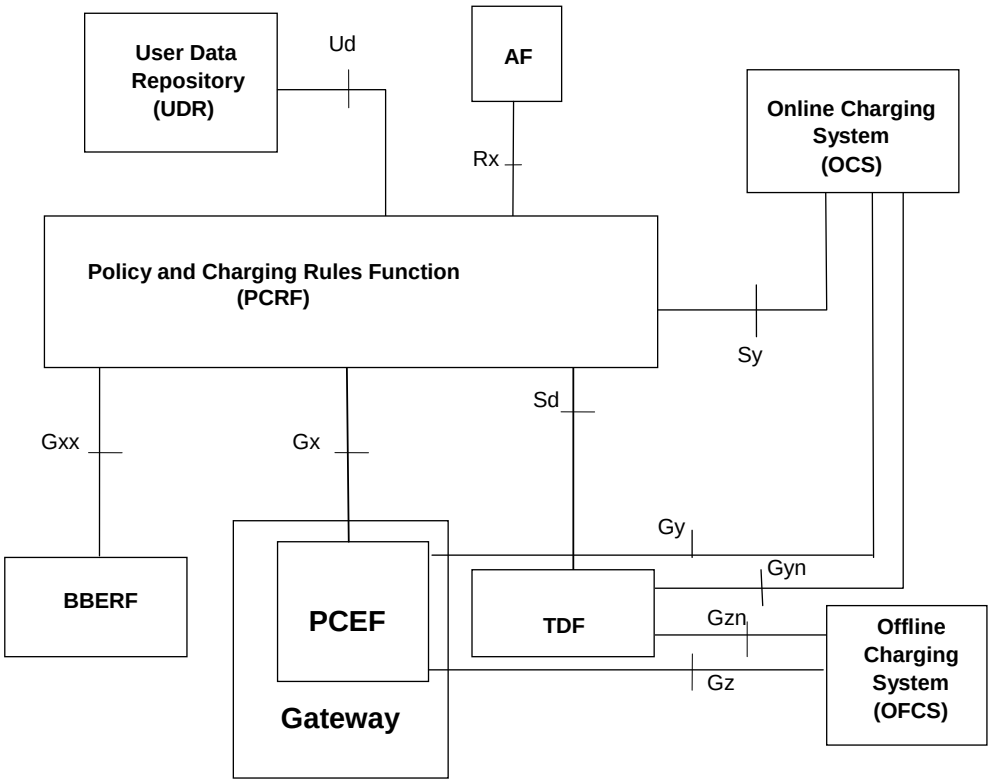


Рис. 8.20. Логическая архитектура PCC (обслуживание в домашней сети) с использованием UDA.

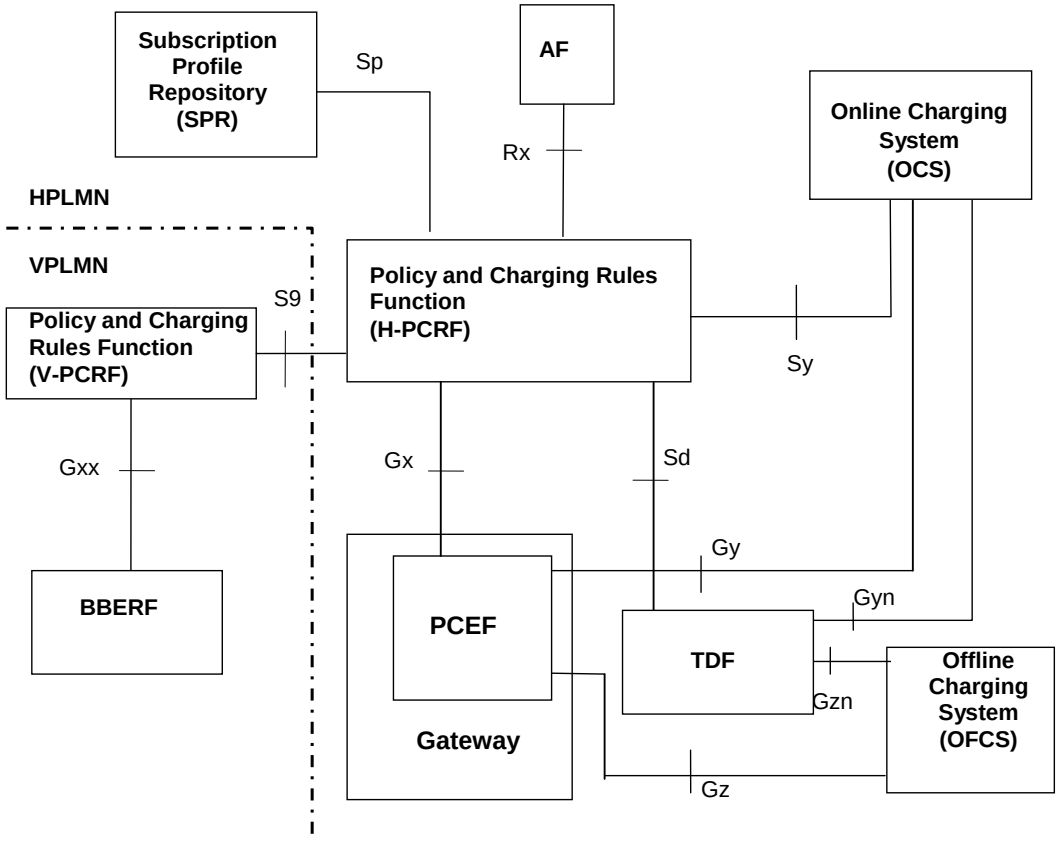


Рис. 8.21. Логическая архитектура PCC (роуминг) с использованием SPR

Описание системы PCC дано в [39]. Рассмотрим назначение функциональных узлов в PCC.

PCRF (Policy Control and Charging Rules Function) – это функциональный элемент в 3GPP сетях связи, который устанавливает правила обслуживания абонентов, включающие разрешение/запрещение услуг и установление параметров QoS (качества обслуживания). PCRF также устанавливает правила тарификации, учитывая следующие факторы: параметры абонентского профиля, объём переданного трафика, время доставки контента, местоположение абонента, и т.д.

Рассмотрим функциональные элементы и интерфейсы, с которыми может взаимодействовать PCRF

PCEF (Policy and Charging Enforcement Function) – функциональный элемент в 3GPP сетях связи, который реализует PCC-правила, полученные от PCRF, к проходящему через него трафику. PCEF осуществляет тарификацию этого трафика в системе тарификации оператора связи в реальном времени. PCEF находится в PDN GW – шлюзе доступа к внешним сетям связи.

PCEF взаимодействует с PCRF по интерфейсу Gx. [40]. Gx интерфейс используют для передачи нотификации о событиях из PCEF на PCRF и управления PCC-правилами на PCEF. По этому интерфейсу PCEF передает в PCRF информацию, необходимую для принятия PCC-решений: идентификатор абонента, информацию о местоположении и часовом поясе, в котором находится абонент, IP-адрес устройства, с которого осуществляется доступ, параметры канала, и другие данные.

TDF (Traffic Detection Function) – функциональный элемент, который определяет проходящий трафик различных приложений и информирует о нем PCRF. В зависимости от полученных правил TDF осуществляет пропуск данного трафика абоненту, его перенаправление и ограничение скорости передачи. TDF взаимодействует с PCRF по интерфейсу Sd [40]: Sd интерфейс используют для установки ADC (Application Detection and Control) – правил управления параметрами трафика конкретных приложений. Функции TDF могут быть включены в ПО PCEF. В этом случае элемент TDF на рис.8.20 и 8.21 отсутствует, отсутствуют и связанные с ним интерфейсы, а необходимые данные передают по интерфейсу Gx.

BBERF (Bearer Binding and Event Reporting Function) – опциональный функциональный элемент, который информирует PCRF о привязке (binding) потоков данных SDF (Service Data Flow) к организованным сквозным каналам с соответствующими QoS и о происходящих изменениях их состояния. BBERF размещают в S-GW. BBERF взаимодействует с PCRF по интерфейсу Gxx. При использовании туннельного сигнального соединения между S-GW и PDN GW интерфейс Gxx отсутствует.

AF (Application Function) – функциональный элемент, который предоставляет PCRF описание потока данных услуги и осуществляет информирование о требуемых этой услуге ресурсах. Взаимодействует с PCRF по интерфейсу Rx [41]. В качестве AF используют CSCF подсистемы IMS.

UDR (User Data Repository)- функциональный элемент в 3GPP сетях связи, где хранят данные пользователей. UDR взаимодействует с PCRF по интерфейсу Ud [42]. Ud-интерфейс используют для получения/изменения пользовательских профилей, которые содержат информацию о сервисах, доступных абоненту, параметрах QoS и других параметрах, необходимых для принятия PCC-решений. Интерфейс Ud используют также для подписки и получения уведомлений об изменениях в профилях абонентов. UDR и интерфейс Ud заменили функциональный элемент SPR (Subscription Profile Repository) и интерфейс Sp в более ранних вариантах PCC (рис.8.21).

OCS (Online Charging System) – сервер кредитного контроля в режиме реального времени. OCS осуществляет тарификацию услуг, контролирует платежный баланс абонента, обрабатывает информацию о начислениях и списаниях средств на счёте, применяет скидки, осуществляет подсчет объёма потребленных услуг. OCS также можно использовать для авторизации абонентов и предоставления информации о стоимости услуг (Advice of Charge). OCS взаимодействует с PCEF по интерфейсу Gy с помощью которого осуществляют тарификацию услуг.

OFCS (Offline Charging System) – система тарификации на основе генерации учетных записей CDR с последующим биллингом абонентов.

PCC и QoS-правила. Назначение PCC-правил – это разделять физический поток данных (IP-CAN) на логические потоки данных SDF (Service Data Flow), определять к каким приложениям и услугам относится трафик, предоставлять параметры QoS и информацию для тарификации. Существует два типа PCC-правил: динамические PCC-правила, которые передают с PCRF на PCEF через Gx интерфейс, и предопределенные на PCEF. Предопределенные правила могут быть активизированы либо PCRF либо самим PCEF. PCC-правило состоит из набора атрибутов: имя правила, идентификатор услуги (сервиса), параметры QoS, параметров для тарификации и других.

Обмен PCC-правилами между PCRF и PCEF может проходить в двух режимах: либо PCEF запрашивает PCC-правила на PCRF (PULL процедура), либо PCRF в соответствии со своей внутренней логикой нотифицирует PCEF (PUSH процедура) об изменении правил или о новых правилах обслуживания. Правила, которыми обмениваются между собой элементы 3GPP сети PCRF и BBERF называются QoS-правилами и их также разделяют на динамические и предопределенные.

Процедуры, происходящие в PCC при запросе услуги и ее окончании, показаны на рис. 8.22.

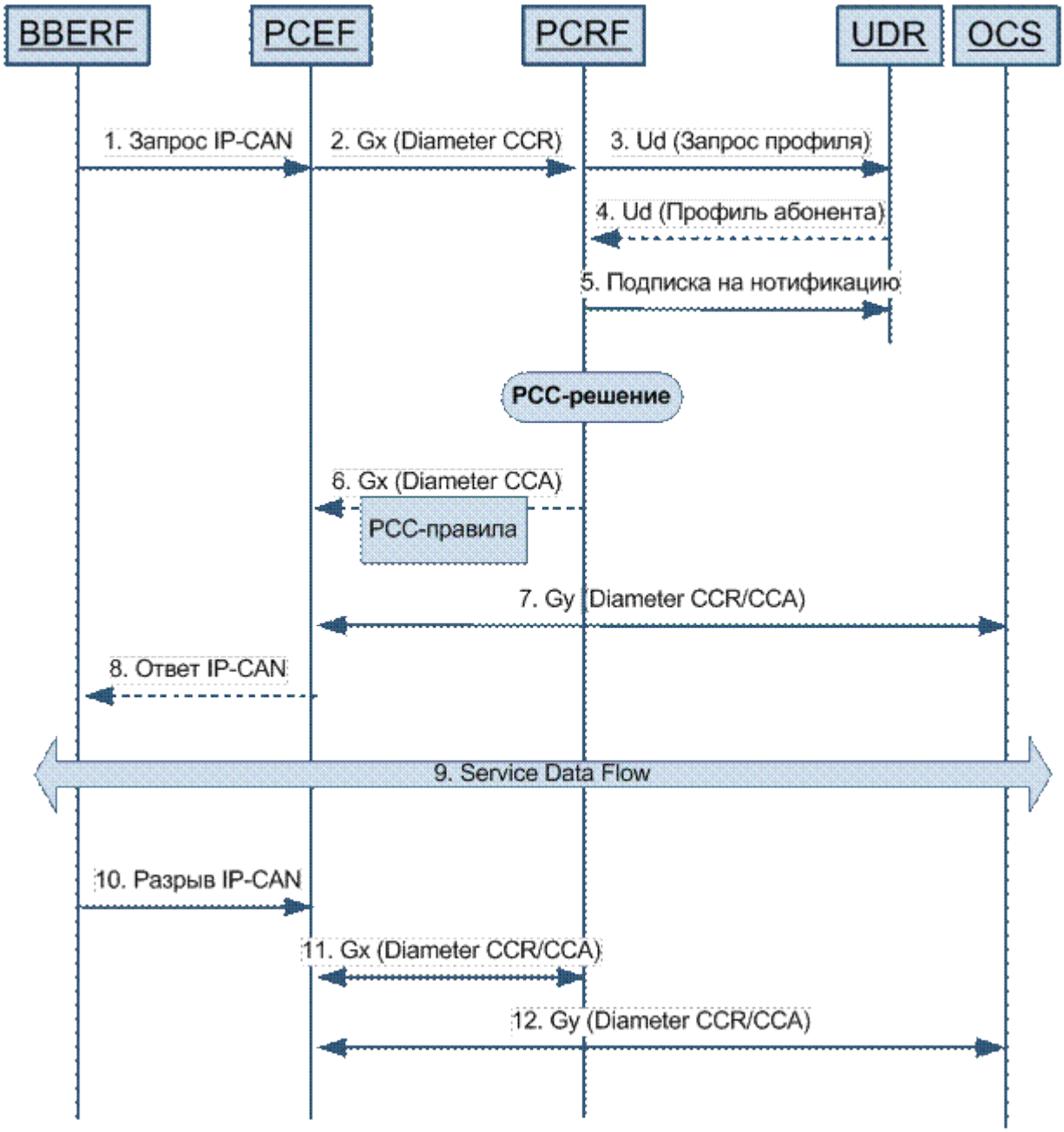


Рис. 8.22. Процедуры в PCC при организации услуг

1. Абонент начинает сессию передачи данных. При этом BBERF посылает на PCEF запрос на создание сессии для пропуска трафика (IP-CAN).

2. PCEF формирует запрос по интерфейсу Gx и посылает его на PCRF. Это заключается в формировании Diameter CCR (Credit-Control-Request) запроса с информацией об абоненте и запрашиваемых услугах.

3. PCRF осуществляет запрос профиля абонента по интерфейсу Ud.

4. Получает профиль с параметрами услуг абонента.

5.Осуществляет подписку на нотификацию об изменениях профиля.

6. PCRF принимает PCC-решение о возможности предоставлении услуг абоненту с определенными параметрами качества. PCRF формирует PCC-правила, которые отправляет на PCEF по интерфейсу Gx в виде ответа Diameter CCA (Credit-Control-Answer) с включенным набором PCC-правил.

7. При получении ответа PCEF устанавливает сессию кредитного контроля с OCS по интерфейсу Gy с помощью обмена сообщениями Diameter CCR/CCA.

8. PCEF разрешает установку IP-CAN сеанса (сессии) связи.

9. Между устройством абонента и внешними сетями связи начинает проходить поток трафика (Service Data Flow).

10.Когда абонент завершает сеанс передачи данных, BBERF посылает на PCEF запрос на разрыв IP-CAN сессии.

11.PCEF осуществляет завершение сессии обменом сообщений по протоколу Diameter CCR/CCA с PCRF по интерфейсу Gx.

12.PCEF осуществляет завершение сессии Diameter на OCS по интерфейсу Gy.

В процессе обслуживания абонента может появиться необходимость изменить параметры сеанса связи, например, когда абонент хочет увеличить скорость трафика за определенную плату. Для этого абонент активизирует “турбо кнопку” в своем кабинете самообслуживания. После этого происходит следующее (рис. 8.23):

1. Информация о данном событии попадает в UDR и по интерфейсу Ud происходит нотификация PCRF.

2.PCRF анализирует пришедшие параметры и принимает PCC-решение увеличить скорость доступа абоненту и изменить правила тарификации трафика. PCRF формирует PCC-правило и по интерфейсу Gx посылает его на PCEF. Это заключается в формировании запроса Diameter RAR (Re-Auth-Request).

3.PCEF отправляет ответ Diameter RAA (Re-Auth-Answer).

4.По интерфейсу Gy PCEF обменивается с OCS сообщениями Diameter CCR/CCA, в результате чего завершается старая сессии кредитного контроля и создается новая с новыми параметрами тарификации.

5.После этого PCEF дает команду BBERF на создание потока данных (Service Data Flow) с увеличенной скоростью.

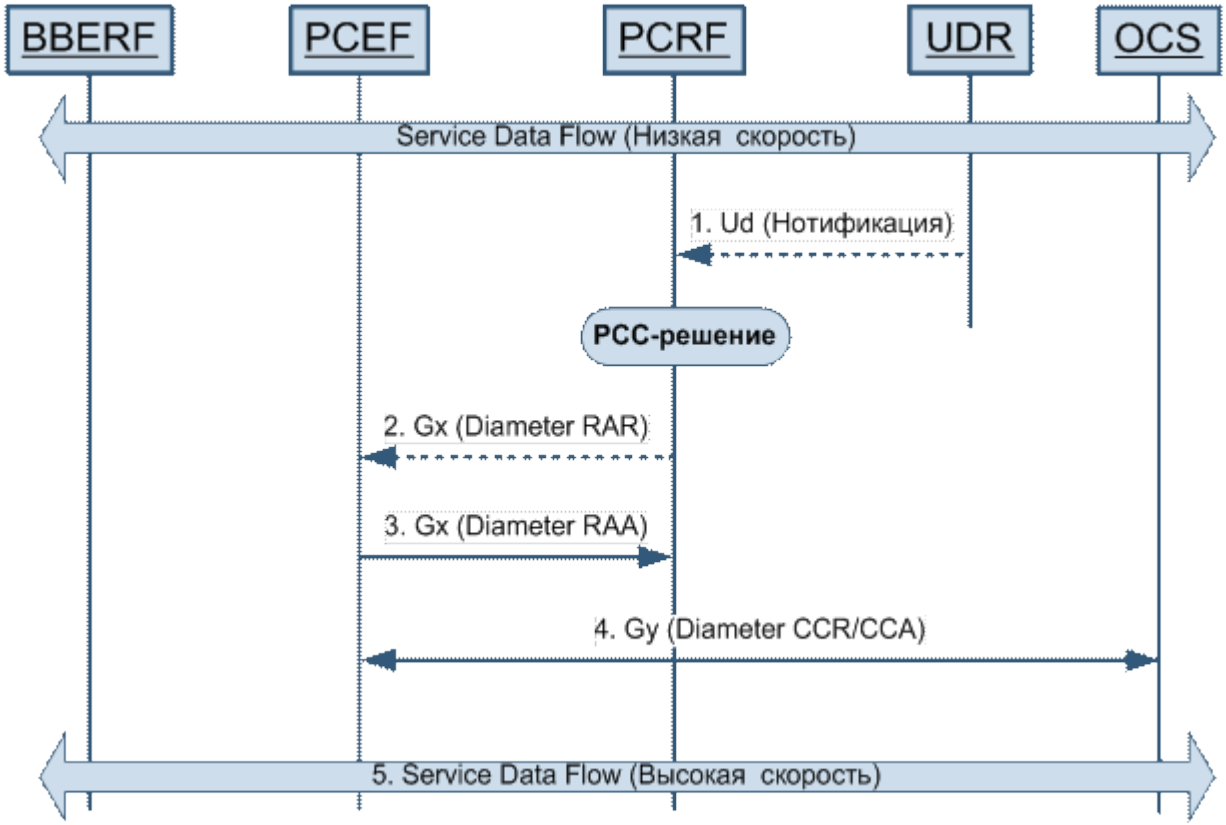


Рис. 8.23. Запрос на изменение параметров

Перечислим функциональные возможности, которыми должен обладать PCRF сервер.

Поддержка максимального числа интерфейсов и возможность поддержки новых.

Возможность для оператора связи создавать и гибко конфигурировать PCC-правила.

Управление мониторингом использования услуги (Usage Monitoring Control). Функциональность дает возможность PCRF осуществлять подсчет использованного объёма услуги в PCEF, а не хранить у себя или в OCS счетчики потребления услуг. Включение мониторинга осуществляется с помощью PCC-правила. При превышении заданного значения PCEF посылает запрос на PCRF по интерфейсу Gx с информацией об использованном трафике.

Установление триггеров на события (Event-Triggering). PCRF может устанавливать триггеры на события, например, обнаружение трафика определенного приложения или смену местоположения абонента. При наступлении данных событий на PCRF будет производится запрос новых PCC-правил обслуживания.

Установка времени активации услуги (Time of Day). PCRF может устанавливать на PCEF время суток или время, через которое PCEF пошлет запрос на новое PCC-правило.

Управление трафиком определенных приложений (Application Detection and Control). PCRF может передавать через Gx-интерфейс правила для управления трафиком конкретных приложений. Если функция TDF реализована в отдельном узле, то данная информация должна передаваться по протоколу Sd.

Учет лимитов потребленного трафика (Subscriber Spending Limits). С помощью интерфейса Sy PCRF может запрашивать статусы накопителей трафика, реализованных на стороне OCS. Также OCS может нотифицировать PCRF о факте преодоления порогов и на основании этой информации PCRF принимает новое PCC-решение.

Возможность установки нескольких PCRF-серверов для резервирования данных. В процессе работы PCRF-сервера обмениваются данными между собой. Таким образом, в случае отказа одного сервера резервный продолжит обслуживание абонентов.

Применение настроечных параметров и изменения в профилях абонентов не должно прерывать обслуживание.

Возможность управления и получение статистической информации из PCRF по стандартным протоколам, например, SNMP или Telnet.

Мультиплатформенность. Чем больше операционных систем поддерживает PCRF-сервер, тем лучше, так как это увеличивает возможности оптимизации оборудования для операторов связи.