Telsoft

vEPC

Инструкция по эксплуатации

Document version: 1

Правовая информация

Copyright © 2002-2025 Telsoft. Все права защищены.

Никакая часть данного документа не может быть воспроизведена или обработана в системах обработки данных, скопирована или использована в других документах без письменного уведомления компании ООО «Телсофт».

Информация, содержащаяся в данном документе, может быть изменена компанией ООО «Телсофт» без предварительного уведомления.

Упомянутые торговые марки являются зарегистрированными торговыми марками их владельцев.

Содержание

1. Введение

1.1. Назначение документа

Настоящий документ представляет собой руководство по эксплуатации системы vEPC.

Данный документ содержит следующие аспекты:

- Общее описание EPC.
- Описание архитектуры решения.
- Описание возможностей системы.
- Описание услуг связи.

1.2. Ограничения и допущения

1.3. Сопутствующая документация

1.4. Используемые обозначения

Таблица 1. Используемые обозначения

Обозначение	Описание
Полужирное начертание	Функциональные элементы (экранные кнопки, название окон и т. д.)
Курсив	Перекрестные ссылки, ссылки на другие документы
ЗАГЛАВНЫЕ БУКВЫ	Название клавиш клавиатуры
`Шрифт Courier New`	Код
Примечание	Пояснение к тексту

1.5. История изменений документа

Таблица 2. История изменений

Версия	Дата	Содержание изменений
.0	01.06.2025	Документ создан

Введение

Evolved Packet Core (EPC) – пакетно-коммутируемое ядро сети LTE по стандартам 3GPP. EPC является эволюцией GPRS Core и представляет собой упрощённую «all-IP» архитектуру с разделением на плоскости управления и передачи данных. EPC обеспечивает сквозную IP-транспортировку и поддерживает мобильность между различными типами доступа (E-UTRAN LTE, 3GPP-legacy GERAN/ UTRAN, а также не-3GPP сети, например Wi-Fi). Основные элементы EPC включают сущности MME (Mobility Management Entity), Serving GW, PDN GW, HSS (Home Subscriber Server) и PCRF (Policy and Charging Rules Function). Они реализуют функции регистрации и аутентификации абонента, установления и управления пакетными сессиями, маршрутизации пакетов во внешние сети, а также применения политик качества обслуживания и тарификации.

Архитектура EPC с учетом CUPS

В базовой архитектуре EPC (до релиза 14) плоскость управления полностью выполняет MME, а пользовательскую плоскость обеспечивают S-GW и P-GW. Начиная с 3GPP Release 14 введена концепция CUPS (Control and User Plane Separation) – разделение контрольной и пользовательской частей узлов S-GW и P-GW. При этом S-GW и P-GW разбиваются на две подсущности: SGW-C и SGW-U (контрольная/пользовательская часть S-GW), а также PGW-C и PGW-U (контрольная/ пользовательская часть P-GW). Такое разделение позволяет независимо масштабировать и размещать функции управления и передачи данных (например, выносить SGW-U ближе к RAN для снижения задержек), не затрагивая при этом механизм сигнализации. В результате архитектура EPC становится более гибкой: CP-узлы выполняют управление (GTP-C, Diameter), а UP-узлы – быструю пересылку пакетов. Для взаимодействия между разделёнными частями используются новые протоколы (например, PFCP) и интерфейсы (Sxa/Sxb/Sxc).

Интерфейсы EPC (таблица)

В EPC определено множество интерфейсов между сетевыми элементами.

Ниже приведена таблица основных интерфейсов с участвующими узлами и назначением (данные по 3GPP TS 23.401 и др.):

Таблица 3. Интерфейсы vEPC

Интерфейс	Участники	Назначение
S1-MME	eNodeB ↔ MME	Управляющий интерфейс (NAS/S1-AP) от базовой станции к MME

S1-U	eNodeB ↔ S-GW	Передача пользовательских пакетов (GTP-U) от eNodeB к S-GW
S2a	Trusted WLAN (TWAG) ↔ PDN-GW	Интерфейс от доверенной WLAN к P-GW
S2b	ePDG ↔ PDN-GW	Интерфейс от недоверенной WLAN через ePDG к P-GW
S3	MME ↔ SGSN	Контрольный интерфейс между MME и SGSN для междоменной мобильности
S4	SGSN ↔ S-GW	Интерфейс пользовательской/управляющей плоскости между SGSN и S-GW
S5	S-GW ↔ P-GW	Интерфейс передачи пакетов внутри PLMN
S8	S-GW ↔ P-GW (в роуминге)	Эквивалент S5 для роуминга
S6a	MME ↔ HSS	Диаметр-интерфейс для передачи профилей и аутентификации абонента
S6d	SGSN ↔ HSS	Аналог S6a для 2G/3G
S10	MME ↔ MME	Интерфейс передачи контекста между MME
S11	MME ↔ S-GW	Управляющий интерфейс GTP-C
S12	eNodeB ↔ RNC	Интерфейс управления (Iu-mode) между eNodeB и RNC
S13	MME ↔ EIR	Проверка IMEI устройства
SGi	P-GW ↔ внешняя сеть	Выход в внешние IP-сети (Internet/IMS/PDN)
Gx	PCRF ↔ P-GW	Интерфейс передачи правил QoS/PCC (Diameter)
Gy	P-GW ↔ OCS	Онлайн тарификация (реальное время, Diameter)
Gz	P-GW ↔ OFCS	Оффлайн тарификация (CDR-файлы)
Rx	PCRF ↔ AF (IMS)	Обмен приложенческими данными сеанса
SGs	MME ↔ MSC/VLR	CS Fallback и CS Paging между LTE и CS-доменом
Sv	MME ↔ MSC Server	Интерфейс для процедуры SRVCC

2. Архитектура vEPC

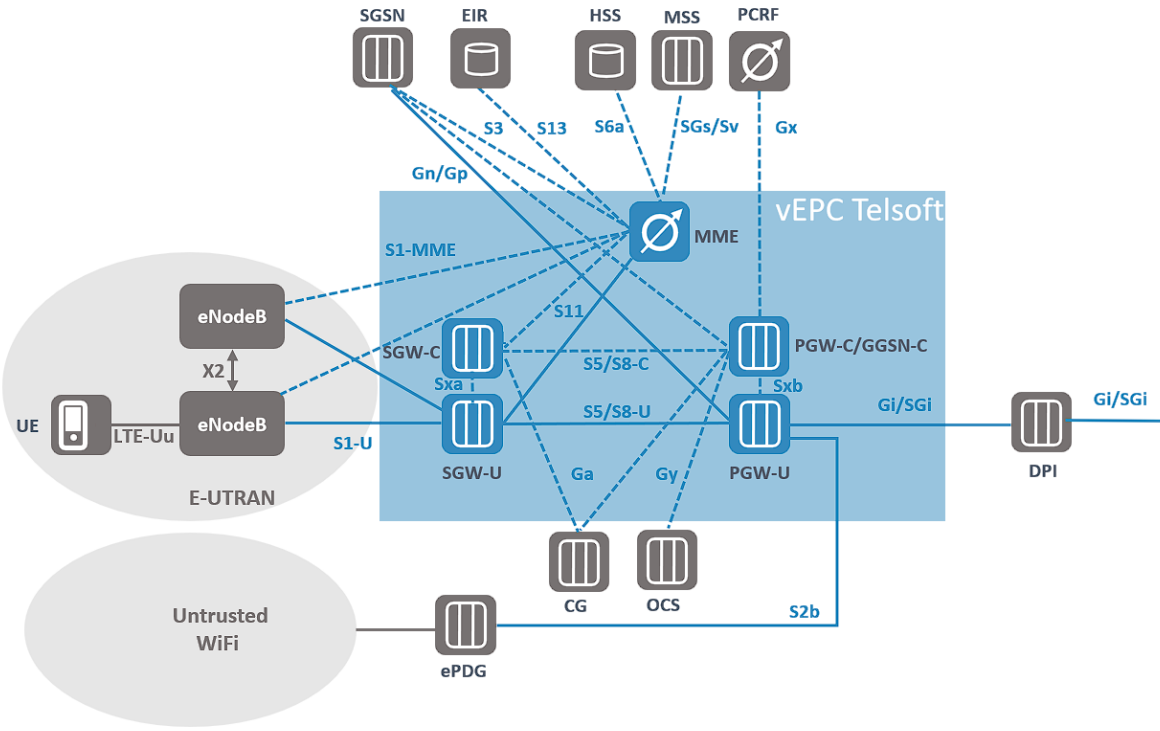


Рис. . Архитектура сети EPC

На схеме показаны ключевые компоненты EPC и связи между ними. UE подключается к сети через eNodeB (для LTE) или через Wi-Fi AP (недоверенный WLAN с ePDG). Основные ядреные узлы EPC – это MME, Serving GW и PDN GW – подключённые к базе подписчиков HSS, политическому контроллеру PCRF, а также к внешним сетям (через SGi к интернет/IMS). Кроме того, на схеме изображены ePDG (для Wi-Fi-доступа), AAA-сервер (для аутентификации не-3GPP доступа) и ANDSF (служба выбора сети). Указаны основные интерфейсы (S1, S11, S5/S8, S6a и др.), которые используются для сигнальной и транспортной связи между этими элементами

2.1. MME

MME (Mobility Management Entity) — ключевой элемент управляющей плоскости EPC в архитектуре LTE. Он осуществляет контроль над мобильностью, управлением сессиями, аутентификацией и взаимодействием с другими сетевыми элементами, такими как HSS, SGW, PCRF и MSC.

MME присутствует только в управляющей плоскости, не обрабатывает пользовательский трафик (IP-пакеты абонентов).

2... Основные функции MME

Мобильность

• Управление перемещением абонентов внутри LTE через Tracking Area Update (TAU)

• Контекстный хендовер между eNodeB через интерфейс S1-MME

• Межтехнологическая мобильность между LTE и 2G/3G через S3/S10/Sv

• Поддержка SRVCC через интерфейс Sv

Управление сессиями

• Установление и удаление EPS-сессий через интерфейс S11 с S-GW

• Назначение S-GW при первой активации PDP-сессии

• Поддержка взаимодействия с PCRF через передачу параметров в P-GW

Аутентификация и безопасность

• Запрос аутентификационных векторов у HSS по протоколу Diameter (S6a)

• Установка ключей шифрования и целостности RRC

• Поддержка проверки IMEI через интерфейс S13 с EIR

Управление NAS-соединениями

• Обработка NAS-сигнализации от UE через eNodeB (S1-MME)

• Инициация процедуры установления безопасности (attach, detach)

• Paging UE в зоне регистрации

Интеграция с CS-доменом

• Реализация CS Fallback и SMS over SGs через интерфейс SGs к MSC/VLR

• Реализация SRVCC с передачей управления в CS

Интерфейс с IMS через PCRF

• Участие в передаче session information в P-GW для последующего взаимодействия с PCRF по Gx

• Установление bearer'ов с учетом IMS QoS

2..2. Поддерживаемые интерфейсы

Интерфейс	Назначение
S1-MME	Сигнализация между eNodeB и MME (NAS + S1-AP)
S6a	Аутентификация/профиль пользователя с HSS
S11	Управление сессиями с S-GW
S10	Передача контекста между MME при хендовере
S3	Мобильность между LTE и 3G (с SGSN)
S13	Проверка IMEI с EIR
SGs	CS Fallback и передача сообщений в GSM/UMTS (через MSC/VLR)
Sv	SRVCC-интерфейс с MSC Server

2..3. Особенности реализации в архитектуре CUPS

- В CUPS (Control and User Plane Separation) MME остается в управляющей плоскости и взаимодействует с разделенными S-GW-C и P-GW-C, используя интерфейс S11.
- Передача управляющих команд идет к S-GW-C, а пользовательский трафик направляется в S-GW-U.
- MME может поддерживать интерфейс с SCEF в случае поддержки NB-IoT через T6a.

2..4. Роль в процедурах VoLTE и VoWiFi

- MME участвует в установлении bearer'ов с IMS QoS и приоритезацией SIP-сигнализации.
- При VoWiFi через ePDG, MME участвует в handover с Wi-Fi в LTE.

- Взаимодействует косвенно с PCRF через параметры, передаваемые P-GW, влияющие на политику QoS.

2..5. Участие в SRVCC (Single Radio Voice Call Continuity)

MME участвует в следующих этапах процедуры SRVCC:

1. Инициация SRVCC: eNodeB отправляет SRVCC Preparation Request в MME.
2. MME ↔ MSC Server (Sv): MME передает Session Transfer Request с информацией о текущем голосовом вызове (QoS, bearer).
3. Создание соединения в CS-домене: MSC резервирует ресурсы.
4. MME уведомляет eNodeB: После подтверждения от MSC, MME инициирует handover.
5. Контекст передается в MSC/VLR, вызов продолжается через CS.

2.2. SPGW

SPGW (S-GW + P-GW) — сетевой элемент в архитектуре Evolved Packet Core (EPC), который выполняет функции передачи пользовательского трафика, маршрутизации, установления подключений к внешним сетям и применения политик управления трафиком. В архитектуре CUPS (Control and User Plane Separation), компоненты SPGW делятся на управляющую часть (S-GW-C, P-GW-C) и пользовательскую (S-GW-U, P-GW-U).

2.2.1. Функции Serving Gateway (SGW)

Категория	Функции
Маршрутизация трафика	• Передача пользовательских пакетов между eNodeB и P-GW • Маршрутизация при хендовере между eNodeB (в пределах TA)
Управление мобильностью	• Обработка handover из других eNodeB или из других технологий (2G/3G) • Хранение и переключение контекстов bearer при изменении точки доступа
Буферизация данных	• Буферизация пользовательских данных при paging/idle • Поддержка откладки при возобновлении соединения
Тарификация и мониторинг	• Генерация CDR и передача на OFCS (через Gz) • Онлайн тарификация через OCS (Gy) в случае встроенной P-GW логики

2.2.2. **Функции PDN Gateway (PGW)**

Категория	Функции
Выход в внешние сети	• Установление и маршрутизация подключения к PDN (интернет, IMS, корпоративные сети) • Назначение IP-адреса UE
QoS и Policy Enforcement	• Применение правил QoS и PCC по командам от PCRF (Gx) • Создание, изменение и удаление dedicated bearer
Безопасность и фильтрация	• Поддержка Deep Packet Inspection (DPI) • Применение правил фильтрации IP-пакетов
Тарификация	• Генерация и экспорт CDR (Gz) • Взаимодействие с OCS по интерфейсу Gy для онлайн тарификации
VoLTE и IMS интеграция	• Обработка IMS bearer'ов с приоритезацией сигнального и медиа-трафика • Применение динамических правил по интерфейсу Rx → PCRF → P-GW

2.2.3. **Поддерживаемые интерфейсы**

Интерфейс	Назначение
S1-U	Передача пользовательского трафика между eNodeB и S-GW
S4	Интерфейс между SGSN и S-GW для поддержки 2G/3G
S5/S8	Связь между S-GW и P-GW (внутри сети и в роуминге)
S11	Управляющая связь с MME
S2a/S2b	Связь с TWAG (trusted Wi-Fi) или ePDG (untrusted Wi-Fi)
SGi	Подключение к внешним сетям (интернет, IMS, PDN)
Gx	PCRF ↔ P-GW: управление политиками и QoS (Diameter)
Gy	Online charging (реальное время) с OCS
Gz	Offline charging через CDR
Rx	Передача session information от IMS/AF к PCRF
T6a/T6b	Взаимодействие с SCEF и SCS (для IoT и NB-IoT)
PFCP (CUPS)	Управляющие команды от S-GW-C и P-GW-C к S-GW-U и P-GW-U

2.2.4. **Особенности в архитектуре CUPS**

Компонент	Назначение
S-GW-C / P-GW-C	Управляющая плоскость, взаимодействие с MME, PCRF, HSS и др.
S-GW-U / P-GW-U	Передача пользовательского трафика, GTP-U туннели

Компонент	Назначение
PFCP	Протокол управления плоскостью пользователя (используется для управления S-GW-U / P-GW-U)

Преимущества CUPS:

- Масштабирование управляющей и пользовательской плоскостей отдельно
- Более гибкое распределение нагрузки
- Поддержка MEC, NB-IoT, 5G Interworking

2.2.5. **Поддержка 2G/3G, VoLTE и VoWiFi**

Технология	Роль SPGW
2G/3G (S4)	Работа с SGSN по интерфейсу S4. Установка bearer и маршрутизация через S-GW
VoLTE	P-GW обрабатывает сигнальный трафик SIP и RTP, применяет IMS-QoS по командам от PCRF
VoWiFi (S2b)	Работа через ePDG, трафик с UE инкапсулируется в IPSec, расшифровывается и передаётся на P-GW

2.3. Масштабирование

Масштабирование большинства элементов vEPC производится через proxy элементы которые далее распределяют сессии по остальным узлам MME и SPGW.

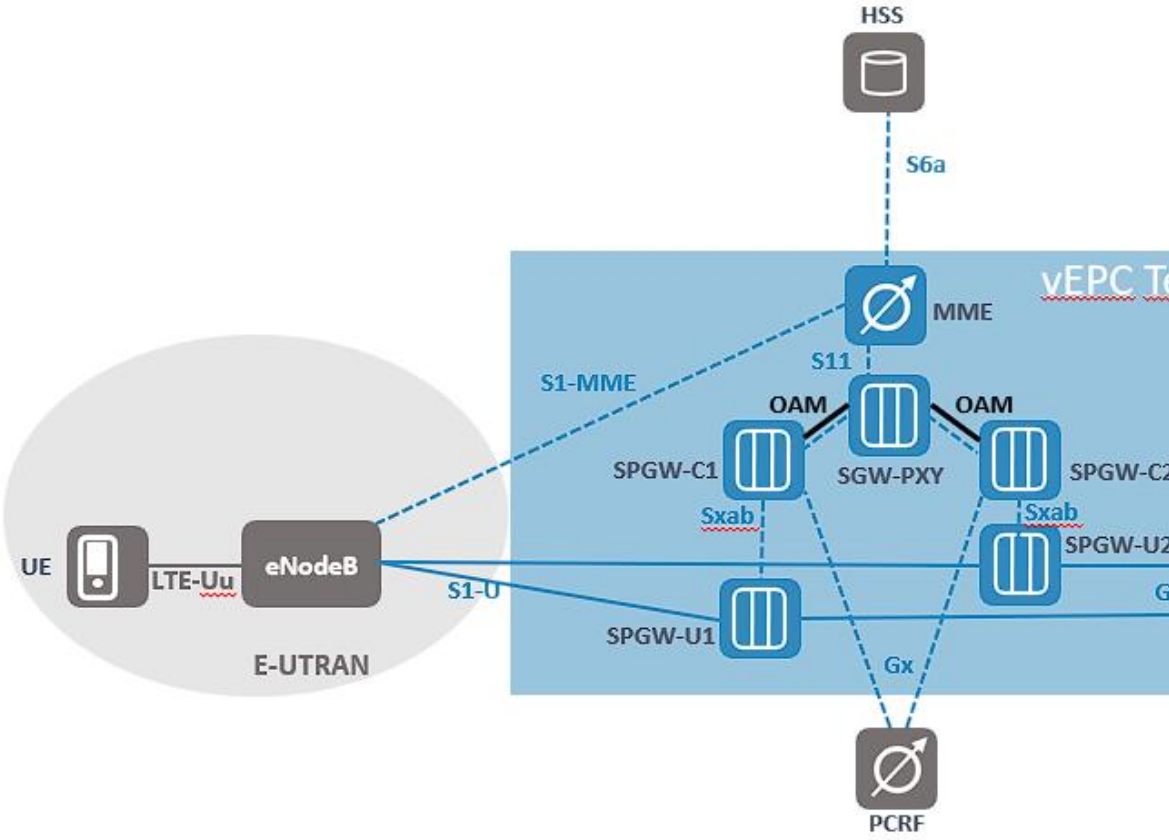


Рисунок 2: Архитектура масштабирования

Архитектура масштабирования представлена на Рисунок 2.

SPGW взаимодействуют с MME через SGW-PXY, CSR приходит на проки далее общение по каждой сессии происходи с конкретным SPGW.

Подразумевается два линка до DRA и дальнейшее масштабирование и резервирование PCRF обеспечивается средствами Diameter Routing Agent.

2.4. Отказоустойчивость и глобальное резервирование

vEPC спроектирована таким образом, что не имеет единой точки отказа. Все модули и функции системы задублированы.

Большинство модулей работают в режиме Master-Master, т.е. все развернутые копии ПО одновременно готовы обслуживать сессии абонентов.

vEPC может быть развернута на разных независимых площадках для обеспечения разделения нагрузки по разным географическим точкам с разными часовыми поясами и обеспечения отказоустойчивости. Для этого используется как и MME pool так и SGW proxy.

Пример схемы гео-резервирования представлен на Рисунок 3

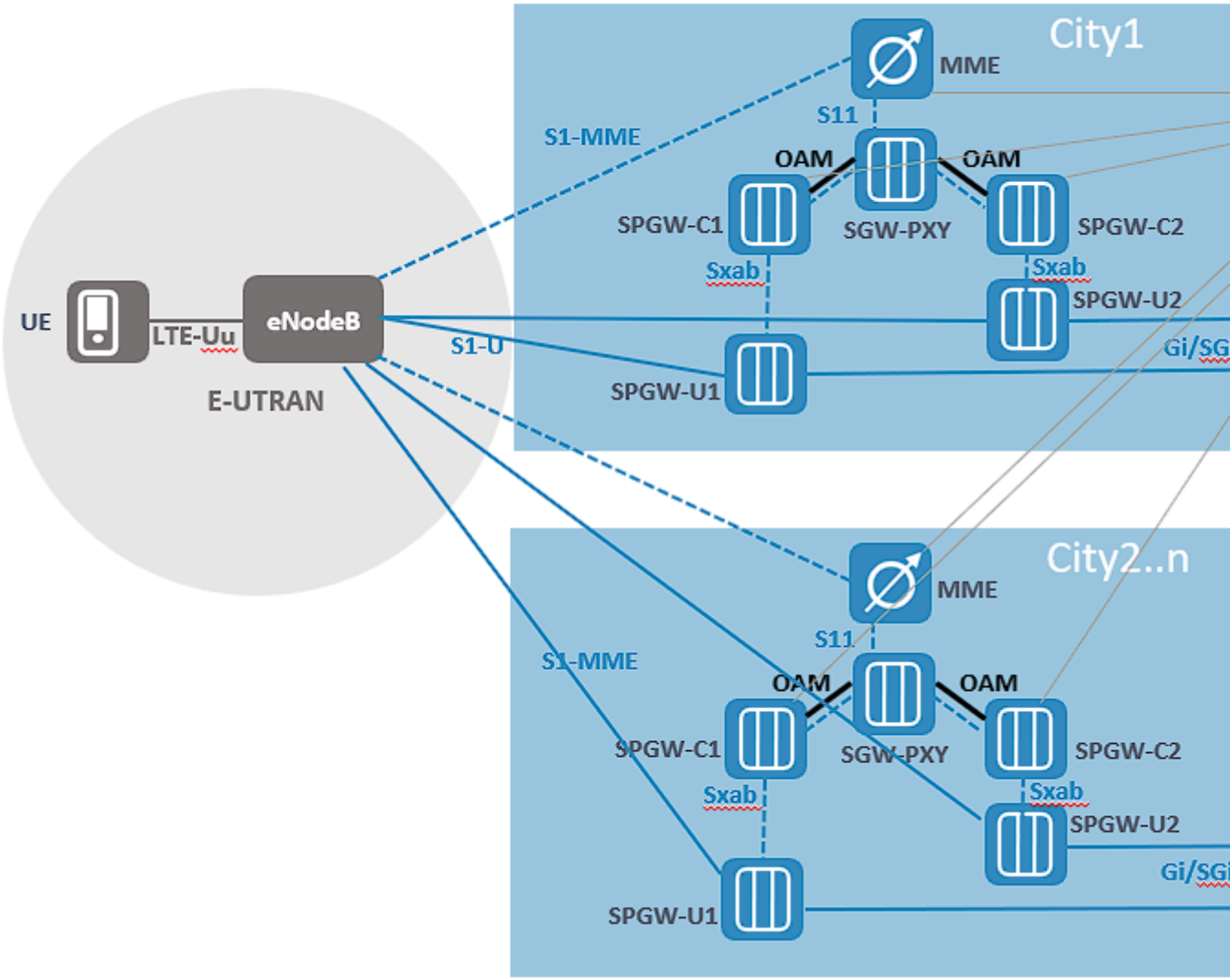


Рисунок 3: Гео-резервирование

2.4.1. **Резервирование подсистем**

Все подсистемы и модули платформы взаимодействуют с HSS и PCRF через DRA.

Компоненты vEPC подключены к Diameter Routing Agent используя два линка, через которые происходит резервирование и балансировка.

Для оценки доступности Diameter линка используются сообщения Diameter - DWR и DWA, которыми элементы обмениваются раз в X сек. Если линк несколько раз не ответил на запрос, то он помечается не активным. Если позже он стал отвечать на запросы, линк помечается активным.

Резервирование PCRF, HSS и DRA выходит за рамки данного описания.

Отказоустойчивость DNS обеспечивается путем анализа доступности линков.

Отказоустойчивость протоколов основанных на SIP обеспечивается посылкой и приемом OPTIONS. На основании X не удачных ответов делается вывод о не доступности узла и он временно исключается из пула.

SPGW-C

- Работа в режиме Master-Master. Распределение сессий между элементами происходит через пару SPGW Proxy.

MME

- Работа в режиме Master-Master. Распределение сессий происходит с использованием технологии MME pool, а также с помощью MME proxy.

SPGW-U:

- Работа в режиме Master-Master. Резервирование линков с пользовательским трафиком происходит за счет динамических протоколов маршрутизации OSPF или BGP.

Monitoring:

- Работа в режиме Master-Slave.

vEPC OAM Portal:

- Работа в режиме Master-Slave.

Admin-DB:

- Работа в режиме Master-Slave.

2.5. Мониторинг и обслуживание

vEPC предусматривает всесторонний съем метрик и счетчиков с компонентов платформы.

Метрики покрывают основные показатели комплекса, например:

Таблица 4. Метрики

Индикаторы качества SGSN-MME

S1_Setup_FR, % - Процент отказов при попытке установления SCTP соединения на S1 интерфейсе.

Paging_FR, % - Процент отказов выполнения процедуры PAGING.

Paging_First_FR, % - Процент отказов выполнения процедуры PAGING после посылки первого запроса.

Service_Req_FR, % - Процент отказов выполнения процедуры Service Request.

Service_Ext_Req_FR, % - Процент отказов выполнения процедуры Extended Service Request.

Attach_FR, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной относящейся к работе сети.

Comb_Attach_FR, % - Процент неуспешных попыток установления Combined Attach, на которые был получен отказ с причиной относящейся к работе сети.

Attach_FR_ESM_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #19 – ESM failure.

Attach_FR_Net_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #17 – Network failure.

Attach_FR_Unspec, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified.

Attach_FR_Unspec_Auth, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified: no response for authentication.

Attach_FR_Unspec_Identity, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified: no response for identity request.

Attach_FR_Unspec_Alg, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified: algorithm negotiation failure.

Attach_FR_Unspec_IMEI, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified: no response for IMEI check.

Attach_FR_Unspec_eNB, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #111 - Protocol error, unspecified: failure response from the eNodeB.

Attach_FR_Cong, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной #22 Congetion.

Intra_TAU_FR, % - Процент неуспешных попыток выполнения процедуры intra-MME TAU, на которые был получен отказ с причиной относящейся к работе сети.

Intra_TAU_FR_Id_Not_Derived, % - Процент неуспешных попыток выполнения процедуры intra-MME TAU, на которые был получен отказ с причиной #9 UE identity cannot be derived by the network.

Intra_TAU_FR_Unspec, % - Процент неуспешных попыток выполнения процедуры intra-MME TAU, на которые был получен отказ с причиной #111 Protocol err, unspec.

Intra_TAU_FR_Cong, % - Процент неуспешных попыток выполнения процедуры intra-MME TAU, на которые был получен отказ с причиной #22 Congestion.

Inter_TAU_FR, % - Процент неуспешных попыток выполнения процедуры inter-MME TAU, на которые был получен отказ с причиной относящейся к работе сети.

Inter_TAU_FR_Id_Not_Derived, % - Процент неуспешных попыток выполнения процедуры inter-MME TAU, на которые был получен отказ с причиной #9 UE identity cannot be derived by the network.

Inter_TAU_FR_Unspec, % - Процент неуспешных попыток выполнения процедуры inter-MME TAU, на которые был получен отказ с причиной #111 Protocol err, unspec.

Detach_FR, % - Процент неуспешных попыток выполнения процедуры Detach.

Identity_FR, % - Процент неуспешных попыток выполнения процедуры Identification.

Auth_FR, % - Процент неуспешных попыток выполнения процедуры Authentication.

Security_FR, % - Процент неуспешных попыток выполнения процедуры Security Mode Control.

PDNC_FR, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной относящейся к работе сети.

PDNC_FR_Insuf_Res, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #26 Insufficient resources.

PDNC_FR_Auth, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #29 User authentication failed.

PDNC_FR_Rej_S/PGW, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #30 Activation rejected by Serving GW or PDN GW.

PDNC_FR_Unspec, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #31 Activation rejected, unspecified.

PDNC_FR_Out_of_order, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #34 Service option temporarily out of order.

PDNC_FR_Net_fail, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #38 Network failure.

PDNC_FR_Prot_err, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #95-111 Protocol error, unspecified.

PDNC_FR_ODB, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #8 Operator determined barring.

PDNC_FR_Unk_Apn, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной #27 Unknown or missing APN.

PDNC_FR_ERAB_Fail, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity, на которые был получен отказ с причиной E-RAB failed.

DEDB_FR, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ с причиной относящейся к работе сети.

DEDB_FR_Insuf_Res, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ с причиной #26 Insufficient resources.

DEDB_FR_Unspec, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ с причиной #31 Activation rejected, unspecified.

DEDB_FR_Prot_err, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ с причиной #95-111 Protocol error, unspecified.

DEDB_FR_ERAB, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ E-RAB setup fails.

DEDB_FR_UE, % - Процент неуспешных попыток выполнения процедуры Activate Dedicated EPS Bearer Context, на которые был получен отказ No Response from UE.

DEFB_FR, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной относящейся к работе сети.

DEFB_FR_Insuf_Res, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #26 Insufficient resources.

DEFB_FR_ Auth, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #29 User authentication failed.

DEFB_FR_ Rej_S/PGW, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #30 Activation rejected by Serving GW or PDN GW.

DEFB_FR_ Unspec, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #31 Activation rejected, unspecified.

DEFB_FR_ Net_fail, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #38 Network failure.

DEFB_FR_ Prot_err, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной #95-111 Protocol error, unspecified.

DEFB_FR_ ERAB_fail, % - Процент неуспешных попыток выполнения процедуры Activate Default EPS Bearer Context, на которые был получен отказ с причиной E-RAB Failed.

BRR_DEACT_FR, % - Процент неуспешных попыток выполнения процедуры Deactivate EPS Bearer Context (Default или Dedicated).

BRR_MOD_FR, % - Процент неуспешных попыток выполнения процедуры Modify EPS Bearer Context (Default или Dedicated).

4Gto3G_RAU_FR, % - Процент неуспешных попыток выполнения процедуры Routing Area Update при переходе из LTE в UTRAN.

4Gto2G_RAU_FR, % - Процент неуспешных попыток выполнения процедуры Routing Area Update при переходе из LTE в GERAN.

4Gto2G/3G_RAU_FR, % - Процент неуспешных попыток выполнения процедуры Routing Area Update при переходе из LTE в GERAN/UTRAN.

In_Attach_FR, % - Процент неуспешных попыток выполнения процедуры Attach (eNodeB→MME)) при переходе из UTRAN/GERAN в LTE.

In_TAU _FR, % - Процент неуспешных попыток выполнения процедуры Tracking Area Update (eNodeB→MME) при переходе из UTRAN/GERAN в LTE.

3Gto4G_TAU_FR, % - Процент неуспешных попыток выполнения процедуры Tracking Area Update при переходе из UTRAN в LTE.

2Gto4G_TAU_FR, % - Процент неуспешных попыток выполнения процедуры Tracking Area Update при переходе из GERAN в LTE.

2G/3Gto4G_TAU_FR, % - Процент неуспешных попыток выполнения процедуры Tracking Area Update при переходе из GERAN/ UTRAN в LTE.

Intra_X2_HO_FR, % - Процент неуспешных попыток выполнения процедуры X2 interface-based handover.

Intra_S1_HO_FR, % - Процент неуспешных попыток выполнения процедуры intra-MME S1 interface-based handover.

Inter_HO_FR, % - Процент неуспешных попыток выполнения процедуры inter-MME S1 interface-based handover.

Comb_Attach_CS_FR, % - Процент неуспешных попыток установления S1 mode combined attach для non-EPS сервисов.

CS_paging_SR, % - Процент успешности выполнения процедуры SGs interface CS paging.

VoLTE_PDNC_FR, % - Процент неуспешных попыток выполнения процедуры UE Requested PDN Connectivity для сервиса VoLTE.

VoLTE_VBRR_FR, % - Процент неуспешных попыток активации VoLTE voice bearer.

VoLTE_INTRA_HO_FR, % - Процент неуспешных попыток выполнения VoLTE Intra-MME Voice bearer handover.

VoLTE_INTER_HO_FR, % - Процент неуспешных попыток выполнения VoLTE Inter-MME Voice bearer handover.

VoLTE_SRVCC_HO_FR, % - Процент неуспешных попыток выполнения SRVCC handover.

HSS_UL_FR, % – Процент неуспешных Update Location Request.

HSS_CL_FR, % – Процент неуспешных Cancel Location Request.

HSS_AI_FR, % – Процент неуспешных Authentication Information Request.

Paging_VoLTE_SR, % - Процент успешности выполнения процедуры IMS paging.

Attach_SR_4G, % - Процент успешных попыток установления Attach в сети LTE.

EBC_SR, % - Процент успешных EPS Bearer Context.

Attach_FR_Prot_Err, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «Protocol error».

Attach_FR_Gr_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «Gr fail».

Attach_FR_Local_Upd_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «Protocol error - location update failure».

Attach_FR_Get_Auth_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «Get authentication sets fail».

Attach_FR_Auth_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «No response of authentication».

Attach_FR_Ident_Fail, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «No response of identity request».

Attach_FR_Ndata_HLR, % - Процент неуспешных попыток установления Attach, на которые был получен отказ с причиной «No data from HLR».

PDP_FR, % - Процент неуспешных попыток установления PDP.

PDP_FR_Insuf_Res, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «Insufficient net resources».

PDP_FR_Unspec, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «Unspecified Reason».

PDP_FR_Auth_Failed, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «User authentication fail»

PDP_FR_Rej_GGSN, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «Rejected by GGSN».

PDP_FR_ODB, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «Operator determined barring».

PDP_FR_Unk_APN, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «Missing or unknown apn».

PDP_FR_DNS_Fail, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «DNS resolution fail».

PDP_FR_RAB_Fail, % - Процент неуспешных попыток установления PDP, на которые был получен отказ с причиной «RAB assignment fail».

PDP_FR_Frg_Subs, % - Процент неуспешных попыток установления PDP для foreign subscribers.

PDP_FR_Detach_actv_over, % - Процент неуспешных попыток установления PDP context по причине «PDP Activation Requests dropped due to detach request while activation was in progress».

PDP_FR_Other_procedure, % - Процент неуспешных попыток установления PDP context по причине «Activate Request during network initiated detach» или «Page timer expiry while trying to send Activate Accept/Reject».

PDP_FR_Before_act, % - Процент неуспешных попыток установления PDP context по причине « Activation Requests dropped due to IU release before the completion of activation procedure».

PDP_FR_Tunnel_deact, % - Процент неуспешных попыток установления PDP context по причине «Activation Requests that fail due to tunnel deactivation».

PDP_FR_APN_RAT, % - Процент неуспешных попыток установления PDP context по причине «APN not supported in PLMN and RAT combination»

PDP_FR_Out_of_order, % - Процент неуспешных попыток установления PDP context по причине « Service option is temporarily out of order»

PDP_UPD_FR_NW, % - Процент неуспешных попыток модификации PDP context, инициированных сетью

Paging_FR, % - Процент отказов выполнения процедуры PAGING (количество Paging запросов может быть больше одного).

Intra_SGSN_RAU_FR, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN RA Update.

Intra_SGSN_RAU_FR_Pro_Err, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN RA Update, на которые был получен отказ с причиной «Protocol error».

Intra_SGSN_RAU_FR_Auth_Fail, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN RA Update, на которые был получен отказ с причиной «No response of authentication».

Intra_SGSN_RAU_FR_Gr_Fail, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN RA Update, на которые был получен отказ с причиной «Gr fail».

Intra_SGSN_Periodic_RAU_FR, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN Periodic RA Update.

Intra_SGSN_Periodic_RAU_FR_Pro_Err, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN Periodic RA Update, на которые был получен отказ с причиной «Protocol error».

Intra_SGSN_Periodic_RAU_FR_Auth_Fail, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN Periodic RA Update, на которые был получен отказ с причиной «No response of authentication».

Intra_SGSN_RAU_FR_PDP, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN Periodic RA Update with PDP.

Intra_SGSN_RAU_FR_wo_PDP, % - Процент неуспешных попыток выполнить процедуру Intra-SGSN Periodic RA Update without PDP.

Inter_SGSN_RAU_FR, % - Процент неуспешных попыток выполнить процедуру Inter-SGSN RA Update.

Inter_SGSN_RAU_FR_Code#9, % - Процент неуспешных попыток выполнить процедуру Inter-SGSN RA Update, на которые был получен отказ с причиной «MS identity cannot be derived by the network».

Inter_SGSN_RAU_FR_Pro_err, % - Процент неуспешных попыток выполнить процедуру Inter-SGSN RA Update, на которые был получен отказ с причиной «Protocol error».

Inter_SGSN_RAU_FR_Gr_Fail, % - Процент неуспешных попыток выполнить процедуру Inter-SGSN RA Update, на которые был получен отказ с причиной «Gr fail».

Inter_SGSN_RAU_FR_Auth_Fail, % - Процент неуспешных попыток выполнить процедуру Inter-SGSN RA Update, на которые был получен отказ с причиной «No response of authentication».

Auth_FR, % - Процент неуспешных запросов на аутентификацию.

RAB_FR, % - Процент неуспешных попыток RAB Assignment requests.

Attach_SR_3G, % - Процент успешных попыток установления Attach в сети 3G.

PDP_SR_3G, % - Процент успешных попыток установления PDP в сети 3G.

MME_SAU, num - Среднее количество одновременно «приаттаченных» абонентов 4G.

MME_EBC, num - Среднее количество одновременно установленных EPS Bearer Context (Default и Dedicated).

SGSN_SAU, num - Среднее количество одновременных «приаттаченных» абонентов 2G/3G.

SGSN_PDP, num - Среднее количество одновременных активных PDP контекстов 2G/3G.

SGSN_SAU_ALL, num - Среднее количество одновременных «приаттаченных» абонентов на SGSN-MME.

SGSN_PDP_BRR, num - Среднее количество одновременных активных PDP контекстов 2G/3G и установленных EPS Bearer Context (Default и Dedicated).

SGSN_Data_Vol, MB – Общий объем пакетных данных в направлениях UL и DL.

2G_Data_Vol, MB – Общий объем 2G пакетных данных в направлениях UL и DL.

3G_Data_Vol, MB – Общий объем 3G пакетных данных в направлениях UL и DL.

SGSN_THR, Mbps - Среднее количество 2G/3G трафика (UL+DL) передаваемого в единицу времени.

EPC_Util_MME_EBC_SW, % - Утилизация MME по количеству одновременно установленных EPS Bearer Context (Default и Dedicated) по лицензионной емкости.

EPC_Util_MME_SW,% - Утилизация MME по лицензионной емкости.

PS_Core_Util_SGSN_PDP_SW, % - Утилизация SGSN по количеству активных PDP контекстов по лицензионной емкости.

PS_Core_Util_SGSN_SW, % - Утилизация SGSN по лицензионной емкости.

PS_Core_Util_SGSN_SAU_HW, % - Утилизация SGSN-MME по количеству одновременно «приаттаченных» абонентов по аппаратной емкости.

PS_Core_Util_SGSN_PDP_HW, % - Утилизация SGSN-MME по количеству активных PDP контекстов и установленных EPS Bearer Context по аппаратной емкости.

PS_Core_Util_SGSN_CPU, % - Утилизация SGSN-MME по процессорной емкости.

PS_Core_Util_SGSN_HW, % - Утилизация SGSN-MME по аппаратной емкости.

MME_Attach_per_subs, num per subs – Среднее количество попыток установления Attach на одного абонента.

MME_DEFB_per_subs, num per subs – Среднее количество default bearer activation procedures на одного абонента.

MME_DEDB_per_subs, num per subs – Среднее количество dedicated bearer activation procedures на одного абонента.

MME_INTRA_TAU_per_subs, num per subs – Среднее количество intra-MME TAU procedures на одного абонента.

MME_INTRA_X2_HO_per_subs, num per subs – Среднее количество intra-MME X2 handover procedures на одного абонента.

MME_INTRA_S1_HO_per_subs, num per subs – Среднее количество intra-MME S1 handover procedures на одного абонента.

VoLTE_Vcall_per_subs, num per subs – Среднее количество VoLTE voice call procedures (включая MO, MT и video call) на одного абонента.

CSFB_Vcall_per_subs, num per subs – Среднее количество CSFB voice call procedures (включая MO и MT) на одного абонента.

SGSN_Attach_per_subs, num per subs – Среднее количество попыток установления Attach на одного абонента.

SGSN_PDP_per_subs, num per subs – Среднее количество попыток активации PDP на одного абонента.

Intra_SGSN_RAU_per_subs, num per subs – Среднее количество попыток выполнения процедуры Intra-SGSN RA Update на одного абонента.

Inter_SGSN_RAU_per_subs, num per subs – Среднее количество попыток выполнения процедуры Inter-SGSN RA Update на одного абонента.

Индикаторы качества GGSN-S/PGW

EBC_FR, % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной относящейся к работе сети.

EBC_FR_Sys_fail, % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной System failure.

EBC_FR_No_res(Bearer), % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной No resources available (no bear context resource).

EBC_FR_No_res(License), % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной No resources available(no License resource).

EBC_FR_No_res(QoS), % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной No resources available(no QOS resource).

EBC_FR_No_res(DHCP), % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной All dynamic addresses are occupied.

EBC_FR_No_res(Memory), % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной No memory available.

EBC_FR_Auth_fail, % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной User authentication failed.

EBC_FR_APN_Den, % - Процент неуспешных попыток выполнения процедуры EPS Bearer Context Establishment (Default и Dedicated), на которые был получен отказ с причиной APN access denied -no subscription.

PGW_DEDB_FR, % – Процент неуспешных попыток выполнения dedicated bearer context creation.

PGW_DEL_BRR_FR, % – Процент неуспешных попыток выполнения bearer context deletion, инициированных S-GW/P-GW.

MME_DEL_DEDR_FR, % – Процент неуспешных попыток выполнения dedicated bearer context deletion, инициированных MME.

PGW_MOD_BRR_woQOS_FR, % – Процент неуспешных попыток выполнения bearer context modification without QoS update.

PGW_MOD_BRR_wQOS_FR, % – Процент неуспешных попыток выполнения bearer context modification with QoS update.

HSS_MOD_BRR_wQOS_FR, % – Процент неуспешных попыток выполнения bearer context modification with QoS update, инициированных HSS.

GTP_UnSR, % - Процент неуспешных процедур создания PDP контекста.

GTP_FR, % - Процент неуспешных процедур создания PDP контекста по причинам, связанным с проблемами на оборудовании.

GTP_FR_No_res, % - Процент неуспешных процедур создания PDP контекста по причине отсутствия ресурса (GTP error: resources unavailable, dynamic address unavailable, memory not available).

GTP_FR_Sys_fail, % - Процент неуспешных процедур создания PDP контекста с причиной «system failure».

GTP_FR_Auth, % - Процент неуспешных процедур создания PDP контекста с причиной «Authentication fail».

PDP_Deact_FR_GGSN, % - Процент неуспешно деактивированных PDP контекстов.

GGSN_PDP_Rate, num per sec – Скорость поступления запросов на создание PDP context.

GTP_UPD_FR, % - Процент неуспешных процедур Update PDP контекста.

IP_Pool_Util, % - Процент утилизации IP pool.

S/PGW_EBC, num - Среднее количество одновременно установленных EPS Bearer Context (Default и Dedicated).

S/PGW_Data_Vol, MB - Общий объем 4G пакетных данных в направлениях UL и DL.

S/PGW_Thr, Mbps - Среднее количество 4G трафика (UL+DL) передаваемого в

единицу времени.

GGSN_PDP, num - Среднее количество одновременных активных PDP контекстов 2G и 3G.

GGSN_Data_Vol, MB – Общий объем 2G/3G пакетных данных в направлениях UL и DL.

GGSN_THR, Mbps - Среднее количество 2G/3G трафика (UL+DL) передаваемого в единицу времени.

GGSN_ S/PGW_PDP_EBC, num - Среднее количество установленных PDP Context и EPS Bearer Context.

GGSN_S/PGW_Thr, Mbps - Среднее количество 2G-3G-4G трафика (UL+DL) передаваемого в единицу времени.

GGSN_AVG_CPU_MPU,% - Средняя загрузка CPU GGSN/SPGW для MPU плат.

GGSN_PEAK_CPU_MPU,% - Пиковая загрузка CPU GGSN/SPGW для MPU плат.

GGSN_AVG_CPU_SPU, % - Средняя загрузка CPU GGSN/SPGW для SPU плат.

GGSN_PEAK_CPU_SPU, % - Пиковая загрузка CPU GGSN/SPGW для SPU плат.

EPC_Util_PGW_EBC_SW, % - Утилизация PGW по количеству одновременно установленных EPS Bearer Context (Default и Dedicated) по лицензионной емкости.

EPC_Util_SGW_EBC_SW, % - Утилизация SGW по количеству одновременно установленных EPS Bearer Context (Default и Dedicated) по лицензионной емкости.

PS_Core_Util_GGSN_PDP_SW, % - Утилизация GGSN по количеству активных PDP контекстов по лицензионной емкости.

PS_Core_Util_GGSN_SW, % - Утилизация GGSN по лицензионной емкости.

PS_Core_Util_GGSN_PDP_HW, % - Утилизация GGSN/SPGW по количеству активных PDP контекстов и установленных EPS Bearer Context по аппаратной емкости.

PS_Core_Util_GGSN_Thr_HW, % - Утилизация GGSN/SPGW по пропускной способности по аппаратной емкости.

PS_Core_Util_GGSN_CPU, % - Утилизация GGSN/SPGW по процессорной емкости.

PS_Core_Util_GGSN_NPU, % - Утилизация GGSN /SGW/PGW по загрузке NPU.

PS_Core_Util_GGSN_HW, % - Утилизация GGSN/SPGW по аппаратной емкости.

Выгрузка метрик может осуществляться во внешнюю систему, например, Globus или др., через sftp/https/nfs.

Обычно используется sftp + csv формат.

Для целей оперативного мониторинга состояния системы используется проверенное решение Prometheus + AlertManager + Grafana. Система генерирует алармы, которые могут быть выгружены в системы мониторинга заказчика, например, NetCool (SNMP or CSV). Кастомизация алармов производится по согласованию с Заказчиком.

Мониторинг доступен в Grafana, несколько дашбордов эффективно показывают общую картину происходящего, текущие нагрузки, пиковые значения, параметры работы серверов и другие показатели.

Администрирование платформы осуществляется через специальный web интерфейс, позволяющий управлять всеми элементами, производить их

вывод из работы, обслуживание, смену конфигов и скриптов и обратный ввод в работу. Часть настроек доступно исключительно через CLI, linux based команды.

Развертывание ПО производиться с помощью автоматизированных сценариев.

Процедура автоматизированных бэкапов позволяет с заданной периодичностью, обычно раз в сутки, сохранять все важные параметры конфигураций в структуре папок, архивировать их и пересылать на внешний sftp сервер.

2.6. Подсистема мониторинга и сбора трейсов

В данной главе рассмотрены следующие модули подсистемы мониторинга:

- Agent Side
- Server Side
- Web Portal
- Prometheus
- SNMP notifier
- Grafana
- tshark.

SIP Trace System – это решение, предназначенное для захвата, анализа и мониторинга SIP трафика с широкими возможностями масштабирования способное обрабатывать огромные объёмы трафика свойственные VoIP-операторам малого или среднего размера.

Эта система призвана облегчить инженерам поиск и устранение неисправностей в IP-сетях при помощи мощного анализа и визуализации IP-диалогов между узлами и детальный просмотр всех IP-сообщений. Решение позволяет сохранять выгружать IP-трейсы вызовов в виде pcap дампов или текстовых файлов. Еще одним преимуществом решения является возможность разнесения компонентов системы по разным узлам, что позволяет масштабировать систему.

Решение IP Trace System состоит из нескольких подсистем. Рассмотрим эти подсистемы и механизм их взаимодействия межу собой.

Архитектура OAM-портала мониторинга и трассировки IP-трафика представлена на Рисунок 4.

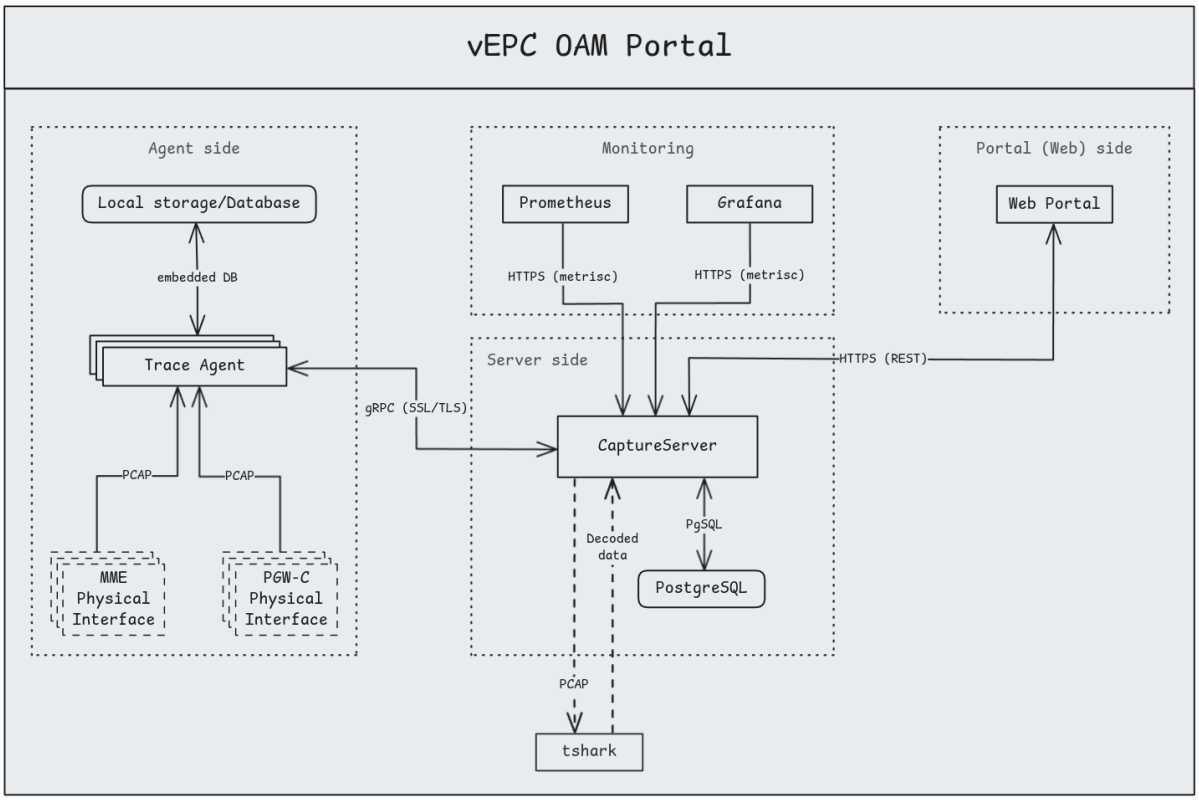


Рисунок 4: Архитектура OAM-портала, предназначенного для централизованного мониторинга, сбора и визуализации IP-трейсов и метрик в системе vEPC.

Архитектура разделена на три основные части:

- Agent Side (Агентская сторона):
  Включает один или несколько модулей Trace Agent, которые собирают SIP-трейсы и сохраняют их во встроенную локальную базу данных. Передача данных к серверной части осуществляется по защищённому каналу gRPC (SSL/TLS)
- Server Side (Серверная сторона):
  Основным компонентом является CaptureServer, получающий данные от агентов трассировки, а также метрики от систем мониторинга Prometheus и Grafana по протоколу HTTPS. Захваченные данные записываются в PostgreSQL, с возможностью углублённого анализа при помощи tshark.
  Также реализован REST-интерфейс (HTTPS) для связи с веб-порталом
- Web Portal (Портальная часть):
  Веб-портал предоставляет пользователю доступ к результатам анализа и мониторинга через защищённый HTTPS-интерфейс.

2.6.1. **Prometheus**

Prometheus — система мониторинга различных систем и микросервисов, которая с заданным интервалом времени опрашивает все целевые объекты для получения их метрик.

Для сбора метрик на целевые объекты (IP Proxy, AS, Database) устанавливаются экспортеры, данные от которых передаются на сервер и хранятся в базе данных. Сервер Prometheus периодически опрашивает экспортеры и в случае их недоступности формирует сообщения об ошибках.

Протокол: http, формат данных: JSON, язык формирования запросов: PromQL (Prometheus Query Language).

Архитектура Prometheus представлена на Рисунок 5.

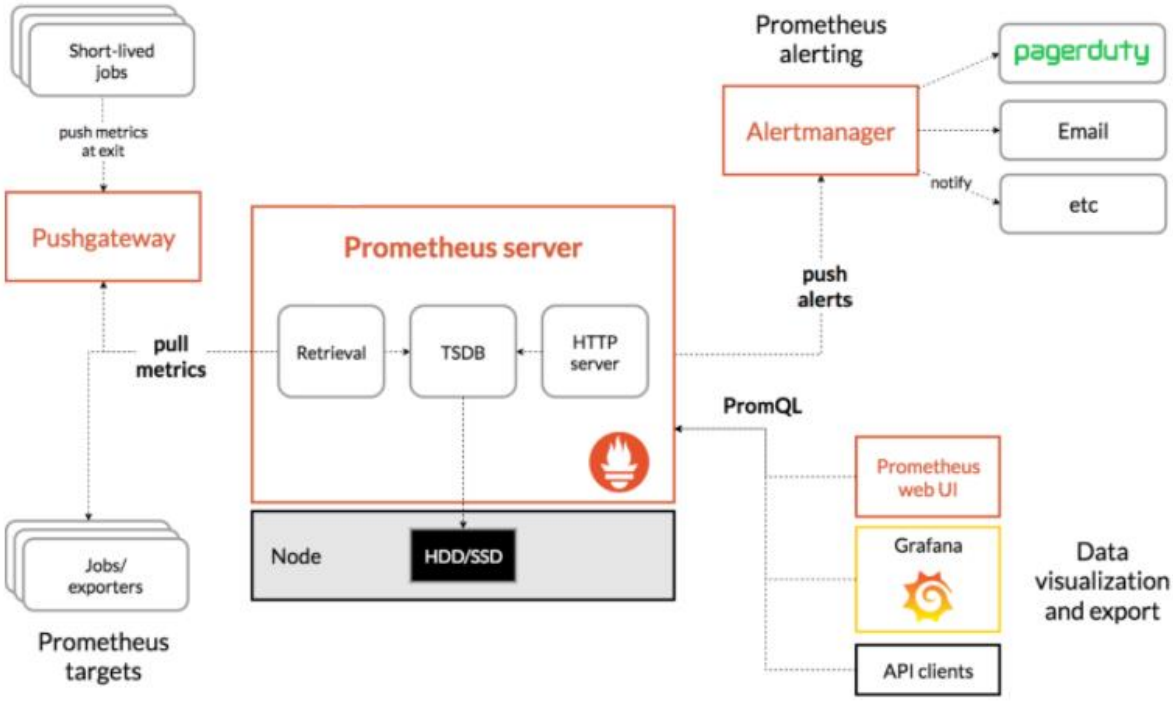


Рисунок 5: Архитектура Prometheus

Prometheus хранит данные в виде временных рядов — наборов значений, соотнесённых с временной меткой (timestamp). Элемент временного ряда (измерение) состоит из имени метрики, временной метки и пары «ключ — значение». Временные метки имеют точность до миллисекунд, значения представлены с 64-битной точностью.

С помощью Grafana можно визуализировать полученные данные в виде наглядных графиков, диаграмм и таблиц.

Для рассылки оповещений используется Alertmanager. Настройки уведомлений задаются в конфигурационном файле, в котором можно добавить ссылки на файлы правил. В правилах прописываются условия, при

которых нужно отправлять уведомления. Отправка уведомлений осуществляется по электронной почте, через веб-хук, HipChat или Telegram.

2.6.2. SNMP notifier

SNMP notifier является проксирующим модулем между Alertmanager и внешними системами и отвечает за отправку snmp trap.

SNMP trap UID задаются в соответствии с корпоративной структурой UID и для TAS имеют префикс: ..3.6..4..19792.30..

Список сообщений об ошибках и их UID представлены в отдельном файле.

2.6.3. Grafana

Grafana — это платформа для визуализации, мониторинга и анализа данных. Использует метрики Prometheus, и отображает их в виде информативных графиков и диаграмм, организованных в настраиваемые панели.

Grafana позволяет создавать различные dashboard для отображения разных срезов данных, группировать и агрегировать данные по различным параметрам.

Grafana имеет собственный WEB интерфейс, хранит данные пользователей с различными правами доступа.

2.6.4. **Trace Agent — агент сбора трейсов**

Trace Agent — это программный компонент, устанавливаемый на целевых узлах сети vEPC, предназначенный для захвата, обработки и передачи сетевых трейсов (в частности, IP-сообщений) в централизованный сервер мониторинга (CaptureServer).

Назначение Trace Agent:

Trace Agent обеспечивает сбор критически важной диагностической информации о IP-сессиях в реальном времени, позволяя операторам и инженерам:

- быстро идентифицировать и анализировать сбои в соединениях
- отслеживать IP-диалоги и сообщения между сетевыми элементами
- проводить анализ с помощью pcap-файлов и веб-интерфейса.

2.6.5. CaptureServer — сервер сбора и обработки IP-трейсов

CaptureServer — центральный компонент серверной части, получающий SIP-трейсы от Trace Agent'ов, а также метрики от систем мониторинга (Prometheus, Grafana).

Основные функции:

- Приём трафика от агентов через gRPC (TLS)
- Хранение данных в СУБД PostgreSQL
- Возможность интеграции с tshark для глубокой декомпозиции SIP-сообщений
- Экспорт данных в другие системы (REST API)
- Агрегация метрик из Prometheus для анализа производительности
- Поддержка нескольких баз данных
- Авторизация пользователей по RADIUS.

2.6.6. Web Portal — веб-интерфейс

Web Portal — веб-интерфейс, предоставляющий доступ к данным мониторинга, IP-трейсам и статистике.

Основные возможности:

- Поиск и фильтрация IP-сессий и вызовов
- Просмотр сообщений IP в структуре диалога
- Загрузка pcap-файлов для анализа
- Аутентификация пользователей и контроль доступа
- Отображение состояния агентов, серверов, соединений и метрик
- Графики со статистикой и аналитикой
- Мощный пользовательский интерфейс для поиска и фильтрации
- Поддержка REST API и виджетов.

2.6.7. HEPlify

Новый легковесный Capture Agent, написанный на GO. Его можно запускать на Linux, ARM или Windows для захвата IPv4 / IPv6 пакетов и отправки их на CaptureServer.

2.6.8. HEpipe

HEPipe – это приложение командной строки для регистрации произвольных данных (логи, CDR, строк отладки) на сервере мониторинга.

2.7. Ролевая модель доступа

Управление учётными записями и правами доступа реализуется с помощью компонента Single Sign On Server (более подробно описан в документе Single Sign On Server Administration Guide).

Он обеспечивает выполнение следующих основных задач:

- предоставление «единого входа» и «единого выхода» для приложений браузера;
- поддержка OpenID Connect;
- поддержка OAuth 2.0;
- поддержка SAML;
- Identity Brokering — Аутентификация с внешними OpenID Connect или провайдерами идентификации SAML;
- поддержка федерации пользователей — синхронизация учетных данных пользователей с серверов LDAP и Active Directory;
- мост Kerberos — автоматическая аутентификация пользователей, вошедших на сервер Kerberos;
- двухфакторная аутентификация — поддержка TOTP/HOTP через Google Authenticator или FreeOTP;
- консоль администратора для централизованного управления пользователями, ролями, отображением ролей, клиентами и конфигурацией;
- управление сеансами — администраторы и могут просматривать и управлять сеансами пользователей;
- поддержка CORS — клиентские адаптеры имеют встроенную поддержку CORS;
- интерфейсы поставщиков услуг (SPI) — ряд SPI, позволяющих настраивать различные аспекты сервера. Потоки аутентификации, провайдеры федерации пользователей, средства отображения протоколов;

В таблице 4 обозначена предопределенная ролевая модель, с которой поставляется система, также возможна настройка ролей под требование заказчика:

Таблица 4. Набор ролей в системе IMS Core

Система/ подсистема/ функция	Главный администратор	Администратор ОЭ	Администратор ИБ	Пользователь ОЭ	Пользователь ОМ (мониторинг)	Пользователь ИБ	Пользователь STS (SIP Trace System)
SSO							
Управление политиками безопасности	RW	R	RW	R	na	R	na
Управление пользователями	RW	RW	RW	R	na	R	na
Управление ролями и группами пользователей	RW	RW	RW	R	na	R	na
O&M							
vEPC Web Portal Backoffice	RW	RW	R	R	R	R	na
Ansible	RW	RW	R	R	R	R	na
Logging Subsystem	RW	R	RW	R	R	R	na
Monitoring Dashboards	RW	RW	R	RW	RW	R	R
IP Trace System	RW	RW	R	R	R	R	RW
CI\CD							
Harbor	RW	RW	R	R	na	R	na

3. **Функциональные возможности и процедуры виртуализированного ядра сети vEPC.**

3.1. Введение

Виртуализированное ядро пакетной сети (vEPC) представляет собой фундаментальный сдвиг в архитектуре мобильных сетей, заменяя традиционное аппаратное оборудование программно-определяемыми сетевыми функциями (NFV). Эта трансформация обеспечивает беспрецедентную гибкость, масштабируемость и экономическую эффективность, что критически важно для удовлетворения растущего спроса на мобильные данные и поддержки новых сервисов, таких как Интернет вещей (IoT) и технологии 5G. Для оператора связи, внедрение vEPC, является стратегическим шагом к модернизации инфраструктуры, повышению операционной эффективности и обеспечению превосходного качества обслуживания абонентов.

3.2. 2. Функциональные возможности и процедуры SGW/PGW

SGW (Serving Gateway) и PGW (Packet Data Network Gateway) являются критически важными элементами Evolved Packet Core (EPC). SGW отвечает за маршрутизацию пользовательского трафика, управление мобильностью данных между базовыми станциями, а также за тарификацию. PGW является точкой выхода абонентского трафика в внешние сети (например, Интернет), выполняет функции присвоения IP-адресов, обеспечения качества обслуживания (QoS) и применения политик. GGSN (Gateway GPRS Support Node) выполняет схожие функции в сетях 2G/3G. В контексте vEPC эти функции могут быть объединены или разделены (CUPS).

В следующей таблице представлены описания ключевых функций SGW/PGW/GGSN, извлеченные из предоставленных материалов. Эта таблица является центральным элементом отчета, напрямую отвечающим на запрос пользователя. Она систематизирует большой объем технических функций, делая их легкодоступными и понятными. Для инженеров и операторов это будет быстрый справочник по возможностям их vEPC, а также основа для дальнейшего анализа и планирования.

3.2.1. **Таблица : Описание функций SGW/PGW**

	Original Description	Русское описание функции (для столбца E)

		Support DSCP marking based on QoS/QCI for UMTS/LTE	Поддержка маркировки трафика (GTP пакетов) с использованием значений DSCP (Differentiated Services Code Point) в зависимости от параметров QoS (Quality of Service) и QCI (QoS Class Identifier) для сетей UMTS и LTE. Это позволяет приоритизировать различные типы трафика.
		Support Coltrol Plane DSCP marking	Поддержка маркировки DSCP для трафика плоскости управления, что обеспечивает приоритизацию управляющих сообщений.
		Support for Direct Tunnel/One Tunnel functionality for UMTS	Поддержка функции прямого туннеля для

		UMTS, позволяющей трафику UE напрямую идти от RNC к GGSN, минуя SGSN, для оптимизации пути данных.
	Support for TCP MSS size separately for each APN	Возможность настройки максимального размера сегмента TCP (TCP MSS) индивидуально для каждой точки доступа (APN), что позволяет оптимизировать передачу данных для различных сервисов.
	Host/Ream-based Diameter Routing on Gx interface	Поддержка маршрутизации Diameter-сообщений на интерфейсе Gx на основе имени хоста или области (Realm), обеспечивая гибкое взаимодей

		ствие с PCRF.
	Host/Ream-based Diameter Routing on S6b interface	Поддержка маршрутизации Diameter-сообщений на интерфейсе S6b на основе имени хоста или области (Realm), обеспечивая гибкое взаимодействие с AAA-серверами для не-3GPP доступа.
	TAU from E-UTRAN to E-UTRAN (Under the Same MME, and Different S-GWs)	Процедура обновления зоны отслеживания (TAU) при перемещении абонента в пределах одной MME, но с изменением обслуживающего шлюза (S-GW).
	TAU from UTRAN (Iu Mode) to E-UTRAN	Процедура TAU при переходе абонента из сети UMTS

		(режим Iu) в сеть LTE.
	TAU from GERAN (Gb Mode) to E-UTRAN	Процедура TAU при переходе абонента из сети GSM/GPRS (режим Gb) в сеть LTE.
	RAU from E-UTRAN to UTRAN (Iu Mode)	Процедура обновления зоны маршрутизации (RAU) при переходе абонента из сети LTE в сеть UMTS (режим Iu).
	RAU from E-UTRAN to GERAN (Gb Mode)	Процедура RAU при переходе абонента из сети LTE в сеть GSM/GPRS (режим Gb).
	UPF selection Based APN	Выбор функции пользовательской плоскости (UPF) на основе точки доступа (APN).
	UPF selection Based Location Area	Выбор UPF на основе зоны

			местополо жения.
		UPF selection Default	Выбор UPF по умолчанию .
		Echo Request/Response GTPv1, GTPv2	Проверка обмена сообщения ми Echo Request/Re sponse по протокола м GTPv1 и GTPv2 на различных интерфейса х (S1-U, S11, S5/S8-C, S5/S8-U) для проверки доступност и и работоспос обности узлов.
		Supporting Default Bearer Activation/Deactivat ion	Поддержка активации и деактиваци и основного (Default) канала передачи данных (Bearer), обеспечива ющего базовое подключен ие UE к сети.

		Network Initiated Dedicated Bearer (new QCI)	Активация выделенного (Dedicated) канала передачи данных, инициированная сетью (например, для VoLTE-вызова), с использованием нового QCI для обеспечения требуемого качества обслуживания.
		Support bearer modification	Поддержка модификации каналов передачи данных, например, изменение параметров QoS по инициативе HLR/HSS.
		Multiple PDN Connections	Поддержка множественных подключений к сетям передачи данных (PDN) для одного абонента (например, для интернета и IMS

		одновременно).
	Multi-HPLMN Access	Поддержка доступа к сети для абонентов из различных домашних PLMN (HPLMN), что критично для роуминга.
	Manual Context Deactivation	Поддержка ручной деактивации контекста абонента (PDP/PDN соединения) со стороны SAEGW.
	GGSN Supporting PDP Context Update and Deactivation Procedures	Поддержка процедур обновления и деактивации PDP-контекста со стороны GGSN.
	PGW restart notification	Уведомление о перезапуске PGW.
	Idle PDP Deactivation by Timer	Деактивация неактивных PDP-контекстов по таймеру

		для эффективного использования ресурсов.
	IP Lease for Dynamicly Assigned Addresses	Управление арендой IP-адресов, динамически присваиваемых абонентам.
	Delete sessions from SGW after MME restart	Удаление сессий из SGW после перезапуска MME для обеспечения согласованности состояния сети.
	IPv4 PDN-context activation	Активация PDN-контекста с использованием адреса IPv4.
	IPv6 PDN-context activation	Активация PDN-контекста с использованием адреса IPv6.
	DualStack IPv4/IPv6 PDN-context activation	Активация PDN-контекста с поддержкой DualStack (одновременное

		использование IPv4 и IPv6).
	Local PGW-C/UPF Dynamic Address Assignment	Динамическое присвоение IP-адресов абонентам из локального пула адресов, настроенного на SAEGW (PGW-C/UPF).
	Radius Authentication (POD)	Аутентификация абонентов через Radius-сервер с использованием сообщений POD (Packet of Disconnect).
	Radius Accounting	Передача учетной информации (Accounting) на Radius-сервер для целей тарификации и мониторинга.
	Carbon-Copy of RADIUS Accounting Messages	Поддержка отправки копий Radius Accounting-

		сообщений на дополнительный (Carbon-Copy) Radius-сервер, что обеспечивает резервирование и аудит данных.
	Support Interim Accounting by time	Поддержка отправки промежуточных Radius Accounting-сообщений по истечении заданного времени, что позволяет отслеживать потребление услуг в реальном времени.
	Support transmitting to Radius: MS Timezone, MS IMEISV, RAT, IMSI, APN, SGW/SGSN/GGSN IP, MS Location Info	Поддержка передачи на Radius-сервер различных параметров абонента и сессии, таких как часовой пояс, IMEISV, тип радиодоступа (RAT), IMSI, APN, IP-адреса шлюзов и информаци

		я о местоположении абонента.
	Time-based CDR Generation SGW/PGW/GGSN	Генерация CDR (Call Detail Record) на SGW/PGW/GGSN на основе времени, с настраиваемым интервалом (например, минута).
	Volume-based CDR Generation SGW/PGW/GGSN	Генерация CDR на SGW/PGW/GGSN на основе объема переданных данных, с настраиваемым порогом.
	CDR Generation by RAT/SGSN/S-GW/timezone/maxconditions/plmn change trigger	Генерация CDR при изменении типа радиодоступа (RAT), SGSN/S-GW, часового пояса, достижении максимальных условий или при смене PLMN.

	IP-CAN Session Establishment with the PCRF	Установление сессии IP-CAN (IP Connectivity Access Network) с PCRF (Policy and Charging Rules Function), позволяющее PCRF доставлять динамические или предопределенные правила.
	PCRF-Delivered PCC Rule Installation	Установка правил PCC (Policy and Charging Control), доставляемых PCRF, для применения политик к трафику.
	PCC Rule Reauthorization	Повторная авторизация правил PCC.
	Support local PCC-rule per APN (Fallback to local PCC Rules when Gx fault)	Поддержка локальных правил PCC для каждой APN, с возможностью перехода на локальные правила в случае сбоя

		интерфейса Gx.
	QoS Update Triggering CCR Messages to the PCRF	Инициирование сообщений CCR (Credit Control Request) к PCRF при изменении QoS, сигнализируя об изменении качества обслуживания.
	Rat Update Triggering CCR Messages to the PCRF	Инициирование сообщений CCR к PCRF при изменении типа радиодоступа (RAT), сигнализируя о смене технологии доступа.
	ULI Change Triggering CCR Messages to the PCRF	Инициирование сообщений CCR к PCRF при изменении информации о местоположении абонента (User Location Information - ULI).

		Revalidation Timeout Triggering CCR Messages to the PCRF	Инициирование сообщений CCR к PCRF по истечении тайм-аута повторной валидации.
		PCRF Reselection Based on Origin-Host AVP in CCA-I/U/T/RAR	Перевыбор PCRF на основе AVP (Attribute-Value Pair) Origin-Host в сообщениях CCA-I/U/T/RAR.
		QoS Update Initiated from PCRF (RAR, CCR)	Обновление QoS, инициированное PCRF (через RAR или CCR).
		Gx result code behavior	Проверка поведения кодов результатов Gx.
		Failover for Gx over direct links to PCRF	Отказоустойчивость интерфейса Gx при прямом подключении к PCRF.
		Failover for Gx over DRA	Отказоустойчивость интерфейса Gx при использовании

			Diameter Routing Agent (DRA).
		VoLTE MO/MT call with activation dedicated bearer	Успешное выполнение исходящих (MO) и входящих (MT) VoLTE-вызовов с активацией выделенного канала передачи данных.
		VoLTE Emergency call	Поддержка экстренных вызовов VoLTE.
		IMS Restoration for P-CSCF Failure	Поддержка восстановления IMS-сервисов в случае сбоя P-CSCF.
		Support S2b + VoWiFi call	Поддержка вызовов VoWiFi через интерфейс S2b, интегрированных с ePDG Huawei.
		APN mapping based on TAC	Маппинг APN (например, isp.com) на виртуальный APN (isp2.com)

		на основе кода зоны отслеживания (TAC).
	APN mapping based on IMSI Range	Маппинг APN на виртуальный APN на основе диапазона IMSI.
	APN mapping based on LAC	Маппинг APN на виртуальный APN на основе кода зоны местоположения (LAC).
	APN load balancing	Балансировка нагрузки между APN.
	Rewrite APN info for CDR/AAA/Gx	Перезапись информации APN для CDR, AAA и Gx.
	Management Plane Isolation	Изоляция плоскости управления, предотвращающая несанкционированный доступ к интерфейсам OAM (Operation, Administration, Maintenanc

		е) с пользовательской стороны.
	Data Plane Isolation	Изоляция плоскости данных, предотвращающая несанкционированный доступ к IP-адресам абонентов с сетевых интерфейсов, не предназначенных для передачи данных.
	ACL Control (Intra APN, Inter APN, System)	Контроль доступа (ACL) для фильтрации трафика внутри одной APN, между различными APN и к внешним IP-адресам.
	NTP syncronization	Синхронизация системного времени SAEGW с внешним NTP-сервером.
	MTU Configuration	Настройка максимального блока передачи (MTU) на

			сетевых портах.
		VLAN tagging interfaces support (Subinterfaces)	Поддержка интерфейсов с тегированием VLAN (подинтерфейсов).
		APN to VRF binding	Привязка APN к VRF (Virtual Routing and Forwarding), обеспечивающая логическую изоляцию маршрутизации для разных APN.
		BGP IPv4 Dynamic routing	Поддержка динамической маршрутизации BGP (Border Gateway Protocol) для IPv4.
		BGP IPv6 Dynamic routing	Поддержка динамической маршрутизации BGP для IPv6.
		BFD protocol support for IPv4/IPv6	Поддержка протокола BFD (Bidirectional Forwarding

		Detection) для IPv4/IPv6, обеспечивающего быстрое обнаружение сбоев в пути передачи данных.
	Gi redirect	Поддержка перенаправления трафика через интерфейс Gi.
	Performance management (THP, PDP)	Управление производительностью, включая графики THP (Throughput) и PDP (Packet Data Protocol) для мониторинга ключевых показателей.
	Fault, alarm management	Управление сбоями и аварийными сигналами, включая отображение и логирование информации об авариях.

	Operation log (user activity logging) management	Управление журналом операций, регистрирующим активность пользователей (логины, команды, перезагрузки).
	User, group security management	Управление безопасностью пользователей и групп, включая создание пользователей с различными правами доступа.
	Operator permission management	Управление разрешениями операторов, позволяющее ограничивать выполнение команд для определенных групп/операторов.
	User tracing based on IMSI	Трассировка сигнализации абонента по IMSI без использова

		ния внешних инструментов, позволяющая декодировать сообщения и выявлять причины отказа в обслуживании.
	Supporting Interface traces (Gx, S11, S5/S8, S1)	Трассировка сигнализации на различных интерфейсах (S1, SGi, S11, Gx, S5/S8) для записи всех сообщений от смежных элементов.
	Full backup/restore	Полное резервное копирование и восстановление конфигурации и системных настроек SGW/PGW.
	HW/SW real-time usage monitoring	Мониторинг использования аппаратных и программных ресурсов в реальном

			времени (CPU, PDP, Throughput).
		Configuration restoration after SGW/PGW/GGSN restarts	Сохранение и восстановление последних изменений конфигурации после перезапуска узла SGW/PGW/GGSN.
		SPGW-C/UPF APP Layer Restart	Перезапуск уровня приложения SPGW-C/UPF с отправкой уведомления о перезапуске PGW.
		SPGW-C/UPF Host Layer restart	Перезапуск уровня хоста (виртуальной машины) SPGW-C/UPF с отправкой уведомления о перезапуске PGW.
		SPGW-C/UPF APP Layer shutdown	Отключение уровня приложения SPGW-C/UPF.

		SPGW-C/UPF Host Layer shutdown	Отключение уровня хоста (виртуальной машины) SPGW-C/UPF.
		Отказ одной из 2-х BGP сессий VRF Radius, VRF Diameter, перемаршрутизация трафика интерфейсов	Отказ одной из двух BGP-сессий для VRF Radius, VRF Diameter и перемаршрутизация трафика интерфейсов.
		Отказ S5/S8, Sgi портов, перемаршрутизация трафика	Отказ портов S5/S8, SGi и перемаршрутизация трафика.
		Проверка отключения и обратного включения оптики, в различных комбинациях	Проверка отключения и повторного включения оптических линков в различных комбинациях.
		Maximum throughput per UE (Supporting maximum QoS)	Проверка максимальной пропускной способности на одного абонента (до .6 Гбит/с для

		LTE Cat 19) с поддержкой максимального QoS.
	Maximum SGW/PGW throughput (10 Gbps)	Проверка максимальной пропускной способности SGW/PGW (до 40 Гбит/с трафика при стабильной работе).
	Maximum eNodeB connected to SGW (100 eNB with Ixia)	Проверка поддержки максимального количества подключенных eNodeB к SGW (100 eNodeB с эмуляцией Ixia).
	Maximum number UE bearers (50000 UE with Ixia)	Проверка поддержки максимального количества абонентских каналов (50000 UE с эмуляцией Ixia) без деградации сервиса.

3.2.2. **Основные функции SGW/PGW/GGSN**

Функции SGW/PGW/GGSN включают в себя поддержку маркировки трафика с использованием значений DSCP (Differentiated Services Code Point) на основе параметров QoS и QCI для сетей UMTS и LTE, что позволяет приоритизировать

различные типы трафика. Также поддерживается маркировка DSCP для плоскости управления, обеспечивая приоритизацию управляющих сообщений. Для UMTS реализована функция прямого туннеля, которая позволяет трафику абонентского оборудования (UE) напрямую идти от RNC к GGSN, минуя SGSN, что оптимизирует путь данных. Возможность настройки максимального размера сегмента TCP (TCP MSS) индивидуально для каждой точки доступа (APN) и поддержка маршрутизации Diameter-сообщений на основе имени хоста или области (Realm) на интерфейсах Gx и S6b обеспечивают гибкое взаимодействие с PCRF и AAA-серверами.

Наличие детализированных настроек, таких как индивидуальная конфигурация TCP MSS для каждого APN, а также продвинутая маршрутизация Diameter на основе хоста/области, указывает на стремление к максимальной гибкости и оптимизации сетевых ресурсов. Такие возможности позволяют оператору адаптировать сеть под специфические требования различных сервисов и абонентов, а также эффективно управлять сигнализацией в сложных сетевых топологиях. Например, тонкая настройка TCP MSS для разных APN напрямую влияет на производительность и эффективность использования полосы пропускания для различных типов трафика, включая интернет, IMS или IoT. Продвинутые механизмы маршрутизации Diameter обеспечивают высокую доступность и гибкость в распределении нагрузки для серверов политики и тарификации, которые критически важны для функционирования сети. Эти функции выходят за рамки базовой связности, демонстрируя стремление к повышению эффективности и внедрению более сложных сервисных моделей.

3.2.3. **Управление мобильностью**

Раздел управления мобильностью включает в себя различные сценарии обновления зоны отслеживания (TAU) и обновления зоны маршрутизации (RAU). Это охватывает процедуры TAU при перемещении абонента в пределах одной MME, но с изменением обслуживающего шлюза (S-GW) , а также при переходе абонента из сетей UMTS (режим Iu) и GSM/GPRS (режим Gb) в сеть LTE. Аналогично, поддерживаются процедуры RAU при переходе абонента из сети LTE в сети UMTS (режим Iu) и GSM/GPRS (режим Gb).

Широкий спектр тестов на TAU/RAU между различными технологиями доступа (2G/3G/4G) подчеркивает важность обеспечения непрерывной мобильности и бесшовного пользовательского опыта. TAU/RAU — это фундаментальные процедуры в мобильных сетях, которые обеспечивают, что сеть всегда знает местоположение абонента для доставки входящих вызовов/данных и поддержания сессии при его перемещении. Тестирование переходов между 2G, 3G и 4G показывает, что оператор стремится обеспечить бесшовную мобильность независимо от используемой технологии доступа. Для конечного пользователя это означает отсутствие обрывов связи или деградации сервиса при перемещении, например, из зоны 4G в зону 3G или 2G. Для оператора это критически важно для поддержания высокого уровня удовлетворенности абонентов, минимизации оттока и эффективного использования сетевых ресурсов в условиях смешанной инфраструктуры. Это также указывает на зрелость развертывания сети, где не только базовые функции 4G, но и взаимодействие с предыдущими поколениями тщательно проработаны.

3.2.4. **Разделение плоскостей управления и пользователя (CUPS)**

Внедрение CUPS (Control and User Plane Separation) позволяет независимо масштабировать плоскости управления и пользователя в узлах SGW и PGW. Тестирование включает выбор функции пользовательской плоскости (UPF) на основе точки доступа (APN) , на основе зоны местоположения, а также выбор UPF по умолчанию.

CUPS является ключевой архитектурной особенностью, введенной в 3GPP Release 14, которая позволяет разделить функции плоскости управления и плоскости пользователя. Это позволяет операторам разворачивать UPF ближе к краю сети (Edge Computing) для снижения задержки и повышения пропускной способности, а также независимо масштабировать каждую плоскость.

3.2.5. **Управление сессиями**

Управление сессиями охватывает широкий спектр функций, включая проверку обмена сообщениями Echo Request/Response по протоколам GTPv1 и GTPv2 на различных интерфейсах (S1-U, S11, S5/S8-C, S5/S8-U) для проверки доступности узлов. Поддерживаются активация и деактивация основного (Default) канала передачи данных , а также активация выделенного (Dedicated) канала, инициированная сетью (например, для VoLTE-вызова), с использованием нового QCI для обеспечения требуемого качества обслуживания. Также реализована поддержка модификации каналов передачи данных, например, изменение параметров QoS по инициативе HLR/HSS. Сеть поддерживает множественные подключения к сетям передачи данных (PDN) для одного абонента (например, для интернета и IMS одновременно) и доступ для абонентов из различных домашних PLMN (HPLMN), что критично для роуминга. Дополнительные функции включают ручную деактивацию контекста абонента со стороны SAEGW , поддержку процедур обновления и деактивации PDP-контекста со стороны GGSN , уведомления о перезапуске PGW , деактивацию неактивных PDP-контекстов по таймеру , управление арендой IP-адресов и удаление сессий из SGW после перезапуска MME для обеспечения согласованности состояния сети.

Управление сессиями является ядром функциональности EPC. Наличие тестов для активации выделенных каналов, инициированных сетью, и поддержки множественных PDN-подключений показывает, что сеть способна поддерживать сложные сценарии использования. Например, для VoLTE-вызовов требуются выделенные каналы с гарантированным качеством обслуживания, а возможность одновременного подключения к нескольким PDN позволяет абонентам использовать различные сервисы (например, интернет и IMS) параллельно.

3.2.6. **Поддержка контекстов PDN IPv4 и IPv6**

Функционал SGW/PGW включает полную поддержку активации PDN-контекстов с использованием адресов IPv4 , IPv6 , а также одновременное использование IPv4 и IPv6 (DualStack).

Полная поддержка IPv4, IPv6 и DualStack является обязательной для современных мобильных сетей. Это демонстрирует готовность сети к исчерпанию IPv4-адресов и обеспечивает совместимость с новыми сервисами, которые могут быть ориентированы

исключительно на IPv6. В то время как мир движется к IPv6 из-за исчерпания IPv4-адресов, большая часть существующего контента и инфраструктуры все еще использует IPv4. Поддержка всех трех вариантов является критически важной для оператора, так как позволяет обеспечить бесперебойный доступ к любому контенту и сервисам, независимо от используемого IP-протокола. Это гарантирует будущую совместимость и устойчивость сети к изменениям в глобальной IP-инфраструктуре.

3.2.7. **Управление адресами**

В части управления адресами поддерживается динамическое присвоение IP-адресов абонентам из локального пула адресов, настроенного на SAEGW (PGW-C/UPF).

Возможность динамического присвоения адресов из локального пула PGW-C/UPF указывает на гибкость в управлении IP-адресами и потенциальное снижение зависимости от внешних DHCP-серверов. Это может улучшить производительность и упростить развертывание в некоторых сценариях. Динамическое присвоение IP-адресов является стандартной функцией, но возможность делать это из локального пула на самом PGW/UPF (в отличие от централизованного DHCP-сервера) дает оператору больше контроля и может уменьшить задержки при установлении сессии. Это повышает автономность узла и может быть полезно для сценариев, где требуется быстрое выделение адресов или когда внешний DHCP-сервер недоступен/нежелателен.

3.2.8. **Управление Radius**

Управление Radius включает аутентификацию абонентов через Radius-сервер с использованием сообщений POD (Packet of Disconnect) и передачу учетной информации (Accounting) на Radius-сервер для целей тарификации и мониторинга. Важной функцией является поддержка отправки копий Radius Accounting-сообщений на дополнительный (Carbon-Copy) Radius-сервер, что обеспечивает резервирование и аудит данных. Также поддерживается отправка промежуточных Radius Accounting-сообщений по истечении заданного времени, что позволяет отслеживать потребление услуг в реальном времени. Кроме того, поддерживается передача на Radius-сервер различных параметров абонента и сессии, таких как часовой пояс, IMEISV, тип радиодоступа (RAT), IMSI, APN, IP-адреса шлюзов и информация о местоположении абонента.

Детализированная поддержка Radius (аутентификация, учет, промежуточный учет, передача расширенных атрибутов, копирование сообщений) демонстрирует зрелость биллинговой и учетной системы. Отправка копий учетных данных на дополнительный сервер является важной функцией для обеспечения надежности и целостности данных тарификации, а также для целей аудита и резервирования. В контексте биллинга и учета данных, потеря или повреждение информации может привести к значительным финансовым потерям или проблемам с регулирующими органами. Отправка копий на второй сервер обеспечивает избыточность и отказоустойчивость системы учета. Это также может быть использовано для целей аудита, аналитики или для интеграции с различными биллинговыми системами, что демонстрирует высокий уровень внимания к надежности и точности финансовых операций.

3.2.9. **Офлайн-тарификация**

Функции офлайн-тарификации включают генерацию CDR (Call Detail Record) на SGW/PGW/GGSN на основе времени, с настраиваемым интервалом , и на основе объема переданных данных, с настраиваемым порогом. Также поддерживается генерация CDR при изменении типа радиодоступа (RAT), SGSN/S-GW, часового пояса, достижении максимальных условий или при смене PLMN.

Разнообразие триггеров для генерации CDR (по времени, по объему, по изменению RAT/PLMN) позволяет оператору реализовать сложные и гибкие тарифные планы, а также обеспечивает точный учет использования ресурсов в динамичной сетевой среде. CDR — это записи о каждой сессии или событии, которые используются для биллинга. Чем больше параметров может быть использовано для генерации CDR, тем более детальными и точными будут биллинговые данные. Наличие таких разнообразных триггеров позволяет оператору создавать очень гибкие и детализированные тарифные планы, например, "безлимит" на определенный объем трафика, или тарификацию, зависящую от типа сети (2G/3G/4G) или даже от местоположения. Это дает оператору мощный инструмент для монетизации услуг и адаптации к рыночным требованиям.

3.2.10. **Управление сессиями Gx PCC**

Управление сессиями Gx PCC включает установление сессии IP-CAN (IP Connectivity Access Network) с PCRF (Policy and Charging Rules Function), позволяющее PCRF доставлять динамические или предопределенные правила. Поддерживается установка правил PCC (Policy and Charging Control), доставляемых PCRF , и их повторная авторизация. Также реализована поддержка локальных правил PCC для каждой APN, с возможностью перехода на локальные правила в случае сбоя интерфейса Gx. Инициирование сообщений CCR (Credit Control Request) к PCRF происходит при изменении QoS , типа радиодоступа (RAT) и информации о местоположении абонента (ULI) , а также по истечении тайм-аута повторной валидации. Поддерживается перевыбор PCRF на основе AVP Origin-Host и обновление QoS, инициированное PCRF. Проверяется поведение кодов результатов Gx и отказоустойчивость интерфейса Gx как при прямом подключении к PCRF, так и при использовании Diameter Routing Agent (DRA).

Глубокая интеграция с PCRF через интерфейс Gx и поддержка множества триггеров для CCR-сообщений (изменения QoS, RAT, ULI) демонстрирует высокий уровень динамического управления политиками и тарификацией. PGW не просто применяет статические правила, а активно информирует PCRF о значимых изменениях в состоянии абонента или сессии. В ответ PCRF может динамически изменять правила PCC для этого абонента. Например, если абонент перемещается в зону с плохим покрытием (изменение RAT) или меняет свое местоположение (изменение ULI), или его QoS-требования изменяются, сеть может автоматически скорректировать его тарифный план или приоритет трафика. Это позволяет оператору в реальном времени адаптировать правила обслуживания абонентов в зависимости от их поведения, местоположения и используемых сервисов, что является краеугольным камнем для персонализированных предложений и эффективного управления трафиком. Это также позволяет оператору реализовать очень сложные и адаптивные политики, например, предлагать скидки на трафик в определенных местах, или автоматически снижать

скорость для абонентов, превысивших лимит, или приоритизировать трафик экстренных служб.

3.2.11. **Голосовые услуги**

В части голосовых услуг поддерживается успешное выполнение исходящих (MO) и входящих (MT) VoLTE-вызовов с активацией выделенного канала передачи данных , а также экстренных вызовов VoLTE. Важной функцией является поддержка восстановления IMS-сервисов в случае сбоя P-CSCF. Также реализована поддержка вызовов VoWiFi через интерфейс S2b, интегрированных с ePDG Huawei.

Наличие процедур для VoLTE, экстренных вызовов VoLTE и особенно "IMS Restoration for P-CSCF Failure" демонстрирует серьезный подход к обеспечению надежности и доступности голосовых услуг по IP. P-CSCF (Proxy-CSCF) является первой точкой контакта для UE в сети IMS и играет ключевую роль в установлении и управлении VoLTE-вызовами. Его отказ может привести к полной недоступности голосовых услуг. Функционал восстановления IMS при сбое P-CSCF показывает, что оператор уделяет первостепенное внимание надежности голосовой связи. Это означает, что даже при частичных сбоях в сети IMS, система способна перенаправить абонентов на доступные P-CSCF, минимизируя прерывания вызовов. Это критически важно для поддержания качества обслуживания и удовлетворенности абонентов, так как голосовая связь по-прежнему воспринимается как основной и наиболее важный сервис.

3.2.12. **Виртуальные APN**

Функционал виртуальных APN включает маппинг APN (например, isp.com) на виртуальный APN (isp2.com) на основе кода зоны отслеживания (TAC) , на основе диапазона IMSI и на основе кода зоны местоположения (LAC). Также поддерживается балансировка нагрузки между APN и перезапись информации APN для CDR, AAA и Gx.

Возможности "Virtual APN" с маппингом на основе TAC, IMSI Range, LAC и "APN load balancing" указывают на продвинутые возможности сегментации сети и управления трафиком. Виртуальные APN позволяют оператору использовать один и тот же физический APN, но логически разделять трафик или применять разные политики в зависимости от таких параметров, как местоположение абонента (TAC/LAC) или его идентификатор (IMSI Range). Это мощный инструмент для сетевой сегментации. Например, оператор может предлагать специальные тарифы или сервисы для абонентов в определенных географических зонах или для корпоративных клиентов, не разворачивая при этом отдельные физические APN. Это также является предвестником концепций сетевого среза (Network Slicing) в 5G, позволяя создавать виртуальные сети для разных вертикалей бизнеса. Балансировка нагрузки дополнительно обеспечивает оптимальное использование ресурсов.

3.2.13. **Управление безопасностью**

В области управления безопасностью поддерживается изоляция плоскости управления, предотвращающая несанкционированный доступ к интерфейсам OAM (Operation, Administration, Maintenance) с пользовательской стороны , а также изоляция плоскости

данных, предотвращающая несанкционированный доступ к IP-адресам абонентов с сетевых интерфейсов, не предназначенных для передачи данных. Также реализован контроль доступа (ACL) для фильтрации трафика внутри одной APN, между различными APN и к внешним IP-адресам.

Разделение и изоляция плоскостей (управления и данных) и детальный контроль доступа через ACL являются фундаментальными принципами безопасности в телекоммуникационных сетях. Изоляция плоскостей предотвращает использование пользовательского трафика для атак на управляющие интерфейсы. ACLs позволяют создавать гранулярные правила для фильтрации трафика, предотвращая несанкционированную связь между различными сегментами сети или с внешними ресурсами. Это не просто соответствие стандартам, а активная защита от угроз, что критически важно для доверия абонентов и предотвращения дорогостоящих инцидентов.

3.2.14. **Управление NTP**

В части управления NTP поддерживается синхронизация системного времени SAEGW с внешним NTP-сервером. Синхронизация времени по NTP является базовой, но критически важной функцией для корректной работы сетевого оборудования, логирования событий и тарификации.

3.2.15. **Сеть**

Сетевые функции включают настройку максимального блока передачи (MTU) на сетевых портах и поддержку интерфейсов с тегированием VLAN (подинтерфейсов). Важной функцией является привязка APN к VRF (Virtual Routing and Forwarding), обеспечивающая логическую изоляцию маршрутизации для разных APN.

Привязка APN к VRF является мощным инструментом для сетевой сегментации и обеспечения безопасности. VRF — это технология, которая позволяет иметь несколько независимых таблиц маршрутизации на одном маршрутизаторе, каждая из которых действует как отдельный виртуальный маршрутизатор. Привязка APN к VRF означает, что трафик, поступающий через определенный APN, будет маршрутизироваться в своей собственной, изолированной таблице маршрутизации. Это обеспечивает логическую изоляцию между различными APN, что критически важно для безопасности (трафик одного APN не может "видеть" трафик другого) и для поддержки различных сервисов с уникальными требованиями к маршрутизации (например, корпоративные VPN, IoT-платформы).

3.2.16. **Маршрутизация**

Функции маршрутизации включают поддержку динамической маршрутизации BGP (Border Gateway Protocol) для IPv4 и IPv6. Также поддерживается протокол BFD (Bidirectional Forwarding Detection) для IPv4/IPv6, обеспечивающий быстрое обнаружение сбоев в пути передачи данных. Дополнительно поддерживается перенаправление трафика через интерфейс Gi.

Поддержка BFD для IPv4/IPv6 в сочетании с динамической маршрутизацией BGP указывает на высокий уровень отказоустойчивости и оптимизации маршрутизации. BGP — это протокол динамической маршрутизации, используемый для обмена информацией о маршрутах между автономными системами. BFD — это протокол, предназначенный для очень быстрого обнаружения сбоев в пути передачи данных между двумя соседними устройствами. Использование BFD совместно с BGP значительно повышает надежность сети. Если BFD обнаруживает сбой канала, он немедленно уведомляет BGP, который затем может очень быстро перемаршрутизировать трафик по альтернативному пути. Это минимизирует время простоя и потерю пакетов, что критически важно для поддержания высокого качества обслуживания, особенно для чувствительного к задержкам трафика (например, голоса).

3.2.17. **Эксплуатация и обслуживание**

Раздел эксплуатации и обслуживания включает управление производительностью (графики THP, PDP) , управление сбоями и аварийными сигналами , управление журналом операций, регистрирующим активность пользователей , управление безопасностью пользователей и групп , а также управление разрешениями операторов. Важными функциями являются трассировка сигнализации абонента по IMSI без использования внешних инструментов и трассировка сигнализации на различных интерфейсах (Gx, S11, S5/S8, S1). Также поддерживается полное резервное копирование и восстановление конфигурации и мониторинг использования аппаратных и программных ресурсов в реальном времени.

Наличие функций трассировки пользователя по IMSI и поддержки трассировки интерфейсов без использования внешних инструментов является очень мощным встроенным диагностическим инструментом. Это значительно ускоряет процесс локализации и устранения неисправностей, поскольку позволяет операторам глубоко анализировать поведение сигнализации и трафика непосредственно на сетевом элементе. В традиционных сетях для глубокого анализа трафика часто требуются внешние анализаторы. Встроенная трассировка означает, что функционал анализа уже интегрирован в само оборудование/ПО. Это значительно упрощает и ускоряет процесс диагностики. Инженеры могут запускать трассировку непосредственно с консоли или GUI сетевого элемента, получать декодированные сообщения и сохранять их для последующего анализа. Это сокращает время на локализацию проблем, особенно в сложных распределенных vEPC-средах, и позволяет оперативно реагировать на инциденты, что напрямую влияет на качество обслуживания и операционные расходы.

3.2.18. **Надежность**

Тесты надежности включают сохранение и восстановление последних изменений конфигурации после перезапуска узла SGW/PGW/GGSN. Особое внимание уделяется перезапускам и отключениям уровней приложения (APP Layer) и хоста (Host Layer) SPGW-C/UPF, с отправкой уведомлений о перезапуске PGW. Также проверяется отказоустойчивость при отказе одной из двух BGP-сессий VRF Radius, VRF Diameter и перемаршрутизация трафика интерфейсов , отказ портов S5/S8, SGi и перемаршрутизация трафика , а также проверка отключения и повторного включения оптических линков в различных комбинациях.

Детализированные тесты надежности, включающие сбои на уровне приложения и хоста, а также сбои BGP-сессий и оптических линков, демонстрируют глубокую проработку отказоустойчивости системы. Это критически важно для vEPC, где виртуализация может привнести новые точки отказа. В виртуализированной среде отказы могут быть более сложными и непредсказуемыми из-за взаимодействия между различными слоями. Тщательное тестирование этих сценариев является обязательным для обеспечения того, чтобы преимущества NFV не были нивелированы проблемами надежности.

3.2.19. **Тесты высокой нагрузки**

Тесты высокой нагрузки охватывают проверку максимальной пропускной способности на одного абонента (до .6 Гбит/с для LTE Cat 19) с поддержкой максимального QoS. Также проверяется максимальная пропускная способность SGW/PGW (до 40 Гбит/с трафика при стабильной работе), поддержка максимального количества подключенных eNodeB к SGW (100 eNodeB с эмуляцией Ixia) и поддержка максимального количества абонентских каналов (50000 UE с эмуляцией Ixia) без деградации сервиса.

Тесты высокой нагрузки с использованием Ixia и проверка максимальной пропускной способности на UE демонстрируют валидации производительности vEPC в реальных условиях эксплуатации. Ixia — это ведущий производитель тестового оборудования, используемого для эмуляции масштабного сетевого трафика и абонентов. Использование Ixia указывает на профессиональный и комплексный подход к тестированию производительности. Эти тесты не просто проверяют, работает ли функция, а проверяют, как она работает под экстремальной нагрузкой. Способность SGW/PGW обрабатывать 40 Гбит/с трафика и поддерживать 50 000 абонентов одновременно является показателем высокой производительности и масштабируемости решения. Это критически важно для оператора, который должен гарантировать качество обслуживания для миллионов абонентов и быть готовым к росту трафика и подключений.

3.3. 3. Функциональные возможности и процедуры MME

MME (Mobility Management Entity) является основным узлом плоскости управления в сети LTE, отвечающим за управление мобильностью абонентов, аутентификацию, авторизацию, выбор SGW/PGW, а также за обработку сигнализации. SGSN (Serving GPRS Support Node) выполняет схожие функции в сетях 2G/3G. MME играет ключевую роль в обеспечении регистрации абонентов, хэндоверов и установления сессий.

В следующей таблице представлены описания ключевых функций MME, извлеченные из предоставленных материалов. Эта таблица является прямым ответом на запрос пользователя, систематизируя и описывая ключевые функции MME. Она служит ценным справочным материалом для технических специалистов, работающих с ядром сети, и способствует более глубокому пониманию возможностей MME в контексте vEPC.

3.3.1. **Таблица 2: Описание функций MME**

TestCaseID	Original Description	Русское описание функции (для столбца E)
1	Support S6a Diameter connection over DRA/Proxy (SCTP) with redundancy	Поддержка соединения Diameter по интерфейсу S6a через DRA (Diameter Routing Agent) или Proxy с резервированием, обеспечивая отказоустойчивость при взаимодействии с HSS.
2	Support for the SGs interface	Поддержка интерфейса SGs для взаимодействия MME с VLR (Visitor Location Register) для обеспечения услуг Circuit Switched Fallback (CSFB) и SMS.
3	Support MME Pool with load balancing	Поддержка пула MME с балансировкой нагрузки для распределения абонентов между несколькими MME.
4	Support MME Pool offload	Поддержка выгрузки абонентов из пула MME на основе NRI

			(Network Resource Identifier) или NE (Network Element), что позволяет перераспределять нагрузку.
5		APN Correction for Inconsistent Subscribe APN and Request APN	Коррекция APN в случае несоответствия между APN, на который подписан абонент, и APN, запрошенным UE.
6		SGW / PGW Topology Selection Support	Поддержка выбора топологии SGW/PGW, включая обработку DNS-ответов для выбора SGW-PGW в том же центре обработки данных.
7		QoS overwritten function support	Поддержка функции перезаписи QoS, позволяющая MME использовать локальные (возможно, худшие) правила QoS.
8		Support extended QCIs (65,165, 69,169)	Поддержка расширенных QCI (QoS Class Identifiers), что позволяет более гибко управлять качеством обслуживания для различных типов трафика.
9		Support DSCP	Поддержка маркировки DSCP

		marking signaling and OAM	для сигнализации и трафика OAM.
10		Support multi TimeZone	Поддержка нескольких часовых поясов для разных TAC (Tracking Area Code).
11		Support local cache DNS	Поддержка локального кэша DNS, что позволяет устанавливать сессии без обращения к внешнему DNS-серверу.
12		Support roaming for LTE, UMTS	Поддержка роуминга для сетей LTE и UMTS.
13		Support APN correction (OI/NI, fail, wildcard, first in subscription)	Поддержка коррекции APN (OI/NI APN correction по префиксу IMSI, wildcard, первый в подписке).
16		Support saving Auth-vectors	Поддержка сохранения векторов аутентификации, что позволяет пропускать процедуру аутентификации при повторном подключении.

2..	Attach procedure using the IMSI	Процедура подключения (Attach) с использованием IMSI.
2..2	Attach procedure using the GUTI	Процедура подключения (Attach) с использованием GUTI.
2..3	Attach UE without CS-domain	Подключение UE без поддержки CS-домена (EPC-only).
2..4	UE Initiating a Combined Attach Procedure	Инициирование абонентом комбинированной процедуры подключения (Attach) к PS и CS доменам.
2..5	UE initiating a Detach Procedure	Инициирование абонентом процедуры отключения (Detach).
2..6	MME initiating a Detach Procedure	Инициирование MME процедуры отключения (Detach).
2..7	UE initiating a periodic TAU Procedure	Инициирование абонентом периодической процедуры TAU.

2..8	UE Initiating a normal TAU Procedure	Инициирование абонентом обычной процедуры TAU.
2..9	UE Initiating a Service Request	Инициирование абонентом запроса на обслуживание (Service Request).
2..10	S1 Interface Resource Release from eNodeB	Освобождение ресурсов интерфейса S1 со стороны eNodeB.
2.2.	Default Bearer Activation During an Attach Procedure	Активация основного канала (Default Bearer) во время процедуры подключения.
2.2.2	HSS-initiated Bearer Modification	Модификация канала, инициированная HSS (Home Subscriber Server).
2.2.3	MME-initiated Bearer Deactivation	Деактивация канала, инициированная MME.
2.2	Bearer Activation with a subscribed Static	Активация канала с использованием статического IP-

. 4	IP Address	адреса, на который подписан абонент.
2 . 2 . 5	Supporting Multiple PDNs	Поддержка множественных PDN-соединений.
2 . 2 . 6	Network-initiated GBR Dedicated Bearer Activation	Активация выделенного GBR (Guaranteed Bit Rate) канала, инициированная сетью (например, для VoLTE).
2 . 2 . 7	Network-initiated Non-GBR Dedicated Bearer Activation	Активация выделенного Non-GBR канала, инициированная сетью (например, для Speedtest).
2 . 2 . 8	UE-initiated PDN Connection	Инициирование абонентом подключения к PDN.
2 . 3 .	S1 Interface with Nokia eNodeB	Проверка интерфейса S1 с eNodeB от Nokia.
2 . 3 . 2	S1 Interface with Huawei eNodeB	Проверка интерфейса S1 с eNodeB от Huawei.

2.4.	Authentication procedure in Attach	Процедура аутентификации при подключении (Attach) с проверкой правильного/неправильного алгоритма Milenage.
2.4.2	Subscriber Identity Confidentiality, Reassigning GUTIs	Конфиденциальность идентификатора абонента и переназначение GUTI.
2.4.3	Security Mode Command procedure in Attach	Процедура Security Mode Command при подключении.
2.4.4	Identity Authentication	Аутентификация идентификатора.
2.5.	Support for Intra-MME S1-based handover	Поддержка хэндовера на основе S1 внутри одной MME.
2.5.2	Support X2-based handover	Поддержка хэндовера на основе X2.

2.5.3	Support for Inter-MME S1-based handover	Поддержка хэндовера на основе S1 между разными MME.
2.6.	Supporting Transmission of IMEI Information to the S-GW	Поддержка передачи информации IMEI (International Mobile Equipment Identity) на S-GW.
2.7.	Attach and activation UE with different HPLMN	Подключение и активация UE с разными домашними PLMN (HPLMN).
2.7.2	MME supporting network share MOCN	Поддержка MME совместного использования сети по модели MOCN (Multi-Operator Core Network).
2.8.	Access Control Based on Subscribed ARD	Контроль доступа на основе ARD (Access Restriction Data), настроенного на HSS.
2.8.2	Packet Service Barring (ODB)	Блокировка пакетных услуг (ODB - Operator Determined Barring).

2.8.3	Access Control Based on the Regional Configuration	Контроль доступа на основе региональной конфигурации (локальные правила доступа по TAC).
2.9.	CSFB MT Call Initiated by the UE in the ECM-CONNECTED State	Входящий CSFB-вызов, инициированный UE в состоянии ECM-CONNECTED.
2.9.2	CSFB MT Call Initiated by the UE in the ECM-IDLE State	Входящий CSFB-вызов, инициированный UE в состоянии ECM-IDLE.
2.9.3	CSFB MO Calls in Active Mode – the Target Access Network Is UTRAN	Исходящий CSFB-вызов в активном режиме, целевая сеть UTRAN.
2.9.4	CSFB MO Calls in Active Mode – the Target Access Network Is GERAN	Исходящий CSFB-вызов в активном режиме, целевая сеть GERAN.

2.9.5	VoLTE MO call	Исходящий VoLTE-вызов.
2.9.6	VoLTE MT call	Входящий VoLTE-вызов.
2.9.7	VoLTE Emergency call	Экстренный VoLTE-вызов.
2.9.8	VoLTE extension for SRVCC support	Расширение VoLTE для поддержки SRVCC (Single Radio Voice Call Continuity).
2.9.9	Restriction VoLTE based on location/TAC	Ограничение VoLTE на основе местоположения/TAC.
2.9.10	Restriction VoLTE for roamers	Ограничение VoLTE для роумеров.
3..	PDP/PDN-context support: IPv4	Поддержка контекстов PDP/PDN для IPv4.

3..2	PDP/PDN-context support: IPv6	Поддержка контекстов PDP/PDN для IPv6.
3..3	DualStack PDP/PDN-context support: IPv4/IPv6	Поддержка контекстов PDP/PDN для DualStack (IPv4/IPv6).
3.2.	NTP syncronization	Синхронизация системного времени MME с внешним NTP-сервером.
3.3.	MTU Configuration	Настройка MTU на сетевых портах.
3.3.3	Support VRF for logical interfaces	Поддержка VRF для логических интерфейсов, позволяющая привязывать APN к VRF для изоляции маршрутизации.
3.3.4	BFD protocol support for IPv4/IPv6	Поддержка протокола BFD для IPv4/IPv6.
3.4.	BGP Dynamic routing	Поддержка динамической маршрутизации BGP на MME.

4.	Configuration restoration after MME restarts	Сохранение и восстановление конфигурации после перезапуска MME.
4.2	MME APP Layer Restart	Перезапуск уровня приложения MME без прерывания сессий UE.
4.3	MME Host Layer Restart	Перезапуск уровня хоста (виртуальной машины) MME.
4.4	MME APP Layer shutdown	Отключение уровня приложения MME, при этом другие сервисы не прерываются, а сервисы с отказавшего хоста мигрируют.
4.5	MME Host Layer shutdown	Отключение уровня хоста (виртуальной машины) MME, после перезапуска сервисы VNF работают нормально.
5.	Performance management (MM, SM)	Управление производительностью, включая сбор статистики по различным счетчикам MM и SM.
5.2	Fault, alarm management	Управление сбоями и аварийными сигналами, включая корректную генерацию

			сообщений в системе мониторинга.
5.3	Operation log (user activity logging) management		Управление журналом операций, регистрирующим активность пользователей (логины, команды, перезагрузки).
5.4	Support RBAC VNF user managment		Поддержка управления пользователями VNF на основе RBAC (Role-Based Access Control), позволяющая ограничивать выполнение команд для определенных групп/операторов.
5.5	User tracing based on IMSI		Трассировка сигнализации абонента по IMSI без использования внешних инструментов, позволяющая декодировать сообщения и выявлять причины отказа в обслуживании.
5.6	Supporting Interface traces (S1, S6a, S11)		Трассировка сигнализации на различных интерфейсах (S1, S6a, S11) для записи всех сообщений от смежных элементов.

5.7	Full backup/ restore	Полное резервное копирование и восстановление конфигурации и системных настроек MME.
5.8	Web/GUI, CLI management interfaces with security	Поддержка защищенных интерфейсов управления Web/GUI и CLI (SSH, HTTPS).
5.9	HW/SW real-time usage monitoring (Web/GUI)	Мониторинг использования аппаратных и программных ресурсов в реальном времени (CPU, PDP, Throughput) через Web/GUI.
6.	Maximum throughput per UE (Supporting maximum QoS)	Проверка максимальной пропускной способности на одного абонента (до .6 Гбит/с для LTE Cat 19) с поддержкой максимального QoS.
6.2	Maximum eNodeB connected to MME (100 eNB with Ixia)	Проверка поддержки максимального количества подключенных eNodeB к MME (100 eNodeB с эмуляцией Ixia).

6.3	Maximum attached 4G subscribers (50000 UE with Ixia)	Проверка поддержки максимального количества подключенных 4G абонентов (50000 UE с эмуляцией Ixia) без деградации сервиса.

3.3.2. **Основные функции MME/SGSN**

Основные функции MME/SGSN включают поддержку соединения Diameter по интерфейсу S6a через DRA (Diameter Routing Agent) или Proxy с резервированием, обеспечивая отказоустойчивость при взаимодействии с HSS. Также поддерживается интерфейс SGs для взаимодействия MME с VLR (Visitor Location Register). Важной функцией является поддержка пула MME с балансировкой нагрузки для распределения абонентов между несколькими MME и выгрузки абонентов из пула MME на основе NRI или NE. MME также выполняет коррекцию APN в случае несоответствия между APN подписки и запрошенным APN , поддерживает выбор топологии SGW/PGW , функцию перезаписи QoS , расширенные QCI , маркировку DSCP для сигнализации и OAM, поддержку нескольких часовых поясов, локальный кэш DNS, роуминг для LTE и UMTS, а также различные методы коррекции APN. Дополнительно поддерживается сохранение векторов аутентификации для пропуска процедуры аутентификации при повторном подключении.

Наличие "MME Pool with load balancing" и "MME Pool offload" демонстрирует способность сети к горизонтальному масштабированию и эффективному управлению ресурсами MME. MME Pool — это группа MME, которые совместно обслуживают одну или несколько Tracking Areas. Это обеспечивает отказоустойчивость (если одна MME выходит из строя, другие MME в пуле могут взять на себя ее нагрузку) и балансировку нагрузки. Функции балансировки нагрузки и выгрузки абонентов позволяют оператору эффективно распределять нагрузку между MME, предотвращая перегрузки и обеспечивая оптимальное использование ресурсов. Это также повышает общую надежность сети, поскольку позволяет гибко управлять отказами и обслуживанием MME без прерывания обслуживания абонентов.

3.3.3. **Базовый доступ 4G**

3.2.. Управление мобильностью

Управление мобильностью включает полный набор процедур: подключение (Attach) с использованием IMSI и GUTI , подключение UE без поддержки CS-домена (EPC-only) , инициирование абонентом комбинированной процедуры подключения к PS и CS доменам. Также поддерживаются инициирование абонентом и MME процедур отключения (Detach). Проверяются инициирование абонентом периодической и обычной процедур TAU, инициирование абонентом запроса на обслуживание (Service Request), а также освобождение ресурсов интерфейса S1 со стороны eNodeB. Полный набор тестов для процедур Attach, Detach, TAU и Service Request является базовым для

функционирования любой мобильной сети. Эти тесты подтверждают корректную работу основных механизмов управления мобильностью и сигнализацией.

3.2.2. Управление сессиями

Управление сессиями включает активацию основного канала (Default Bearer) во время процедуры подключения , модификацию канала, инициированную HSS , и деактивацию канала, инициированную MME. Поддерживается активация канала с использованием статического IP-адреса , множественные PDN-соединения , активация выделенных GBR и Non-GBR каналов, инициированная сетью (например, для VoLTE или Speedtest), а также инициирование абонентом подключения к PDN.

Поддержка активации выделенных GBR и Non-GBR каналов, инициированных сетью, со стороны MME, в дополнение к аналогичным тестам на SGW/PGW, подчеркивает сквозную поддержку QoS и дифференцированного обслуживания. MME является узлом плоскости управления, который инициирует и координирует создание, модификацию и удаление каналов. SGW/PGW реализуют эти каналы на плоскости пользователя. Наличие этих процедур на обоих узлах подтверждает, что вся цепочка сигнализации и данных, от инициации до применения, поддерживает дифференцированное качество обслуживания. Это критически важно для таких сервисов, как VoLTE, где гарантированная пропускная способность и низкая задержка являются обязательными.

3.2.3. Взаимодействие с eNodeB

Взаимодействие с eNodeB включает проверку интерфейса S1 с eNodeB от Nokia и Huawei.

Тестирование интерфейса S1 с eNodeB от разных вендоров (Nokia, Huawei) указывает на приверженность к мульти-вендорной стратегии. В крупных телекоммуникационных сетях часто используется оборудование от нескольких поставщиков. Это позволяет оператору избежать зависимости от одного поставщика, договариваться о лучших ценах и выбирать лучшие в своем классе решения для различных частей сети. Успешное тестирование совместимости с оборудованием разных вендоров критически важно для обеспечения бесперебойной работы сети в условиях мульти-вендорного развертывания. Это демонстрирует стратегическую гибкость в построении своей инфраструктуры.

3.2.4. Управление безопасностью

Управление безопасностью включает детальное тестирование процедур аутентификации при подключении (Attach) с проверкой правильного/неправильного алгоритма Milenage , конфиденциальности идентификатора абонента и переназначения GUTI , процедуры Security Mode Command при подключении , а также аутентификации идентификатора. Детальное тестирование этих процедур является базовой, но критически важной мерой для защиты абонентов и сети от несанкционированного доступа и мошенничества.

3.2.5. Хэндовер

Поддерживаются различные типы хэндоверов: на основе S1 внутри одной MME , на основе X2 и на основе S1 между разными MME.

Поддержка различных типов хэндоверов является ключевым для обеспечения бесшовной мобильности и непрерывности сервисов при перемещении абонента. X2-based handover, в частности, является более эффективным, так как происходит напрямую между eNodeB, минимизируя задержку и нагрузку на MME. S1-based handovers (как внутри, так и между MME) более ресурсоемки для MME, но необходимы, когда X2-соединение отсутствует или не может быть использовано. Поддержка всех этих типов хэндоверов гарантирует, что абонент будет испытывать минимальные прерывания или деградацию сервиса при перемещении в сети. Это напрямую влияет на удовлетворенность абонентов и является показателем хорошо спроектированной и оптимизированной сети.

3.2.6. Поддержка информации IMEI

Поддерживается передача информации IMEI (International Mobile Equipment Identity) на S-GW. Передача IMEI на S-GW важна для целей автопровиженинга VoLTE, безопасности (например, блокировка украденных устройств) и аналитики.

3.2.7. Совместное использование сети

Функции совместного использования сети включают подключение и активацию UE с разными домашними PLMN (HPLMN) и поддержку MME совместного использования сети по модели MOCN (Multi-Operator Core Network).

Поддержка "Network Sharing MOCN" является важной функцией для операторов, которые совместно используют инфраструктуру (например, радиосеть) для снижения затрат. MOCN — это модель совместного использования сети, при которой несколько операторов используют одну и ту же радиосеть (eNodeB), но каждый имеет свою собственную сеть ядра (MME, SGW, PGW). Это позволяет операторам снизить капитальные и операционные затраты, особенно при развертывании в новых или малонаселенных районах. Поддержка MOCN со стороны MME означает, что Megafon готов к сотрудничеству с другими операторами или уже участвует в таких схемах. Это демонстрирует гибкость архитектуры сети и способность адаптироваться к различным бизнес-моделям и регуляторным требованиям.

3.2.8. Контроль доступа

Контроль доступа включает механизмы на основе ARD (Access Restriction Data), настроенного на HSS , блокировку пакетных услуг (ODB - Operator Determined Barring) , а также контроль доступа на основе региональной конфигурации (локальные правила доступа по TAC).

Разнообразие механизмов контроля доступа предоставляет оператору мощные инструменты для управления доступом абонентов к услугам, что критически важно для реализации тарифных планов, роуминговых ограничений и соблюдения законодательства. ARD и ODB позволяют оператору управлять доступом к услугам на уровне подписки абонента (например, запретить роуминг данных). Региональный контроль доступа позволяет применять правила в зависимости от географического местоположения абонента (например, запретить доступ к определенным сервисам в конкретных областях). Эти функции дают оператору очень гибкий контроль над тем, какие абоненты могут получить доступ к каким услугам и в каких условиях. Это важно для реализации сложных тарифных планов, управления роумингом, обеспечения соответствия регуляторным требованиям и даже для борьбы с мошенничеством.

3.2.9. Голосовые услуги

Голосовые услуги включают комплексное тестирование как Circuit Switched Fallback (CSFB), так и Voice over LTE (VoLTE). Это охватывает входящие CSFB-вызовы, инициированные UE в состояниях ECM-CONNECTED и ECM-IDLE , а также исходящие CSFB-вызовы в активном режиме с целевыми сетями UTRAN и GERAN. Для VoLTE поддерживаются исходящие и входящие вызовы, экстренные вызовы VoLTE и расширение VoLTE для поддержки SRVCC (Single Radio Voice Call Continuity). Также предусмотрены ограничения VoLTE на основе местоположения/TAC и для роумеров.

Комплексное тестирование как CSFB, так и VoLTE, а также поддержка SRVCC и ограничений для роумеров/по местоположению, демонстрирует всестороннюю стратегию Megafon по предоставлению голосовых услуг. CSFB — это механизм, позволяющий абонентам LTE совершать и принимать голосовые вызовы через 2G/3G сети, когда VoLTE недоступен или не используется. VoLTE — это голосовая связь по IP, использующая LTE-сеть. SRVCC — это механизм для бесшовного хэндовера VoLTE-вызова с LTE на 2G/3G. Поддержка CSFB важна для абонентов, не использующих VoLTE, или в зонах, где VoLTE еще не развернут. SRVCC обеспечивает непрерывность VoLTE-вызовов при перемещении в зоны 2G/3G. Дополнительные ограничения для роумеров или по местоположению показывают, что оператор может управлять доступом к VoLTE на основе бизнес-логики или регуляторных требований.

3.3.4. **Сеть**

3.3.. Поддержка контекстов PDP/PDN IPv4 и IPv6

Аналогично SGW/PGW, MME поддерживает контексты PDP/PDN для IPv4 , IPv6 и DualStack (IPv4/IPv6). Полная поддержка IPv4, IPv6 и DualStack на MME является обязательной для современных мобильных сетей и обеспечивает совместимость с будущими IP-сервисами.

3.3.2. Управление NTP

MME поддерживает синхронизацию системного времени с внешним NTP-сервером. Аналогично SGW/PGW, синхронизация времени по NTP на MME критически важна для корректной работы сигнализации и логирования.

3.3.3. Сеть

Сетевые функции MME включают настройку MTU на сетевых портах , поддержку VRF для логических интерфейсов, позволяющую привязывать APN к VRF для изоляции маршрутизации , а также поддержку протокола BFD для IPv4/IPv6.

Аналогично SGW/PGW, привязка APN к VRF обеспечивает логическую изоляцию между различными APN, что критически важно для безопасности и для поддержки различных сервисов с уникальными требованиями к маршрутизации. Поддержка BFD совместно с BGP значительно повышает надежность сети, позволяя быстро обнаруживать сбои и перемаршрутизировать трафик, минимизируя время простоя и потерю пакетов. Это подтверждает, что эти критически важные сетевые функции реализованы сквозным образом в различных элементах ядра сети.

MME поддерживает динамическую маршрутизацию BGP. Поддержка BGP на MME обеспечивает гибкость и отказоустойчивость в маршрутизации сигнализационного трафика MME.

3.3.5. **Надежность**

Процедуры надежности MME включают сохранение и восстановление конфигурации после перезапуска MME. Особое внимание уделяется перезапускам и отключениям уровня приложения (APP Layer) MME и уровня хоста (Host Layer) MME. Ожидаемые результаты этих тестов включают "no interruption of UE session" и "Other services not interrupted, services from faulty host migrate to other".

Эти процедуры демонстрируют высокую степень отказоустойчивости и зрелость виртуализированной инфраструктуры. Способность MME поддерживать непрерывность сессий абонентов даже при перезапусках или отключениях на уровне приложения или хоста является ключевым показателем надежности vEPC. Это означает, что даже при частичных сбоях в виртуализированной среде, система способна обеспечить непрерывность обслуживания абонентов, что критически важно для поддержания качества связи и удовлетворенности клиентов.

3.3.6. **Эксплуатация и обслуживание**

Раздел эксплуатации и обслуживания MME охватывает управление производительностью (сбор статистики MM и SM) , управление сбоями и аварийными сигналами , управление журналом операций , поддержку управления пользователями VNF на основе RBAC (Role-Based Access Control). Также реализована трассировка сигнализации абонента по IMSI без использования внешних инструментов и трассировка сигнализации на различных интерфейсах (S1, S6a, S11). Поддерживается полное резервное копирование и восстановление конфигурации и системных настроек MME , защищенные интерфейсы управления Web/GUI и CLI (SSH, HTTPS) , а также мониторинг использования аппаратных и программных ресурсов в реальном времени через Web/GUI.

Наличие функций трассировки пользователя по IMSI и поддержки трассировки интерфейсов без использования внешних инструментов является очень мощным встроенным диагностическим инструментом. Это значительно ускоряет процесс локализации и устранения неисправностей, поскольку позволяет операторам глубоко анализировать поведение сигнализации и трафика непосредственно на сетевом элементе. Включение RBAC для управления пользователями и поддержка защищенных интерфейсов управления (SSH, HTTPS) являются стандартными передовыми практиками для обеспечения безопасности доступа к критически важным сетевым элементам. Эти возможности демонстрируют продвинутые диагностические возможности и безопасное управление, что критически важно для эффективной и безопасной эксплуатации сети.

3.3.7. **Тесты высокой нагрузки**

Тесты высокой нагрузки MME включают проверку максимальной пропускной способности на одного абонента (до 1.6 Гбит/с для LTE Cat 19) с поддержкой максимального QoS. Также проверяется поддержка максимального количества подключенных eNodeB к MME (100 eNodeB с эмуляцией Ixia) и максимального количества подключенных 4G абонентов (50000 UE с эмуляцией Ixia) без деградации сервиса.

Эти тесты подтверждают способность MME обрабатывать значительные объемы сигнализации и большое количество абонентов. Использование Ixia для эмуляции масштабного трафика и абонентов указывает на профессиональный подход к валидации производительности. Способность MME стабильно работать со 100 eNodeB и 50 000 абонентов одновременно является показателем высокой производительности и масштабируемости плоскости управления. Это критически важно для оператора, который должен гарантировать качество обслуживания для миллионов абонентов и быть готовым к росту трафика и подключений.

4. Перечень стандартов

В текущем разделе представлен перечень стандартов, использованных при:

- разработке элементов системы
- реализации интерфейсов к:
    - внутренним элементам ядра vEPC
    - сторонним элементам ядра vEPC
    - внешним соединениям

5. Комплексный анализ стандартов 3GPP и IETF, лежащих в основе функциональных возможностей vEPC

5.1. Введение в функциональные возможности vEPC и соответствие стандартам

Виртуализированное ядро пакетной сети (vEPC) представляет собой фундаментальный компонент современной мобильной инфраструктуры, обеспечивающий обработку данных и управление мобильностью для абонентов LTE. В его состав входят ключевые элементы, такие как Mobility Management Entity (MME), отвечающий за управление мобильностью и сессиями, а также Serving Gateway (SGW) и Packet Data Network Gateway (PGW), которые управляют пользовательским трафиком и обеспечивают подключение к внешним сетям. Для обеспечения бесперебойной работы, взаимодействия с оборудованием различных поставщиков и соответствия постоянно развивающимся требованиям мобильной связи, строгое соблюдение отраслевых стандартов является первостепенным.

5.2. Функциональные возможности MME и связанные стандарты

Mobility Management Entity (MME) является центральным элементом ядра LTE, отвечающим за управление мобильностью, аутентификацию абонентов и установление соединений. Функциональные возможности MME, протестированные для Мегафон, демонстрируют широкое соответствие отраслевым стандартам.

5.2.1. Основные функции MME/SGSN

Поддержка соединения S6a Diameter через DRA/Proxy (SCTP) с резервированием является критически важной функцией, обеспечивающей надежную связь между MME и Home Subscriber Server (HSS) для управления профилями абонентов и аутентификацией. Интерфейс S6a определен в 3GPP TS 29.272 (версия V11.12.0 от 2015-10), который описывает протокол на основе Diameter. Сам базовый протокол Diameter стандартизирован в IETF RFC 6733, который заменяет предыдущие версии и является обязательным для новых реализаций Diameter. Использование SCTP (Stream Control Transmission Protocol) в качестве транспортного уровня обеспечивает надежную передачу сообщений с поддержкой мультихоминга для резервирования. Явное упоминание "резервирования" и "маршрутизации на основе домена" (realm-based routing) для соединения S6a Diameter указывает на высокий уровень проектирования, ориентированный на обеспечение непрерывности обслуживания. Это означает, что архитектура включает в себя активные/резервные или активные/активные конфигурации для агента маршрутизации Diameter (DRA) или прокси, что предотвращает единую точку отказа и обеспечивает эффективное распределение сигнального трафика, соответствуя требованиям к надежности операторского класса.

Поддержка интерфейса SGs позволяет координировать работу MME и Mobile Switching Center (MSC) для услуг Circuit Switched (CS) fallback. Этот интерфейс подробно описан в 3GPP TS 23.272 (версия V17.0.0 от 2022-05), который регулирует процедуры CS fallback в Evolved Packet System (EPS).

Поддержка пула MME с балансировкой нагрузки и выгрузкой позволяет нескольким MME обслуживать одну и ту же географическую область, повышая масштабируемость и устойчивость сети. Функциональность пула MME, включая механизмы балансировки нагрузки и выгрузки (например, по NRI - Network Resource Identifier), подробно описана в 3GPP TS 23.401 (версия V18.8.0 от 2025-01). Сочетание балансировки нагрузки и выгрузки демонстрирует архитектурный подход, ориентированный на операционную эффективность и отказоустойчивость. Балансировка нагрузки обеспечивает оптимальное использование ресурсов и предотвращает перегрузку отдельных MME, в то время как механизмы выгрузки предоставляют возможность плавного управления трафиком во время обслуживания или непредвиденных перегрузок. Эта двойная возможность является ключевым фактором для обеспечения бесперебойной работы и высокой доступности.

Коррекция APN для несогласованных APN подписки и запроса гарантирует правильное разрешение APN даже при расхождениях между запрошенными и подписанными точками доступа. Механизмы разрешения и коррекции APN являются частью основных процедур EPS, определенных в 3GPP TS 23.401, а также в 3GPP TS 23.003 (версия V17.8.0 от 2023-01) , который регулирует нумерацию, адресацию и идентификацию.

Поддержка выбора топологии SGW/PGW позволяет MME выбирать подходящие SGW/PGW на основе топологии, часто используя ответы DNS. Функции выбора SGW/PGW определены в 3GPP TS 23.401.

Поддержка функции перезаписи QoS позволяет MME применять локальные правила QoS, потенциально переопределяя подписанные параметры QoS. Обработка QoS в EPS в первую очередь определена в 3GPP TS 23.401 и 3GPP TS 23.203 (версия V18.0.0 от 2024-04) для архитектуры управления политикой и тарификацией (PCC).

Поддержка расширенных QCI (65,165, 69,169) относится к поддержке специфических идентификаторов классов качества обслуживания. QCI определены в 3GPP TS 23.401 и 3GPP TS 23.203. Расширенные QCI часто связаны с конкретными требованиями операторов или развивающимися сервисными потребностями, выходящими за рамки стандартного набора.

Поддержка маркировки DSCP для сигнализации и OAM обеспечивает маркировку Differentiated Services Code Point для приоритизации трафика. DSCP определен в IETF RFC 2474, который описывает 6-битовое поле DSCP в заголовке IP для QoS.

Поддержка нескольких часовых поясов позволяет обрабатывать различные часовые пояса для разных зон отслеживания (TAC). Хотя это не является специфическим интерфейсом 3GPP, информация о часовом поясе обычно управляется в сетевых элементах и может быть частью механизмов отчетов о местоположении в 3GPP TS 23.401 или связанных спецификациях O&M.

Поддержка локального кэша DNS означает способность MME разрешать DNS-запросы локально без обращения к внешним DNS-серверам. Это оптимизация реализации, которая опирается на фундаментальные протоколы DNS.

Поддержка роуминга для LTE, UMTS позволяет абонентам получать доступ к услугам во время роуминга. Процедуры роуминга широко охвачены в 3GPP TS 23.401 для LTE и других спецификациях 3GPP для мобильности UMTS/GSM.

Поддержка сохранения векторов аутентификации позволяет MME пропускать процедуру аутентификации при повторных подключениях путем кэширования векторов аутентификации. Процедуры аутентификации и контекст безопасности определены в 3GPP TS 23.401.

5.2.2. **Базовый доступ 4G и управление мобильностью**

Процедуры присоединения/отсоединения являются фундаментальными для регистрации и отмены регистрации UE. Эти основные процедуры EPS определены в 3GPP TS 23.401. Это включает присоединение с использованием IMSI, GUTI, присоединение только к EPC, комбинированное присоединение (для CSFB), а также отсоединение, инициированное как UE, так и MME.

Процедуры обновления зоны отслеживания (TAU) обеспечивают мобильность UE в рамках EPS. Процедуры TAU (периодические и обычные) определены в 3GPP TS 23.401.

Запрос на обслуживание — это процедура для перехода бездействующего UE в подключенное состояние для доступа к услугам. Процедуры запроса на обслуживание определены в 3GPP TS 23.401.

Освобождение ресурсов интерфейса S1 от eNodeB относится к освобождению ресурсов на интерфейсе S1. Процедуры интерфейса S1 определены в 3GPP TS 23.401.

5.2.3. **Управление сессиями**

Активация/деактивация несущей включает установление и освобождение несущих по умолчанию и выделенных несущих. Процедуры управления несущими (по умолчанию, модификация, инициированная HSS, деактивация, инициированная MME) определены в 3GPP TS 23.401.

Активация несущей с подписанным статическим IP-адресом поддерживает получение UE статического IP-адреса. Присвоение IP-адресов обрабатывается в контексте установления соединения PDN в соответствии с 3GPP TS 23.401. Сама IP-адресация регулируется RFC 791 (IPv4) и RFC 8200 (IPv6).

Поддержка нескольких PDN позволяет UE устанавливать несколько одновременных соединений PDN. Несколько соединений PDN поддерживаются в соответствии с 3GPP TS 23.401.

Активация выделенной несущей GBR/Non-GBR, инициированная сетью, относится к созданию выделенных несущих для специфических требований QoS (например,

VoLTE, speedtest). Активация выделенной несущей, включая GBR (Guaranteed Bit Rate) и Non-GBR, определена в 3GPP TS 23.401 и находится под влиянием правил PCC из 3GPP TS 23.203.

Инициированное UE соединение PDN позволяет UE запрашивать дополнительное соединение PDN. Это часть процедур подключения PDN в 3GPP TS 23.401.

5.2.4. **Взаимодействие с eNodeB**

Интерфейс S1 с Nokia/Huawei eNodeB демонстрирует совместимость с eNodeB различных поставщиков. Интерфейс S1 стандартизирован в 3GPP TS 23.401. Явное тестирование взаимодействия с конкретными поставщиками eNodeB, такими как Nokia и Huawei , указывает на сосредоточенность на реальных проблемах развертывания, а не только на теоретическом соответствии стандартам. Хотя 3GPP определяет интерфейс S1, реализации поставщиков могут иметь нюансы. Такой подход к тестированию подтверждает зрелость и практичность решения для обеспечения бесперебойной работы в многовендорных средах.

5.2.5. **Управление безопасностью**

Процедура аутентификации при присоединении включает проверку личности UE во время присоединения. Процедуры аутентификации определены в 3GPP TS 23.401.

Конфиденциальность идентификатора абонента, переназначение GUTI относится к защите идентификатора абонента и переназначению временных идентификаторов. Выделение и переназначение GUTI являются частью управления мобильностью и безопасностью в 3GPP TS 23.401 и 3GPP TS 23.003.

Процедура команды режима безопасности при присоединении устанавливает контекст безопасности (шифрование и защиту целостности). Эта процедура определена в 3GPP TS 23.401.

Аутентификация личности включает проверку личности UE. Процедуры идентификации являются частью общей структуры присоединения и безопасности в 3GPP TS 23.401.

5.2.6. **Хэндовер**

Поддержка хэндовера на основе S1 внутри MME, на основе X2 и на основе S1 между MME обеспечивает бесшовную мобильность между eNodeB и MME. Процедуры хэндовера всесторонне определены в 3GPP TS 23.401. Детальное тестирование различных типов хэндовера (внутри MME S1, X2, между MME S1) с явным ожидаемым результатом "успешная процедура, ECM-CONNECTED, без потери пакетов" подчеркивает критическое внимание к поддержанию непрерывности обслуживания и качества во время событий мобильности. Это жизненно важно для таких приложений, как VoLTE, где даже незначительная потеря пакетов может ухудшить качество вызова. Это указывает на приверженность высокопроизводительному управлению мобильностью.

5.2.7. **Поддержка информации IMEI**

Поддержка передачи информации IMEI в S-GW относится к передаче международного идентификатора мобильного оборудования. Обработка и передача IMEI в EPS указаны в 3GPP TS 23.401 и 3GPP TS 23.003. IMEI передается в сообщениях GTP , которые определены в 3GPP TS 29.274 (плоскость управления, версия V16.6.0 от 2021-01) и 3GPP TS 29.281 (плоскость пользователя, версия V18.3.0 от 2025-01).

5.2.8. **Совместное использование сети**

Присоединение и активация UE с различными HPLMN и поддержка MME совместного использования сети MOCN обеспечивают поддержку сценариев совместного использования сети с несколькими домашними PLMN. Архитектуры совместного использования сети, включая MOCN, определены в 3GPP TS 23.251 (версия V17.0.0 от 2022-04). Включение функций совместного использования сети, таких как "различные HPLMN" и "MOCN" , указывает на бизнес-стратегию, использующую совместное использование инфраструктуры для повышения экономической эффективности или расширения рынка. Это сложная функция, требующая тщательного соблюдения 3GPP TS 23.251 для обеспечения надлежащей обработки абонентов и выставления счетов в рамках совместно используемых сетевых элементов.

5.2.9. **Контроль доступа**

Контроль доступа на основе подписанного ARD, блокировки пакетных услуг (ODB), региональной конфигурации включает механизмы ограничения доступа абонентов на основе различных критериев. Функции контроля доступа обычно управляются через профили абонентов (из HSS, регулируемые 3GPP TS 29.229 (версия V17.2.0 от 2022-07) для интерфейсов Cx/Dx) и сетевые политики.

5.2.10. **Голосовые услуги (CSFB, VoLTE, SRVCC)**

Вызовы CSFB (Circuit Switched Fallback) MT/MO позволяют осуществлять голосовые вызовы для UE, поддерживающих только LTE, путем отката к сетям 2G/3G с коммутацией каналов. Процедуры CSFB определены в 3GPP TS 23.272.

Вызовы VoLTE MO/MT, экстренные вызовы обеспечивают поддержку Voice over LTE, включая экстренные службы. Вызовы VoLTE основаны на архитектуре IMS (IP Multimedia Subsystem), определенной различными стандартами 3GPP, включая 3GPP TS 23.216 (SRVCC, версия V18.0.0 от 2024-05). Экстренные вызовы специально рассматриваются в 3GPP TS 23.167 (IMS Emergency Sessions, версия V18.2.0 от 2024-05).

Расширение VoLTE для поддержки SRVCC (Single Radio Voice Call Continuity) позволяет бесшовно передавать вызовы VoLTE в сети 2G/3G CS. SRVCC определен в 3GPP TS 23.216.

Ограничение VoLTE на основе местоположения/TAC, для роумеров относится к ограничениям службы VoLTE на основе политики. Это политики, определенные

оператором, реализованные через правила PCC, опирающиеся на 3GPP TS 23.203 и 3GPP TS 29.212 (интерфейс Gx) для применения политики.

5.2.11. **Сетевые аспекты**

Поддержка контекста PDP/PDN IPv4 и IPv6 обеспечивает поддержку одностековой и двухстековой IP-адресации. Присвоение IP-адресов и активация контекста PDN являются частью 3GPP TS 23.401. Базовые IP-протоколы - RFC 791 (IPv4) и RFC 8200 (IPv6).

Синхронизация NTP использует протокол сетевого времени для синхронизации времени. NTP определен в IETF RFC 5905 (NTPv4).

Конфигурация MTU (Maximum Transmission Unit) для сетевых портов. MTU является фундаментальной сетевой концепцией, не привязанной к одному RFC, но критически важной для предотвращения фрагментации IP-пакетов и производительности, неявно связанной с RFC 791 (IPv4) , RFC 8200 (IPv6) и RFC 9293 (TCP).

Поддержка VRF для логических интерфейсов (Virtual Routing and Forwarding) для сегментации сети. VRF - это концепция, используемая в MPLS VPN, определенная в IETF RFC 4364.

Поддержка протокола BFD для IPv4/IPv6 (Bidirectional Forwarding Detection) для быстрого обнаружения сбоев каналов. BFD определен в IETF RFC 5880 [27] (базовый протокол) и RFC 5881 (BFD для IPv4 и IPv6 Single Hop).

Динамическая маршрутизация BGP (Border Gateway Protocol) для динамической маршрутизации. BGP определен в IETF RFC 4271 (BGP-4), который поддерживает семейства адресов IPv4 и IPv6. Комплексная поддержка таких передовых сетевых протоколов, как BFD и BGP для динамической маршрутизации, наряду с VRF , указывает на высокосложную и отказоустойчивую сетевую инфраструктуру для vEPC. Эти протоколы имеют решающее значение для быстрого обнаружения неисправностей, автоматической сходимости маршрутов и сегментации сети, что в совокупности способствует общей стабильности и безопасности мобильного ядра.

5.2.12. **Надежность**

Восстановление конфигурации после перезапуска MME обеспечивает сохранение конфигурации при перезагрузках.

Перезапуск/отключение уровня приложения MME, перезапуск/отключение уровня хоста MME [1] тестирует устойчивость к сбоям на уровне приложения и хоста. Хотя эти аспекты напрямую не связаны с одним стандартом 3GPP, они являются критически важными эксплуатационными требованиями для надежности сетевых элементов и часто являются частью специфических для поставщика спецификаций реализации, соответствующих принципам высокой доступности. Детальное тестирование перезапусков/отключений уровня приложения и хоста MME с ожидаемыми результатами, такими как "отсутствие прерывания сессии UE" и "перенос услуг с неисправного хоста на другие" , подчеркивает сильный акцент на непрерывности обслуживания и отказоустойчивости. Это указывает на активную/резервную или

кластерную архитектуру, разработанную для минимизации воздействия на обслуживание во время сбоев или планового обслуживания.

5.2.13. **Эксплуатация и техническое обслуживание**

Управление производительностью (MM, SM) включает сбор и отчетность по статистике управления мобильностью и сессиями.

Управление сбоями и аварийными сигналами относится к генерации и управлению аварийными сигналами для аппаратных и сервисных сбоев.

Управление журналом операций (ведение журнала активности пользователей) включает ведение журнала команд пользователя и системных событий.

Поддержка управления пользователями RBAC VNF (Role-Based Access Control) для пользователей виртуальных сетевых функций.

Трассировка пользователей на основе IMSI, поддержка трассировки интерфейсов (S1, S6a, S11) — это инструменты диагностики для устранения неполадок конкретных абонентов и интерфейсов.

Полное резервное копирование/восстановление — это возможность резервного копирования и восстановления конфигурации MME и системных настроек.

Веб/GUI, интерфейсы управления CLI с безопасностью обеспечивают безопасный доступ к интерфейсам управления (SSH, HTTPS).

Мониторинг использования HW/SW в реальном времени (Web/GUI) обеспечивает мониторинг CPU, PDP, пропускной способности в реальном времени.

Эти функции O&M обычно руководствуются общими передовыми практиками управления сетью. Обширный список функций O&M свидетельствует о сильном акценте на операционную пригодность и ремонтопригодность vEPC. Такие функции, как RBAC, подробное ведение журнала, трассировка пользователей/интерфейсов и безопасные интерфейсы управления, имеют решающее значение для эффективного устранения неполадок, аудита и безопасных операций в действующей сети.

5.2.14. **Тесты высокой нагрузки**

Максимальная пропускная способность на UE тестирует индивидуальные скорости передачи данных абонентов до LTE Cat 19 (1,6 Гбит/с).

Максимальное количество eNodeB, подключенных к MME , проверяет способность MME обрабатывать 100 eNodeB.

Максимальное количество подключенных абонентов 4G тестирует MME под нагрузкой 50 000 UE.

Эти тесты производительности демонстрируют способность реализации соответствовать или превосходить целевые показатели производительности,

подразумеваемые стандартами 3GPP для возможностей LTE (например, Cat 19 для пропускной способности, как указано в) и планированием сетевой емкости. Включение строгих "Тестов высокой нагрузки" для пропускной способности, подключений eNodeB и емкости абонентов, с использованием таких инструментов, как Ixia, свидетельствует о сильной приверженности производительности и масштабируемости. Это выходит за рамки функционального соответствия и учитывает критическую потребность vEPC в обработке реальных объемов трафика и плотности абонентов. Явное упоминание LTE Cat 19 (1,6 Гбит/с) указывает на перспективное планирование емкости для высокоскоростных услуг передачи данных.

5.2.15. **Таблица 1: Функциональные возможности MME и соответствующие стандарты**

5.3. Функциональные возможности SGW/PGW и связанные стандарты

Serving Gateway (SGW) и Packet Data Network Gateway (PGW), включая аспекты GGSN, являются ключевыми элементами для управления пользовательским трафиком и предоставления доступа к внешним сетям. Протестированные функциональные возможности SGW/PGW демонстрируют комплексное соответствие стандартам.

5.3.1. **Основные функции SGW/PGW/GGSN**

Поддержка маркировки DSCP на основе QoS/QCI для UMTS/LTE обеспечивает приоритизацию трафика на основе значений QoS и QCI. DSCP определен в IETF RFC 2474. QoS и QCI определены в 3GPP TS 23.401 и 3GPP TS 23.203.

Поддержка функциональности Direct Tunnel/One Tunnel для UMTS оптимизирует маршрутизацию пользовательской плоскости для UMTS. Функциональность Direct Tunnel указана в 3GPP TS 23.060.

Поддержка отдельного размера TCP MSS для каждого APN позволяет настраивать максимальный размер сегмента TCP для каждого APN. TCP MSS является параметром протокола TCP, определенным в RFC 9293 (TCP). Его настройка для каждого APN является специфической для реализации функцией для оптимизации трафика.

Маршрутизация Diameter на основе хоста/домена на интерфейсах Gx/S6b обеспечивает маршрутизацию Diameter для управления политикой и тарификацией (Gx) и ePDG/AAA (S6b) интерфейсов. Интерфейс Gx определен в 3GPP TS 29.212 (версия V18.2.0 от 2024-09) для PCC. Базовый протокол Diameter - RFC 6733.

5.3.2. **Управление мобильностью**

Тестирование различных сценариев TAU и RAU между E-UTRAN, UTRAN и GERAN демонстрирует комплексный подход к управлению мобильностью в мультитехнологической сети. Эти процедуры мобильности между различными технологиями радиодоступа (RAT) определены в 3GPP TS 23.401 и 3GPP TS 23.060. Такая обширная проверка гарантирует бесшовное обслуживание при перемещении абонентов между зонами покрытия 4G, 3G и 2G, подчеркивая роль vEPC в конвергентной сети доступа.

5.3.3. **CUPS (Разделение плоскостей управления и пользователя)**

Явное включение функциональных возможностей CUPS (Control and User Plane Separation) и критериев выбора UPF (User Plane Function) [1] является значительным показателем современной архитектуры vEPC и ее готовности к будущей эволюции сети. CUPS - это фундаментальная концепция для сетей 5G, позволяющая гибко развертывать функции пользовательской плоскости ближе к периферии для снижения задержки и увеличения пропускной способности. Это указывает на перспективный дизайн, даже если основной контекст - LTE. CUPS и выбор UPF определены в 3GPP TS 23.214 (версия V18.0.0 от 2024-04) и 3GPP TS 23.237 (IMS Service Continuity, версия V17.0.0 от 2022-03-30).

5.3.4. **Управление сессиями**

Эхо-запрос/ответ GTPv1, GTPv2 используется для проверки связности GTP (GPRS Tunnelling Protocol). GTP-C (плоскость управления) определен в 3GPP TS 29.274 , а GTP-U (плоскость пользователя) - в 3GPP TS 29.281.

Поддержка активации/деактивации несущей по умолчанию , активация выделенной несущей, инициированная сетью (новый QCI) , поддержка модификации несущей [1] и несколько соединений PDN являются основными функциями управления несущими и сессиями.

Поддержка Multi-HPLMN Access обеспечивает поддержку абонентов из различных домашних PLMN. Ручная деактивация контекста позволяет вручную завершать абонентские сессии. Поддержка GGSN процедур обновления и деактивации контекста PDP относится к управлению сессиями, специфичному для GGSN.

Уведомление о перезапуске PGW , деактивация бездействующего PDP по таймеру , аренда IP для динамически назначаемых адресов и удаление сессий из SGW после перезапуска MME обеспечивают надежность и эффективное управление ресурсами. Все эти аспекты управления сессиями в первую очередь определены в 3GPP TS 23.401 для LTE/EPS и 3GPP TS 23.060 для GPRS/UMTS. Присвоение IP-адресов также связано с RFC 791 (IPv4) и RFC 8200 (IPv6).

5.3.5. **Поддержка контекста PDN IPv4 и IPv6**

Активация контекста PDN IPv4, IPv6, DualStack IPv4/IPv6 обеспечивает комплексную поддержку версий IP. Как упоминалось выше, это фундаментальные IP-протоколы: RFC 791 (IPv4) и RFC 8200 (IPv6). Процедуры активации находятся в 3GPP TS 23.401.

5.3.6. **Управление адресами**

Локальное динамическое назначение адресов PGW-C/UPF означает, что PGW/UPF действует как DHCP-сервер. Это включает управление IP-адресами, часто через DHCP, определенный в RFC 2131.

5.3.7. **Управление Radius**

Обширная поддержка RADIUS , включая аутентификацию, подробный учет (начало, остановка, промежуточный, копирование), а также широкий спектр передаваемой информации об абонентах (часовой пояс MS, IMEISV, RAT, IMSI, APN, IP SGW/SGSN/GGSN, информация о местоположении MS), подчеркивает надежную и гибкую интеграцию систем биллинга и операционной поддержки (OSS). Это критически важно для точного учета доходов, обнаружения мошенничества и обслуживания клиентов в крупномасштабной мобильной сети. Аутентификация RADIUS определена в IETF RFC 2865 , а учет RADIUS - в IETF RFC 2866.

5.3.8. **Оффлайн-тарификация**

Генерация CDR на основе времени SGW/PGW/GGSN, генерация CDR на основе объема, генерация CDR по триггеру изменения RAT/SGSN/S-GW/часового пояса/максимальных условий/PLMN относится к генерации записей о вызовах (CDR) для оффлайн-тарификации. Оффлайн-тарификация определена в 3GPP TS 32.251 и 3GPP TS 32.298, которые определяют содержание и триггеры для CDR.

5.3.9. **Управление сессиями Gx PCC**

Обширное тестирование управления сессиями Gx PCC , включая установку динамических правил, различные триггеры обновления (QoS, RAT, ULI), перевыбор PCRF и механизмы отказоустойчивости, демонстрирует высокодинамичную и отказоустойчивую структуру управления политиками. "Переход на локальные правила PCC при сбое Gx" является критически важной функцией отказоустойчивости, обеспечивающей непрерывность обслуживания даже в случае потери соединения с PCRF. Это жизненно важно для поддержания качества обслуживания и применения

бизнес-политик. Интерфейс Gx и архитектура PCC в первую очередь определены в 3GPP TS 29.212 и 3GPP TS 23.203. Diameter - RFC 6733.

5.3.10. **Голосовые услуги**

Вызовы VoLTE MO/MT с активацией выделенной несущей , экстренный вызов VoLTE , восстановление IMS при сбое P-CSCF и поддержка вызова S2b + VoWiFi обеспечивают комплексные голосовые услуги. Включение "Восстановления IMS при сбое P-CSCF" [1] является критически важной функцией отказоустойчивости для услуг VoLTE. P-CSCF (Proxy-CSCF) является первой точкой контакта для UE в IMS. Его отказ может нарушить текущие вызовы. Способность SAEGW отправлять "Update PDP Context Request или Update Bearer Request, содержащий список адресов P-CSCF с доступными P-CSCFs" демонстрирует проактивное восстановление после сбоев и непрерывность обслуживания для голосовой связи в реальном времени. VoLTE и экстренные вызовы основаны на IMS, регулируемом 3GPP TS 23.216 и 3GPP TS 23.167. Восстановление IMS охвачено 3GPP TS 23.237.

5.3.11. **Виртуальный APN**

Расширенные возможности виртуального APN, включая сопоставление на основе TAC, диапазона IMSI и LAC , наряду с балансировкой нагрузки APN и перезаписью информации APN для CDR/AAA/Gx , указывают на высокогибкую и коммерчески адаптируемую vEPC. Это позволяет операторам предлагать высокодетализированные услуги, поддерживать MVNO или оптимизировать маршрутизацию трафика и биллинг на основе различных критериев. Виртуальный APN и сопоставление APN являются специфическими для реализации функциями, расширяющими базовую концепцию APN из 3GPP TS 23.003 и 3GPP TS 23.401.

5.3.12. **Управление безопасностью**

Изоляция плоскости управления, изоляция плоскости данных и контроль ACL (Intra APN, Inter APN, System) относятся к фундаментальным принципам безопасности и передовым практикам в сетевом проектировании. Эти меры имеют решающее значение для защиты мобильного ядра.

5.3.13. **Сеть и маршрутизация**

Синхронизация NTP определена в IETF RFC 5905 (NTPv4).

Конфигурация MTU неявно связана с RFC 791 (IPv4) , RFC 8200 (IPv6) и RFC 9293 (TCP).

Поддержка интерфейсов с тегированием VLAN (подинтерфейсы) относится к поддержке виртуальных локальных сетей. VLAN определены в IEEE 802.1Q.

Привязка APN к VRF (Virtual Routing and Forwarding) определена в IETF RFC 4364.

Динамическая маршрутизация BGP IPv4/IPv6 определена в IETF RFC 4271 (BGP-4).

Поддержка протокола BFD для IPv4/IPv6 определена в IETF RFC 5880 и RFC 5881.

Gi redirect относится к перенаправлению трафика на интерфейсе Gi, который является точкой отсчета между сетью GPRS/EPS и внешней сетью пакетной передачи данных.

5.3.14. **Надежность и производительность при высокой нагрузке**

Восстановление конфигурации после перезапуска SGW/PGW/GGSN обеспечивает сохранение конфигурации.

Перезапуск уровня приложения SPGW-C/UPF, перезапуск/отключение уровня хоста SPGW-C/UPF, отказ одной из двух сессий BGP VRF Radius, VRF Diameter, перемаршрутизация трафика интерфейсов , отказ портов S5/S8, SGi, перемаршрутизация трафика и проверка отключения и обратного включения оптики являются критически важными эксплуатационными требованиями и тестами отказоустойчивости, демонстрирующими приверженность принципам проектирования с высокой доступностью. Детальные тесты надежности для SGW/PGW , включая перезапуски компонентов, сбои сессий BGP и физические сбои портов с явной перемаршрутизацией и восстановлением трафика, подчеркивают надежную конструкцию для обеспечения высокой доступности. Акцент на "перемаршрутизации трафика" подтверждает, что система разработана для активного восстановления после сбоев, минимизируя влияние на обслуживание.

Максимальная пропускная способность на UE тестирует индивидуальные скорости передачи данных абонентов до LTE Cat 19 (1,6 Гбит/с). Максимальная пропускная способность SGW/PGW (10 Гбит/с) проверяет общую пропускную способность. Максимальное количество eNodeB, подключенных к SGW , и максимальное количество несущих UE (50000 UE с Ixia) тестируют возможности SGW/PGW под нагрузкой. Эти тесты производительности являются важными показателями способности системы обрабатывать большие объемы трафика и абонентов.

5.3.15. **Эксплуатация и техническое обслуживание**

Управление производительностью (THP, PDP), управление сбоями и аварийными сигналами, управление журналом операций (ведение журнала активности пользователей), управление безопасностью пользователей и групп, управление разрешениями операторов, трассировка пользователей на основе IMSI, поддержка трассировки интерфейсов (Gx, S11, S5/S8, S1), полное резервное копирование/восстановление и мониторинг использования HW/SW в реальном времени являются комплексными функциями O&M, которые соответствуют общим принципам управления сетью и имеют решающее значение для операционной эффективности SGW/PGW.

5.3.16. **Таблица 2: Функциональные возможности SGW/PGW и соответствующие стандарты**

5.4. Обзор ключевых стандартов

В данном разделе представлен консолидированный, категоризированный список всех идентифицированных технических спецификаций 3GPP, RFC IETF и стандартов IEEE, а также их последние версии и краткое описание их основной значимости для функциональных возможностей vEPC.

5.4.1. **Таблица 3: Консолидированный список упомянутых стандартов**

				Основная значимость для vEPC
				Управление идентификацией

			subscriptionIdentification	фикатораминабонентов(IMSI,GUTI,IMEI)иточкамидоступа(APN

				).
				Основополагающий для функционального DirectTunnel имо

				билькостиUMTS/GERAN.
			IPMultimediaSubsystem(IMS)	Поддержкаэкстренныхвызововв VoLT

				Е.
				Управлениекачествомобслуживания(QoS),прав

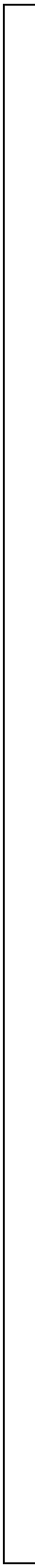
				илами РСС и интерфейсом Gx.
			Architecture enhancements for co	Основа для архитектуры CUPS и выбо

				paUPF.
				Обеспечение бесшовной пре

				рывностиголосовыхвызововприпереключениимеждусетями.

				Механизмы восстановления IMS, включая сбои P-CSCF.

				Поддержка совместного использования сети (MOCN) и различных

				PLMN.
				Процедуры CSFB для голосовых вызовов в сетях LTE.

				Основополагающий для большинства функций ММ

			erts for E-U-RAM access	E/SGW/PGW, включая присоединение, отсоединение, мобильност

				ь, управлениенесущимиироумингг.
				Управлениеполитиками

			I(PCC); Reference point Gx	рификацией через интерфейс Gx.
			Mobility Management Entity (	Протокол Diameter для интерф

				ейсаS6а(MME-HSS).

				Интерфейс S6b для VoWiFi.

				Протоколплоскостиуправлениядляинтерфейсов S11, S5/S8

				- С.
				Протоколплоскостипол

				ьзователядляинтерфейсовS1-U,S5/S8-U.
				Протокол

				olsyDiameterдляинтерфейсовHSS.

				Общие принципы управления сетью (производительность, отказы

				,конфигурация).
				Архитектурабезопасностиeps,включая про

				цедуры аутентификации ММЕ.
				Протокол уровня приложения для

				нтерфейсаS1.
				Протоколуровняприложениядляинтерфейсах

2.				
Фундаментальный для поддержки IPv4.	Internet Protocol version 4 (IPv4)			
Фундаментальный	Transmission Control			

				для связи на основе TCP.
				Маркировка DSCP для приоритизации тра

			ices field (DS field) in the IPv4 and IPv6 headers	фика.
			Perform the Authe	Аутентифика

				ция RADIUS.
				Учет RADIUS.

				Динамическая маршрутизация BGP.
				Поддержка VRF для сегмен

			ate Networks (VPNs)	тации сети.
			Bidirectional Forwarding Detection (BF	Базовый протокол для быстрого обнаружен

				ия сбоев каналов.
				Спецификации BFD для IPv4 и IPv6.

					Синхронизация времени NTP.

				Фундаментальный дл

			collaboration	Является интерфейсом Diameter (S6a, Gx, S6b, Cx/Dx).
			Internet	Фундамент

			multicast, Version (IPv6)	альный для поддержки IPv6.
			VLANs	Поддержка тегирования VLAN.

6. Глоссарий

*3GPP (3rd Generation Partnership Project)** – Сотрудничество телекоммуникационных организаций, разрабатывающее стандарты для мобильной связи, включая GSM, UMTS, LTE и 5G.*

AAA (Authentication, Authorization, and Accounting) – Протоколы и системы для аутентификации (проверки личности), авторизации (предоставления прав доступа) и учета (сбора данных об использовании услуг) абонентов.

ACL (Access Control List) – Список правил, используемый для фильтрации сетевого трафика и контроля доступа к ресурсам.

APN (Access Point Name) – Имя точки доступа, которое определяет тип сервиса (например, интернет, MMS) и шлюз, через который абонентское устройство подключается к внешней сети.

APP Layer (Уровень приложения) – Программный уровень, на котором работают сетевые функции в виртуализированной среде.

ARD (Access Restriction Data) – Данные об ограничениях доступа, хранящиеся в HSS, которые определяют, к каким услугам абонент может или не может получить доступ.

Attach Procedure (Процедура подключения) – Процедура, с помощью которой абонентское устройство (UE) регистрируется в мобильной сети для получения услуг.

BFD (Bidirectional Forwarding Detection) – Протокол, обеспечивающий быстрое обнаружение сбоев в пути передачи данных между двумя сетевыми устройствами.

BGP (Border Gateway Protocol) – Протокол динамической маршрутизации, используемый для обмена информацией о маршрутах между автономными системами в Интернете.

CDR (Call Detail Record) – Запись о деталях вызова или сессии, используемая для тарификации и анализа использования услуг.

CLI (Command Line Interface) – Интерфейс командной строки для управления сетевым оборудованием.

CSFB (Circuit Switched Fallback) – Механизм, позволяющий абонентам LTE совершать и принимать голосовые вызовы через сети 2G/3G с коммутацией каналов, когда VoLTE недоступен.

CUPS (Control and User Plane Separation) – Разделение плоскостей управления и пользователя в сетевых элементах (например, SGW, PGW), что позволяет независимо масштабировать каждую плоскость.

Diameter – Протокол, используемый для аутентификации, авторизации и учета (AAA), а также для обмена информацией о политиках в мобильных сетях (например, интерфейсы S6a, Gx).

Direct Tunnel (Прямой туннель) – Функция в сетях UMTS, позволяющая пользовательскому трафику напрямую идти от RNC к GGSN, минуя SGSN, для оптимизации пути данных.

DSCP (Differentiated Services Code Point) – 6-битовое поле в заголовке IP-пакета, используемое для классификации и приоритизации сетевого трафика (QoS).

eNodeB (evolved NodeB) – Базовая станция в сети LTE, отвечающая за радиоинтерфейс с абонентскими устройствами.

EPC (Evolved Packet Core) – Архитектура ядра пакетной сети LTE, включающая MME, SGW, PGW и HSS.

EPS (Evolved Packet System) – Общая архитектура мобильной сети, включающая E-UTRAN (радиосеть LTE) и EPC.

GGSN (Gateway GPRS Support Node) – Шлюзовой узел поддержки GPRS, отвечающий за подключение сетей 2G/3G к внешним сетям передачи данных.

GTP (GPRS Tunnelling Protocol) – Семейство протоколов, используемых для туннелирования пользовательского трафика (GTP-U) и сигнализации (GTP-C) в сетях GPRS/UMTS/LTE.

GUI (Graphical User Interface) – Графический пользовательский интерфейс для управления сетевым оборудованием.

GUTI (Globally Unique Temporary Identity) – Временный идентификатор, присваиваемый абонентскому устройству (UE) для обеспечения конфиденциальности и оптимизации процедур мобильности.

Gx Interface (Интерфейс Gx) – Интерфейс между PGW и PCRF, используемый для обмена информацией о политиках и тарификации.

HPLMN (Home Public Land Mobile Network) – Домашняя публичная наземная мобильная сеть, к которой принадлежит абонент.

HSS (Home Subscriber Server) – База данных, хранящая информацию о профилях абонентов, их услугах и местоположении в сети LTE.

IETF (Internet Engineering Task Force) – Организация, разрабатывающая и продвигающая интернет-стандарты, включая RFC.

IMEI (International Mobile Equipment Identity) – Международный идентификатор мобильного оборудования, уникальный номер каждого мобильного телефона.

IMS (IP Multimedia Subsystem) – Подсистема IP-мультимедиа, архитектура для предоставления мультимедийных услуг по IP, таких как VoLTE.

IMSI (International Mobile Subscriber Identity) – Международный идентификатор мобильного абонента, уникальный номер, связанный с SIM-картой.

IoT (Internet of Things) – Концепция сети физических объектов, оснащенных датчиками, программным обеспечением и другими технологиями для подключения и обмена данными с другими устройствами и системами через Интернет.

IP-CAN (IP Connectivity Access Network) – Сеть доступа к IP-соединению, которая предоставляет абоненту IP-связь.

Ixia – Производитель тестового оборудования, используемого для эмуляции сетевого трафика и абонентов для тестирования производительности и масштабируемости.

LAC (Location Area Code) – Код зоны местоположения, используемый в сетях 2G/3G для определения географической области.

LTE (Long Term Evolution) – Технология мобильной связи четвертого поколения (4G).

MME (Mobility Management Entity) – Узел управления мобильностью в сети LTE, отвечающий за сигнализацию, управление мобильностью, аутентификацию и выбор шлюзов.

MOCN (Multi-Operator Core Network) – Модель совместного использования сети, при которой несколько операторов используют одну и ту же радиосеть, но каждый имеет свое собственное ядро сети.

MTU (Maximum Transmission Unit) – Максимальный размер пакета, который может быть передан по сетевому интерфейсу без фрагментации.

NFV (Network Function Virtualization) – Виртуализация сетевых функций, замена традиционного аппаратного оборудования программно-определяемыми сетевыми функциями.

NTP (Network Time Protocol) – Протокол сетевого времени, используемый для синхронизации часов компьютеров в сети.

OAM (Operation, Administration, Maintenance) – Функции эксплуатации, администрирования и обслуживания сетевого оборудования.

ODB (Operator Determined Barring) – Блокировка услуг, определяемая оператором, позволяющая ограничивать доступ абонентов к определенным услугам.

PCC (Policy and Charging Control) – Управление политиками и тарификацией, архитектура, позволяющая динамически применять правила к трафику абонентов.

PCRF (Policy and Charging Rules Function) – Функция правил политики и тарификации, центральный узел, который принимает решения о политиках и тарификации.

P-CSCF (Proxy-Call Session Control Function) – Прокси-функция управления сессиями вызовов, первая точка контакта для абонентского устройства в сети IMS.

PDN (Packet Data Network) – Сеть пакетной передачи данных, например, Интернет или корпоративная сеть.

PDP Context (Packet Data Protocol Context) – Контекст протокола пакетных данных, логическое соединение, устанавливаемое для передачи данных в сетях 2G/3G.

PGW (Packet Data Network Gateway) – Шлюз пакетной сети данных, точка выхода абонентского трафика в внешние сети в LTE.

PLMN (Public Land Mobile Network) – Публичная наземная мобильная сеть, идентифицируемая уникальным кодом.

QCI (QoS Class Identifier) – Идентификатор класса качества обслуживания, используемый для определения характеристик QoS для различных типов трафика.

QoS (Quality of Service) – Качество обслуживания, набор параметров, определяющих производительность и приоритет сетевого трафика.

RADIUS (Remote Authentication Dial-In User Service) – Протокол для централизованной аутентификации, авторизации и учета пользователей, подключающихся к сети.

RAT (Radio Access Technology) – Технология радиодоступа, например, GSM, UMTS, LTE.

RAU (Routing Area Update) – Обновление зоны маршрутизации, процедура, используемая в сетях 2G/3G для обновления местоположения абонента.

RBAC (Role-Based Access Control) – Управление доступом на основе ролей, модель, которая ограничивает доступ к системе для пользователей на основе их ролей.

RFC (Request for Comments) – Документы, публикуемые IETF, описывающие интернет-стандарты и протоколы.

S6a Interface (Интерфейс S6a) – Интерфейс между MME и HSS, используемый для обмена информацией о профилях абонентов.

SGSN (Serving GPRS Support Node) – Обслуживающий узел поддержки GPRS, отвечающий за управление мобильностью и сессиями в сетях 2G/3G.

SGW (Serving Gateway) – Обслуживающий шлюз, отвечающий за маршрутизацию пользовательского трафика и управление мобильностью данных в сети LTE.

SGs Interface (Интерфейс SGs) – Интерфейс между MME и VLR, используемый для поддержки услуг CSFB и SMS.

SCTP (Stream Control Transmission Protocol) – Протокол передачи потоков управления, обеспечивающий надежную передачу данных с поддержкой мультихоминга.

SRVCC (Single Radio Voice Call Continuity) – Непрерывность голосовых вызовов по одному радио, механизм для бесшовного хэндовера VoLTE-вызова с LTE на 2G/3G.

TAC (Tracking Area Code) – Код зоны отслеживания, используемый в сети LTE для определения географической области.

TAU (Tracking Area Update) – Обновление зоны отслеживания, процедура, используемая в сети LTE для обновления местоположения абонента.

TCP MSS (TCP Maximum Segment Size) – Максимальный размер сегмента TCP, который может быть передан без фрагментации.

UE (User Equipment) – Абонентское оборудование, например, мобильный телефон или планшет.

ULI (User Location Information) – Информация о местоположении абонента.

UMTS (Universal Mobile Telecommunications System) – Технология мобильной связи третьего поколения (3G).

UPF (User Plane Function) – Функция пользовательской плоскости, компонент архитектуры CUPS, отвечающий за обработку пользовательского трафика.

vEPC (Virtualized Evolved Packet Core) – Виртуализированное ядро пакетной сети, программная реализация EPC.

VLAN (Virtual Local Area Network) – Виртуальная локальная сеть, позволяющая логически сегментировать сеть.

VLR (Visitor Location Register) – Реестр местоположения посетителей, база данных, хранящая временную информацию о роуминговых абонентах.

VoLTE (Voice over LTE) – Голосовая связь по IP, использующая сеть LTE.

VoWiFi (Voice over Wi-Fi) – Голосовая связь по Wi-Fi.

VRF (Virtual Routing and Forwarding) – Виртуальная маршрутизация и пересылка, технология, позволяющая иметь несколько независимых таблиц маршрутизации на одном маршрутизаторе.

X2 Interface (Интерфейс X2) – Интерфейс между eNodeB, используемый для прямого обмена информацией и поддержки хэндоверов.