Опорная сеть 5G
21.X

Проектный документ по технологии MEC

Редакция 04

Дата 30.10.2020

HUAWEI TECHNOLOGIES CO., LTD.

Товарные знаки и разрешения

 и другие товарные знаки Huawei являются товарными знаками компании Huawei Technologies Co., Ltd.

Все остальные товарные знаки и торговые наименования, упоминаемые в этом документе, являются собственностью соответствующих владельцев.

Внимание

Перечень приобретаемых продуктов, услуг и функций приводится в договоре, заключаемом между компанией Huawei и заказчиком. Продукты, услуги и функции, описываемые в настоящем документе, могут не входить в объем закупок или использования. Если иное не установлено условиями договора, все утверждения, информация и рекомендации в настоящем документе приводятся на условиях «КАК ЕСТЬ», без явных или подразумеваемых гарантий или заявлений.

Информация, приведенная в данном документе, может быть изменена без предварительного уведомления. Составители настоящего документа приняли все возможные меры, чтобы обеспечить достоверность и точность его содержания, однако приведенные в нем утверждения, информация и рекомендации не содержат каких бы то ни было явных или подразумеваемых гарантий.

Huawei Technologies Co., Ltd.

Адрес: Промышленная база Huawei
Баньтянь, Лунган
Шэньчжэнь, 518129
Китайская Народная Республика

Веб-сайт: http://www.huawei.com

Эл. почта: support@huawei.com

Об этом документе

Назначение

Технологии периферийных вычислений мультисервисного доступа (MEC) позволяют операторам связи развертывать определенные функции обработки услуг и планирования ресурсов на периферии сети со стороны доступа. Службы развертываются как можно ближе к пользователям, а приложения, контент и сетевые ресурсы координируются для обеспечения надежного и максимального взаимодействия с пользователем.

Целевая аудитория

Этот документ предназначен для следующих групп сотрудников:

- Специалисты по сбыту
- Специалисты по маркетингу
- Менеджеры по маркетингу
- Менеджеры по продуктам

Условные обозначения

Далее описаны символы, которые могут встречаться в настоящем документе.

Символ	Описание
⚠ ОПАСНОСТЬ	Указывает на неизбежную опасную ситуацию, которая может привести к летальному исходу или серьезной травме, если не будут приняты меры по ее предотвращению.
⚠ ПРЕДУПРЕЖДЕНИЕ	Указывает на потенциальную опасную ситуацию, которая может привести к летальному исходу или серьезной травме, если не будут приняты меры по ее предотвращению.
⚠ ВНИМАНИЕ	Указывает на потенциальную опасную ситуацию, которая может привести к травме легкой или средней степени тяжести, если не будут приняты меры по ее предотвращению.

Символ	Описание
УВЕДОМЛЕНИЕ	Указывает на потенциально опасную ситуацию, которая может привести к повреждению оборудования, потере данных, ухудшению рабочих характеристик или непредвиденным результатам, если не будут приняты меры по ее предотвращению. Символ «УВЕДОМЛЕНИЕ» используется для указания рисков, не связанных с травмами.
ПРИМЕЧАНИЕ	Этот символ также привлекает внимание к важной информации, практическим рекомендациям и советам. Символ «ПРИМЕЧАНИЕ» используется для обозначения информации, не связанной с травмами, повреждением оборудования и ухудшением состояния окружающей среды.

История изменений

Редакция	Дата выпуска	Описание
01	15.12.2019	Первая официальная редакция
02	31.03.2020	Вторая официальная редакция
03	30.06.2020	Третья официальная редакция
04	30.10.2020	Четвертая официальная редакция. Добавлен ряд функций, включая балансировку нагрузки, управление полосой частот и вставку UPF UL CL, инициируемую данными подписки + TAI.

Содержание

1 Об этом документе

В этом документе представлены факторы развития, применимые сценарии, процессы обработки услуг, а также примеры развертывания и пилотные проекты технологии периферийных вычислений мультисервисного доступа (MEC) для базовой сети 5G (5GC). Документ призван помочь соответствующему персоналу в изучении технологии MEC компании Huawei, ее особенностей и тенденций развития.

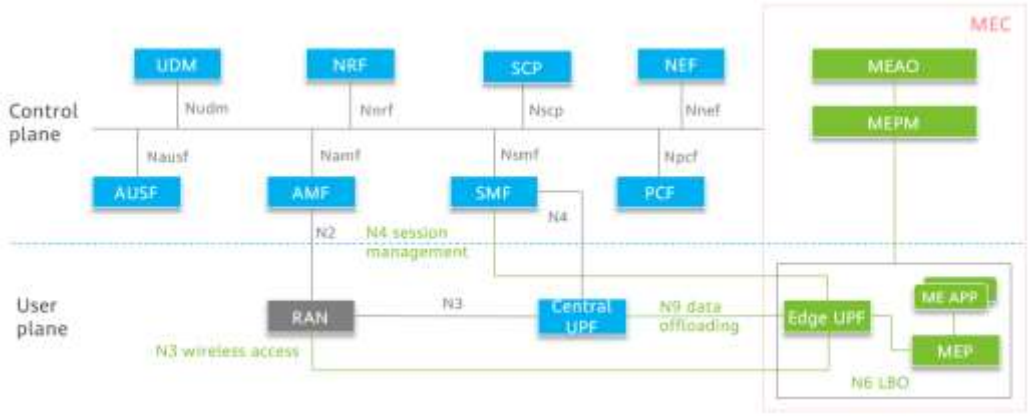
2 Обзор

2.1 Факторы развития

В процессе развития услуг мобильного Интернета стали появляться различные сервисы, такие как онлайн-видео, покупки в Интернете и мобильные платежи. Эти сервисы предоставляют широкий спектр возможностей для общения и взаимодействия людей. В связи с быстрым развитием отраслевых технологий, таких как Интернет вещей (IoT), искусственный интеллект (ИИ), облачные вычисления, мобильный Интернет, «большие данные» и «большие видео», сервисы предъявляют все более высокие требования к сетям. Например, сервисам требуется более высокая пропускная способность, меньшая задержка, более гибкое и быстрое развертывание и возможности массового доступа.

Однако существующие сети EPC не могут удовлетворять указанным требованиям. Это связано с тем, что архитектура EPC не поддерживает обработку запросов на месте (LBO); кроме того, сеть EPC отличается высокой сквозной задержкой. В этих условиях внедряется технология 5G MEC. Технология доступа 5G поддерживает более широкую полосу частот, а периферийная функция плоскости пользователя (UPF) поддерживает LBO для обеспечения более низкой задержки. Периферийная функция UPF интегрирует приложения через платформу MEP для гибкого и быстрого развертывания сторонних приложений.

Рис. 2-1 Архитектура 5G MEC

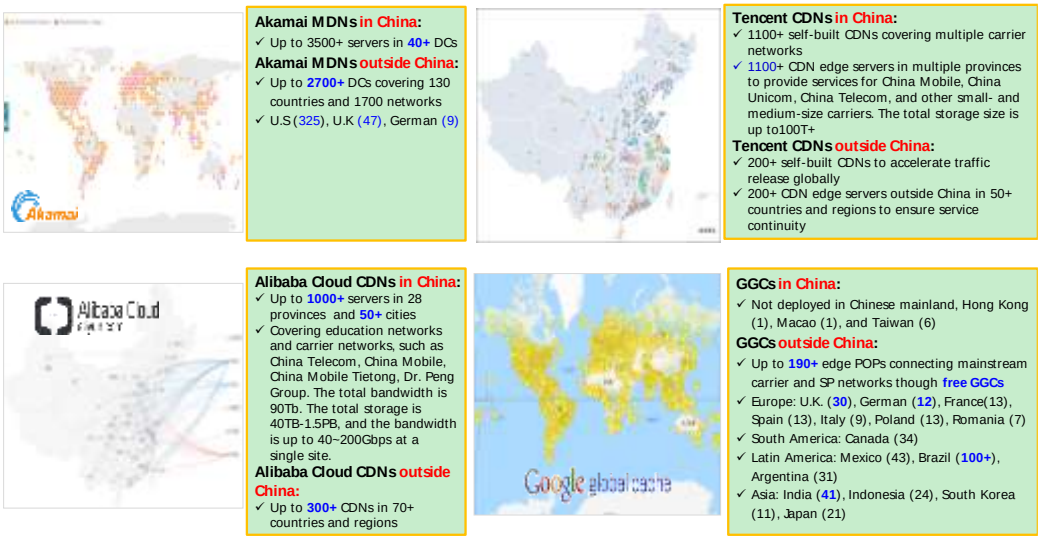


2.1.1 Высочайшее удобство использования

Операторы стремятся к улучшению пользовательского интерфейса и полагаются на расширенные возможности взаимодействия для привлечения и удержания клиентов и

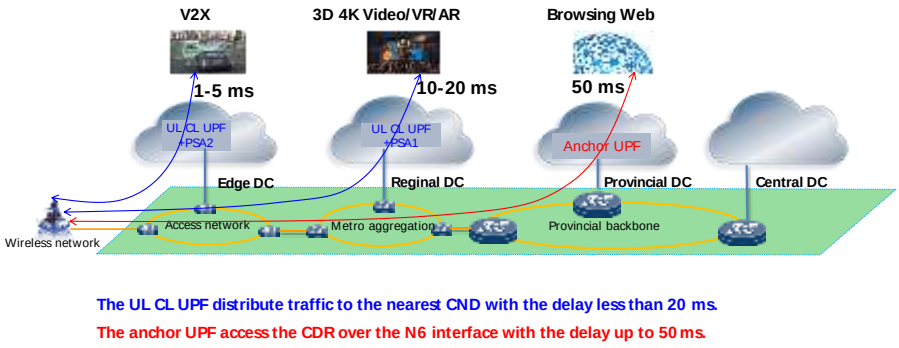
повышения ценности бренда. Что касается сети, то более короткая задержка сквозного доступа к сервису (E2E) способствует улучшению взаимодействия с пользователем. Например, результаты тестирования объекта в КНР (кроме Гонконга, Макао и Тайваня) показывают, что когда задержка видеоуслуги уменьшается на 10–15 мс, средняя оценка видео (vMOS) повышается на 0,1–0,2. Таким образом, можно понять, что задержку доступа к сервису можно сократить путем развертывания контент-серверов как можно ближе к пользователям.

Рис. 2-2 Развертывание контент-серверов как можно ближе к пользователям



Как показано на предыдущем рисунке, большое количество узлов основной сети распространения контента (CDN) было перемещено вниз. Таким образом, узлы CDN разворачиваются в городах в развитых районах. Таким образом, узлы CDN находятся ближе к пользователям, чем шлюзы опорной сети. Чтобы мобильные пользователи могли получить доступ к ближайшему серверу службы CDN, плоскость пользователя шлюза должна быть развернута ближе к пользователям или поддерживать LBO.

Рис. 2-3 Использование LBO в плоскости пользователя для улучшения взаимодействия с пользователем



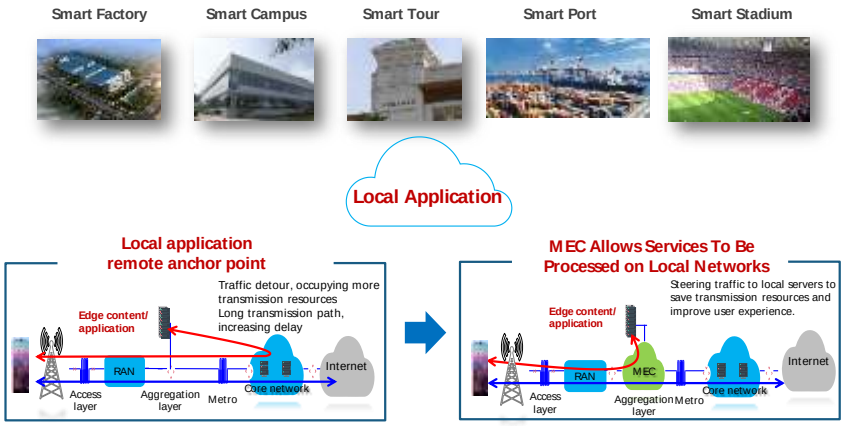
Как показано на предыдущем рисунке, шлюз распределяет трафик плоскости пользователя на локальный контент-сервер, что сокращает задержку доступа к услуге E2E и улучшает взаимодействие с пользователем.

2.1.2 Услуги обработки в локальных сетях

В таких сценариях, как рабочие городки, фабрики, порты, стадионы и промышленный Интернет, сервисные серверы развертываются локально для предоставления услуг для выделенных устройств и сотрудников местных организаций. Такие услуги отличаются тем, что поставщики услуг и пользователи находятся в одном регионе, а конфиденциальные данные, например данные о промышленном производстве и работе предприятия, передаются через услуги. Предполагается, что пользователи могут получить доступ к локальным серверам и использовать услуги, предоставляемые локальными серверами. Это помогает повысить эффективность доступа и обеспечить безопасность и надежность услуг.

При отсутствии технологии MEC предприятия обычно используют проводные сети или собственные сети Wi-Fi для реализации услуг в описанных выше сценариях. Однако сети Wi-Fi имеют ряд недостатков, в частности небольшое покрытие, ненадежная передача, низкая мобильность и низкий уровень безопасности. В результате предприятия не хотят использовать технологии Wi-Fi для создания сетей. Предприятия, имеющие сети Wi-Fi, также ищут решение для перехода на доступ 4G/5G.

Рис. 2-4 Услуги обработки в локальных сетях



2.1.3 Частные кампусные сети

Некоторые клиенты, например правительство и предприятия, партийные, правительственные и военные структуры, энергетические и портовые предприятия, предъявляют более высокие требования к безопасности данных. Они требуют, чтобы данные передавались только в пределах кампуса. Доступ к общедоступной сети в таких случаях не может соответствовать строгим требованиям к безопасности и надежности данных. Требуется построение частной кампусной сети.

Для частной кампусной сети должна быть сформирована выделенная опорная сеть. Частная кампусная сеть может использовать эксклюзивные спектры или использовать спектры совместно с другими общедоступными сетями.

Сценарий	Эксклюзивные спектры	Совместно используемые спектры
Между кампусом и общедоступными сетями	Кампусные и общедоступные сети используют отдельные спектры, соты и зоны отслеживания (TA).	В кампусной сети используется выделенная сеть PLMN. Доля ресурсов спектра, используемых кампусными и общедоступными сетями, настраивается на базовых станциях.
Между кампусными сетями	Каждая кампусная сеть использует отдельные спектры, соты и TA.	Режим 1: базовые станции в каждом кампусе независимы друг от друга, но могут совмещаться с базовыми станциями сети общего пользования. Режим 2: базовые станции совместно используются в кампусах, и каждая кампусная сеть использует отдельную PLMN.

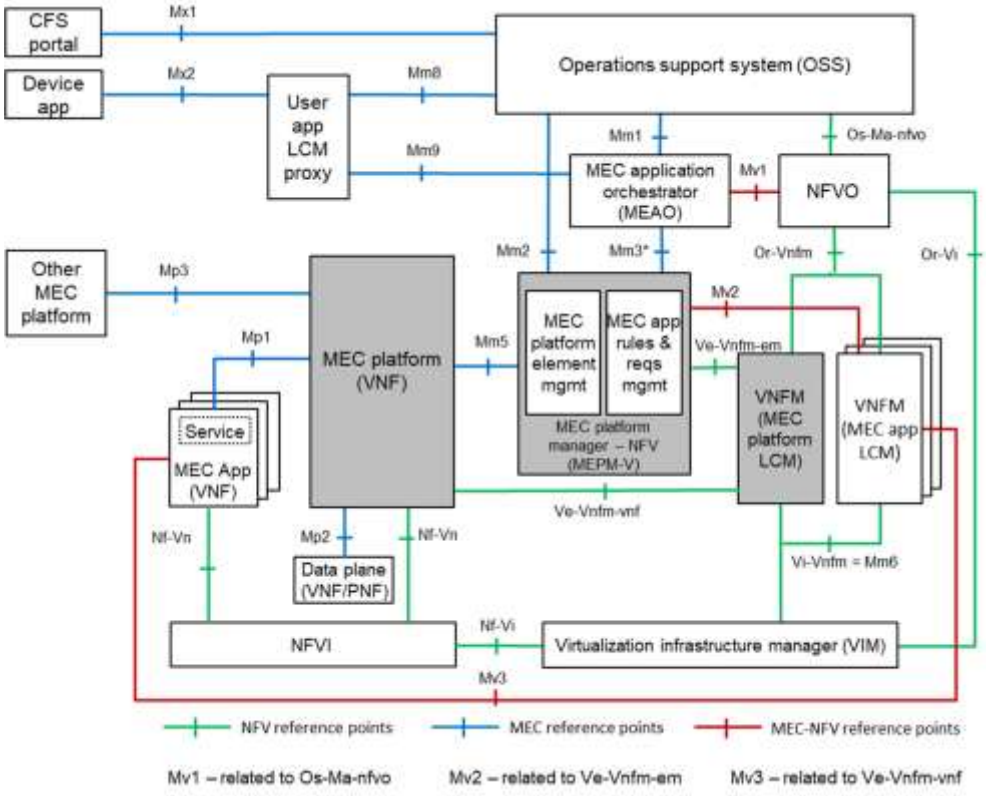
Операторам связи, имеющим большие ресурсы спектра, рекомендуется использовать кампусные сети с выделенными спектрами. Для операторов с ограниченными ресурсами спектра рекомендуются кампусные сети, использующие общие спектры.

Частная кампусная сеть использует выделенные ресурсы радиосвязи и опорной сети и развертывается рядом с опорной сетью. В этом случае частная кампусная сеть поддерживает LBO и позволяет передавать данные в сети кампуса, обеспечивая безопасную, надежную и эффективную работу кампусной сети.

2.2 Технология MEC

Технология MEC включает оркестратор приложений MEC (MEAO), менеджера мобильной периферийной платформы (MEPM), платформу MEC, приложения MEC и плоскость данных. На рисунке ниже показана архитектура MEC, предусмотренная ETSI.

Рис. 2-5 Архитектура MEC в режиме NFV



- MEAO: предоставляет следующие основные функции для управления на уровне системы при периферийных вычислениях:
  - Поддерживает структуру топологии системы MEC и отображает общий вид.
  - Загружает и поддерживает пакеты приложений.
  - Запускает создание экземпляра приложения или завершает работу приложений.
- MEPM: управляет правилами приложений MEC, платформой MEC и жизненными циклами приложений и платформы MEC.
- Платформа MEC: управляет регистрацией служб приложений, службами, правилами распределения трафика, правилами DNS и встроенными службами MEC.
- Приложение MEC: предоставляет услуги на периферийных узлах. Периферийный узел может содержать большое количество приложений.
- Плоскость данных: содержит сетевые функции (NF) в плоскости пользователя в сети 3GPP. В 5GC UPF развертывается в плоскости данных.

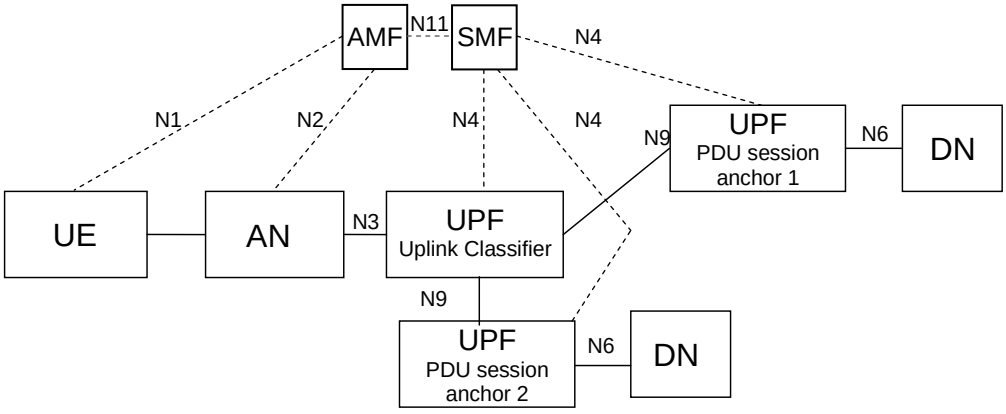
В Табл. 2-1 представлено соответствие между логическими компонентами и продуктами.

Табл. 2-1 Соответствие между логическими компонентами и продуктами

Логический компонент	Продукт
MEAO, MEPM	MAE
Платформа MEC и плоскость данных	UEG
Приложение MEC	Сторонний продукт

2.2.1 ULCL LBO

3GPP определяет функцию классификатора восходящей линии связи (UL CL) для распределения данных 5G в плоскости пользователя. UPF UL CL представляет собой узел обработки, который управляет служебными данными восходящей линии связи и агрегирует управляемые данные нисходящей линии связи. На рисунке ниже показана архитектура, определенная в 3GPP TS 23.501.

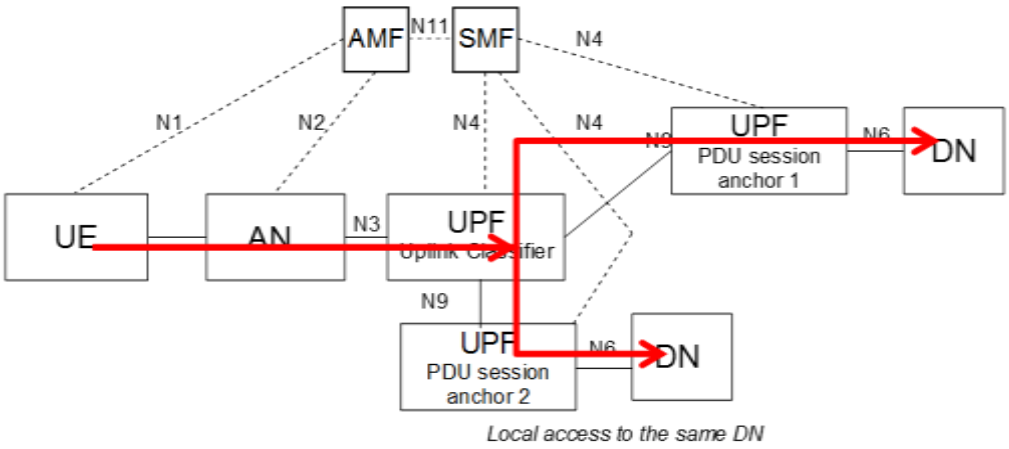


На предыдущем рисунке присутствуют два типа UPF: якорь сеанса PDU UPF (UPF PSA) и классификатор восходящей линии связи UPF (UPF UL CL).

Различия между UPF PSA и UPF UL CL заключаются в следующем:

- UPF PSA функционирует как якорная точка сеансов PDU и точки обработки оконечных туннелей GTP. Только UPF PSA может предоставить интерфейс N6.
- Существует два типа PSA. Как показано на предыдущем рисунке, PSA1 представляет собой UPF, который назначает IP-адрес для UE в ходе активации UE. Соответственно, PSA назначает IP-адреса для UE, когда UE активируются. PSA1 также называют основной якорной точкой. PSA2 является необязательным и развертывается, если доступен UPF UL CL, и UE должны обращаться к периферийным DN. В этом случае PSA2 предоставляет интерфейс N6, через который PSA2 передает сеансы PDU периферийным DN. PSA 2 обычно называют вспомогательной якорной точкой.
- Входящий интерфейс UPF UL CL — N3, а исходящий интерфейс — N9.
- Если UPF PSA функционирует как основная якорная точка и UPF UL CL не развернут, входящим интерфейсом является N3, а исходящим интерфейсом — N6.
- Если UPF PSA функционирует как основная якорная точка и UPF UL CL развернут, входящим интерфейсом является N9, а исходящим интерфейсом — N6.
- Если UPF PSA функционирует как вспомогательная якорная точка, входящим интерфейсом является N9, а исходящим интерфейсом — N6.
- UL CL UPF принимает трафик восходящей линии связи и на основе правил распределения трафика определяет, следует ли отправлять пакеты на основную или вспомогательную якорную точку. Как правило, пакеты, соответствующие правилам распределения трафика, отправляются от вспомогательного якорного порта в локальную сеть DN через интерфейс N6, а прочие пакеты отправляются на основную якорную точку привязки по туннелям GTP через интерфейс N9 для доступа в Интернет.
- UPF PSA, действующий как основная якорная точка, может назначать IP-адреса для UE. Как основные, так и вспомогательные якорные точки могут обеспечивать такие функции, как тарификация, снятие информации и управление услугами для данных, проходящих через них.

Рис. 2-6 Распределение данных восходящей линии связи через UPF UL CL



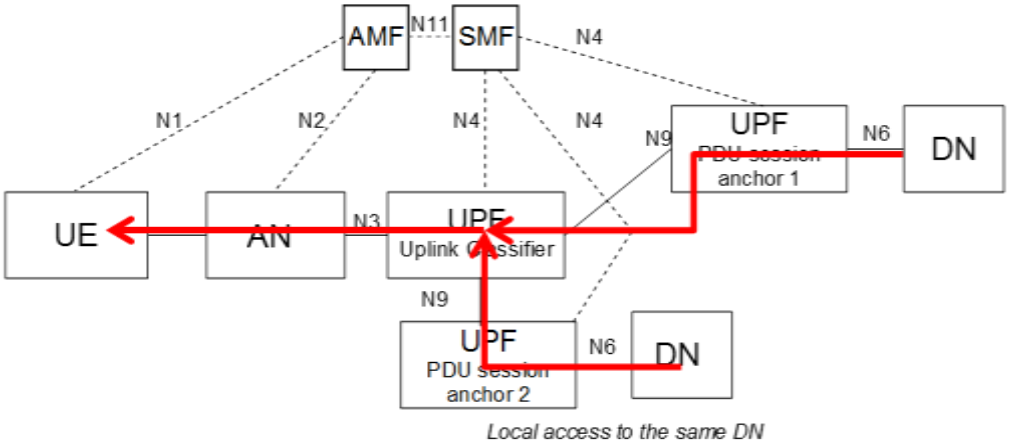
После того, как UPF UL CL принимает IP-пакеты от (R)AN через туннели GTP восходящей линии связи через интерфейс N3, UPF UL CL ищет правило сопоставления на основе информации уровня 3 или 4 (IP-адрес + номер порта) или на основе информации уровня 7 (доменное имя DNS). UPF UL CL отправляет пакеты, соответствующие правилу, в UPF PSA2 через интерфейс N9. UPF UL CL и UPF PSA2 могут быть развернуты совместно или по отдельности. Затем UPF PSA2 отправляет эти пакеты в локальную сеть DN через интерфейс N6. Трансляция сетевых адресов (NAT) должна выполняться через интерфейс N6.

Пакеты, которые не соответствуют правилам, пересылаются на основную якорную точку UPF PSA1 через интерфейс N9. Затем UPF PSA1 направляет их в центральную сеть DN (обычно в Интернет) через интерфейс N6.

ПРИМЕЧАНИЕ

- На предыдущем рисунке периферийная функция UPF логически разделена на UPF UL CL и UPF PSA. В настоящее время продукты Huawei UPF на периферии сети обеспечивают функции UL CL и PSA. Таким образом, UPF UL CL и UPF PSA развертываются совместно.
- В сценарии управления трафиком правила уровня 7 применяются только в том случае, когда UDP используется на транспортном уровне, а DNS — на уровне приложений. Это связано с тем, что пакеты установки канала TCP обрабатываются как нераспределенные пакеты на уровне приложения (например, HTTP) до того, как эти пакеты достигнут UPF для поиска соответствующих правил распределения. Если пакеты установки канала TCP распределяются после того, как найдено соответствующее правило уровня 7, пакеты установки канала TCP и пакеты уровня приложения не могут передаваться по одному пути. В результате происходит прерывание служб. Эту проблему можно решить техническими способами.

На следующем рисунке показан процесс агрегирования нисходящей линии связи UL CL.



Пакеты нисходящей линии связи, соответствующие пакетам данных, распределенным в локальные сети DN, передаются по маршруту сегмента сети, заявленному интерфейсом N6 UPF PSA2, или пересылаются в UPF PSA2 по туннелям через интерфейс N6. UPF PSA2 выполняет инкапсуляцию туннеля GTP и отправляет инкапсулированные пакеты в CL UPF UL.

Пакеты нисходящей линии связи, соответствующие пакетам восходящей линии связи, направляемым в центральную сеть DN, возвращаются в PSA1 UPF через интерфейс N6. PSA1 UPF инкапсулирует пакеты с помощью GTP через интерфейс N9 и отправляет инкапсулированные пакеты в UL CL UPF.

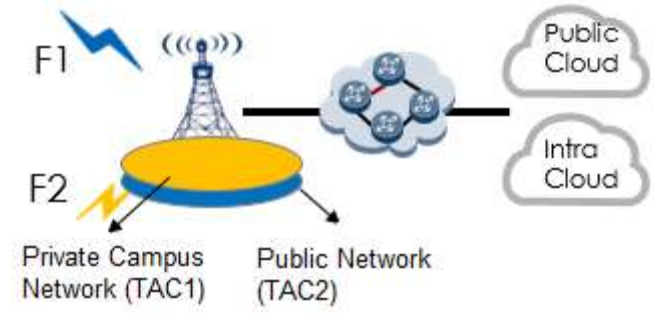
UPF UL CL агрегирует пакеты нисходящей линии связи от PSA1 и PSA2, инкапсулирует пакеты, используя GTP через интерфейс N3, и отправляет пакеты в (R)AN.

2.2.2 Изоляция частной сети

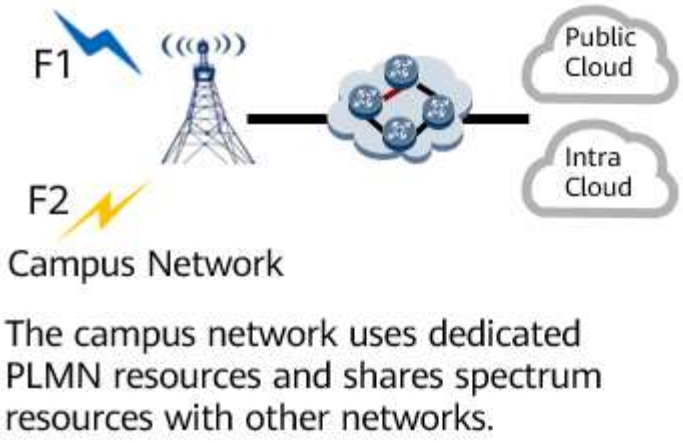
Требования к изоляции частной сети в разных кампусах отличаются в зависимости от типов услуг и требований к стоимости. Сети можно отделить от беспроводных сетей или опорных сетей.

Изоляция беспроводной сети

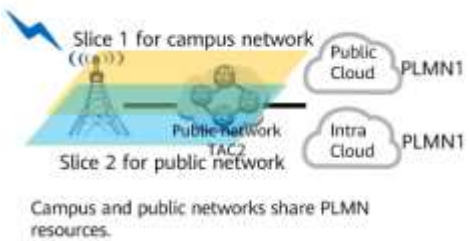
На начальном этапе развертывания кампусной службы кампусные и общедоступные сети совместно используют ресурсы беспроводной сети. По мере развития кампусных служб многим крупным предприятиям требуются эксклюзивные беспроводные ресурсы для предотвращения конфликтов между службами общедоступных сетей и межкампусными службами. В этом случае кампусная сеть должна использовать выделенные ресурсы спектра или занимать исключительно общие ресурсы спектра. Если кампусные и общедоступные сети совместно используют ресурсы спектра, вы можете настроить долю ресурсов спектра, которые могут быть исключительно заняты каждой базой кампусной сети на основе PLMN и информации о сегментировании.

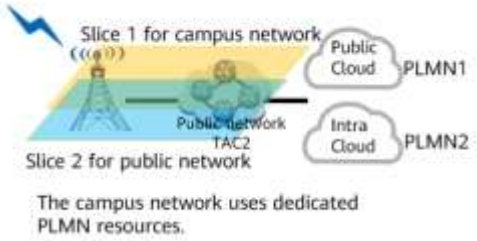


- Для операторов связи, которые используют общие PLMN, но имеют резервные ресурсы спектра, используйте отдельные ресурсы спектра, TA и соты для кампусных и общедоступных сетей.



- У операторов связи, которые не имеют дополнительных ресурсов спектра, кампусные и общедоступные сети должны совместно использовать ресурсы спектра. В этом случае следует предусмотреть объединенную кампусную PLMN для кампусной сети. Базовые станции, которые обслуживают как общедоступные, так и кампусные сети, могут выделять различные доли ресурсов спектра для кампусных и общедоступных сетей на основе информации PLMN.





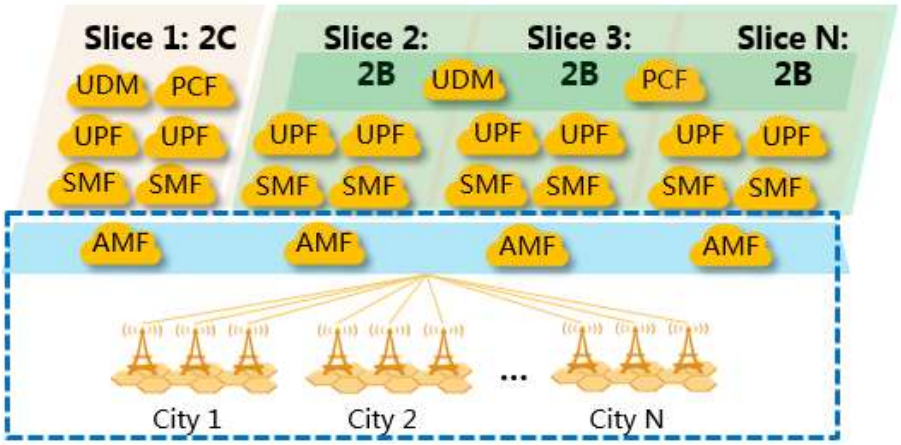
- Базовая станция может распределять различные доли ресурсов спектра по сегментам на основе конфигураций.

Изоляция опорной сети

Режимы работы служб кампусных и общедоступных сетей различаются. Рекомендуется независимо развертывать UDM/PCF в кампусной сети. SMF и UPF могут совместно использоваться разными кампусными сетями или быть изолированы на уровне сегментов.

Однако во избежание массового беспроводного межсетевого соединения рекомендуется, чтобы в кампусных и общедоступных сетях использовался унифицированный AMF, что облегчает управление доступом пользователей с атрибутами как кампусной, так и общедоступной сети в будущем.

Разверните отдельные AMF в кампусной и общедоступной сетях, если срочно требуется изоляция, и операторы связи не беспокоятся о стоимости.



2.2.3 Интеграция сторонних приложений

ETSI MEC01002 определяет интерфейсы управления и процессы управления жизненным циклом приложений, включая процессы загрузки пакетов приложений, создания экземпляров приложений и завершения работы приложений.

Перед созданием экземпляра приложения необходимо загрузить пакет приложения в MEAO через интерфейс Mm1. На рисунке ниже показана процедура загрузки пакета приложения.

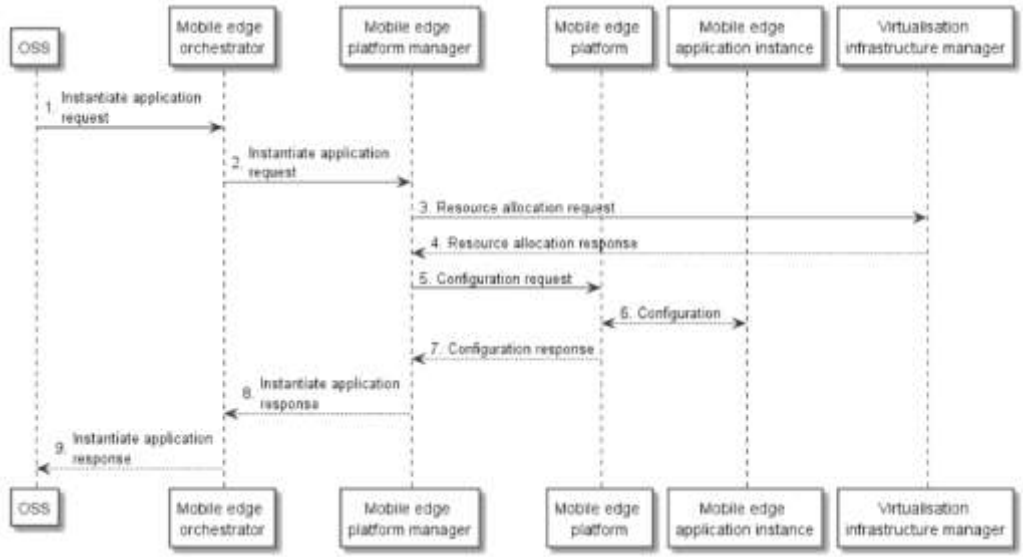
Рис. 2-7 Загрузка пакета приложения

1. OSS направляет запрос на загрузку пакета приложения в MEAO. MEAO выполняет валидацию пакета приложения, проверяет целостность пакета и выполняет аутентификацию.
2. MEAO отвечает на запрос, сохраняет пакет приложения в репозитории программного обеспечения и обеспечивает доступность пакета приложения на периферии.

MEAO поддерживает запросы информации о пакете приложений, отмену регистрации пакетов приложений, активацию и удаление пакетов приложений.

На рисунке ниже показан процесс создания экземпляра

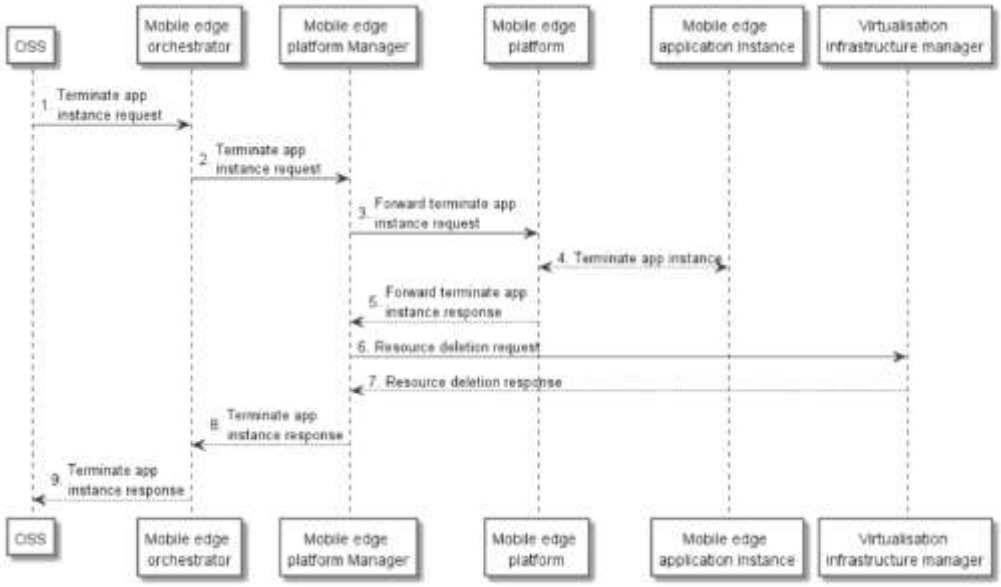
Рис. 2-8 Процесс создания экземпляра



1. OSS направляет запрос в MEAO через интерфейс Mm1.
2. MEAO проверяет и авторизует информацию о конфигурации экземпляра приложения и направляет запрос на создание экземпляра в MEPM через интерфейс Mm3.
3. MEPM отправляет VIM запрос на предоставление ресурсов (ЦП, хранилище и сетевые ресурсы).
4. VIM выделяет ресурсы. Если текущий образ приложения доступен, приложение запускается. Затем VIM направляет ответ MEAO.
5. MEPM направляет сервисную конфигурацию приложения на платформу MEP через интерфейс Mm5, включая правила трафика, правила DNS и другие дополнительные службы, необходимые для приложения.
6. MEP настраивает правила трафика и правила DNS для экземпляра приложения. После правильного запуска экземпляра MEP активирует правила трафика и правила DNS через интерфейс Mp1.
7. Платформа MEP направляет ответ MEPM.
8. MEPM направляет ответ MEAO и возвращает информацию, относящуюся к экземпляру приложения.
9. MEAO направляет ответ OSS.

На следующем рисунке показан процесс завершения работы приложения.

Рис. 2-9 Процесс завершения работы приложения

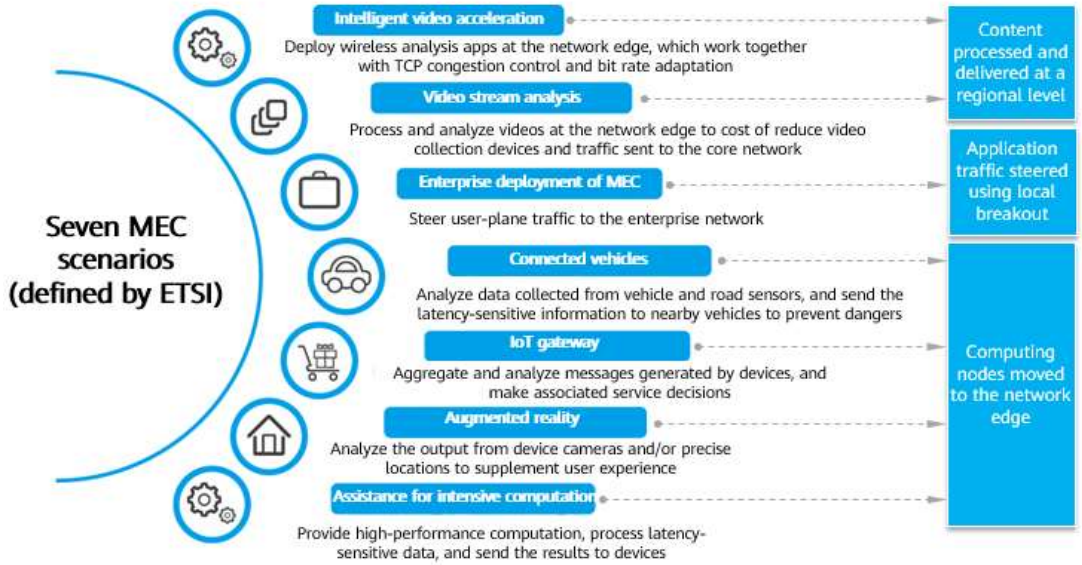


1. OSS направляет запрос на прекращение работы экземпляра приложения в MEAO. Запрос содержит конкретную информацию о приложении.
2. MEAO авторизует запрос, подтверждает, что запрошенный экземпляр существует, и отправляет запрос на завершение работы экземпляра в MEPM.
3. MEPM направляет запрос на прекращение работы экземпляра в MEP.
4. MEP прекращает работу экземпляра приложения.
5. MEP направляет MEPM ответ о завершении работы экземпляра приложения.
6. MEPM направляет VIM запрос на освобождение ресурсов.
7. VIM освобождает ресурсы.
8. MEPM направляет ответ MEAO.
9. MEAO направляет ответ OSS.

2.2.4 Стандартные варианты применения

ETSI представила варианты применения службы MEC, включая интеллектуальное ускорение работы видеосервисов, дополненную реальность, развертывание MEC на предприятии, транспортные средства с сетевым соединением, услуги шлюза IoT, анализ видеопотока и помощь при выполнении интенсивных вычислений. Эти варианты делятся на следующие категории: контент обрабатывается и доставляется на региональном уровне, трафик приложений управляется с использованием схемы обработки запросов на месте, а вычислительные узлы перемещаются на периферию сети.

Рис. 2-10 Семь вариантов применения технологии MEC



Интеллектуальное ускорение работы видеосервисов

Приложения для дистанционного анализа развертываются на периферии сети и работают совместно со службами контроля перегрузки TCP и адаптации скорости передачи данных для повышения эффективности работы видеосервисов.

Анализ видеопотока

Приложения видеоанализа развертываются на периферии сети для идентификации людей, объектов и событий в видео, реализации локальной обработки услуг и уменьшения объема данных, направляемых в опорную сеть.

Развертывание MEC на предприятии

Шлюзы, поддерживающие управление периферийным трафиком, развертываются для точного управления локальными потоками сервисов на предприятии и обеспечения доступа к Интернет-сервисам.

Подключенные автомобили

Серверы V2X развертываются на периферии сети для анализа данных транспортных средств и придорожных датчиков и своевременной передачи данных окружающим транспортным средствам. Приложения для подключенных транспортных средств обычно требуют довольно низкой задержки.

IoT-шлюз

Приложения, связанные с Интернетом вещей, анализируют сообщения, генерируемые устройствами, и принимают соответствующие решения в отношении служб.

Дополненная реальность

Приложения на периферии сети анализируют выходные данные с камер устройств и (или) данные о точном местоположении для повышения уровня взаимодействия с пользователем.

Помощь при выполнении интенсивных вычислений

Приложения MEC обеспечивают высокопроизводительные вычисления, обрабатывают данные, требующие минимальной задержки, и отправляют результаты на устройства.

С точки зрения служебных объектов сценарии применения MEC можно разделить на сценарии для отдельных пользователей, корпоративных пользователей, Интернета вещей и других вертикальных отраслей.

Рис. 2-11 Сценарии применения MEC, классифицированные по служебным объектам

Сценарии 2C

Индивидуально ориентированные сценарии обслуживания, в которых услуги преимущественно требуют низкой задержки и высокой пропускной способности, например облачные игры и потоковая передача VR в реальном времени.

Сценарии 2B

Различные сценарии обслуживания, ориентированные на предприятия и организации, например интеллектуальное производство, здравоохранение и порты.

2.2.5 Уникальные преимущества MEC

Технология MEC предлагает следующие преимущества:

- Более эффективное взаимодействие со службами

  Нисходящее развертывание источников контента и доступ к ближайшему узлу для уменьшения задержки и повышения качества обслуживания.
- Локальная обработка данных

  Обработка запросов на месте на плоскости пользователя для реализации локальной обработки данных на периферии сети и доступа к данным в Интернете
- Частные сети для специализированного использования

  Частные беспроводные и опорные сети для обеспечения более безопасного и надежного сетевого обслуживания

- Интеграция сторонних приложений

  Быстрая интеграция сторонних приложений для расширения возможностей локальных служб и сокращения TTM
- Разработка локальной экосистемы

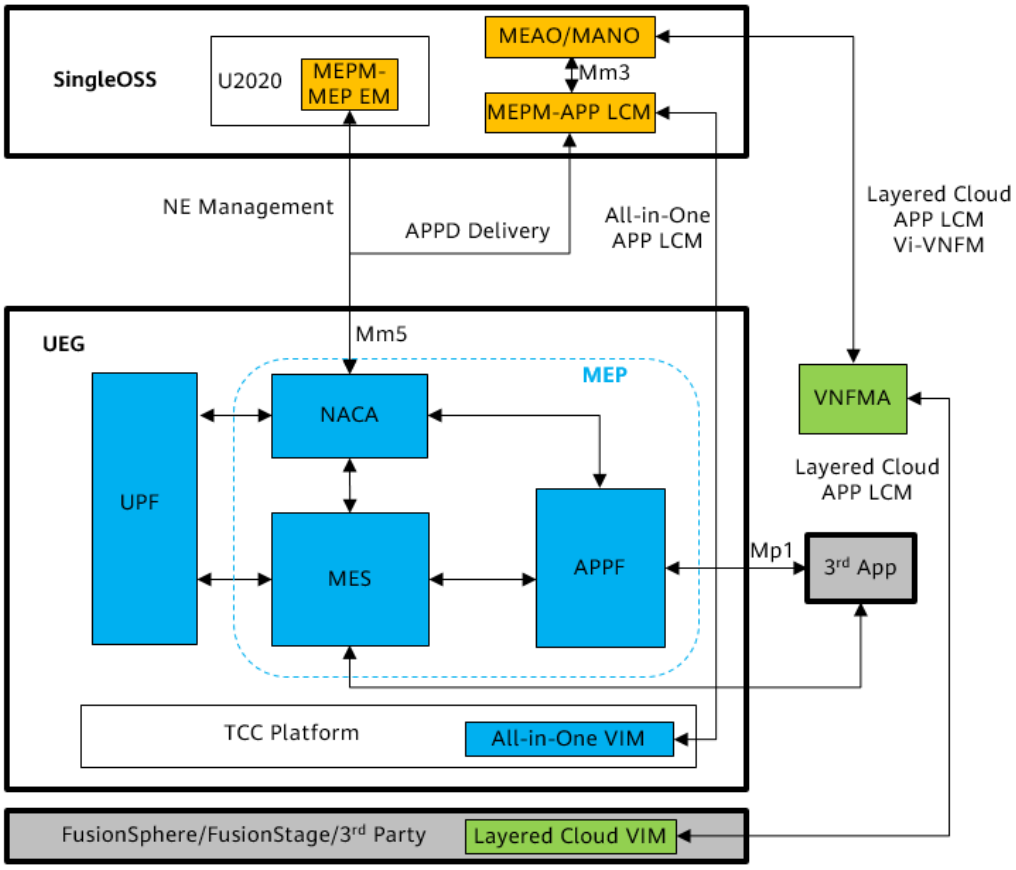
  Возможности управления услугами и функциями для создания локальной экосистемы

2.3 Технология Huawei MEC

2.3.1 Архитектура решения

На Рис. 2-12 показана архитектура решения Huawei MEC, усовершенствованного на основе архитектуры MEC ETSI.

Рис. 2-12 Архитектура решения MEC



Функции подсистемы:

- **MEAO**: стандартная функция MEAO, реализованная посредством усовершенствования MANO, включая подключение и завершение работы приложений, управление пакетами программного обеспечения и управление авторизацией API-интерфейсов доступа к периферийной сети.
- **MEPM**: стандартная функция MEPM, реализованная посредством усовершенствования MANO, в том числе:

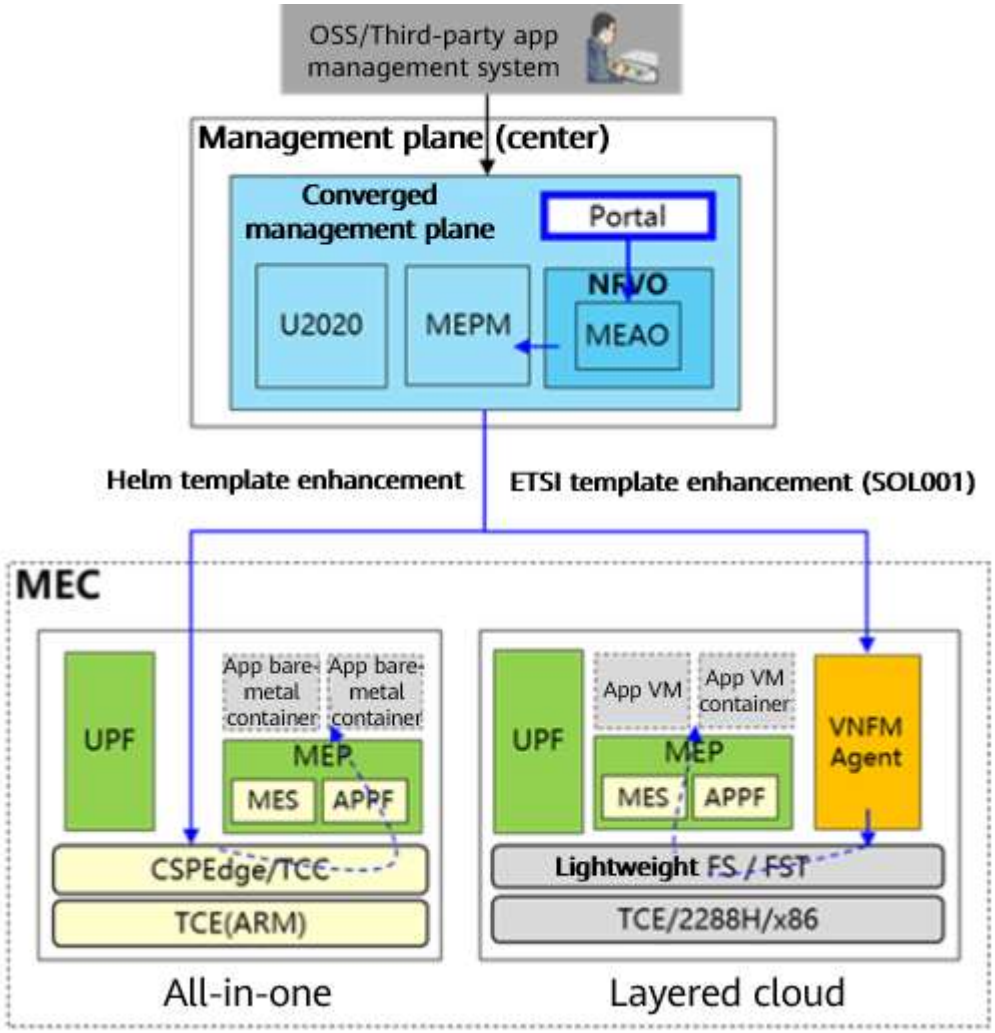
  - MEPM-MEP EM для конфигурации APPF и MES, а также эксплуатации и технического обслуживания, реализованные посредством расширения U2020;
  - MEPM-APP LCM для универсального приложения APP LCM, ARRM (создание APPD, охватывающих правила и требования приложений) и контроль авторизации API-интерфейсов доступа к периферийной сети, реализованные посредством усовершенствования MANO.
- **NACA**: агент NAC, который добавляет MES в центральный узел для управления и регистрации услуг и осуществляет управление жизненным циклом MES, включение услуг и устранение неполадок, а также синхронизацию конфигурации MES и APPF, и агент по эксплуатации и техническому обслуживанию (O&M).
- **MES**: служба MEC, включая междоменный шлюз передачи данных, приложение LB, службу DNS и FW/NAT.
- **APPF**: инфраструктура APP, которая реализует такие функции, как управление службами приложений ME и проверка работоспособности, а также открытый шлюз API.
- **VNFMA**: агент VNFM, который представляет собой функцию агента VNFM, развернутую на периферийных узлах. В многоуровневом облачном сценарии он управляет жизненным циклом UPF, MEP, приложениями и MES.
- **UPF**: предоставляет такие услуги, как LBO служебных данных (UL CL и DNS LBO), тарификация услуг LBO и оповещение о состоянии служб (SA).

2.3.2 Сервисная процедура

Процедура интеграции приложений

Решение Huawei MEC соответствует стандартам ETSI для интеграции приложений. На Рис. 2-13 приведена общая процедура интеграции.

Рис. 2-13 Процедура интеграции приложений



Технология Huawei MEC позволяет оптимизировать интеграцию приложений в следующих аспектах:

- Подготовка приложений в сети управления, оркестрация шаблонов на основе мастера и гибкая разработка шаблонов развертывания.
- Шаблон оркестрации ресурсов. Технология Huawei MEC поддерживает стандарты ETSI и оркестрацию ресурсов приложений BM для сценария многоуровневого облака.

Примечание: функции подключения и завершения работы приложений для универсального сценария (All-in-One) будут поддерживаться в более поздних версиях 21.X.

Процедура UL CL

Процедура UL CL может быть запущена в следующих случаях:

- DNN+TAI (поддерживается)
- S-NSSAI+TAI (на этапе планирования, в настоящее время не поддерживается)
- Пользовательская подписка + TAI (поддерживается)
- Тестирование службы ADC (на этапе планирования, в настоящее время не поддерживается)

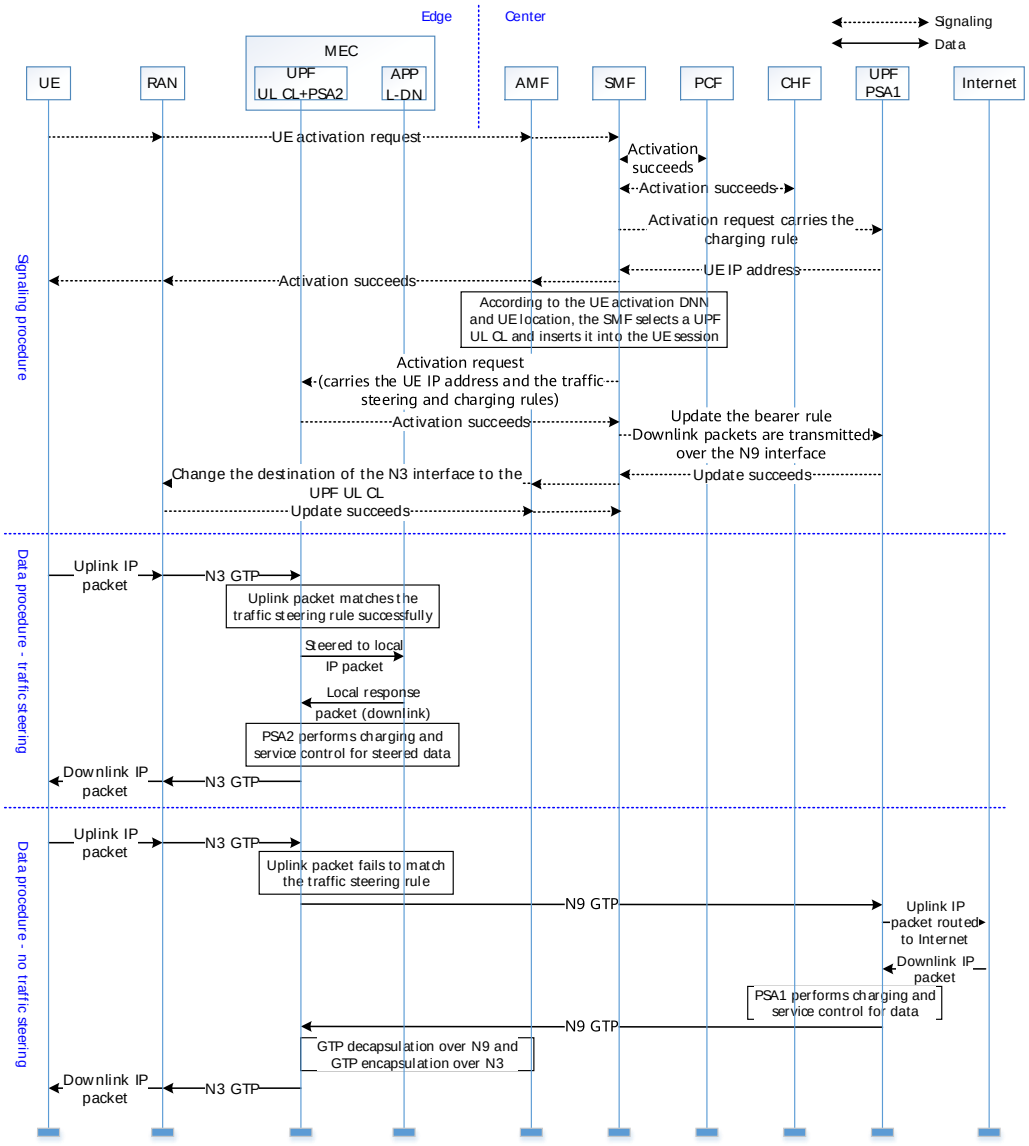
- Влияние функций приложения на маршрутизацию трафика (на этапе планирования, в настоящее время не поддерживается)

Последняя версия 5G Core 21.1 поддерживает вставку UPF UL CL в сеансы UE, инициируемую DNN + TAI или данными подписки + TAI. В следующих разделах описываются сервисные процедуры в двух сценариях: активация UE и изменение местоположения UE. Вставка CL UPF UL в сеансы UE, инициируемая данными подписки + TAI, аналогична вставке, инициируемой DNN + TAI, но действует только для абонентов с подпиской на соответствующие услуги.

Процедура UL CL, инициируемая DNN + TAI при активации UE

Выбор и вставка UPF UL CL, инициируемые DNN + TAI, могут быть реализованы следующим образом: SMF выбирает UPF UL CL при активации UE и вставляет в сеанс UE. Либо сопоставление DNN + TAI не выполняется во время активации UE, и SMF выбирает CL UPF UL и вставляет в сеанс UE, когда местоположение UE меняется, и сопоставление DNN + TAI успешно выполняется.

На следующем рисунке показана процедура запуска вставки UPF UL CL, когда DNN, к которому обращается UE, и место, где UE активируется, соответствуют правилу DNN + TAI при активации UE.



- Процедура сигнализации:

1. UE успешно активировано.
2. UPF PSA1, якорь, выбранный для начальной активации UE, выделяет IP-адрес для UE.
3. На основании DNN активации UE и местоположения SMF выбирает UPF, который соответствует настроенному правилу DNN + TAI, и вставляет UPF в сеанс PDU UE как UL CL.
4. Через интерфейс N4 с UPF UL CL + PSA2 MEC функция SMF направляет инструкции UPF UL CL + PSA2 о создании контекста UE и направлении правил управления трафиком и тарификации для сеанса UE.
5. SMF дает UPF PSA1 инструкции по указанию, что пакеты нисходящей линии связи для сеанса PDU UE, полученные через интерфейс N6, отправляются через интерфейс N9.
6. AMF информирует интерфейс RAN N3, что одноранговым узлом туннеля GTP является UL CL UPF.

- Процедура передачи данных с функцией управления трафиком:

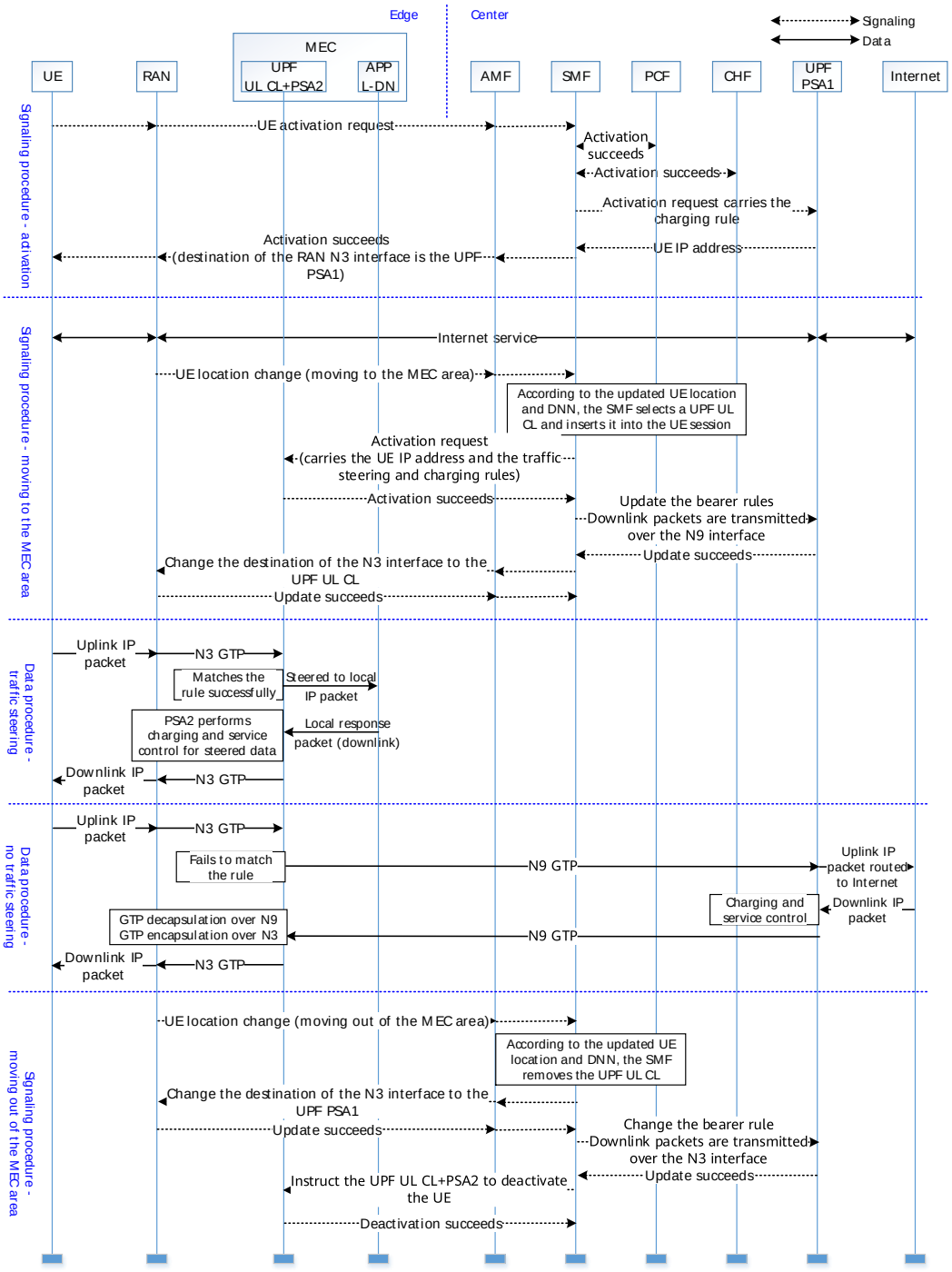
1. UE отправляет IP-пакет восходящей линии связи. gNodeB инкапсулирует пакет в пакет GTP, предназначенный для UPF UL CL.
2. UL CL UPF успешно сопоставляет пакет GTP с правилом управления трафиком, декапсулирует пакет GTP и направляет IP-пакет в локальный DN/APP через интерфейс N6 PSA2.
3. Пакет ответа нисходящей линии связи возвращается в UPF PSA2 на основе маршрута, заявленного сервером NAT, или по туннелю через интерфейс N6. UPF PSA2 осуществляет тарификацию и управление услугами для данных восходящей и нисходящей линий связи управляемого пакета.
4. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

- Процедура передачи данных без функции управления трафиком:

1. UE отправляет IP-пакет восходящей линии связи. gNodeB инкапсулирует пакет в пакет GTP, предназначенный для UPF UL CL.
2. UL CL UPF сопоставляет пакет GTP с правилом управления трафиком, но безуспешно, декапсулирует пакет с использованием GTP через интерфейс N3 и инкапсулирует пакет в пакет GTP через интерфейс N9. Одноранговым узлом туннеля является UPF PSA1.
3. UPF PSA1 декапсулирует пакет GTP через интерфейс N9 и направляет пакет восходящей линии связи в Интернет через интерфейс N6.
4. Пакет ответа нисходящей линии связи возвращается в UPF PSA1 на основе маршрута, заявленного сервером NAT. UPF PSA1 выполняет тарификацию и управление услугами для данных восходящей и нисходящей линии связи неуправляемого пакета, инкапсулирует данные с использованием GTP через интерфейс N9 и направляет в CL UPF UL.
5. UPF UL CL инкапсулирует пакет GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

Процедура UL CL, инициируемая DNN + TAI при изменении местоположения UE

Изменение местоположения UE может инициировать вставку или удаление UL CL, как показано на следующем рисунке.



- Процедура сигнализации — активация:

1. UE успешно активировано.
2. UPF PSA1, якорь, выбранный для начальной активации UE, выделяет IP-адрес для UE.
3. Пунктом назначения интерфейса RAN N3 является UPF PSA1.

- Процедура сигнализации — перемещение в область MEC:

1. UE обращается к сети Интернет через интерфейс N6 UPF PSA1.
2. UE перемещается в область MEC.

3. На основании DNN, к которому обращается UE, и последнего местоположения (TAI) SMF выбирает UPF, который соответствует настроенному правилу DNN + TAI, и вставляет UPF в сеанс PDU UE как UL CL.
4. Через интерфейс N4 с UPF UL CL + PSA2 MEC функция SMF направляет инструкции UPF UL CL + PSA2 о создании контекста UE и направлении правил управления трафиком и тарификации для сеанса UE.
5. SMF дает UPF PSA1 инструкции по указанию, что пакеты нисходящей линии связи для сеанса PDU UE, полученные через интерфейс N6, отправляются через интерфейс N9, но не N3.
6. AMF информирует интерфейс RAN N3, что одноранговый узел туннеля GTP изменился с UPF PSA1 на UPF UL CL.

- Процедура передачи данных с функцией управления трафиком:

1. UE отправляет IP-пакет восходящей линии связи. gNodeB инкапсулирует пакет в пакет GTP, предназначенный для UPF UL CL.
2. UL CL UPF успешно сопоставляет пакет GTP с правилом управления трафиком, декапсулирует пакет GTP и направляет IP-пакет в локальный DN/APP через интерфейс N6 PSA2.
3. Пакет ответа нисходящей линии связи возвращается в UPF PSA2 на основе маршрута, заявленного сервером NAT, или по туннелю через интерфейс N6. UPF PSA2 осуществляет тарификацию и управление услугами для данных восходящей и нисходящей линий связи управляемого пакета.
4. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

- Процедура передачи данных без функции управления трафиком:

1. UE отправляет IP-пакет восходящей линии связи. gNodeB инкапсулирует пакет в пакет GTP, предназначенный для UPF UL CL.
2. UL CL UPF сопоставляет пакет GTP с правилом управления трафиком, но безуспешно, декапсулирует пакет с использованием GTP через интерфейс N3 и инкапсулирует пакет в пакет GTP через интерфейс N9. Одноранговым узлом туннеля является UPF PSA1.
3. UPF PSA1 декапсулирует пакет GTP через интерфейс N9 и направляет пакет восходящей линии связи в Интернет через интерфейс N6.
4. Пакет ответа нисходящей линии связи возвращается в UPF PSA1 на основе маршрута, заявленного сервером NAT. UPF PSA1 выполняет тарификацию и управление услугами для данных восходящей и нисходящей линии связи неуправляемого пакета, инкапсулирует данные с использованием GTP через интерфейс N9 и направляет в CL UPF UL.
5. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

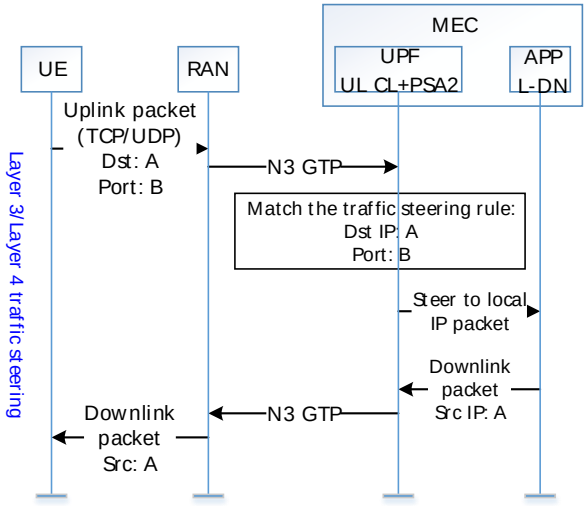
- Процедура сигнализации — перемещение из области MEC:

1. UE перемещается из области MEC.
2. На основании DNN, к которому обращается UE, и последнего местоположения (TAI) SMF определяет, что TAI UE не соответствует списку TAI для UPF UL CL, настроенному в SMF, и UPF UL CL вставлен в сеанс UE, после чего удаляет вставленный CL UPF UL.
3. AMF информирует интерфейс RAN N3, что одноранговый узел туннеля GTP изменился с UPF UL CL на UPF PSA1.
4. SMF дает UPF PSA1 инструкции по указанию, что пакеты нисходящей линии связи для сеанса PDU UE, полученные через интерфейс N6, отправляются через интерфейс N3, но не N9.
5. Через интерфейс N4 с UPF UL CL + PSA2 MEC, SMF направляет UPF UL CL + PSA2 инструкции представить результаты тарификации и статистику трафика UE, а затем деактивировать UE.

Процедуры управления трафиком в плоскости данных

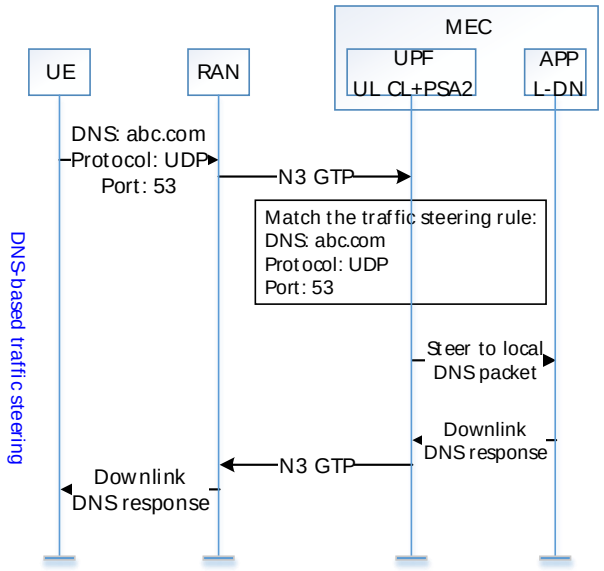
Управление трафиком может осуществляться на основе нескольких правил, например правил уровня 3 / 4 (IP-адрес + номер порта), доменного имени DNS и перенаправления DNS.

- Процедуры управления трафиком в плоскости данных на основе правил уровня 3 / 4 (IP-адрес + номер порта)



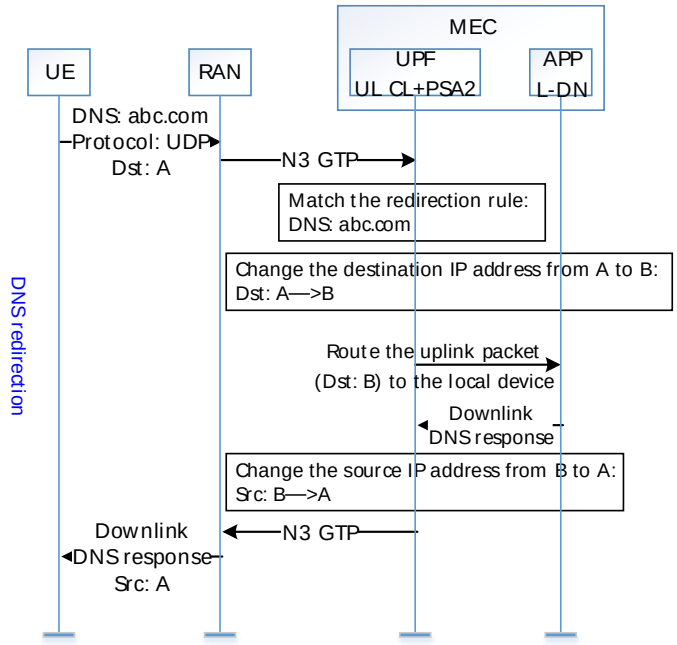
1. UE отправляет IP-пакет восходящей линии связи с использованием TCP или UDP.
2. gNodeB инкапсулирует пакет в пакет GTP через интерфейс N3 с UPF UL CL в качестве пункта назначения.
3. UL CL UPF успешно сопоставляет пакет GTP с правилом управления трафиком уровня 3 / 4 (IP-адрес точки назначения пакета — A, а номер порта — B, как указано в правиле), а затем направляет трафик.
4. UPF UL CL + PSA2 декапсулирует пакет GTP и направляет IP-пакет в локальный DN / APP через интерфейс N6 PSA2.
5. Пакет ответа нисходящей линии связи (IP-адрес источника — A, а номер порта источника — B) возвращается в UPF PSA2 на основе маршрута, заявленного сервером NAT, или по туннелю через интерфейс N6. UPF PSA2 осуществляет тарификацию и управление услугами для данных восходящей и нисходящей линий связи управляемого пакета.
6. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

- Процедура управления трафиком в плоскости данных на основе DNS



1. UE направляет IP-пакет восходящей линии связи с использованием UDP через порт 53, имя домена — **abc.com**. UDP используется, поскольку управление трафиком на основе правил уровня 7 недопустимо для TCP-служб.
2. gNodeB инкапсулирует пакет в пакет GTP через интерфейс N3 с UPF UL CL в качестве пункта назначения.
3. UPF UL CL сопоставляет пакет GTP с правилом управления трафиком по имени домена DNS (тип протокола — UDP, номер порта назначения — 53, имя домена — **abc.com**), а затем направляет трафик.
4. UPF UL CL + PSA2 декапсулирует пакет GTP и направляет IP-пакет в локальный DN / APP через интерфейс N6 PSA2.
5. Пакет ответа нисходящей линии связи (тип протокола — UDP, а номер порта источника — 53) возвращается в UPF PSA2 на основе маршрута, заявленного сервером NAT, или по туннелю через интерфейс N6. UPF PSA2 осуществляет тарификацию и управление услугами для данных восходящей и нисходящей линий связи управляемого пакета.
6. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

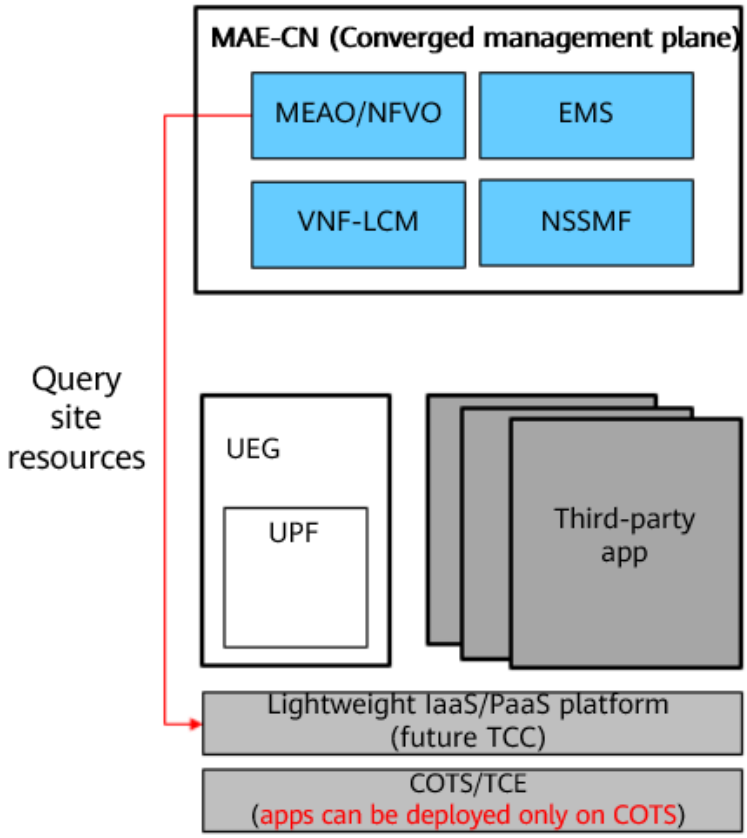
- Процедура перенаправления DNS в плоскости данных



1. UE отправляет IP-пакет восходящей линии связи с использованием UDP через порт 53. IP-адресом пункта назначения является IP-адрес DNS-сервера A, который опорная сеть отправляет на UE через сообщение ответа активации при активации UE, а доменное имя DNS — **abc.com**.
2. gNodeB инкапсулирует пакет в пакет GTP через интерфейс N3 с UPF UL CL в качестве пункта назначения.
3. UPF UL CL сопоставляет пакет GTP с правилом управления трафиком по имени домена DNS (тип протокола — UDP, номер порта назначения — 53, имя домена — **abc.com**), а затем направляет трафик.
4. UPF PSA2 успешно сопоставляет пакет с политикой перенаправления (имя домена DNS — **abc.com**), изменяет IP-адрес пункта назначения пакета запроса DNS с A на B и направляет пакет на локальный DNS-сервер B через интерфейс N6.
5. Пакет ответа нисходящей линии связи (с IP-адресом источника B) возвращается в UPF PSA2 на основе маршрута, заявленного сервером NAT, или по туннелю через интерфейс N6. UPF PSA2 изменяет IP-адрес пункта назначения пакета ответа нисходящей линии связи с B на A.
6. UPF UL CL инкапсулирует пакет с использованием GTP через интерфейс N3 и направляет пакет нисходящей линии связи в gNodeB. gNodeB декапсулирует пакет GTP и направляет IP-пакет нисходящей линии связи в UE.

Процедура управления ресурсами

Процедура управления ресурсами на периферийных узлах

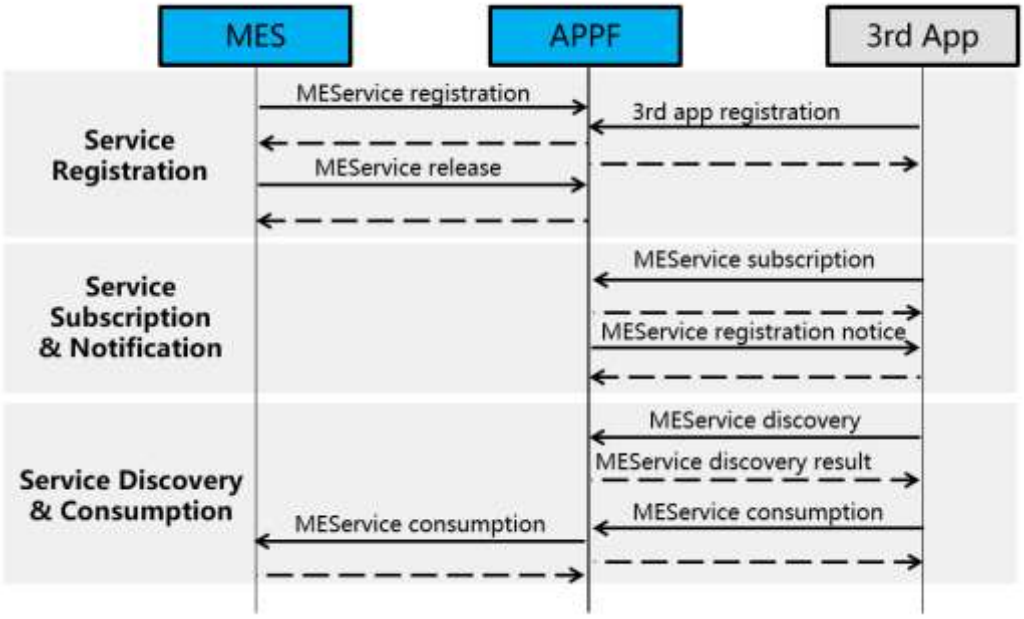


Конвергированная сеть управления позволяет реализовать два режима управления ресурсами:

- Модуль MEAO конвергированной сети управления MAE-CN напрямую вызывает связанные интерфейсы облегченной платформы IaaS/PaaS для запроса общего количества ресурсов, используемых ресурсов и доступных ресурсов на узлах MEC.
- Модуль MEAO конвергированной сети управления MAE-CN резервирует ресурсы при предоставлении ресурсов сторонних приложений, а затем вызывает интерфейсы облегченной платформы IaaS/PaaS для запроса виртуальных ресурсов. Виртуальные ресурсы включают BM, сети и контейнеры.

Процедура управления службами

Процессы управления службами реализуются на периферийных узлах.

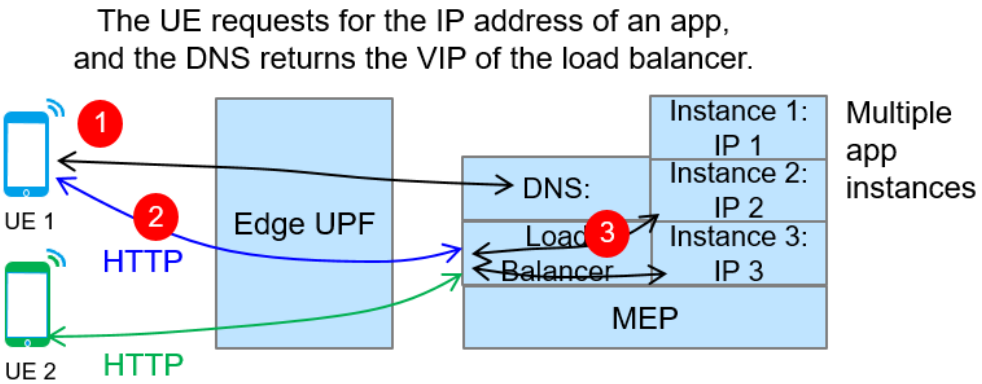


Процедура выглядит следующим образом:

1. MES отправляет в APPF запрос на регистрацию службы (Mp1) для подключения службы к сети. Стороннее приложение направляет в APPF запрос на подключение.
2. Стороннее приложение ориентируется на статус MES из APPF. После регистрации MES APPF направляет уведомление о регистрации стороннему приложению и уведомляет стороннее приложение о том, что MES находится в сети.
3. Стороннее приложение запрашивает в APPF контент службы, предоставляемый MES. APPF возвращает результат обнаружения службы. Стороннее приложение инициирует запрос на использование MES на основе возвращенного результата обнаружения службы для завершения процесса использования службы.

Процедура балансировки нагрузки

Процессы балансировки нагрузки на периферийных узлах:



Процедура выглядит следующим образом:

1. UE запрашивает разрешение доменного имени приложения.

   Если для приложения включена балансировка нагрузки, DNS возвращает UE виртуальный IP-адрес балансировщика нагрузки.
2. UE отправляет запрос услуги на виртуальный IP-адрес балансировщика нагрузки.
3. Балансировщик нагрузки перенаправляет запрос услуги экземпляру приложения на основе политики балансировки нагрузки для обработки услуг.

Экземпляр приложения направляет UE ответ службы по пути, по которому был получен запрос.

Процедура управления полосой пропускания

Платформа MEC обеспечивает для приложений управление полосой пропускания на уровне приложений и на уровне сеанса через интерфейс Mp1. Процесс управления полосой пропускания происходит следующим образом:

1. Приложения запрашивают функцию управления полосой пропускания на уровне приложений или на уровне сеанса на платформе MEC. Платформа MEC идентифицирует эти приложения на основе имен приложений и идентифицирует сеансы на основе имен приложений и пятиэлементных структур.
2. Когда UE направляют пакеты для доступа к этим приложениям, платформа MEC идентифицирует их и контролирует полосу пропускания для пакетов данных. Это гарантирует, что пропускная способность служебных потоков поддерживается в пределах заданного диапазона. Платформа MEC управляет служебными потоками восходящей и нисходящей линий связи отдельно.

2.4 Основные преимущества решения

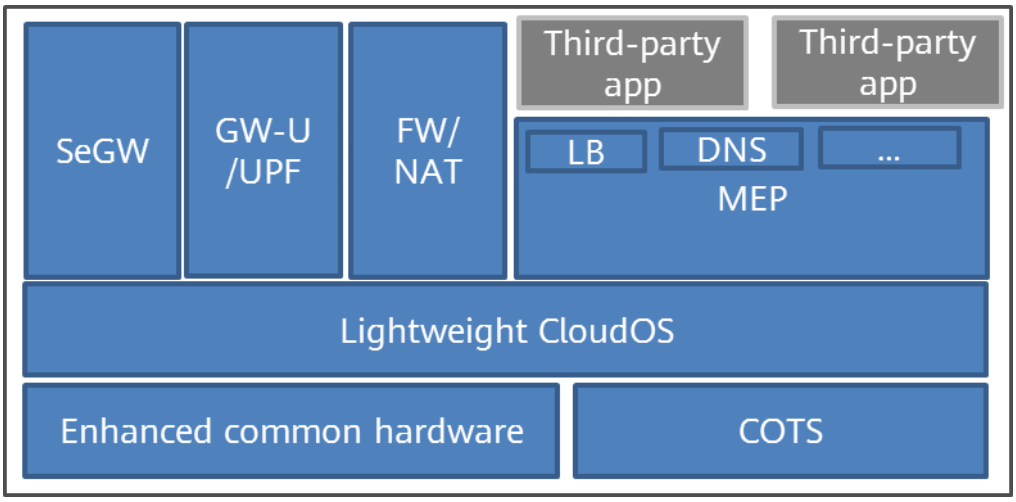
2.4.1 Единая плоскость пользователя

MEC развертывается на периферийных узлах, где сетевые условия значительно различаются, а условия развертывания относительно неблагоприятны. Помимо общих служебных функций, для успешного развертывания шлюза MEC на периферии сети также требуются такие функции, как упрощенное развертывание и сниженные сетевые требования.

Шлюз Huawei MEC поддерживает совместное развертывание UPF и MEP и предоставляет встроенные SeGW, NAT/FW, DNS и LB, обеспечивая универсальное развертывание в плоскости пользователя.

Если на периферии сети требуется безопасное подключение, функция IPsec встроенного SeGW может использоваться для подключения к gNodeB со стороны беспроводной сети и (или) к шлюзу безопасности со стороны опорной сети через туннели IPsec для реализации безопасного подключения для периферийных данных. В периферийных сценариях, если внешний брандмауэр не развернут по причине сетевых ограничений, встроенный NAT/FW может использоваться для трансляции IP-адреса UE и изоляции интерфейса N6 из соображений безопасности, что позволяет снизить сетевые требования. Если стороннему приложению, интегрированному в MEC, требуется внешний DNS-сервер или функционал LB, встроенные службы DNS и LB MEC могут использоваться для обеспечения разрешения доменных имен и служб LB для приложения. Дополнительный сервер DNS или LB не требуется.

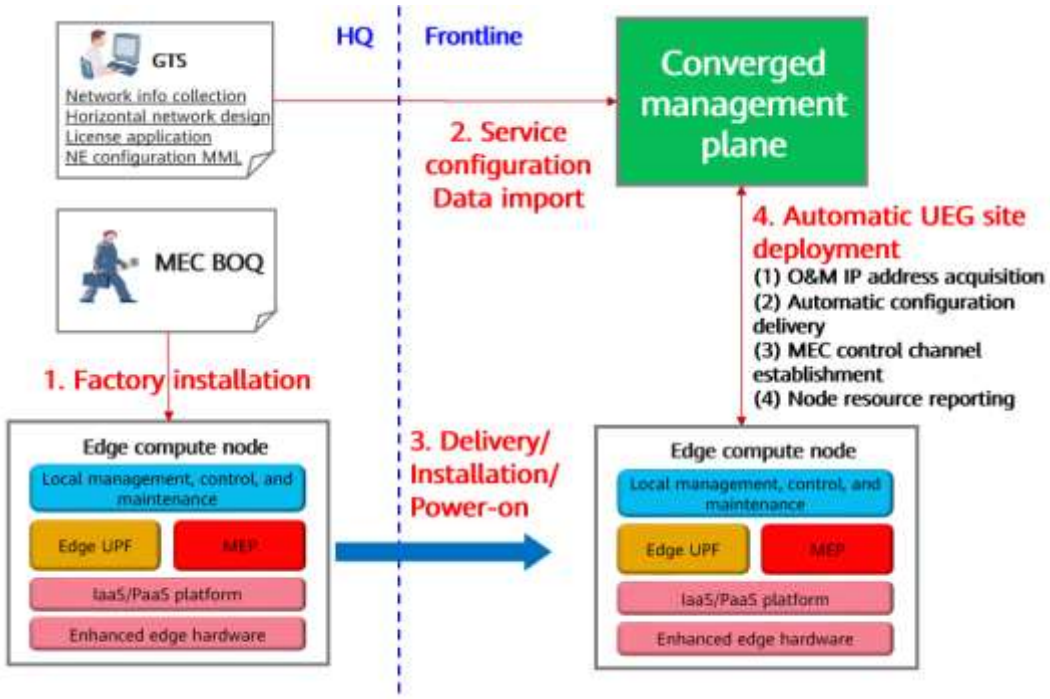
Рис. 2-14 Развертывание единой плоскости пользователя



2.4.2 Автоматическое развертывание объекта

Технология Huawei MEC поддерживает автоматическое развертывание периферийных узлов. Процесс происходит следующим образом:

Рис. 2-15 Процесс автоматического развертывания объекта



Процесс автоматического развертывания объекта включает четыре этапа:

1. Выполнение заводской установки на производственной линии в соответствии с коммерческим предложением (BOQ).

2. GTS завершает проектирование сервисной сети, предоставляет команды настройки служебного MML, подает запрос на выдачу лицензии и импортирует соответствующие данные в конвергированную сеть управления.
3. Оборудование доставляется на первую линию, устанавливается, подключается и включается.
4. IP-адрес O&M меняется, конфигурации служб доставляются автоматически, устанавливаются каналы управления NAC, и сообщаются ресурсы узла. Затем автоматически развертывается объект UEG.

Автоматическое развертывание объекта позволяет повысить эффективность и значительно снизить стоимость развертывания и обслуживания. В различных условиях автоматическое развертывание объекта занимает следующее время:

- Сценарии с облегченными FS+TCE: развертывание объекта занимает не более 1 часа
- Сценарии с CSP Edge+TCE: развертывание объекта занимает не более 15 минут

2.4.3 Единое управление ресурсами

MEAO в MAE-CN отображает, контролирует и авторизует ресурсы всех управляемых объектов MEC по единой методике, упрощая управление ресурсами MEC и O&M.

Рис. 2-16 Пример единого управления ресурсами

2.5 Стандарты и спецификации

MEC соответствует следующим стандартам и спецификациям:

- 3GPP 23.501 Архитектура системы для системы 5G
- 3GPP 23.502 Процедуры для системы 5G
- ETSI GS MEC 003 Технология периферийных вычислений мультисервисного доступа (MEC); инфраструктура и эталонная архитектура
- ETSI GS MEC 011 Технология мобильных периферийных вычислений (MEC); реализация приложения мобильной периферийной платформы

3 Безопасность MEC

3.1 Угрозы безопасности MEC

Риски для продуктов MEC: в отличие от центрального оборудования 5GC, продукты MEC (UPF и MEP) можно развертывать в аппаратном помещении корпоративного кампуса или оператора связи, а также на периферии сети, где существует вероятность несанкционированных физических вторжений. Кроме того, продукты MEC поддерживают установку сторонних приложений. Если такие приложения несут угрозы безопасности, они могут использоваться для создания угрозы в отношении MEC и центрального 5GC.

Риски для сторонних приложений: сторонние приложения могут подвергаться атакам из других приложений или MEC, что приведет к утечке данных и несанкционированному изменению программного обеспечения. Помимо развития собственных возможностей безопасности, сторонние приложения предполагают, что платформа MEC предоставит среду для изоляции ресурсов.

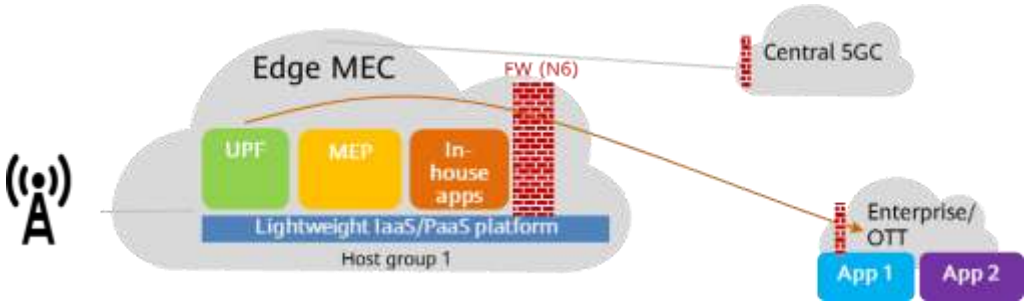
3.2 Решение по обеспечению безопасности MEC

3.2.1 Безопасность продуктов MEC

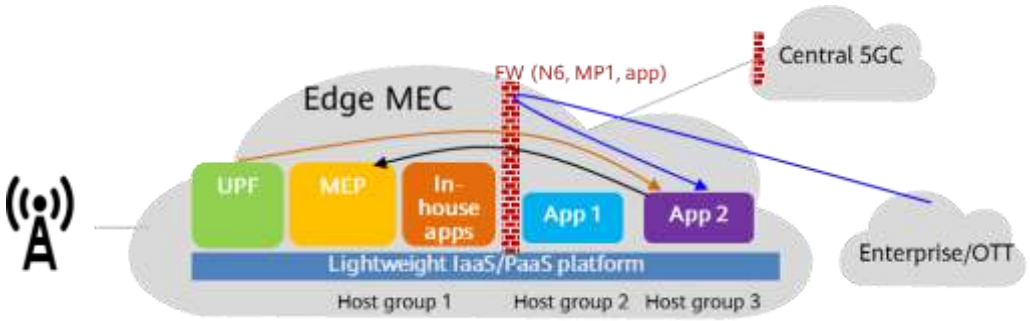
Безопасность сети

Внешние брандмауэры развертываются для изоляции сетей и защиты от угроз.

- Если сторонние приложения не развернуты в MEC, рекомендуется добавлять UPF/MEP/внутренние приложения в защищенную зону, а корпоративные элементы — в незащищенную зону.



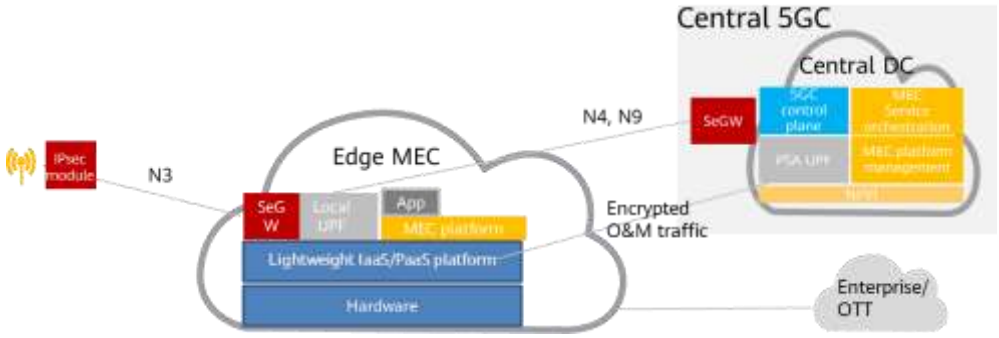
- Если сторонние приложения развернуты в MEC, рекомендуется добавлять UPF/MEP/внутренние приложения в защищенную зону, сторонние приложения — в демилитаризованную зону (DMZ), а корпоративные элементы — в незащищенную зону.



Безопасность передачи данных

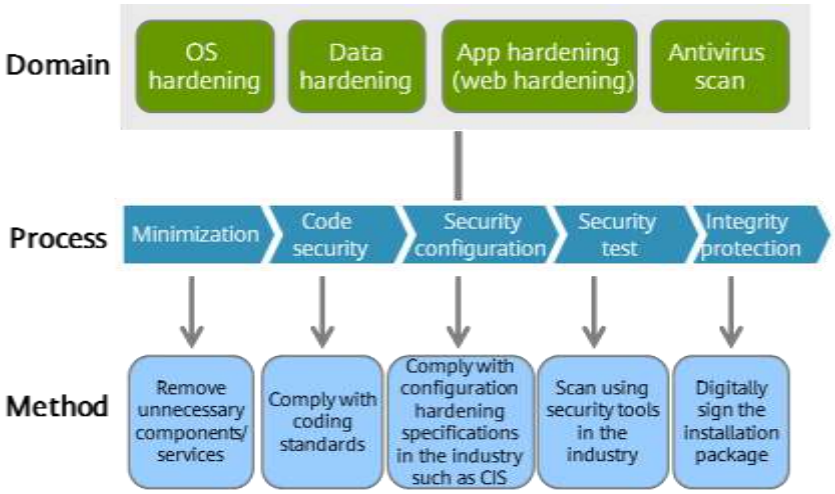
Интерфейсы плоскости управления и плоскости пользователя являются стандартными интерфейсами (N3/N4/N9), определенными 3GPP. Туннели IPsec могут использоваться для защиты их целостности и конфиденциальности. IPsec могут предоставляться через SeGW клиента. IPsec выполняет привязку IP-адресов и обеспечивает взаимодействие только с настроенными IP-адресами.

Центральная плоскость управления и периферийная MEC используют протоколы передачи данных с шифрованием, например TLS, SNMPv3 и SSH.



Безопасность UPF/MEP

Huawei повышает уровень безопасности своих продуктов в соответствии с едиными корпоративными требованиями. Повышение уровня безопасности включает усиление защиты операционной системы, баз данных, усиление защиты на уровне приложений и антивирусное сканирование программных пакетов.



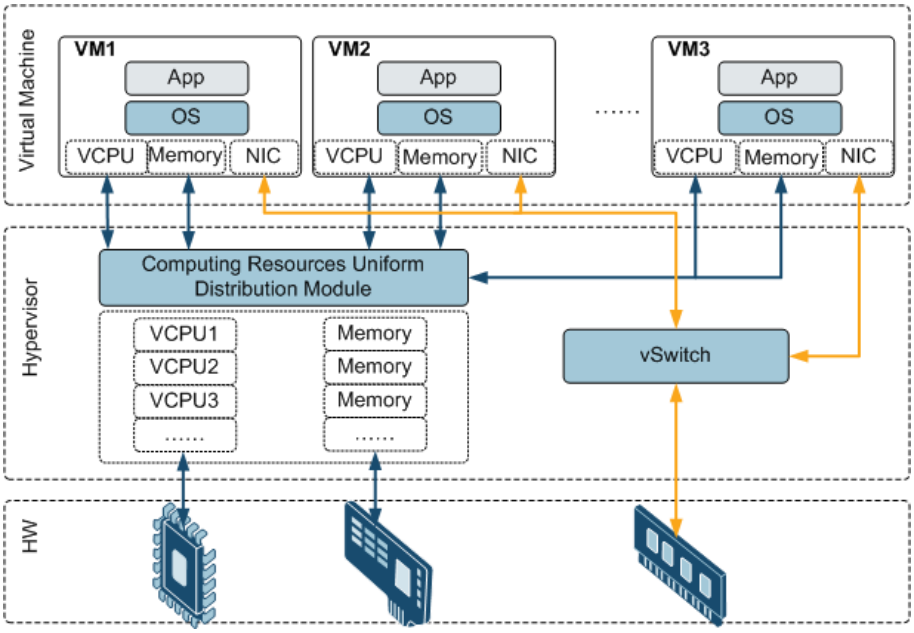
Безопасность виртуализации

В сценариях многоуровневого облачного развертывания единая платформа виртуализации Huawei (UVP) виртуализирует физические ресурсы сервера, например ресурсы ЦП, памяти и ввода-вывода, в группу логических ресурсов, что обеспечивает возможность централизованного управления, гибкого планирования и динамического распределения. Логические ресурсы создают среду на отдельном физическом сервере для одновременной работы нескольких изолированных виртуальных машин.

UVP работает на физических серверах, обеспечивает возможности виртуализации с использованием технологии виртуализации с аппаратной поддержкой (например, Intel VT-x) и предлагает рабочие среды для виртуальных машин. UVP обеспечивает работу виртуальных машин в подходящем пространстве для предотвращения атаки ВМ на UVP или другие ВМ.

Гипервизор изолирует ресурсы для ВМ, работающих на одной физической машине, для предотвращения кражи данных между ВМ, атак или вмешательств. Конечные пользователи могут получить доступ к ресурсам (оборудованию, программному обеспечению и данным) только на своих ВМ. На Рис. 3-1 показана схема изоляции ВМ.

Рис. 3-1 Изоляция ресурсов BM



В сценариях с универсальными устройствами платформа MEC обеспечивает безопасность пустых контейнеров.

- Повышение базового уровня безопасности: помимо исходной изоляции ресурсов контейнеров, платформа MEC обеспечивает повышение уровня безопасности для конфигураций запуска контейнеров на основе тестов Центра интернет-безопасности (CIS) для обеспечения безопасности конфигурации по умолчанию. Меры по повышению уровня безопасности включают конфигурацию безопасности хоста, а также охранный процесс Docker и файл конфигурации.
- Безопасность образа контейнера: так, платформа MEC обеспечивает безопасность процесса сборки, если он выполняется без полномочий root, и не позволяет Dockerfile содержать конфиденциальную информацию.
- Безопасность запуска контейнеров: платформа MEC оценивает занятость ресурсов и осуществляет контроль доступа для запущенных контейнеров, удаляет ненужные порты, монтирует системные файлы как доступные только для чтения и запрещает совместное использование пространства имен. Перед выпуском образы контейнеров проверяются с использованием соответствующих инструментов.

Если сторонние приложения развертываются на платформе MEC, приложения и UPF/MEP не развертываются на одном блейд-сервере, что снижает риск атаки приложений на UPF/MEP после покидания BM или контейнера.

Безопасность аппаратного обеспечения

Включены только интерфейсы, которые должны использоваться в действующей сети. Для всех открытых интерфейсов аутентификация личных данных должна выполняться для любого пользователя или узла связи, которые пытаются получить доступ к интерфейсу. Порты, которые не используются часто, следует включать только при необходимости. При включении порта такого типа в журнал вносится запись, а сигнал оповещения о событии направляется в NMS.

Безопасность аппаратного зала: при соблюдении условий аппаратный зал, в котором развернут периферийный MEC, может быть реконструирован по мере необходимости для обеспечения безопасной и надежной среды для работы.

- Обеспечение физической безопасности: выберите для развертывания место вдали от источников стихийных бедствий, опасностей и помех, принимая во внимание местные политические, географические и климатические факторы, чтобы обеспечить безопасность инженерных коммуникаций и физических сооружений.
- Защита границ: разверните системы контроля доступа, охранной сигнализации и видеонаблюдения для мониторинга и контроля входа и выхода из здания. Убедитесь, что вентиляционные отверстия и кабели соответствуют нормам, для предотвращения проникновения и несанкционированного доступа.
- Система безопасности: классификация на основе ролей, отображение и контроль состояния системы, сигнализация и предварительная обработка сигналов, а также запись и запрос событий.
- Надежность питания: использование источников питания POE/UPS с двумя входами, которые взаимодействуют с системой безопасности. Следует использовать архитектуру B/S для реализации «горячего» резервного копирования двух систем.
- Рекомендуемые стандарты проектирования аппаратного зала: международный стандарт (TIA-942 Стандарт телекоммуникационной инфраструктуры для центров обработки данных), национальный стандарт Китая (GB 50174-2008 Правила проектирования помещений для электронных информационных систем) или другие применимые корпоративные стандарты.

3.2.2 Безопасность приложений

Защита границ: для трафика от интерфейса N6 к приложению можно установить политику доступа брандмауэра на внешнем брандмауэре интерфейса N6 в соответствии с требованиями приложения.

Изоляция безопасности: как VNF приложение работает в контейнере или виртуальной машине, предоставляемых на уровне платформы MEC. Для изоляции приложений используется технология виртуализации или изоляции контейнеров.

Безопасное развертывание приложений: MEAO проверяет цифровую подпись выбранного пакета программного обеспечения приложения. Развертываться могут только действительные приложения.

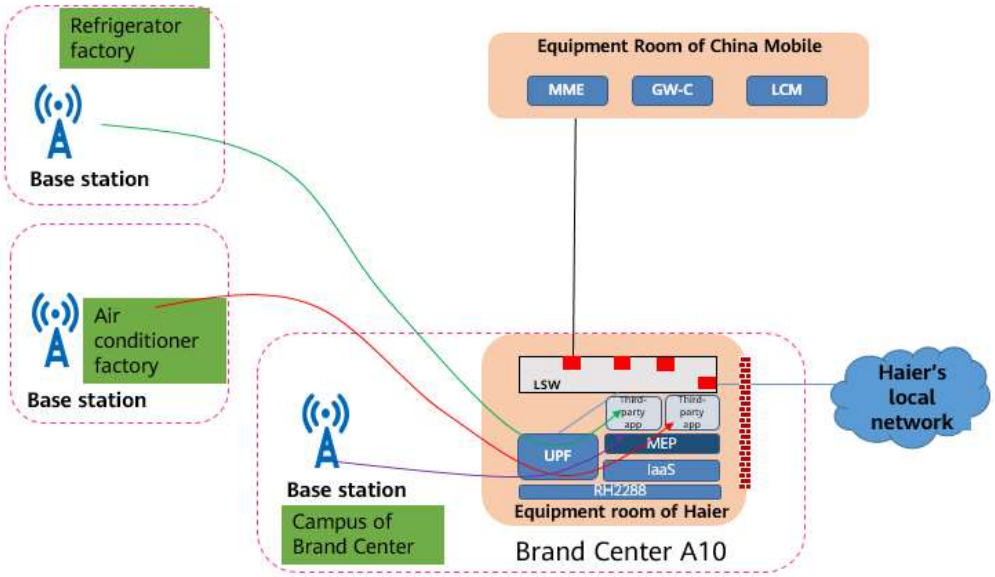
4 Развертывание решения

4.1 Способы и случаи применения

4.1.1 Умное предприятие Haier в Циндао

Умное предприятие, как важный вариант применения технологии 5G MEC, в основном используется для интеллектуального управления, контроля качества, идентификации событий и вспомогательных производственных процессов в промышленной сфере. Технологии машинного обнаружения и распознавания широко применяются в промышленном производстве, но некоторые факторы ограничивают дальнейшее развитие от промышленного производства к умному производству.

Рис. 4-1 Подключение умного предприятия Haier в Циндао к сети



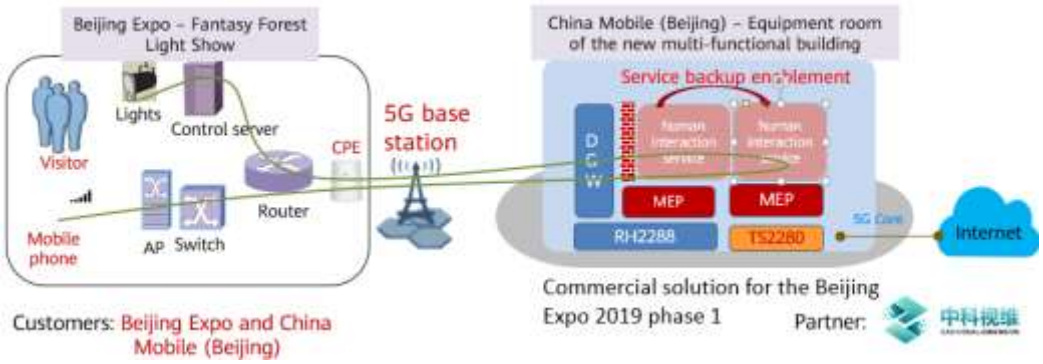
Haier совместно с China Mobile, Huawei и HC Vision (Mstar Technologies) разработали решение 5G + Machine Vision. На основе вычислительных возможностей 5G + MEC машинное зрение выбрано в качестве приложения верхнего уровня для формирования комплексного решения. Приложения машинного зрения развертываются на платформе MEC, что обеспечивает облачное управление, самооптимизацию алгоритмов и безопасность корпоративных данных, которые обрабатываются на локальном уровне. Кроме того, это позволяет избежать таких сложностей

традиционного машинного зрения, как высокая стоимость, ограниченная эффективность и нестабильное качество. Алгоритмы переносятся в облако, что позволяет значительно снизить инвестиционные затраты. Высокоскоростная сеть с малой задержкой делает обнаружение более гибким и значительно повышает эффективность работы. Обработка больших данных и взаимодействие в процессе глубокого обучения позволяют повысить качество. Облачное развертывание значительно ускоряет процессы ввода в эксплуатацию, обслуживания и расширения и делает их более удобными.

4.1.2 Световое шоу «Сказочный лес» на выставке «Пекин Экспо»

Развлекательные приложения и видеоприложения, требующие высокой пропускной способности и низкой задержки, например AR/VR, также являются одним из важных вариантов применения 5G MEC. На Международной садоводческой выставке 2019 года компании Huawei, Beijing CAS-Visual-Dimension Culture Technology и China Mobile совместно представили первое интерактивное световое шоу «Сказочный лес» на основе технологии 5G MEC.

Рис. 4-2 Создание сети светового шоу «Сказочный лес» на выставке «Пекин Экспо»



В течение дня посетители используют приложения на мобильных телефонах, чтобы сканировать павильон и просматривать волшебную сцену в естественной среде с использованием технологии дополненной реальности. Ночью посетители могут активировать устройство распознавания поведения или использовать приложения на мобильных телефонах для управления проекторами, светом, звуком и другим оборудованием, погружаясь в страну чудес.

Это световое шоу предполагает рендеринг виртуальной сцены в реальном времени и управление светотеневыми эффектами. Развернутые на месте серверы помогают произвести столь захватывающее впечатление на посетителей благодаря высокой пропускной способности и низкой задержке. Для облегчения установки вместо проводных датчиков на месте используются беспроводные датчики. Сервер визуализации AR и сервер взаимодействия интегрированы в платформу MEC для реализации универсального развертывания, что позволяет предприятиям снизить расходы на развертывание, эксплуатацию и техническое обслуживание.

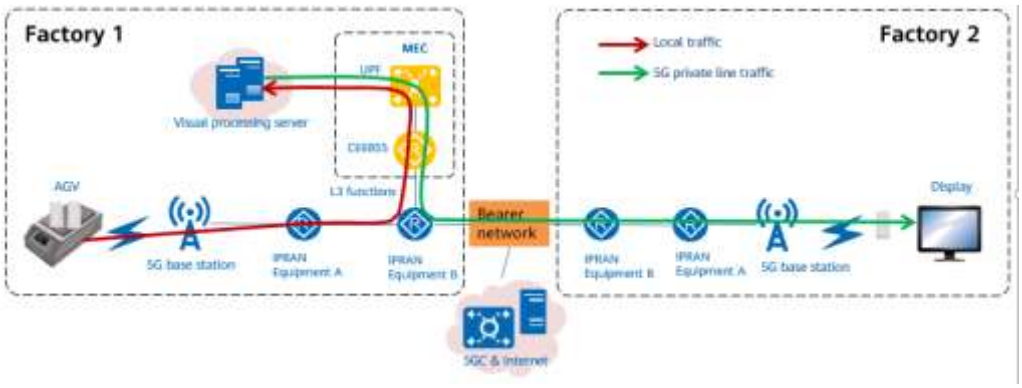
4.1.3 Проект Sany Heavy Industry

С развитием новых информационных технологий, таких как сеть 5G, близится глобальная промышленная революция, и цифровая трансформация уже началась.

Автоматизированное транспортное средство (AGV), обычно используемое на умных предприятиях, оснащено автоматической системой управления. Как правило, маршрут и поведение AGV можно контролировать с помощью коммуникационных технологий. Руководствуясь спросом на полную автоматизацию умных предприятий, AGV развиваются в направлении многофункционального автономного робота, который поддерживает функции обнаружения в реальном времени, идентификации безопасности, избежания множественных препятствий, интеллектуального принятия решений и автоматического выполнения.

Соответственно, AGV предъявляют все более высокие требования к вычислительным возможностям. AGV, использующие локальные вычислительные мощности и режим интеллектуального восприятия на одной машине, являются дорогостоящими и сложными в планировании и управлении, что значительно ограничивает развитие AGV.

Рис. 4-3 Управление AGV через сеть



Инновационный проект AGV на основе 5G MEC, совместно запущенный Sany Heavy Industry, China Telecom и Huawei, предполагает использование исключительно платформы 5G MEC. Платформа достаточно надежна, чтобы интегрировать сторонние приложения и вычислительные возможности графического процессора, и может выполнять задачи повторного вычисления визуального и лазерного радиолокационного восприятия AGV, преодолевая ограничения вычислительных возможностей AGV. Это позволяет значительно упростить функции и снизить затраты для отдельного AGV, а также повысить уровень интеллектуальности и стандартизации AGV. Сквозная задержка поддерживается на уровне миллисекунд с учетом сбора информации, интеллектуального анализа и обработки на периферии, а также действий, предпринимаемых на основе команд управления. Это решение в сочетании с технологией V2X обеспечивает защиту AGV во многих аспектах, позволяет реализовать интеллектуальную сеть и повысить эффективность планирования производства и способствует переходу от AGV к автономному мобильному роботу следующего поколения с интеллектуальным подключением (AMR). Это также выводит AGV на широкие промышленные рынки.

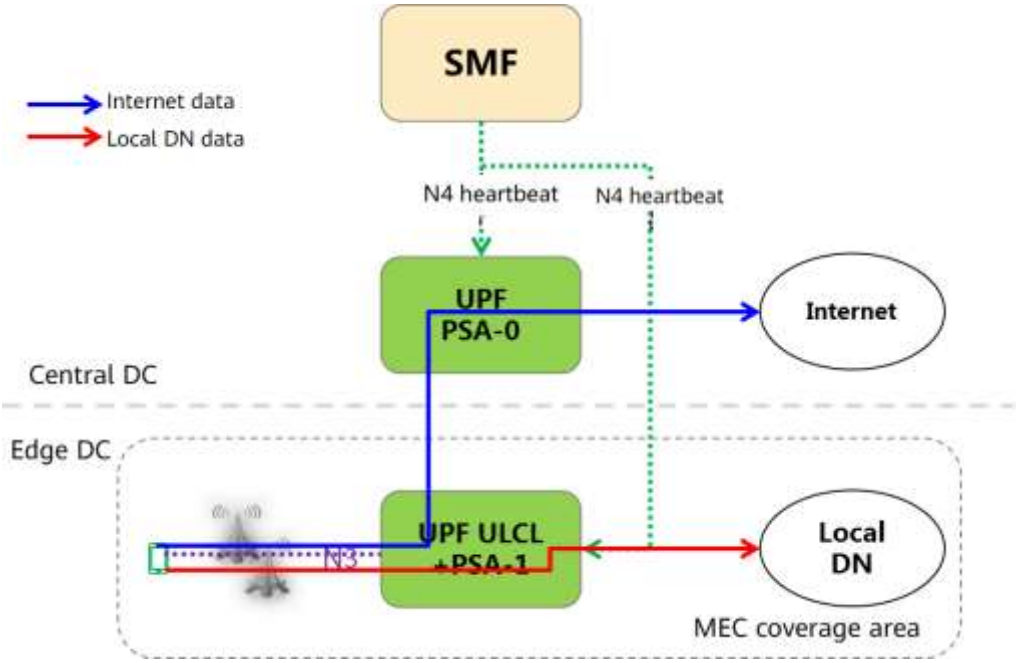
4.2 Политика развертывания

4.2.1 Обработка запросов на месте в кампусе

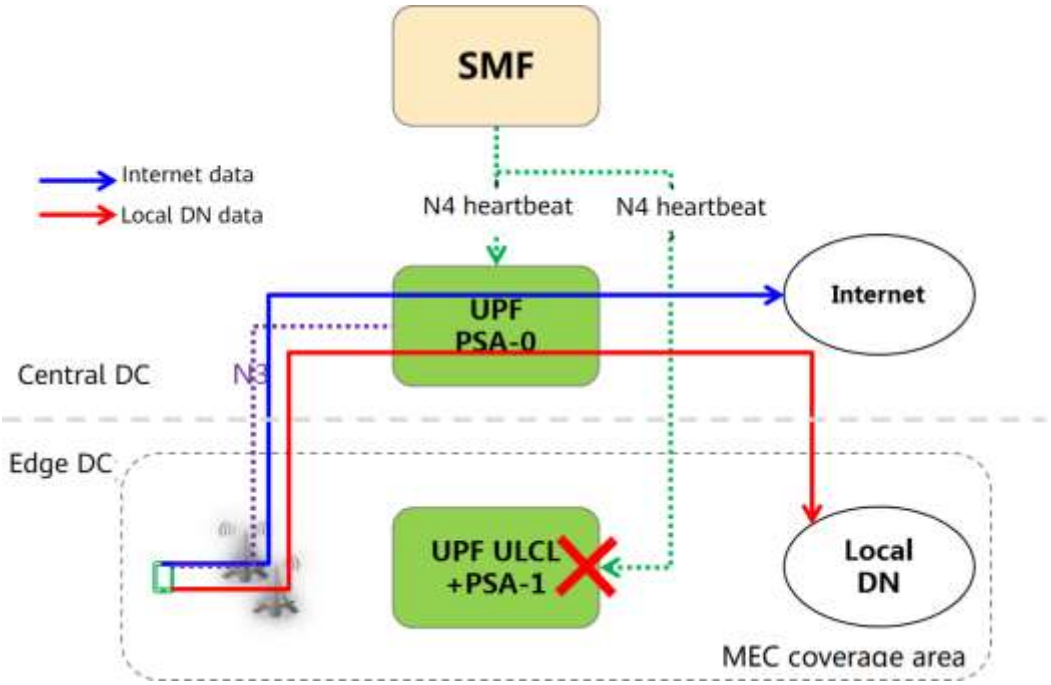
Что касается обработки запросов на месте в кампусе, рекомендуется, чтобы система MEC была развернута в кампусной сети как UL CL + PSA (классификатор восходящей линии связи и основной якорь) и направлена в локальную кампусную сеть через интерфейс N6. Политика развертывания подразделяется на два сценария:

Обработка запросов на месте в общедоступной кампусной сети

Если локальная кампусная сеть является общедоступной, любой выход из общедоступной сети может направлять данные в локальную сеть. При развертывании MEC требуется низкий уровень надежности. Поэтому рекомендуется развернуть одну систему MEC в кампусной сети для обработки запросов на месте. Процедура показана на следующем рисунке:



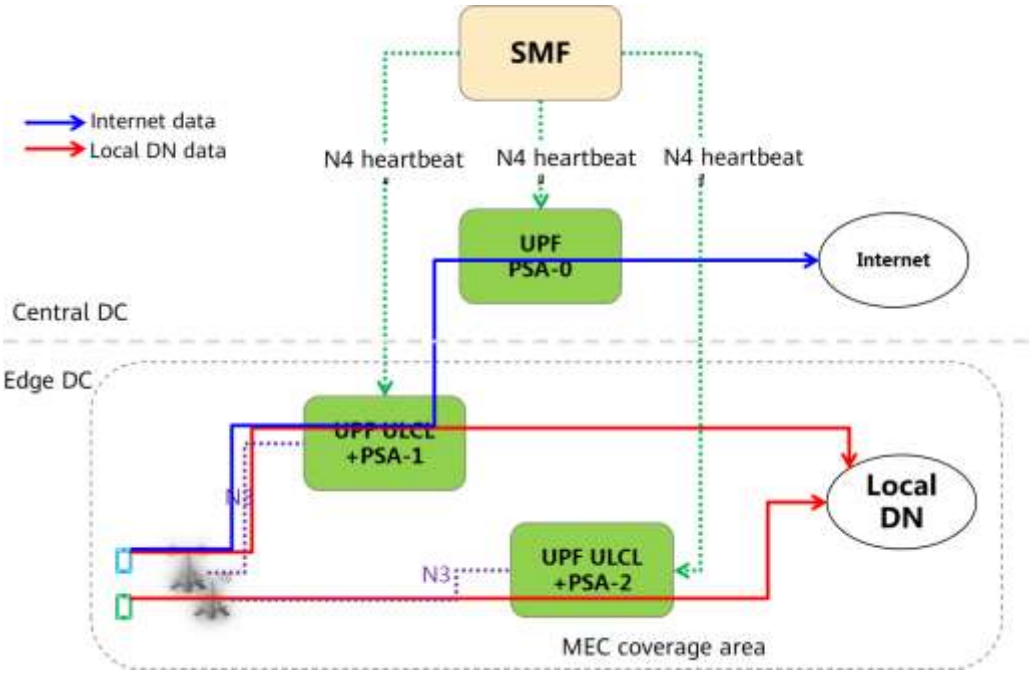
На периферийном узле, где развернута система MEC, доступ к локальным службам можно получить из общедоступной сети. Таким образом, IP-адрес DN или приложения представляет собой общедоступный IP-адрес. Рекомендуется развертывание UPF UL CL + PSA MEC на одном узле. Когда периферийные пользователи обращаются к локальным службам, MEC распределяет данные в локальную DN/приложение. Когда периферийные пользователи получают доступ в Интернет, служебный поток сначала сопоставляется на основе правила MEC, а затем направляется в Интернет через центральный основной якорь UPF.



Если MEC в кампусе выходит из строя, SMF удаляет некорректный UPF UL CL из пользовательского сеанса. Локальные сервисы и интернет-сервисы направляются в локальную сеть DN и Интернет через центральный основной якорь UPF и интерфейс N6.

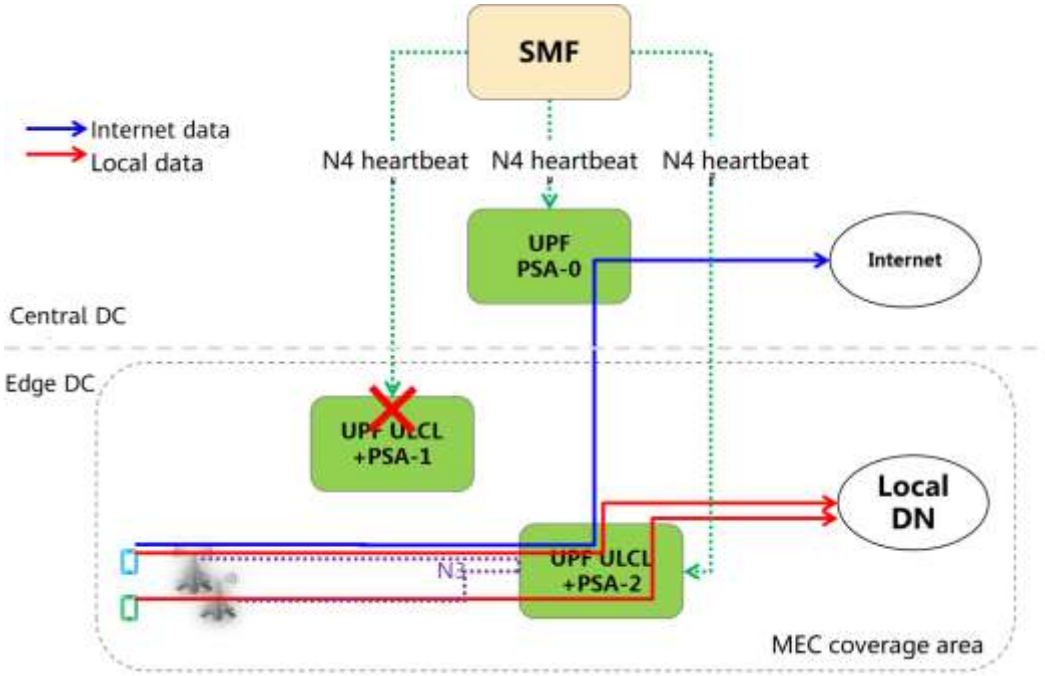
Обработка запросов на месте в кампусной сети LAN

Если локальная кампусная сеть является сетью LAN, к ней нельзя получить доступ в режиме обхода через центральный UPF, если он не подключен к другим сетям. При развертывании MEC требуется высокий уровень надежности. Поэтому рекомендуется использовать UPF UL CL + PSA с двойным активным распределением нагрузки в качестве классификатора трафика MEC для обработки запросов на месте в кампусной сети. Процедура показана на следующем рисунке:



На периферийном узле, где развернута система MEC, доступ к локальным службам можно получить через LAN. Таким образом, IP-адрес DN или приложения представляет собой частный IP-адрес. Рекомендуется развертывание UPF UL CL + PSA MEC в режиме двойного активного распределения нагрузки.

SMF выбирает два двойных активных UPF по очереди как UL CL для вставки сеансов для UE. Например, когда периферийный пользователь A обращается к локальным службам, UPF-1 направляет трафик в локальную сеть DN/приложение. Когда периферийный пользователь B обращается к локальным службам, UPF-2 направляет трафик в локальную сеть DN/приложение. Когда периферийные пользователи получают доступ в Интернет, служебные потоки сначала направляются в Интернет на основе правил сопоставления UPF UL CL, интегрированных в каждый сеанс, а затем направляются в Интернет через центральный основной якорь UPF.

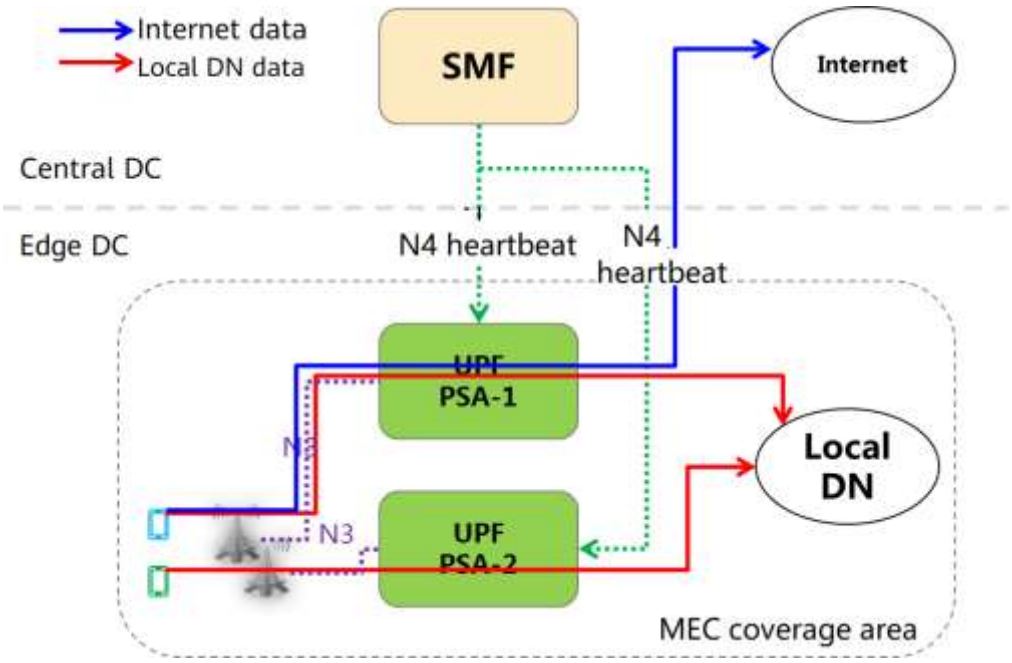


Если один из UPF UL CL + PSA MEC, развернутых в режиме двойной активности в кампусе, выходит из строя, SMF удаляет некорректный UPF UL CL из пользовательского сеанса и вставляет другой, корректный UPF UL CL + PSA. Что касается локальных услуг, все локальные пользователи получают доступ к локальному DN/приложению после того, как обычный UPF UL CL используется для обработки запросов на месте. Что касается Интернет-услуг, локальные пользователи направляются в Интернет через интерфейс N6 центрального основного якоря UPF после обработки запросов на месте с использованием обычного периферийного UPF.

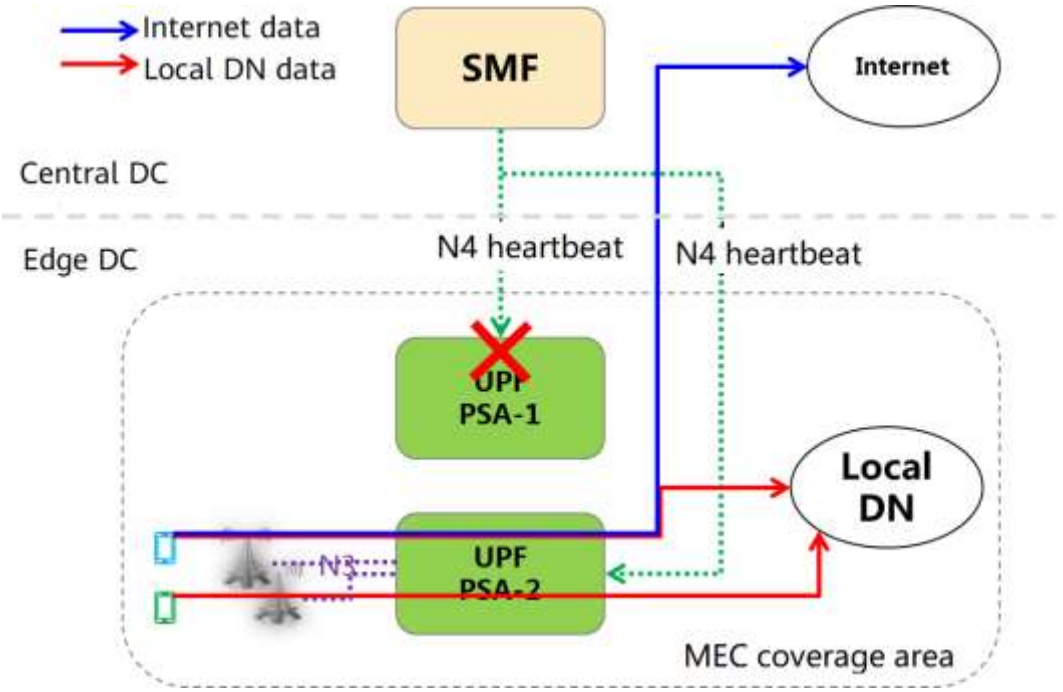
Выгрузка данных в локальном кампусе

Если кампусным службам требуется доступ как к локальной сети, так и к Интернету (выход общедоступной сети развернут на территории кампуса), а для кампуса планируется независимое DNN, рекомендуется развернуть основной якорь UPF на периферийном узле. Развертывание MEC должно иметь высокий уровень надежности. Рекомендуется развертывание UPF с двойным активным распределением нагрузки в качестве основных якорей для разгрузки данных кампуса.

Пример показан на рисунке ниже:



SMF поочередно выбирает два двойных активных UPF в качестве основного якоря для сеанса UE. Например, когда абонент периферийной сети A обращается к локальным службам, SMF направляет запрос услуги в локальную сеть DN/приложение и Интернет через UPF PSA-1. Когда абонент периферийной сети B обращается к локальным службам, SMF направляет запрос услуги в локальную сеть DN/приложение и Интернет через UPF PSA-2.



Когда один из двух активных якорей UPF, развернутых для MEC в кампусе, выходит из строя, например SMF путем отправки контрольных сообщений N4 обнаруживает, что UPF PSA-1 неисправен, SMF отключает абонентов на UPF PSA-1. После повторного подключения абонента SMF выбирает UPF PSA-2 для создания сеанса абонента. Такой метод гарантирует, что рабочий UPF может принять сервисы от основного якоря UPF в случае отказа основного якоря.

4.2.2 Частные кампусные сети

Более высокие требования по изоляции частной кампусной сети требуют больше ресурсов. Выбор изоляции беспроводной и (или) опорной сети предлагается в зависимости от условий операторов связи.

В сценарии изоляции беспроводной сети рекомендуется, чтобы операторы с незанятыми спектрами совместно использовали PLMN, а кампус имел эксклюзивные спектры, TA и соты. Операторы, не имеющие свободных спектров, могут использовать PLMN только в кампусной сети и регулировать долю ресурсов беспроводного интерфейса в кампусной и общедоступной сетях на основе информации PLMN.

В сценарии изоляции опорной сети рекомендуется, чтобы в кампусной и общедоступной сетях использовался унифицированный AMF (во избежание массового беспроводного межсетевого соединения), а также чтобы UDM/PCF развертывались в кампусной сети независимо. SMF и UPF могут использоваться совместно или изолироваться в соответствии с требованиями изоляции.

4.2.3 Интеграция приложений

В периферийном сценарии MEC необходимо интегрировать сторонние приложения для предоставления локальных услуг. Однако существуют различные типы приложений, которые предъявляют разные требования к ресурсам и платформам. Для решения MEC рекомендуется интегрировать в первую очередь приложения на основе ARM (включая BM и контейнеры). Если приложения на основе ARM недоступны, возможна интеграция приложений на основе x86.

5 Часто задаваемые вопросы

В чем заключаются уникальные преимущества MEC?

- Высочайшее удобство использования
- Локальная обработка данных
- Частная сеть для специализированного пользования
- Быстрая интеграция сторонних приложений
- Разработка локальной экосистемы

A Сокращения и аббревиатуры

Числовые	
3GPP	Проект партнерства третьего поколения
5G	5 поколение
5GC	Опорная сеть 5G
A	
AMF	Функция управления доступом и мобильностью
AN	Сеть доступа
App	Приложение
ARM	Усовершенствованная RISC-машина
C	
CDN	Сеть доставки контента (Content Delivery Network, CDN)
CPU (ЦП)	Центральный процессор
D	
DMZ	Демилитаризованная зона
DN	Сеть передачи данных
DNN	Имя сети передачи данных
DNS	Сервер доменных имен
E	
EMS	Система управления элементами сети
EPC	Ядро пакетной сети нового поколения

ETSI	Европейский институт телекоммуникационных стандартов
F	
FW	Брандмауэр
G	
GTP	Протокол туннелирования GPRS
I	
IPsec	Безопасность интернет-протокола
M	
MEAO	Оркестратор приложений MEC
MEC	Технология периферийных вычислений мультисервисного доступа
MEP	Платформа MEC
MEPM	Менеджер платформы MEC
MOS	Средняя экспертная оценка
N	
NAC	Контроллер сетевой автоматизации
NAT	Преобразование сетевых адресов
NFV	Виртуализация сетевых функций
NFVO	Оркестратор виртуализации сетевых функций
O	
O&M	Эксплуатация и техническое обслуживание
OSS	Система поддержки операционной деятельности
OTT	Технология Over The Top
P	
PCF	Функция контроля политики
PDU	Блок данных протокола
PLMN	Наземная сеть мобильной связи общего пользования

PSA	Якорь сеанса PDU
R	
RAN	Сеть радиодоступа
S	
SeGW	Шлюз безопасности
SMF	Функция управления сеансами
SNMP	Простой протокол сетевого управления
SSH	Безопасная оболочка
T	
TA	Зона отслеживания
TAC	Код зоны отслеживания
TLS	Защита на транспортном уровне
U	
UDM	Единое управление данными
UDP	Протокол передачи датаграмм пользователя
UE	Оборудование пользователя
UL CL	Классификатор восходящей линии связи
UPF	Функция плоскости пользователя
V	
VIM	Управление виртуализированной инфраструктурой
BM (VM)	Виртуальная машина
W	
WiFi	Беспроводная локальная сеть

