



МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

Серия Q
Добавление 52
(12/2004)

СЕРИЯ Q: КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ

**Требования к управлению
мобильностью NNI для систем,
разрабатываемых после IMT-2000**

Рекомендация МСЭ-Т Q – Добавление 52

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ Q
КОММУТАЦИЯ И СИГНАЛИЗАЦИЯ

СИГНАЛИЗАЦИЯ ПРИ РУЧНОМ СПОСОБЕ УСТАНОВЛЕНИЯ МЕЖДУНАРОДНЫХ СОЕДИНЕНИЙ	Q.1–Q.3
АВТОМАТИЧЕСКОЕ И ПОЛУАВТОМАТИЧЕСКОЕ МЕЖДУНАРОДНОЕ СОЕДИНЕНИЕ	Q.4–Q.59
ФУНКЦИИ И ИНФОРМАЦИОННЫЕ ПОТОКИ ДЛЯ СЛУЖБ В ЦСИС	Q.60–Q.99
СЛУЧАИ, ПРИМЕНИМЫЕ К СТАНДАРТИЗИРОВАННЫМ СИСТЕМАМ МСЭ-Т	Q.100–Q.119
ТРЕБОВАНИЯ К СИСТЕМАМ СИГНАЛИЗАЦИИ № 4, 5, 6, R1 И R2	Q.120–Q.499
ЦИФРОВЫЕ СТАНЦИИ	Q.500–Q.599
ВЗАИМОДЕЙСТВИЕ СИСТЕМ СИГНАЛИЗАЦИИ	Q.600–Q.699
ТРЕБОВАНИЯ К СИСТЕМЕ СИГНАЛИЗАЦИИ № 7	Q.700–Q.799
ИНТЕРФЕЙС Q3	Q.800–Q.849
ЦИФРОВАЯ АБОНЕНТСКАЯ СИСТЕМА СИГНАЛИЗАЦИИ № 1	Q.850–Q.999
СЕТЬ СУХОПУТНОЙ ПОДВИЖНОЙ СВЯЗИ ОБЩЕГО ПОЛЬЗОВАНИЯ	Q.1000–Q.1099
ВЗАИМОДЕЙСТВИЕ СО СПУТНИКОВЫМИ ПОДВИЖНЫМИ СИСТЕМАМИ	Q.1100–Q.1199
ИНТЕЛЛЕКТУАЛЬНАЯ СЕТЬ	Q.1200–Q.1699
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ И ПРОТОКОЛЫ IMT-2000	Q.1700–Q.1799
ТРЕБОВАНИЯ К СИГНАЛИЗАЦИИ, ОТНОСЯЩЕЙСЯ К УПРАВЛЕНИЮ ВЫЗОВОМ, НЕЗАВИСИМО ОТ КАНАЛА-НОСИТЕЛЯ	Q.1900–Q.1999
ШИРОКОПОЛОСНАЯ ЦСИС	Q.2000–Q.2999

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Добавление 52 к Рекомендациям МСЭ-Т серии Q

Требования к управлению мобильностью NNI для систем, разрабатываемых после IMT-2000

Резюме

В настоящем Добавлении приведены требования к управлению мобильностью для систем, разрабатываемых после IMT-2000 и основанных на Рекомендациях МСЭ-Т Q.1702 [7] и Q.1703 [8], а также Рекомендации МСЭ-Р M.1645 [23]. Был рассмотрен и проанализирован ряд протоколов управления мобильностью в соответствии с указанными требованиями.

Источник

Добавление 52 к Рекомендациям МСЭ-Т серии Q было принято 16 декабря 2004 года 19-й Исследовательской комиссией МСЭ-Т (2004–2005 гг.).

Ключевые слова

Мобильность, управление мобильностью, протоколы управления мобильностью, требования к управлению мобильностью, системы, разрабатываемые после IMT-2000.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

Всемирная ассамблея по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяет темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей публикации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной публикации носит добровольный характер. Однако в публикации могут содержаться определенные обязательные положения (например, для обеспечения возможности взаимодействия или применимости), и тогда соответствие данной публикации достигается в случае выполнения всех этих обязательных положений. Для выражения необходимости выполнения требований используются соответствующие слова ("должен", "обязан" и т. п.), а также их отрицательные эквиваленты. Использование таких слов не предполагает обязательного характера соблюдения данной публикации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на то, что практическое применение или реализация этой публикации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, обоснованности или применимости заявленных прав интеллектуальной собственности, независимо от того, отстаиваются ли они членами МСЭ или другими сторонами вне процесса подготовки публикации.

На момент утверждения настоящей публикации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для реализации этой публикации. Однако те, кто будет применять публикацию, должны иметь в виду, что это может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ.

© ITU 2005

Все права сохранены. Никакая часть данной публикации не может быть воспроизведена с помощью каких-либо средств без письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1	Область применения 1
2	Определения 1
3	Сокращения 2
4	Введение..... 4
5	Соображения по поводу управления мобильностью в SBI2K 6
5.1	Предполагаемая сетевая обстановка для SBI2K 6
5.2	Сценарии взаимодействия для сети SBI2K 7
5.3	Уровень поддержки мобильности 8
5.4	Базовые функции управления мобильностью 9
5.5	Классификация управления мобильностью 9
5.6	Соображения по вопросам работы 3GPP и 3GPP2 для поддержки межсетевого ММ..... 11
6	Требования к протоколам управления мобильностью для SBI2K 11
6.1	Независимость от технологий доступа к сети 12
6.2	Согласование с базовыми сетями на основе IP 12
6.3	Разделение функций управления и транспортировки 12
6.4	Обеспечение функции определения местоположения 12
6.5	Обеспечение механизмов для идентификации пользователей/оконечных устройств 12
6.6	Межсетевое взаимодействие с установленными схемами AAA и схемами защиты 12
6.7	Обеспечение механизмов передачи контекста 13
6.8	Эффективное межсетевое взаимодействие между разными уровнями протоколов ММ..... 13
6.9	Конфиденциальность информации о местоположении 13
6.10	Поддержка "перемещающейся сети" 13
6.11	Поддержка пейджинга (персонального вызова) с помощью определения местоположения..... 13
6.12	Поддержка IP-версии 4 и IP-версии 6 13
6.13	Предоставление функции управления хендовером для бесперебойного обслуживания 13
7	Существующие протоколы управления мобильностью 14
7.1	Протокол Mobile IP (MIP) 14
7.2	Протокол начала сеанса (SIP) 16
7.3	Протокол Cellular IP (CIP) 17
7.4	Протокол передачи для управления потоком информации в сетях подвижной связи (mSCTP)..... 20
7.5	Протоколы управления мобильностью 3GPP 22
7.6	Протоколы управления мобильностью 3GPP2 24
7.7	Возможный протокол мобильности BRAIN (BCMP)..... 26

	Стр.
8 Анализ существующих протоколов ММ для SBI2K	29
8.1 Обзор существующих ММР	29
8.2 Возможные протоколы управления мобильностью для управления мобильностью	30
8.3 Заключительные замечания	32
БИБЛИОГРАФИЯ	33

Требования к управлению мобильностью NNI для систем, разрабатываемых после IMT-2000

1 Область применения

Настоящее Добавление предназначено для определения требований к управлению мобильностью (ММ) для межсетевого интерфейса (NNI) в системах, разрабатываемых после IMT-2000 (SBI2K), и для анализа возможных вариантов протокола ММ на основе этих требований.

При разработке общего набора требований к ММ были использованы следующие критерии:

- они должны быть совместимы с появляющимися сетями на основе IP, и
- они должны соответствовать результатам проводимых в МСЭ исследований в области перспектив, гармонизации и сближения фиксированной и подвижной служб.

Общий набор требований к ММ затем был использован для анализа различных возможных вариантов протокола ММ со следующими целями:

- поддержка глобального роуминга (автоматической настройки на местную сеть) и расширенных услуг и
- в максимально возможной степени повторное использование существующих технических требований IETF, организаций по разработке стандартов (SDO) стран-партнеров, партнерских проектов по системам 3GPP и 3GPP2, IEEE и других соответствующих групп.

Для создания перспективных представлений о системах SBI2K с точки зрения ММ совершенно необходимо тесное сотрудничество с экспертами из указанных выше и других заинтересованных организаций, чтобы обеспечить плавный переход в целях длительного выполнения предъявляемых к ММ требований.

2 Определения

В настоящем Добавлении определены следующие термины.

2.1 мобильность: Возможность для пользователя получить доступ к абонированным им услугам в процессе перемещения и возможности сети идентифицировать и определить местонахождение оконечного устройства пользователя.

2.2 хендовер: Возможность для подвижного пользователя/оконечного устройства/сети менять местоположение в процессе передачи потоков данных.

2.3 домашняя сеть: Сеть, к которой обычно подключен подвижный пользователь, или поставщик услуг, с которым связан подвижный пользователь и у которого хранится информация об абонировании пользователя.

2.4 визитная сеть: Сеть за пределами домашней сети, которая предоставляет услуги подвижному пользователю.

2.5 управление мобильностью: Набор функций, используемых для управления доступом подвижного пользователя к другой локальной сети, отличной от домашней сети пользователя. Эти функции включают связь с домашней сетью для целей идентификации, разрешения на предоставление доступа, изменения местонахождения и загрузки информации о пользователе.

2.6 мобильность сети: Способность сети, в которой соединен между собой ряд стационарных или подвижных узлов, изменять в качестве единого узла точки их присоединения к соответствующей сети во время перемещения самой сети.

2.7 роуминг: Возможность для подвижного пользователя осуществлять связь из посещаемой сети. Во время роуминга пользователь имеет возможности изменять точки доступа к сети в процессе перемещения. Однако текущий сеанс его обслуживания полностью прекращается в старом месте, а в новом месте начинается новый сеанс, то есть хендовер отсутствует.

2.8 бесшовный хендовер: Процесс, в котором время ожидания и потеря данных во время хендовера сохраняется в допустимых для пользователя пределах (то есть ниже некоторого предела) для обслуживания в реальном масштабе времени.

2.9 бесперебойное обслуживание: Бесперебойное обслуживание позволяет исключить для пользователя любые перерывы в обслуживании, одновременно сохраняя мобильность.

2.10 мобильность оконечного устройства: Это мобильность для тех сценариев, когда одно и то же оконечное устройство перемещается или используется в разных местах. При этом оконечное устройство обеспечивается доступом к услугам электросвязи из разных мест и в процессе движения, а сеть имеет возможность идентифицировать и определять местонахождение этого оконечного устройства.

3 Сокращения

В настоящем Добавлении использованы следующие сокращения:

3GPP	Партнерский проект по системам третьего поколения
3GPP2	Партнерский проект 2 по системам третьего поколения
AAA	Идентификация, авторизация и учет
ACK	Подтверждение
ЛОПУ	Логический объект прикладного уровня
AGW	Шлюз доступа
AN	Сеть доступа
ANG	Шлюз сети доступа
ANP	Опорная точка
ANSI	Американский национальный институт стандартов
AR	Маршрутизатор доступа
ASE	Сервисный объект прикладного уровня
BAR	Маршрутизатор доступа BRAIN
BCMP	Возможный протокол мобильности BRAIN
BR	Граничный маршрутизатор
БС	Базовая станция
CCoA	Совмещенный адрес для передачи
CH	Главный компьютер корреспондента
CIP	Протокол Cellular IP (Протокол IP для сетей сотовой связи)
CN	Базовая сеть (сети)
CoA	Адрес для передачи
DB	База данных
DHCP	Протокол динамического конфигурирования главного компьютера
РИО	Регистр идентификатора оборудования
FA	Внешний агент
FM	Член семейства
FMIP	Быстрый хендовер для MIP

GERAN	Сеть доступа радио GSM EDGE
GFA	Шлюз FA
GGSN	Узел поддержки шлюза GPRS
GPRS	Служба пакетной радиосвязи общего пользования
GSM	Глобальная система подвижной связи
GTP	Протокол туннелирования GPRS
HA	Внутренний агент
HLR	Регистр местонахождения внутренней сети
HMIP	Иерархический MIP
HoA	Внутренний адрес
HSS	Подсистема внутренних абонентов
IETF	Целевая группа по инженерным проблемам Интернет
INIT	Инициализация
IMS	Мультимедийная подсистема на основе IP
IMT	Международная подвижная электросвязь
I2K	Международная подвижная электросвязь-2000
IOS	Технические требования к возможности взаимодействия сетей
IP	Межсетевой протокол
LMA	Агент местной мобильности
MAP	Подсистема обеспечения подвижной станции
MAP	Опорная точка мобильности
MIP	Протокол Mobile IP (Протокол IP для сетей подвижной связи)
MIPv4	Протокол Mobile IP версии 4
MIPv6	Протокол Mobile IP версии 6
MM	Управление мобильностью
MMD	Мультимедийный домен
MMP	Протокол управления мобильностью
MMR	Требования к управлению мобильностью
MN	Мобильный узел связи
ПС	Подвижная станция
MSC	Центр коммутации подвижной связи
mSCTP	Протокол передачи для управления потоком информации в подвижной связи
MT	Мобильное оконечное устройство
MT	Оконечная операция подвижной связи
NNI	Межсетевой интерфейс
PC	Быстродействующая буферная память для пейджинга
PDF	Функция принятия решений по политике в области связи

PDN	Сеть пакетной передачи данных
PDS	Подсистема пакетной передачи данных
PDSN	Узел обслуживания пакетной передачи данных
PDP	Протокол пакетной передачи данных, например IP
ССПСП	Сеть сухопутной подвижной связи общего пользования
PMM	Управление мобильностью в пакетной связи
PS	Служба пакетной передачи
QoS	Качество обслуживания
RAN	Сеть радиодоступа
RC	Быстродействующая буферная память при маршрутизации
RFC	Запрос на комментарий
SBI2K	Системы, разрабатываемые после IMT-2000
SCCP	Сигнализация в подсистеме управления соединением
SCTP	Протокол передачи для управления потоком данных
SDO	Организация по разработке стандартов
SGSN	Узел обеспечения GPRS
SMS	Служба коротких сообщений
SIP	Протокол начала сеанса
SS7	Система сигнализации № 7
TCAP	Подсистема обеспечения возможностей транзакции
TCP	Протокол управления передачей
UA	Агент пользователя
UAC	Клиент агента пользователя
UAS	Сервер агента пользователя
UDP	Протокол дейтаграммы пользователя
UMTS	Универсальная система подвижной электросвязи
URI	Унифицированный идентификатор ресурсов
UTRAN	Универсальная наземная сеть радиодоступа
BPM	Визитный регистр местонахождения
WLAN	Беспроводная локальная сеть
xDSL	Цифровые абонентские линии x

4 Введение

Системы, разрабатываемые после IMT-2000 (SBI2K), служат целям сближения стационарных и беспроводных сетей и, в конечном счете, на переход к функционально совместимой и согласованной архитектуре сетей. Это направление в области развития сетей стало необходимым для отрасли, и одна из задач такого развития состоит в прозрачном предоставлении услуг пользователям для различных схем доступа. В связи с этим в данном документе поставлен вопрос: "Какие требуются новые протоколы управления мобильностью или расширения существующих протоколов управления мобильностью для обеспечения глобальной мобильности пользователя и обслуживания в SBI2K?".

В этом контексте в данном документе установлены требования к управлению мобильностью NNI для SBI2K, основанные на Рекомендациях МСЭ-Т Q.1702 и Q.1703, а также Рекомендации МСЭ-Р М.1645. В соответствии с установленными требованиями был рассмотрен ряд протоколов управления мобильностью и проведен их анализ с целью определения той области, в которой может быть найдено решение для возможного протокола управления мобильностью (ММР).

Ключевой особенностью, присущей подвижным системам, служит возможность осуществления связи для подвижного пользователя в любой момент и из любой точки. Это облегчается использованием радиодоступа, который дает возможность пользователям осуществлять связь на радиочастотах и с помощью протоколов управления мобильностью постоянно следить за местонахождением подвижных пользователей.

За последние годы были разработаны современные методы ММ, которые были внедрены в подвижные системы для эффективного управления регистрацией, идентификацией и перемещением подвижных пользователей. Однако эти методы были разными для каждой развертываемой системы и управляли перемещением пользователей в рамках схожих взаимодействующих подвижных систем (например, в системах члена семейства ИМТ-2000). В связи с этим бесперебойное предоставление услуг и обеспечение мобильности в разнородных системах наталкивалось на трудности вследствие ряда факторов:

- различия используемых для радиодоступа методов;
- различия в предоставляемых услугах и невозможность их взаимозаменяемости;
- различия в применяемых методах ММ; и
- отсутствие подходящего механизма функциональной совместимости для устранения указанных выше различий между разными подвижными системами.

Интенсивный рост числа подвижных пользователей и продолжающееся развертывание разнородных подвижных систем (например, несколько систем-членов семейства ИМТ-2000, беспроводные локальные сети (WLAN), Bluetooth), потребность в предоставлении бесперебойного обслуживания для подвижных пользователей только увеличивалась со временем, и такие тенденции ставят новые задачи и предъявляют новые требования к новым типам ММ, функционально совместимым с разнородными системами.

Кроме того, предполагается, что будущие подвижные сети должны взаимодействовать с их базовыми сетями на основе межсетевого протокола (IP), как указано в Рекомендации МСЭ-Т Q.1702 и Рекомендации МСЭ-Р М.1645, в которых описана дальняя перспектива для будущих подвижных систем, под названием SBI2K, соответственно с точки зрения организации сети и радиосвязи. Поэтому перспективные требования направлены на сближение подвижных систем и сети Интернет. Для обеспечения такого сближения требуются новые, функционально совместимые способы ММ.

В Рекомендации МСЭ-Т Q.1702 указано: "Наблюдается четкая тенденция к интеграции сетей доступа (например, сотовых, беспроводных локальных сетей, персональных беспроводных сетей, спутниковых систем и Интернет). Основываясь на этой тенденции, представляется, что среда сети SBI2K будет состоять из инфраструктуры сети с коммутацией пакетов, предоставляющей все изобилие конвертированных услуг".

Перспективное решение для нового типа ММ в SBI2K должно учитывать долгосрочные тенденции развития сетей, потребность в плавном развитии инфраструктуры, а также проблему обратной совместимости с существующими сетями, особенно сетями по стандартам семейства ИМТ-2000.

Долгосрочные тенденции (как указано в Рекомендации МСЭ-Т Q.1702) для ММ можно суммировать следующим образом.

- базовая сеть полностью основана на межсетевом протоколе (IP);
- бесперебойное обслуживание требуется для большого числа пользователей;
- ММ должно обеспечивать не только поддержку необходимых услуг в объектах, передвигающихся с высокой скоростью, например, в автомобилях, но и обязано поддерживать приложения, требующие большие объемы мультимедийного IP трафика, вместе с предоставлением возможностей разнообразной связи между людьми, между машинами, человека с машиной и в обратном направлении;

- концепция бесперебойного обслуживания будет расширяться за рамки услуг хендовера и роуминга для однородных сетей и будет включать бесперебойное обслуживание для разнородных сетей;
- поддержка подвижных сетей (например, в самолетах, поездах и на судах); и
- разделение функций управления и транспортирования.

Предлагаемая архитектура должна поддерживать разнообразные режимы мобильности пользователей в разных сетях доступа, включая глобальный роуминг и блуждающую/бесшовную мобильность.

Например, тот или иной пользователь подключается к стационарной сети доступа (например, к цифровым абонентским линиям x (xDSL)) и опознается с помощью соответствующего механизма, предоставляемого этой системой доступа. Затем он начинает сеанс мультимедийной связи. Далее, продолжая этот сеанс, тот же пользователь переключается на сотовую систему (например, на универсальную систему подвижной электросвязи (UMTS) cdma2000) и опознается механизмом защиты доступа. После этого он может попытаться начать сеанс мультимедийной связи, и этот сеанс будет обрабатываться сетью доступа в соответствии с предварительно согласованным профилем пользователя, известным в данной сотовой сети. При таком развитии событий может возникнуть ряд проблем для обеспечения надлежащей и бесперебойной работы:

- придется справляться с множеством механизмов идентификации, таких как способы доступа, например, с соответствующими идентификаторами при использовании разных регистрационных имен и паролей;
- стационарная сеть доступа должна поддерживать проведение сеанса пользователя, чтобы отслеживать перемещение пользователя, расходуя при этом ресурсы; и
- в связи с возможными различиями профиля пользователя в неоднородных доменах может оказаться недостаточно надежным и удовлетворительным управление бесшовной мобильностью и обеспечение обслуживанием из-за различий между системами.

Функции управления мобильностью нового типа, которые должны быть функционально совместимы в неоднородных сетях, будут способны эффективно решать такие проблемы, как идентификация, разрешение на предоставление доступа и выбор между разными способами доступа, которые возникают при обращении к одному и тому же уровню обслуживания для бесперебойной работы через разные сети.

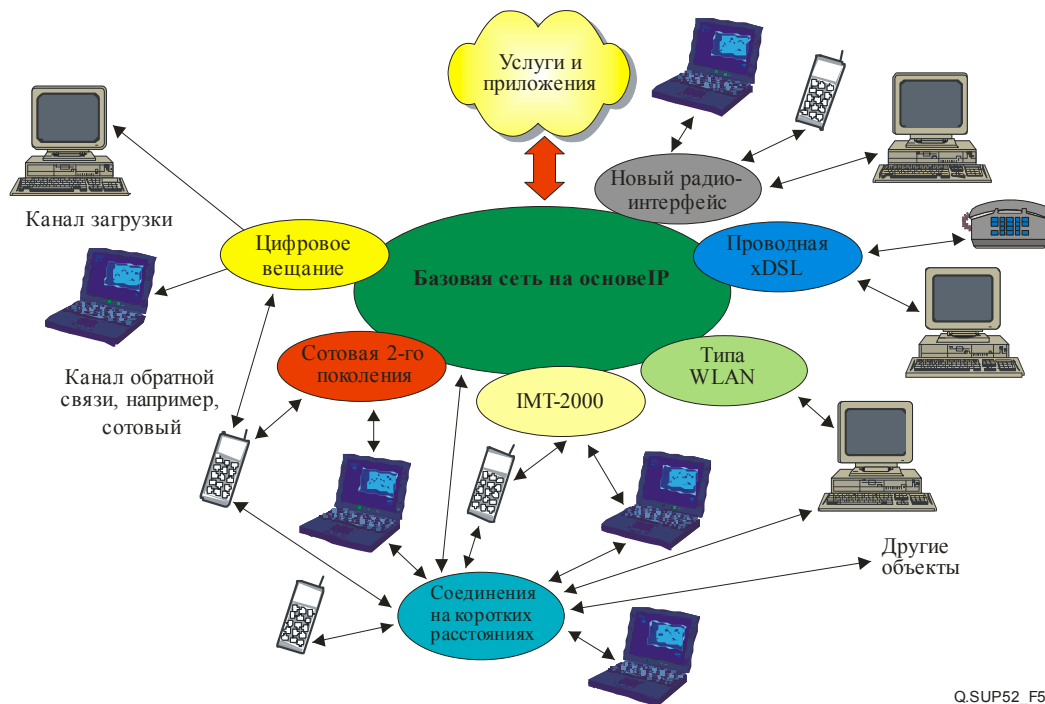
В этом документе описан набор требований для протоколов управления мобильностью в SBI2K. Для этого в разделе 5 рассмотрены общие особенности и вопросы управления мобильностью в SBI2K. В разделе 6 установлены и охарактеризованы требования к MMP в применении к SBI2K. В разделе 7 рассмотрен ряд возможных MMP для SBI2K. В разделе 8 проведен анализ возможных MMP и их сравнение на основе требований к MMP, установленных в разделе 6.

5 Соображения по поводу управления мобильностью в SBI2K

В этом разделе описаны типовые особенности и приведены соображения по вопросам управления мобильностью, которую могут облегчить определение требований к MM и протоколов для систем, разрабатываемых после IMT-2000.

5.1 Предполагаемая сетевая обстановка для SBI2K

В Рекомендации МСЭ-R М.1645 разработано представление о SBI2K. Там предусмотрена приведенная на рисунке 5.1 архитектура SBI2K. В этой архитектуре предполагается, что оператор может иметь базовую сеть и одну или несколько сетей доступа, содержащих либо проводную, либо беспроводную сети доступа и обеспечивать своим абонентам бесперебойное обслуживание через эти разнородные сети доступа.



Q.SUP52_F5.1

Рисунок 5.1 – Рисунок 4 /Рекомендация МСЭ-R М.1465: будущая сеть для систем, разрабатываемых после IMT-2000 (SBI2K), включая возможные разнообразные взаимодействующие системы доступа

5.2 Сценарии взаимодействия для сети SBI2K

Для определения требований к ММ в SBI2K было бы полезно представить себе общую архитектуру сети SBI2K. На рисунке 5.2 приведена общая схема взаимодействия сети для SBI2K со стороны ММ.

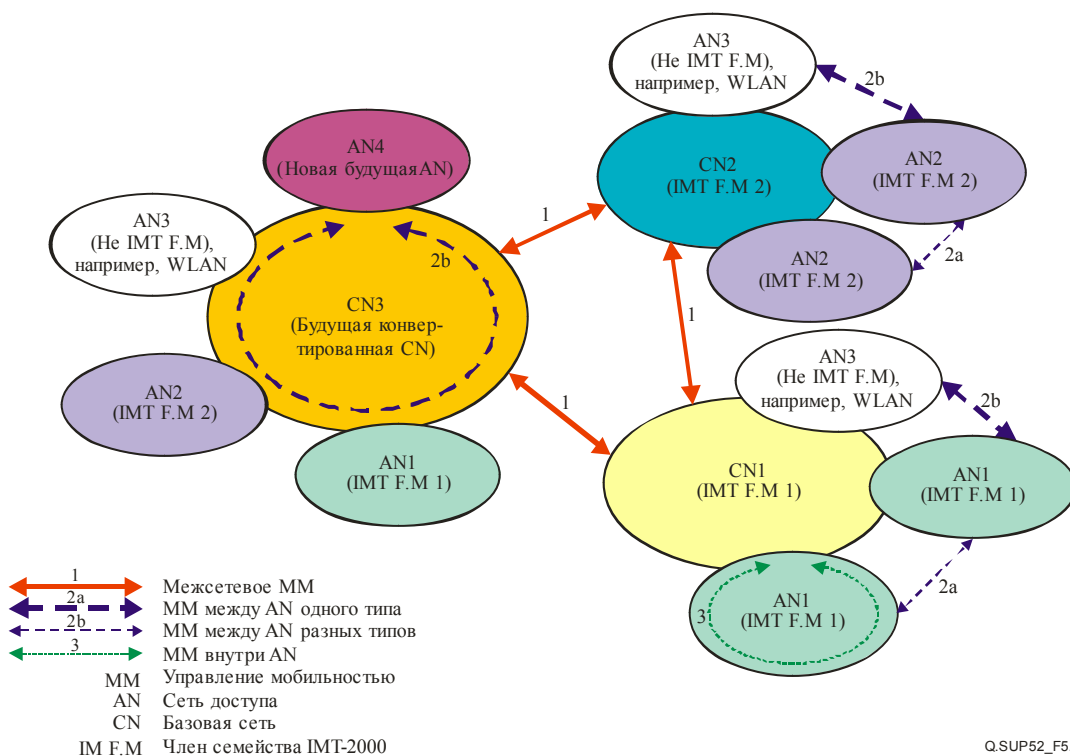


Рисунок 5.2 – Сценарии взаимодействия для сети SBI2K

Сеть на рисунке состоит из базовой сети и одной или нескольких сетей доступа. Несколько AN взаимодействуют между собой через CN.

- *Базовая сеть (CN)*

Термин "базовая сеть" относится к архитектуре части SBI2K, которая не зависит от способа связи конечных устройств.

- *Сеть доступа (AN)*

Сеть доступа представляет собой объект или несколько объектов между пользователем и CN, которые соединяют пользователя с CN с помощью определенной технологии доступа. Примерами технологии доступа могут служить сотовая система (cdma2000, WCDMA), WLAN, xDSL.

5.3 Уровень поддержки мобильности

Поддерживаемые уровни мобильности можно принципиально разделить на "блуждающую" и "бесшовную" мобильность.

- *Бесшовная (seamless) мобильность*

Пользователь может менять точку доступа к сети по мере своего передвижения, не прерывая текущего сеанса обслуживания, то есть поддерживаются хендоверы с эксплуатационными характеристиками, достаточными для применений в реальном масштабе времени или чувствительных к потерям. В неблагоприятной ситуации такой хендовер может все же приводить к кратковременной приостановке сеанса обслуживания. Однако желательно свести к минимуму продолжительность такого прерывания сеанса. Поэтому поддержка бесшовной мобильности потребует более передовых и сложных схем ММ, чем другие варианты мобильности, например, блуждающая мобильность (определена далее). Задача поддержки бесшовной мобильности состоит в обеспечении бесперебойного сеанса с помощью сведения к минимуму времени прерывания сеанса в процессе хендовера, которое наблюдается из-за связанной с ним задержки и потери данных, когда мобильное оконечное устройство перемещается на новый участок сети доступа и меняет точку подключения к обслуживающей сети.

- *Блуждающая (nomadic) мобильность*

Блуждающая мобильность поддерживает непрерывность обслуживания, но с ограниченной непрерывностью сеанса между разными сетями. При переходе пользователя из одной сети в другую она обеспечивает ограниченный уровень хендовера, который может быть достаточен для обслуживания не в реальном масштабе времени (например, услуги электронной почты), но не для услуг в реальном масштабе времени. Блуждающая мобильность включает также концепцию роуминга с ограниченной мобильностью.

5.4 Базовые функции управления мобильностью

Управление ММ в SBI2K будет осуществляться на основе связанных с мобильностью базовых функций и сопряженных с ними функций. Базовые функции относятся непосредственно к управлению мобильностью для подвижных пользователей и оконечных устройств, в то время как сопряженные функции используются для поддержки ММ или для обмена соответствующей информацией для целей общего контроля и управления.

Базовые функции ММ включают управление средствами определения местоположения и хендовера.

- *Определение местоположения*

Определение местоположения проводится для установления текущего местонахождения в сети мобильного оконечного устройства (МТ) и для отслеживания его перемещений. Такое определение местоположения используется для управления вызовами и сеансами, подключенными к МТ. С помощью функции определения местоположения корреспондентский узел может определить местонахождение МТ и открыть сеанс связи, используя соответствующую сигнализацию.

- *Управление хендовером*

Управление хендовером используется для обеспечения непрерывности сеанса МТ, когда оконечные устройства перемещаются в район другой сети и меняют свою точку подключения к сети во время сеанса. Основная задача бесшовного хендовера состоит в сведении к минимуму прерываний сеанса за счет потери данных и задержки в процессе хендовера. Большинство протоколов ММ осуществляют управление хендовером вместе с соответствующей схемой определения местоположения. В соответствии с интересующими районами хендовера типы хендовера можно разделить на "хендовер внутри AN", когда МТ перемещается по участкам одной и той же AN в системах SBI2K и "хендовер между разными AN или CN", когда МТ меняет свою систему доступа в ходе продолжающегося сеанса.

5.5 Классификация управления мобильностью

Как описано в разделе 5.3, поддерживаемые уровни ММ можно разделить на блуждающую и бесшовную мобильность. Обычно бывает довольно трудно добиться бесшовной мобильности, если мобильное оконечное устройство меняет технологию связи для обеспечения доступа или оператора сети в процессе сеанса. Отсюда ясно, что требования к ММ будут различаться в зависимости от рассматриваемого типа ММ, а также типа AN и оператора CN.

5.5.1 Типы ММ

При учете различий в зоне действия хендовера типы ММ для SBI2K делят на внутрисетевое ММ и межсетевое ММ. Внутрисетевое ММ можно далее разделить на ММ внутри AN и ММ между AN.

Ниже приведено более подробное описание межсетевого и внутрисетевого ММ:

- *Внутрисетевое ММ*

"Внутрисетевое" ММ занимается аспектами ММ внутри сети. Его можно разделить на ММ "внутри АН" и ММ "между АН".

 - ММ внутри АН
ММ "внутри АН" ММ занимается аспектами ММ в пределах АН. Например, на рисунке 5.2 ММ в пределах АН1 в СN1, помеченное цифрой "3" на рисунке, можно отнести к ММ внутри АН.
 - ММ между АН
ММ "между АН" ММ занимается аспектами ММ между разными АН в пределах СN. ММ между АН можно далее разделить на следующие два подтипа:
 - 1) ММ между АН одного и того же типа (например, ММ между двумя АН1 в пределах СN1, помеченный как 2а на рисунке 5.2); и
 - 2) ММ между АН разного типа (например, ММ между АН1 и АН3 в пределах СN1, помеченные как 2b на рисунке 5.2).
- *Межсетевое ММ (ММ от сети к сети (NNI))*

"Межсетевое" ММ занимается аспектами ММ между сетями. Межсетевое ММ всегда связано с вопросами ММ между двумя АН, то есть это ММ между АН. В дополнение к этому, межсетевое ММ должно заниматься вопросами ММ, которые возникают в процессе хендовера МТ между двумя разными базовыми сетями (то есть межсетевого интерфейса (NNI)), такими как разрешение на допуск пользователя и обсуждение условий соглашения об уровне обслуживания (SLA). На рисунке 5.2 в качестве примера приведено ММ между СN1 и СN3, помеченное как 3 на рисунке, которое является межсетевым ММ.

5.5.2 Соображения по вопросу применения ММ исходя из перспектив FM IMT-2000(I2K)

Приведенное выше разделение типов ММ можно использовать для приведенных ниже специальных вопросов с учетом точек зрения членов семейства I2K.

- *ММ в межсетевых интерфейсах (NNI) внутри одного члена семейства NNI*

ММ этого типа соответствует ММ внутри сети АН и уже было частично задано соответствующими SDO при определении характеристик устройств члена семейства I2K.
- *ММ в NNI между разными членами семейства*

ММ этого типа можно представить как межсетевые ММ. Существуют три принципиальных варианта для NNI между разными членами семейства I2K, то есть между членами семейства FM1 и FM2.

 - 1) Использование протокола MMP NNI, заданного для внутренних NNI в составе FM1, для которого требуется подходящее взаимодействие со стороны FM2.
 - 2) Использование протокола MMP NNI, заданного для внутренних NNI в составе FM2, для которого требуется подходящее взаимодействие со стороны FM1.
 - 3) Введение нового "глобального" протокола MMP NNI, который отличается от протоколов FM1 и FM2 и для которого потребуется межсетевое взаимодействие с обеих сторон NNI. Такой протокол для использования в NNI между устройствами двух разных членов семейства IMT-2000 можно стандартизировать с помощью прямого сотрудничества в рамках партнерских проектов с указанием членов семейства или с помощью третьей стороны.
- *ММ в интерфейсах NNI, которые соединены с базовыми сетями, не относящимися к IMT-2000*

И для такого ММ можно использовать межсетевое ММ. Это может быть управление, идентичное протоколу MMP или его расширению, заданному для использования между базовыми сетями IMT-2000 (устройствами одного члена семейства или разных членов семейства); либо это может быть другой, специальный MMP, например, специально предназначенный для сближения стационарной и подвижной сетей (для случая NNI между базовыми сетями стационарной и сухопутной подвижной сетей общего пользования (ССПС)), либо возможен какой-то иной вариант.

Желательно, чтобы число подлежащих стандартизации разных протоколов ММР NNI было не больше необходимого. Возможность согласования протоколов NNI увеличивается при переходе к сетям на основе IP.

В зависимости от рассмотренного выше типа NNI можно ожидать разных требований к ММР. Надо особо отметить, что могут различаться "Требования к ММ" для устройств NNI внутри одного члена семейства и устройств NNI между разными членами. Сравнительно легко установить требования к ММ для ММ устройств внутри одного члена семейства I2K, поскольку они включены в стандарт устройств одного члена семейства I2K. С другой стороны, ММ между устройствами разных членов семейства I2K, в принципе, связаны с разными протоколами, используемыми в устройствах разных членов семейства, и поэтому соответствующие требования к ММ могут оказаться плохо определенными. Возможно, еще труднее установить требования для NNI для других сетей, отличных от I2K.

5.6 Соображения по вопросам работы 3GPP и 3GPP2 для поддержки межсетевого ММ

В связи с расширением 3G в ближней и среднесрочной перспективе развития могут быть учтены приведенные ниже аспекты, как это указано в [24].

- *Согласованная CN между 3GPP и 3GPP2*

Цель такого согласования состоит в обеспечении однородного обслуживания пользователей при неоднородных механизмах доступа, которые служат для доступа к независимой согласованной базовой сети. Для 3GPP и 3GPP2 принята одна эталонная модель мультимедийной подсистемы IP (IMS) и согласованная терминология для описания их общих функциональных объектов в IMS.

3GPP и 3GPP2 предназначены для обеспечения функциональной совместимости между оконечными устройствами системы IMS 3GPP и оконечными устройствами мультимедийного домена 3GPP2 (MMD), с тем чтобы оконечные устройства системы IMS 3GPP могли осуществлять сеансы связи с оконечными устройствами MMD 3GPP2, и наоборот, а также роуминг межсистемных IMS на уровне приложений (если такое оконечное устройство поддерживает сеть доступа для визитной сети и технологию транспортирования IP, то оконечное устройство системы IMS 3GPP должно иметь возможность осуществить роуминг в сеть 3GPP2 и наоборот).

- *Взаимодействие между подвижными сетями 3GPP/3GPP2 и другими сетями*

Сходство услуг и приложений в разных системах выгодно для пользователей, и это совпадает с совместной тенденцией к сближению. В будущем операторы могут применять комплекс технологий, которые могут включать сотовые системы, WLAN, цифровое радиовещание, спутниковые и другие системы доступа. Это потребует бесшовного взаимодействия таких систем, с тем чтобы пользователь мог получать самые разные данные по различным механизмам их доставки в зависимости от возможностей конкретного оконечного устройства, его местоположения и профиля пользователя.

Различные системы радиодоступа будут подключаться через гибкие CN. Это позволит подключать отдельного пользователя через разнообразные системы доступа к нужным ему сетям и услугам.

6 Требования к протоколам управления мобильностью для SBI2K

В этом разделе описан ряд требований к протоколам для ММ в SBI2K. Основываясь на установленных требованиях, будет проведено изучение и анализ вариантов протокола ММ для SBI2K.

- Независимость от технологий доступа к сети.
- Согласование с появляющимися базовыми сетями на основе IP.
- Разделение функций управления и транспортировки.
- Обеспечение функции определения местоположения.
- Обеспечение механизмов для идентификации пользователей оконечных устройств.

- Взаимодействие с установленными схемами идентификации, авторизации и учета (AAA), а также со схемами защиты.
- Обеспечение механизмов передачи контекста.
- Эффективное межсетевое взаимодействие между разными уровнями протоколов MM.
- Конфиденциальность местоположения.
- Поддержка "перемещающейся сети".
- Поддержка персонального вызова (пейджинга) с помощью определения местоположения.
- Поддержка как IP версии 4, так и IP версии 6.
- Предоставление функции управления хендовером для бесперебойного обслуживания.

6.1 Независимость от технологий доступа к сети

Ожидается, что SBI2K будет состоять из базовой сети на основе IP с несколькими сетями доступа, в которых может использоваться разная технология доступа, как показано на рисунке 5.1. При такой архитектуре MM должно обеспечивать мобильность для сетей с однородным или разнородным доступом, которые принадлежат одному или разным операторам. Следовательно необходимо, чтобы MM не зависело от технологий используемых сетей доступа, например, сотовой 2/3G, WLAN и т. д.

6.2 Согласование с базовыми сетями на основе IP

Предполагается, что будущие конвертированные CN в SBI2K будут основаны на IP. Соответственно, протоколы MM для SBI2K должны быть основаны на IP или, по крайней мере, хорошо согласованы с технологией IP, чтобы они могли эффективно работать и встраиваться в такие будущие CN. Рекомендуются также максимально использовать существующие методы/технологии MM при проектировании протоколов для SBI2K, что возможно с помощью сотрудничества с внешними организациями и SDO.

6.3 Разделение функций управления и транспортировки

Вопросы транспортировки должны быть отделены от вопросов управления для обеспечения эффективного управления мобильностью и масштабирования. Такое разделение плоскостей управления и транспортировки обеспечивает гибкость архитектуры, что облегчает введение новых технологий и услуг. Для реализации такого разделения требуются открытые интерфейсы между функциями в плоскости управления и функциями в плоскости транспортировки.

6.4 Обеспечение функции определения местоположения

Для обеспечения мобильности пользователей/оконечных устройств выполняется отслеживание и определение местонахождения пользователей/оконечных устройств с помощью одной или нескольких функций определения местоположения при любом перемещении пользователей. В соответствии с предполагаемой общей структурой на основе IP, определение местоположения должно основываться на задаваемом IP подходе, таком как внутренний агент протокола Mobile IP или регистратор протокола начала сеанса (SIP).

6.5 Обеспечение механизмов для идентификации пользователей/оконечных устройств

Протоколы MM в SBI2K должны устанавливать, как идентифицируются пользователи/оконечные устройства в сетях или системах для управления мобильностью. Введение этой функции идентификации должно быть первым шагом, который необходимо предпринять в процессе управления мобильностью и использовать для идентификации, проверки разрешения на предоставление доступа и учета пользователей/оконечных устройств.

6.6 Межсетевое взаимодействие с установленными схемами AAA и схемами защиты

Протоколы MM в SBI2K должны устанавливать, как проводится идентификация, проверка разрешения на предоставление доступа и учет для пользователей/оконечных устройств, и как осуществляется защита обслуживания с помощью стандартных механизмов AAA и защиты.

Результатом действия функции AAA будет решение "да" или "нет" на запрос об обслуживании от пользователя. В качестве следующего шага конфигурация сети доступа приспосабливается к подвижному/блуждающему пользователю, так чтобы она обеспечивала определенный уровень

качества обслуживания (QoS) и защиту при предоставлении запрошенного обслуживания. Эти механизмы должны быть основаны на абонентском профиле пользователя и ограничениях для технических ресурсов в соответствующих сетях доступа.

Хотя предполагается, что многие пользователи будут иметь оконечные устройства исключительно для своего личного использования, во многих случаях оконечное устройство будет находиться в общем пользовании нескольких пользователей (например, телефоны общего пользования), а в ряде случаев тот или иной пользователь по вполне обоснованным и законным причинам возьмет займы оконечное устройство у другого пользователя, который обычно лично пользуется своим оконечным устройством, но захочет по обоснованным и законным причинам предоставить его для использования кому-то другому (например, аварийный вызов, когда сели батареи оконечного устройства). В этих и иных обстоятельствах считается необходимым разделить механизмы идентификации пользователей и оконечных устройств, то есть, чтобы пользователь идентифицировался отдельно от идентификации оконечного устройства и чтобы пользователь не был постоянно связан с определенным оконечным устройством, причем такой подход может быть временным или действующим в течение длительного времени в зависимости от обстоятельств. Пользователи также могут иметь несколько оконечных устройств и должны иметь возможность в соответствии со своими потребностями переходить от одного оконечного устройства к другому. Поскольку все это происходит в условиях мобильности, важно также отделить географическую информацию от идентификации пользователя и идентификации оконечного устройства. Механизмы для обеспечения всего этого потребуют тщательного исследования, поскольку также необходимо, чтобы они были функционально совместимы с действующими механизмами именования, нумерации, адресации и маршрутизации.

6.7 Обеспечение механизмов передачи контекста

Когда МТ перемещается между разными сетями, информация о контексте для текущего сеанса, включая уровень QoS, способ защиты, механизм AAA, используемый тип сжатия и т. д., может оказаться полезной для осуществления хендовера сеанса в новую сеть доступа (например, сведение к минимуму задержки при передаче сеанса связи новому обслуживаемому объекту). Правильное использование механизма передачи контекста может существенно уменьшить объем служебной информации в серверах, которая сама или в сочетании с другими данными используется для обеспечения QoS, защиты, AAA и т. д.

6.8 Эффективное межсетевое взаимодействие между разными уровнями протоколов ММ

Для общей бесшовной мобильности межсетевой протокол ММ должен обеспечивать эффективное взаимодействие с протоколами ММ внутри АН и между разными АН.

6.9 Конфиденциальность информации о местоположении

Информация о местоположении конкретных пользователей должна быть защищена от несанкционированного доступа. Это предусматривает взаимную идентификацию, согласование защиты и другие требования по защите для IP между мобильными оконечными устройствами и функцией определения местоположения.

6.10 Поддержка "перемещающейся сети"

Предполагается, что SBI2K будет включать перемещающиеся сети, как и перемещающиеся оконечные устройства. Типичными примерами платформ для перемещающихся сетей могут быть автобус, поезд, судно, самолет и т. д. Протоколы ММ в SBI2K должны эффективно поддерживать такие типы перемещающихся сетей.

6.11 Поддержка пейджинга (персонального вызова) с помощью определения местоположения

Возможности пейджинга необходимы для сетей большого масштаба, поскольку это позволяет экономить энергию мобильного оконечного устройства, а также уменьшать объем сигнализации в сети, что будет способствовать масштабируемости SBI2K. В частности, поддержку пейджинга нужно обеспечить с помощью определения местоположения.

6.12 Поддержка IP-версии 4 и IP-версии 6

Протоколы ММ должны поддерживать IPv6, а также IPv4.

6.13 Предоставление функции управления хендвером для бесперебойного обслуживания

ММ должен поддерживать управление хендвером для обеспечения непрерывности сеанса при перемещении. Это требование может оказаться неприменимым в среде, в которой задержка на коммутацию в технологиях доступа или при работе операторов неприемлема для некоторых приложений. Однако настоятельно рекомендуется, чтобы ММ в SBI2K могло выполнять функцию плавного хендвера, доступную для подвижных пользователей, которые перемещаются между разными сетями доступа и операторами сети. От функции управления хендвером требуется также, чтобы она работала в согласии с механизмом передачи контекста.

7 Существующие протоколы управления мобильностью

В этом разделе рассмотрены некоторые из существующих и возможных протоколов.

7.1 Протокол Mobile IP (MIP)

7.1.1 Общие сведения

Протокол Mobile IP (MIP) представляет собой протокол для поддержки мобильности IP, установленный в IETF. Протокол Mobile IP можно разделить на протоколы: Mobile IP версии 4 (MIPv4) и Mobile IP версии 6 (MIPv6) в соответствии с принятой версией IP. Эти два протокола, в принципе, обеспечивают одинаковые функции с некоторыми исключениями, связанными с подробностями механизма их действия. Подробно протоколы MIPv4 и MIPv6 описаны в IETF RFC 3344 [44] и IETF RFC 3775 [45], соответственно.

В настоящее время MIP не поддерживает быстрого хендвера для приложений, критичных по времени и чувствительных к потерям. Для решения этой проблемы в IETF разрабатываются некоторые расширения MIP, такие как быстрый хендвер для MIP (FMIP) и иерархический MIP (HMIP). Предполагается, что сочетание MIP с расширениями окажется эффективным для ММ в SBI2K, что обсуждается в разделе 8, ниже.

7.1.2 Работа MIP

MIPv4 работает между следующими объектами: мобильное оконечное устройство (MT)¹, внутренний агент (НА), внешний агент (ФА) и главный компьютер корреспондента (СН). Основные операции MIPv4 приведены на рисунке 7.1, ниже.

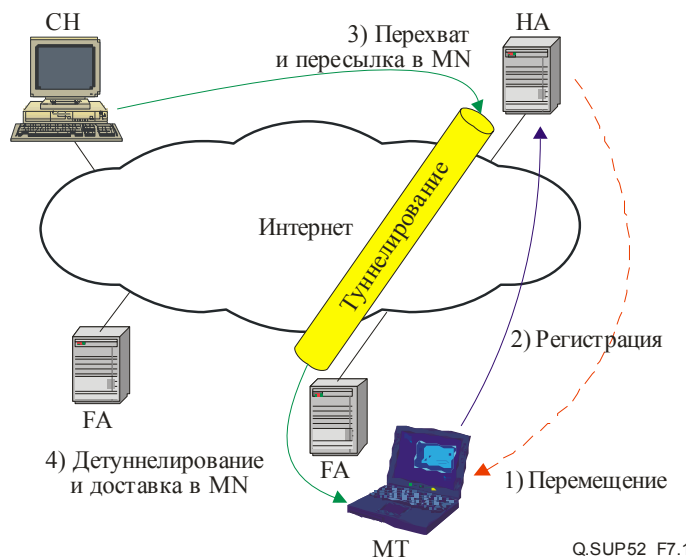


Рисунок 7.1 – Основные операции MIPv4

¹ Мобильное оконечное устройство (MT) равнозначно мобильному узлу связи (MN) в том смысле, как это определено в [44] и [45].

При переходе МТ в новую подсеть он регистрируется в НА с адресом для передачи (CoA). CoA может быть CoA внешнего агента FA (IP адрес FA) или совмещенным CoA (например, полученным с помощью протокола динамического конфигурирования главного компьютера (DHCP)). МТ должен регистрировать свой CoA в НА каждый раз, когда МТ меняет свою подсеть.

Если НА получает от СН пакеты, адресованные МТ, и МТ перемещается в визитную сеть, НА перехватывает эти пакеты и направляет их по адресу для передачи (CoA) через туннель протокола Mobile IP. FA (или МТ в случае совмещенного CoA) вскрывает полученные от НА пакеты и направляет исходные пакеты на МТ.

7.1.3 Расширения МIP: НМIP и FMIP

МIP не может действовать эффективно, если хендоверы происходят часто или требуют приложений в реальном масштабе времени. Для решения этих проблем предложено множество расширений МIP. Сюда входит иерархический МIP (НМIP) и быстрый хендовер для МIP (FMIP).

- *Иерархический МIP*

Для базового протокола Mobile IP терминал МТ должен регистрироваться (или обновлять подключение) в НА и/или СН (при использовании оптимизации маршрута) каждый раз, когда МТ меняет свою подсеть. Эта регистрация может приводить к ненужной задержке хендовера и служебной информации сигнализации. Если хендовер происходит часто или НА находится далеко от МТ, эта проблема становится еще более серьезной.

В архитектуре НМIP сети доступа организованы в иерархическом порядке. Агенты местной мобильности (LMA), называемые внешними агентами шлюза (GFA) в МIPv4, или опорные точки мобильности (MAP) в МIPv6 отвечают за управление мобильностью мобильных оконечных устройств в пределах доменов. Поэтому информация о перемещении мобильных оконечных устройств в пределах локального домена не передается на НА и СН других сетей, и это позволяет существенно уменьшить задержку при регистрации и объем служебной сигнализации. Архитектура НМIP для МIPv4 называется также "региональной регистрацией".

- *Быстрый хендовер для МIP*

Процедура регистрации МIP может начаться только после завершения хендовера на уровне линии. Отмечается, что получение соответствующей информации с более низкого уровня (до завершения операции хендовера в линии) может уменьшить задержку хендовера для МIP. Это основной принцип подхода FMIP. Кроме того, используется двунаправленный туннель между маршрутизаторами доступа для обеспечения хендовера с низкими потерями. IETF допускает применение протоколов подвижной связи с низкой задержкой хендовера для IP версии 4 и быстрого хендовера для протокола Mobile IP версии 6.

На рисунке 7.2 показана архитектура МIP с расширениями для MM. Как видно из рисунка, MM между LMA поддерживается с помощью протокола Mobile IP. Каждый LMA используется для локального управления мобильностью внутри местного домена. Протокол быстрого хендовера используется для поддержки быстрого хендовера внутри домена LMA. Эти LMA могут быть организованы как многоуровневая иерархия.

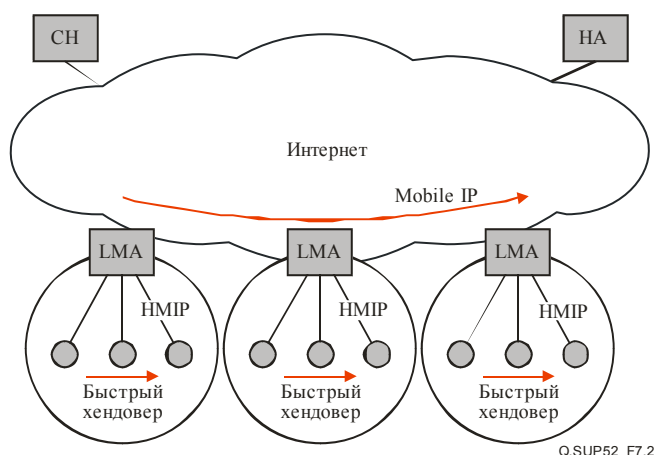


Рисунок 7.2 – MIP и его расширения для MM

7.1.4 Резюме

Следует отметить, что сочетание MIP с его расширениями для MM представляет собой подход на основе IP. Поэтому его легко объединить с сетями на основе IP. MIP уже применяется, и его расширения типа FMIP и HMIP можно реализовать с минимальными изменениями MIP. Однако этот подход может потребовать специальной информации об уровне линии (такой как триггеры L2, например, на линии вниз и на линии вверх) для поддержки быстрого хендовера FMIP. Для использования этого подхода к MM в SBI2K потребуются дополнительные исследования для задания таких триггеров на уровне линии.

7.2 Протокол начала сеанса (SIP)

7.2.1 Общие сведения

Протокол начала сеанса (SIP) был установлен в IETF для поддержки управления мультимедийными сеансами на основе IP в качестве протокола сигнализации. Более подробно SIP описан в запросах RFC 3261 IETF [41].

SIP представляет собой протокол управления на уровне приложения, который может открывать, менять и заканчивать мультимедийные сеансы. В SIP используются унифицированные идентификаторы ресурсов SIP (URI), которые по своей схеме адресации подобны адресам электронной почты. Он работает независимо от применяемых протоколов уровня транспортировки, таких как протокол управления передачей (TCP), протокол дейтаграммы пользователя (UDP) и протокол передачи для управления потоком данных (SCTP).

SIP также обеспечивает функцию определения местоположения для поддержки мобильности на основе регистрации пользователя с помощью регистратора SIP. Когда агент пользователя SIP (UA) перемещается в район новой сети, он регистрирует его текущее местоположение в базе данных о местоположении с помощью регистратора SIP. К базе данных о местоположении обращаются через прокси-сервер SIP или сервер переадресовки, когда UA является инициатором сеанса или же заканчивает этот сеанс.

Функциональные объекты SIP включают UA, прокси-сервер, сервер переадресовки, регистратор и базу данных о местоположения. Сообщения SIP делятся на два типа: запрос, который направляется клиентом агента пользователя (UAC) на сервер агента пользователя (UAS), и ответ, который содержит статус запроса.

7.2.2 ММ на основе SIP

Протокол SIP обеспечивает функцию определения местоположения для мобильности оконечного устройства. Когда мобильное оконечное устройство перемещается в новую сеть, оно регистрирует свое текущее местоположение, посылая сообщение SIP REGISTER регистратору SIP. Регистратор может отклонить или принять запрос. В случае приема запроса сервер SIP обновляет базу данных о местоположениях информацией о новом местоположении.

Когда МТ перемещается в новую сеть или систему, процедура регистрации в SIP повторяется для обновления данных о местоположении. К обновленной информации о местоположении обращаются также через прокси-серверы, когда UA является инициатором или же заканчивает этот сеанс.

Базовый SIP не обеспечивает управления бесшовным хендвером. Поэтому сеанс SIP заканчивается, когда МТ меняет свою сеть IP, поскольку основные адреса гнезд TCP/UDP больше не будут действовать для измененного адреса IP.

Однако SIP можно использовать в сочетании с другими схемами управления хендвером:

- протокол Mobile IP (MIP);
- протокол Cellular IP (CIP) (или другие протоколы локальной мобильности); и
- протокол транспортировки для управления потоком информации в сетях подвижной связи (mSCTP) (на уровне транспортировки).

7.2.3 Резюме

SIP принят в 3GPP/3GPP2 в качестве протокола управления сеансом/вызовом и также широко применяется в других сетях. SIP является перспективным вариантом протокола ММ для определения местоположения. Следует отметить, что SIP не поддерживает бесшовной мобильности. Для межсетевого ММ его можно использовать вместе с MIP или SCTP. Для внутрисетевого ММ его можно использовать вместе с CIP, MIP или mSCTP.

7.3 Протокол Cellular IP (CIP)

7.3.1 Общие сведения

CIP был первоначально предназначен для внутрисетевого ММ в беспроводных сетях доступа, а не для межсетевого ММ. Для получения эффективного внутрисетевого ММ протокол CIP принял свою собственную маршрутизацию на основе главного компьютера, для которой требуется шлюз с целью осуществления взаимодействия с Интернетом, как показано на рисунке 7.3 [46].

Маршрутизация CIP осуществляется с помощью специально предназначенной для CIP быстродействующей буферной памяти для маршрутизации или пейджинга во всех узлах CIP. Быстродействующая буферная память для маршрутизации (RC) используется для маршрутизации пакетов, а быстродействующая буферная память для пейджинга (PC) используется для поддержки пассивного соединения в сети CIP. RC и PC обновляются специальными пакетами обновления, посылаемыми МТ.

В CIP используется также внутренний адрес (HoA) МТ в качестве идентификатора местоположения МТ в сети CIP. Поэтому дополнительный идентификатор местоположения (CoA в MIP) задавать не нужно, и не требуется формирование пакетов и преобразование адреса при транспортировке данных.

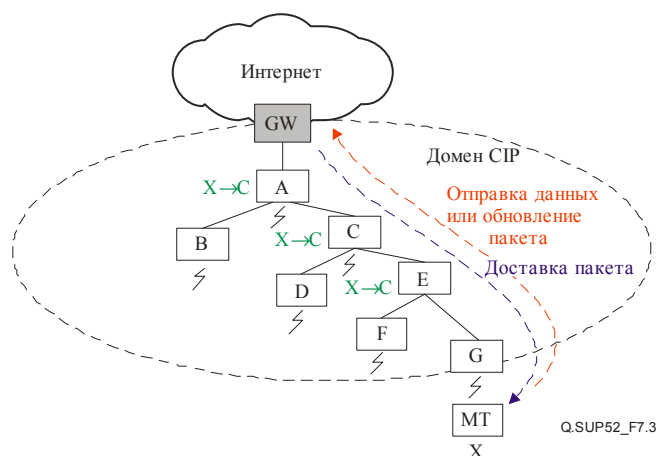


Рисунок 7.3 – Операции протокола SIP

Как показано на рисунке 7.3, каждый узел ведет таблицу пересылки с помощью RC для маршрутизации пакетов и PC для пейджинга. Эта быстродействующая буферная память обновляется данными или управляющими пакетами, посылаемыми MT X. Информация о маршрутизации или пейджинге для MT в быстродействующей буферной памяти управляется в соответствии с гибкой программой, и поэтому она остается до тех пор, пока соответствующие пакеты обновления не поступят в течение заданного времени.

Если MT расположено в пределах охвата узла G и имеет пакеты для передачи в СН, эти пакеты будут пересылаться в шлюз SIP любым узлом с маршрутизацией по кратчайшему пути. Узлы на пути передачи данных с помощью этих пакетов обновляют свои RC и PC. После этого, если пакеты направляются в MT из СН, они пересылаются в следующий узел по таблицам пересылки в RC и PC. Если в MT нет пакетов для отправки, оно посылает пакет обновления для обновления быстродействующей буферной памяти маршрутизации и пейджинга.

7.3.2 Протокол SIP вместе с MIP для MM

Протокол SIP можно использовать для MM вместе с MIP. В качестве примера на рисунке 7.4 показано сочетание MIPv4 и SIP для MM. В этой схеме MIPv4 используется для межсетевых MM между разными сетями SIP, а SIP используется для внутрисетевого MM в сети SIP. Внешние агенты (FA) для MIPv4 расположены в шлюзе SIP.

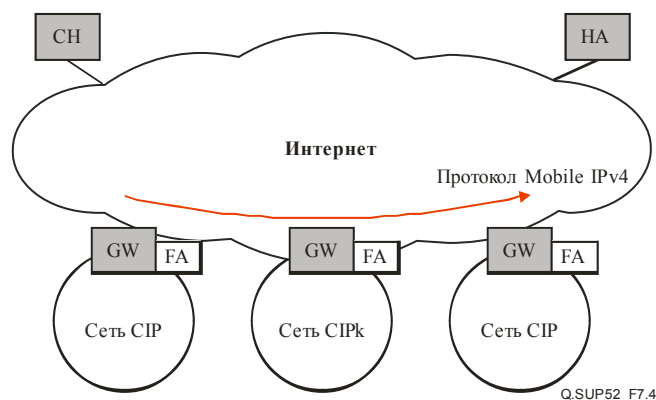


Рисунок 7.4 – Протокол SIP вместе с MIPv4 для MM

Когда МТ входит в район СІР, оно сначала проводит регистрацию в МІРv4, посылая сообщения об изменении подключения в НА и/или СН (при использовании оптимизации маршрута), которые доставляются через шлюз (GW) СІР. После этого перемещение внутри домена СІР управляется протоколом СІР. Если МТ переходит в домен другого СІР, оно должно снова выполнить регистрацию в МІРv4. Соответствующая схема синхронизации приведена на рисунке 7.5.

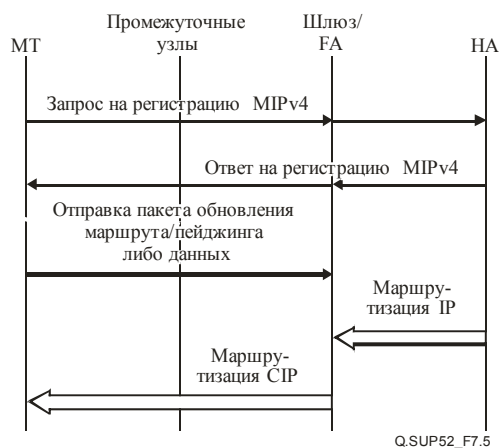


Рисунок 7.5 – Поток вызовов для СІР вместе с МІРv4

7.3.3 Протокол СІР вместе с SIP для ММ

На рисунке 7.6 показана архитектура, основанная на сочетании SIP и СІР.

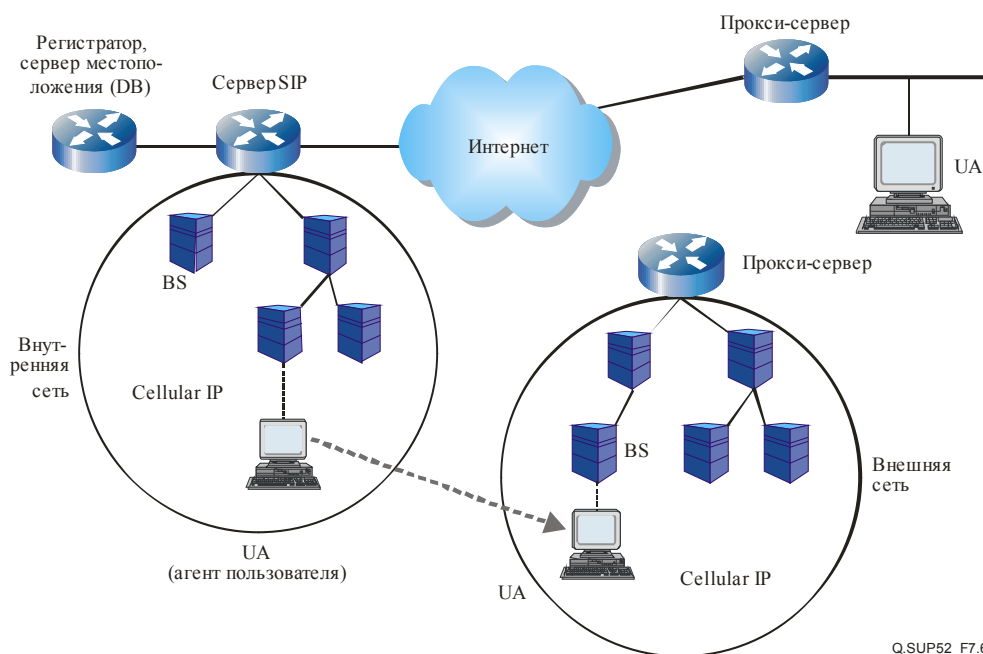


Рисунок 7.6 – Архитектура СІР вместе с SIP

CIP можно использовать в сочетании с SIP; где CIP осуществляет функции внутрисетевого MM, а SIP используется для межсетевого MM. Однако SIP может обеспечить только функцию определения местоположения, но не управление хендвером.

Как показано на рисунке 7.6, система SIP состоит из прокси-сервера SIP, регистратора SIP и UA, а сеть CIP состоит из шлюза и базовых станций (БС). Сервер SIP (прокси) используется для отслеживания перемещения UA (MT) во внутренней и внешней сетях. Сервер SIP работает как шлюз CIP. Протокол Cellular IP используется для поддержания бесшовной мобильности в пределах домена CIP.

Когда UA подключен к своей внутренней сети, он регистрирует информацию о своем текущем местоположении в сервере SIP, расположенном во внутренней сети. Пока UA перемещается в домене CIP после регистрации в SIP, внутрисетевое MM осуществляется по протоколу CIP. Если UA перемещается в другую сеть CIP, его нужно снова зарегистрировать, чтобы предоставить информацию о его текущем местоположении для сервера SIP внутренней сети, что можно осуществить с помощью внешнего прокси-сервера.

Регистрация в SIP включает процедуры для обновления местоположения и для удаления UA. Если UA перемещается в другую сеть CIP, его текущее местоположение нужно зарегистрировать с помощью регистратора. Эта информация будет использована при сигнализации настройки вызова для MT.

7.4 Протокол передачи для управления потоком информация в сетях подвижной связи (mSCTP)

7.4.1 Общие сведения

Протокол передачи для управления потоком данных (SCTP), определенный в запросе RFC 2960 IETF [35], представляет собой протокол сквозной передачи, ориентированный на соединение, который передает множество потоков данных.

Наличие нескольких внутренних сетей у SCTP позволяет поддерживать для конечных точек SCTP несколько адресов IP. Наличие нескольких внутренних сетей защищает соединение от возможных сбоев сетей, направляя трафик по другому адресу IP. При инициировании соединения конечные точки SCTP обмениваются перечнями адресов IP. Поэтому каждая конечная точка может посылать и принимать сообщения от любого имеющегося в перечне адреса IP, указанного в удаленной конечной точке. Например, один из перечисленных адресов IP задается при инициировании как первичный адрес. Если первичный адрес многократно сбрасывает пакеты данных, то все последующие пакеты данных будут передаваться по другому адресу, пока не будет восстановлено соединение с первичным адресом.

Следует отметить, что наличие нескольких внутренних сетей у SCTP может поддерживать мобильность IP. Конкретнее, SCTP с расширением для динамического конфигурирования адресов можно использовать для обеспечения плавного хендвера мобильного оконечного устройства (MT), перемещающегося в районы действия других сетей IP во время текущего сеанса. Это называется протоколом SCTP для сетей подвижной связи (mSCTP), который применим для IP-версии 4 и IP-версии 6. [47]

Протокол mSCTP представляет собой многообещающую схему хендвера. В отличие от схем хендвера на основе протокола Mobile IP, которые опираются на поддержку маршрутизаторов сети для туннелирования между маршрутизаторами доступа, mSCTP обеспечивает управление хендвером на уровне транспортировки без дополнительных изменений имеющихся маршрутизаторов.

7.4.2 Протокол mSCTP для хендвера на уровне транспортировки

Протокол mSCTP можно использовать для осуществления хендвера мобильного оконечного устройства, которое перемещается между двумя различными сетями IP с разными префиксами адресов IP. В этом разделе описан обобщенный алгоритм mSCTP для хендвера в сетях IP.

Рассмотрим мобильное оконечное устройство (MT), которое иницирует соединение SCTP с главным компьютером корреспондента (CH). После инициации соединения SCTP MT перемещается из положения А (маршрутизатор доступа А) в положение В (маршрутизатор доступа В), как показано на рисунке 7.7, на котором приведен пример использования mSCTP для хендвера в сетях IP-версии 6. Процедуры хендвера описаны подробнее ниже. Этот пример можно аналогичным образом использовать для сетей IP-версии 4.

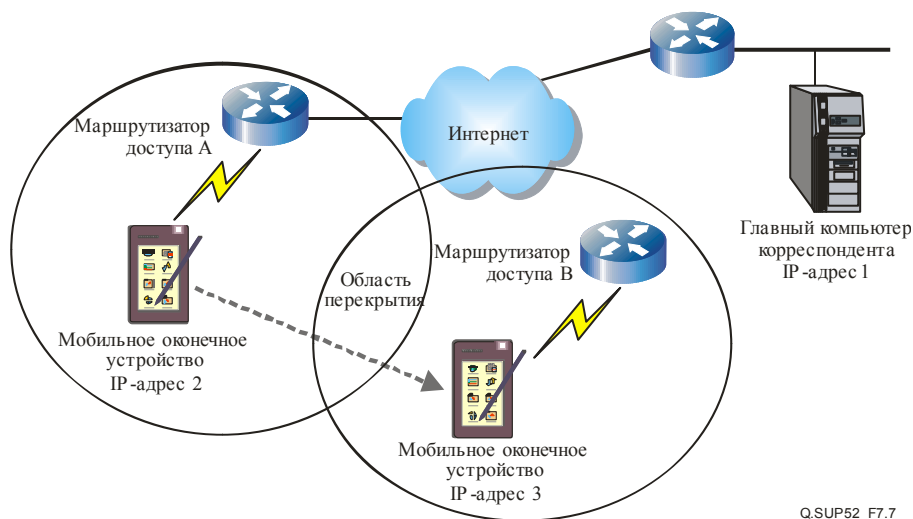


Рисунок 7.7 – Протокол mSCTP для хендовера

- *Инициирование сеанса мобильным оконечным устройством*

MT инициирует соединение SCTP с помощью CH. MT получает адрес IP от маршрутизатора доступа (AR) А через автоконфигурацию адреса без запоминания в IP версии 6 или DHCPv6.

- *Получение адреса IP для нового местоположения*

MT перемещается от AR А к AR В и входит в район перекрытия охвата двумя AR. MT получает новый IP-адрес 3 от AR В с помощью DHCPv6 или автоконфигурации адреса без запоминания в IP-версии 6. Вновь полученный IP-адрес 3 передается SCTP на уровне транспортировки, и SCTP связывает новый адрес IP с перечнем адресов, ведущимся соединением SCTP.

- *Добавление нового адреса IP к соединению SCTP*

После получения нового адреса IP протокол SCTP данного MT сообщает SCTP компьютера CH, что он будет использовать новый адрес IP. Это осуществляется с помощью посылки изменения конфигурации адресов SCTP (ASCONF) в CH. MT может получить в ответ подтверждение ASCONF-ACK от CH.

После этого MT оказывается в состоянии с двумя внутренними сетями. Старый адрес IP (IP-адрес 2) продолжает использоваться как первичный адрес, пока MT не задаст новый IP-адрес 3 в качестве "первичного адреса". До установки нового первичного адреса IP-адрес 3 используется как резервный путь.

- *Изменение первичного адреса IP*

По мере дальнейшего движения MT к AR В возникает необходимость перевести его новый адрес IP в разряд первичного адреса IP по соответствующим правилам. Структура этого специального правила для включения такого "изменения первичного адреса" является решающим вопросом при разработке mSCTP.

После изменения первичного адреса CH посылает данные в MT по новому первичному адресу IP (IP-адресу 3). Любые утраченные данные можно повторно передать по резервному (старому) адресу IP (IP-адресу 2) для MT.

- *Удаление старого адреса IP из соединения SCTP*

По мере дальнейшего движения MT к AR В, если старый адрес IP (IP-адрес 2) перестает действовать, MT удаляет его из перечня адресов. Правило определения того, что адрес IP не работает, можно ввести, воспользовавшись дополнительной информацией из используемой сети или физического уровня.

Описанные выше этапы этой процедуры для обеспечения бесшовного хендвера повторяются каждый раз, когда МТ перемещается в новое место, пока не будет отключено соединение SCTP.

7.4.3 Использование протокола mSCTP вместе со схемой определения местоположения

Для поддержки сеансов подвижной связи, инициируемых СН для МТ, можно использовать протокол mSCTP вместе со схемой определения местоположения, такой как SIP или MIP. В этом сценарии SIP или MIP используется для СН с целью определения местоположения МТ и для установления соединения SCTP с МТ. После успешного установления соединения SCTP протокол mSCTP используется для обеспечения бесшовного хендвера для МТ. После установления соединения транспортировка данных между МТ и СН основывается только на mSCTP и не использует MIP.

- *mSCTP с SIP*

SIP является протоколом уровня приложения, а SCTP – протоколом уровня транспортировки. В этом сценарии SIP используется для определения местоположения и сигнализации при управлении вызовами. После установления сеанса SIP (например, через TCP/UDP/SCTP) можно использовать новое соединение SCTP для транспортировки данных между двумя рассматриваемыми UA. Еще предстоит изучить возможности транспортировки через mSCTP данных в реальном масштабе времени. Когда UA перемещается к новому AR, срабатывают механизмы хендвера mSCTP и начинается процедура регистрации SIP для введения нового адреса в базу данных о местоположениях.

- *mSCTP с MIP*

В этом сценарии функция определения местоположения MIP используется для доставки сигнала включения SCTP от СН к МТ. После успешного включения SCTP управление хендвером осуществляется в соответствии с процедурами mSCTP. (Подробнее см. раздел 7.4.2.)

7.5 Протоколы управления мобильностью 3GPP

Технические требования для базовых сетей GSM с включением базовой сети UMTS были разработаны в партнерском проекте по системам третьего поколения (3GPP) и переданы участвующим региональным организациям по разработке стандартов (SDO). В этом разделе описан протокол MM для пакетного обслуживания системы 3GPP выпуска 5, который приведен в технических характеристиках 3GPP, указанных в Рекомендации МСЭ-Т Q.1741.3 [13].

7.5.1 Архитектура сети для домена PS

Базовая сеть домена пакетного обслуживания (PS) для 3GPP выпуска 5 включает подсистему службы пакетной радиосвязи общего пользования (GPRS) и компоненты, используемые для управления мобильностью (MM) [13].

Пакетный домен использует методы пакетного режима для передачи данных с высокой и низкой скоростью и эффективной сигнализации. Пакетный домен оптимизирует использование сети и радиоресурсов. Поддерживается строгое разделение подсистемы радиосвязи и подсистемы сети, что позволяет использовать подсистему сети с другими технологиями радиодоступа.

Общая базовая сеть пакетного домена используется как для сетей радиодоступа (RAN), сетей радиодоступа GSM EDGE (GERAN), так и для универсальной наземной сети радиодоступа (UTRAN). Такая общая базовая сеть вместе с этими RAN обеспечивает услуги GPRS. Она предназначена для поддержки нескольких уровней качества обслуживания, чтобы обеспечить эффективную передачу автономного трафика (например, для перемежающихся и пакетных передач данных, нерегулярной передачи больших объемов данных) и передачу трафика в реальном масштабе времени (например, голосового, видео). Поддерживаются приложения, основанные на стандартных протоколах передачи данных и услугах коротких сообщений (SMS), а взаимодействие определяется с помощью сетей IP.

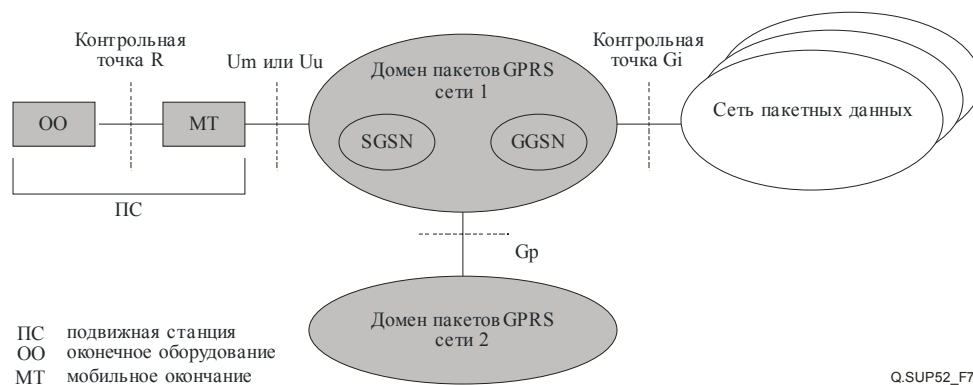


Рисунок 7.8 – Архитектура для услуг пакетированных данных (система GPRS)

Обслуживающий узел поддержки GPRS (SGSN) отслеживает местоположение мобильного оконечного устройства (MT) и выполняет функции защиты и управления доступом. Операции управления мобильностью (MM) для абонента характеризуются с помощью одного из трех различных состояний. В режиме A/Gb для абонента GPRS MM может находиться в состоянии IDLE, STANDBY и READY. В режиме Iu для абонента GPRS MM может находиться в состояниях управления мобильностью в пакетной связи (PMM) DETACHED, PMM IDLE и PMM CONNECTED. Каждое состояние характеризует определенный уровень функций и распределения информации. Информационные комплекты, удерживаемые на MT и SGSN, обозначаются в контексте MM.

Состояние MM относится только к операциям GPRS MM абонента. Состояние MM не зависит от числа и состояния контекстов протокола пакетных данных (PDP) для этого абонента.

Узел поддержки GPRS шлюза (GGSN) обеспечивает взаимодействие с сетями пакетных данных и соединен с SGSN через магистральную сеть ССПСП для пакетного домена на основе IP.

В регистре местонахождения внутренней сети (HLR) содержится информация об абонентах.

Дополнительно может быть расширен центр коммутации подвижной связи (MSC)/визитный регистр местонахождения (VLR) для более эффективной координации служб и функций с коммутацией пакетов и с коммутацией линий, например, совместного обновления местоположения для GPRS и не для GPRS.

Чтобы можно было пользоваться услугами GPRS, мобильное оконечное устройство (MT) должно сначала оповестить сеть о своем присутствии, выполнив присоединение к GPRS. Это делает MT доступным для пейджинга через SGSN и уведомления о входящих пакетных данных.

Чтобы можно было посылать и принимать пакетные данные с помощью GPRS, мобильное оконечное устройство (MT) должно активировать контекст протокола пакетных данных, который оно собирается использовать. Эта операция оповещает MT в соответствующем узле GGSN и может начаться взаимодействие с сетями передачи данных.

Данные пользователя передаются в прозрачном режиме между мобильным оконечным устройством (MT) и сетями пакетных данных с формированием пакетов и туннелированием, причем пакеты данных снабжаются информацией о специальном протоколе GPRS и передаются между MT и GGSN. Этот прозрачный метод передачи смягчает требования к ССПСП по интерпретации внешних протоколов передачи данных и облегчает введение дополнительных протоколов межсетевое взаимодействия в будущем.

7.5.2 Управление мобильностью в системе 3GPP на основе подсистемы обеспечения подвижной станции (MAP)

Для работы с MT в режиме роуминга необходимо передавать информацию между объектами ССПСП.

В системе 3GPP такая передача информации осуществляется с помощью подсистемы обеспечения подвижной станции (MAP), которая задана в 3GPP как сервисный объект прикладного уровня (ASE) в пределах логического объекта прикладного уровня (ЛОПУ), работающий в системе сигнализации № 7 (SS7), которая определена в Рекомендациях МСЭ-Т серии Q.700 и охватывает сегмент передачи

сообщений (MTP, серия Q.70x), сигнализацию в подсистеме управления соединением (SCCP, серия Q.71x) и подсистему обеспечения возможностей транзакции (TCAP, серия Q.77x). Структура объекта прикладного уровня и его ASE, а также его положение в SS7 описано в Рекомендации МСЭ-Т Q.1400 [5].

3GPP TS 29.002 [26] определяет подсистему обеспечения подвижной станции (MAP), требования к системе сигнализации и процедуры, требуемые на прикладном уровне для обеспечения этих потребностей сигнализации.

MAP также используется в качестве MMP в пакетном домене (домене GPRS) системы 3GPP.

7.5.3 Протокол MIP и SIP в системе 3GPP

Сеть GPRS предусматривает поддержку дополнительных услуг MIP для межсетевых MM.

Для эффективной поддержки дополнительных услуг протокола Mobile IP с помощью GPRS необходимо предусмотреть в GGSN функции внешнего агента (FA) [25]. Интерфейс между GGSN и FA, включая отображение между адресом IP для передачи и туннелем для протокола туннелирования GPRS (GTP) в ССПСП, не стандартизован, поскольку GGSN и FA рассматриваются как один объединенный узел.

SIP используется как протокол управления вызовами для мультимедийной подсистемы базовой сети на основе IP (IMS) в 3GPP выпуска 5 [13]. Регистрация пользователя на основе SIP в сочетании с подсистемой внутренних абонентов (HSS) обеспечивает уровень отслеживания местоположения, не зависящий от технологии доступа.

7.5.4 Резюме

Для внутрисетевого и межсетевого MM в системе 3GPP отслеживание местоположения и мобильность в домене PS основана на процедурах MM в GPRS с использованием протоколов, таких как GTP и GSM MAP.

Для межсетевого MM в GGSN может быть дополнительно введен протокол MIP.

Начиная с выпуска 5, в 3GPP определяется IMS, которая основана на протоколе SIP и обеспечивает SIP на основе MM в дополнение к имеющейся GPRS на основе MM.

7.6 Протоколы управления мобильностью для 3GPP2

В этом разделе описана базовая сеть мультимедийного домена IP (MMD), разработанная в рамках ANSI-41 Американского национального института стандартов (ANSI), с точки зрения протокола MMP 3GPP2, который основан на Рекомендации МСЭ-Т Q.1742.3 [16].

7.6.1 Общие сведения о базовой сети MMD, полностью основанной на IP и разработанной в рамках стандарта ANSI-41

Базовая сеть для cdma2000 основана на системе, разработанной в рамках стандарта ANSI-41. Технические требования к базовой сети были разработаны в партнерском проекте 2 по системам третьего поколения (3GPP2) и переданы участвующим региональным организациям по разработке стандартов (SDO).

Эта система поддерживает различные приложения от узкополосных до широкополосных систем связи с встроенной мобильностью пользователя и оконечного устройства для выполнения требований пользователя и обслуживания.

Основная архитектура разработанной в рамках стандарта ANSI-41 базовой сети с членом семейства сети доступа по методу cdma2000 включает основанную на коммутации каналов и пакетов базовую сеть и полностью основанный на IP мультимедийный домен (MMD). Базовая сеть полностью основанного на IP MMD может рассматриваться как возможный вариант базовой сети для SBI2K. На рисунке 7.9 представлена общая архитектура разработанной в рамках стандарта ANSI-41 полностью основанной на IP базовой сети с сетью доступа по методу cdma2000, которая определена в Рекомендации МСЭ-Т Q.1742.3 [16].



Рисунок 7.9 – Упрощенная архитектура разработанной в рамках стандарта ANSI-41 и полностью основанной на IP базовой сети с сетью доступа по методу cdma2000

MMD сети, полностью основанной на IP, обеспечивает как общую поддержку пакетных данных, так и возможности мультимедийных сеансов (мультимедийная подсистема на основе IP (IMS)). Возможности мультимедийных сеансов дополняют возможности общей поддержки пакетных данных. Общие возможности для пакетных данных можно реализовать без введения мультимедийных сеансов. Некоторые объекты сети используются одновременно для обеспечения обеих возможностей.

SIP используется как протокол управления вызовами для IMS в системе 3GPP2. Регистрация пользователя на основе SIP в сочетании с HSS предоставляет уровень отслеживания местоположения, который не зависит от технологии доступа.

7.6.2 ММ в разработанной в рамках стандарта ANSI-41 базовой сети IP MMD

На рисунке 7.10 показана подсистема пакетных данных (PDS) разработанной в рамках стандарта ANSI-41 базовой сети IP MMD. Каждый из объектов обладает следующими функциями.

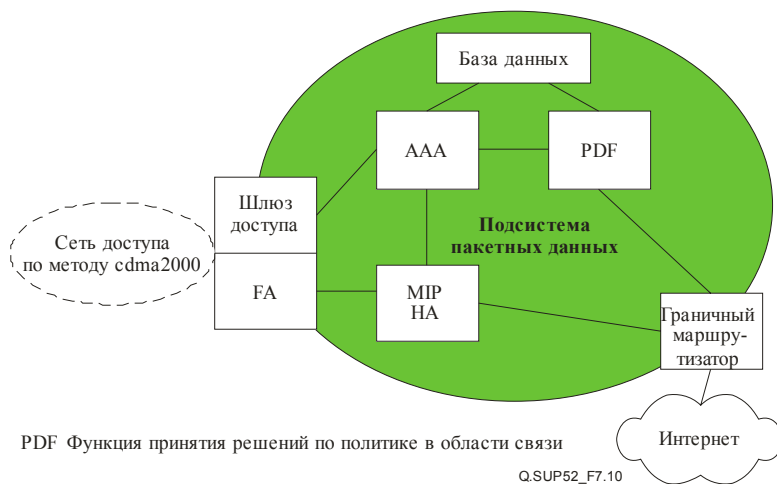


Рисунок 7.10 – PDS разработанной в рамках стандарта ANSI-41 и полностью основанной на IP базовой сети MMD

- Шлюз доступа (AGW)

Шлюз AGW по методу cdma2000 состоит из узла обслуживания пакетной передачи данных (PDSN) и других логических функций, требуемых для стыковки базовой сети с сетью доступа по методу cdma2000 (AN). PDSN маршрутизирует исходящий из МТ и заканчивающийся в МТ трафик пакетных данных. PDSN вводит, поддерживает и заканчивает сеансы на уровне линии с МТ.

- *Внутренний агент протокола Mobile IP (НА)*

НА обеспечивает две основные функции: регистрацию текущей точки подключения пользователя и пересылку пакетов IP к текущей точке подключения пользователя и от нее (передаваемый адрес для IP версии 4 или совмещенный передаваемый адрес для IP-версии 6). НА принимает запрос на регистрацию, используя протокол Mobile IP, и использует информацию в этих запросах для обновления внутренней информации о текущей точке подключения пользователя, то есть текущем адресе IP, который надо использовать для передачи IP-пакетов пользователю и приема пакетов от него.

Агент НА взаимодействует с сервером AAA для идентификации и авторизации запросов на регистрацию протокола Mobile IP и возвращает ответы с регистрацией Mobile IP. Агент НА также взаимодействует с AGW для получения последующих запросов на регистрацию Mobile IP.

- *Сервер идентификации, авторизации и учета (AAA)*

Сервер AAA обеспечивает идентификацию, авторизацию и учет на основе IP. Сервер AAA поддерживает соединения в целях защиты с равноправными объектами AAA для обеспечения функций AAA внутри административного домена и между доменами. Функция идентификации обеспечивает идентификацию оконечных устройств и абонентов. Функция авторизации AAA осуществляет авторизацию запросов на обслуживание и имеет доступ к стратегическим архивным данным, справочной службе, профилям абонентов и регистратору устройств. Функция учета собирает данные, относящиеся к обслуживанию, QoS и мультимедийным ресурсам, запрашиваемым и используемым отдельными абонентами.

- *База данных (DB)*

Информация в базах данных базовой сети включает регистр идентификатора оборудования (РИО), динамическую информацию об абоненте, стратегические правила для сети и профили абонентов, но может не ограничиваться этим.

- *Граничный маршрутизатор (BR)*

BR соединяет базовую сеть с равноправными сетями (например, сетями других поставщиков услуг, корпоративными сетями, сетью Интернет). BR осуществляет маршрутизацию пакетов IP, обрабатывает протоколы маршрутизации внешних шлюзов и обеспечивает соответствие входящего и выходящего трафика предварительно установленным соглашениям об уровне обслуживания между равноправными сетями.

- *Функция принятия решений по политике в области связи (PDF)*

PDF обеспечивает управление ресурсами QoS базовой сети в пределах своей базовой сети, которые требуются для поддержки обслуживания пользователей сети.

7.6.3 Резюме

Для внутрисетевого ММ в системе 3GPP2 определение местоположения и управление хендовером осуществляются с помощью протоколов, таких как MIP, ANSI-41 и технических требований к возможности взаимодействия (IOS).

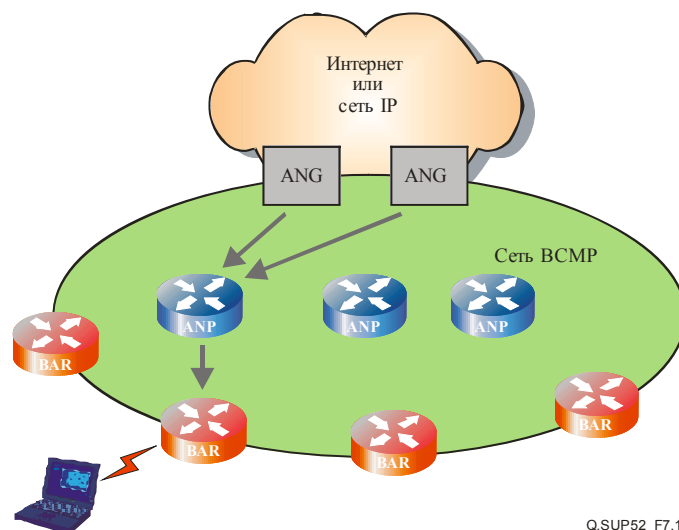
Для межсетевого ММ можно использовать MIP.

В 3GPP2 дополнительно определено управление межсетевым и внутрисетевым ММ на основе SIP (IMS).

7.7 Возможный протокол мобильности BRAIN (BCMP)

7.7.1 Общие сведения по BCMP

Протокол BCMP (возможный протокол мобильности BRAIN) был разработан в рамках проекта BRAIN для улучшения существующих схем мобильности. На рисунке 7.11 приведены его общие операции. В общем, сети доступа состоят из прежних маршрутизаторов IP и для поддержки протокола BCMP нужны дополнительные функции, которые должна обеспечивать сеть доступа.



Q.SUP52_F7.11

Рисунок 7.11 – Архитектура ВСМР

- Маршрутизаторы доступа BRAIN (BAR), расположенные на краю BRAIN AN, обеспечивают связь по IP для мобильных оконечных устройств (MT). Для обслуживаемых ими MT они работают как маршрутизаторы по умолчанию.
- Опорные точки (ANP) расположены внутри AN в избранных положениях. ANP имеют и распределяют адреса IP, идентифицируют пользователей, поддерживают регистрацию пользователей и туннелируют пакеты к MT.

В этом контексте для шлюза сети доступа (ANG) не требуется специальная функция мобильности, так как он действует как стандартный пограничный маршрутизатор, изолируя AN от внешних протоколов маршрутизации и распределяя трафик по нужным точкам ANP. Специальная функция мобильности обеспечивается с помощью ANP, осуществляя при этом развязку пограничных функций, предоставляемых ANG. Такое разделение ролей обеспечивает более гибкую реализацию и устанавливает явную границу для AN.

ANP находятся в пространстве глобальной маршрутизации адресов и распределяют адреса IP для MT, когда они регистрируются в AN. Адрес MT не меняется, пока MT перемещается внутри AN. Это обеспечивает маршрутизацию по префиксу пакетов, направляемых по адресу MT к точке ANP, в которой был выведен этот адрес. Эта ANP туннелирует пакеты в BAR, в котором в данный момент расположено MT местоназначения. ANP должны поддерживать обновляемую информацию о местоположении MT, для которых они выделили адреса, и обновлять эту информацию, когда MT меняют свой BAR. Кроме того, имеется механизм изменения ANP, который можно включать, когда маршрут к MT оказывается неэффективным. ВСМР поддерживает хендовер и пейджинг.

7.7.2 Протокол ВСМР с MIP для MM

На рисунке 7.12 показано сочетание MIP и ВСМР для MM. В этой схеме MIP используется для межсетевого MM между разными сетями ВСМР, а ВСМР используется для внутрисетевого MM в каждой сети ВСМР. Функции конфигурации адреса FA для MIP находятся в ANP.

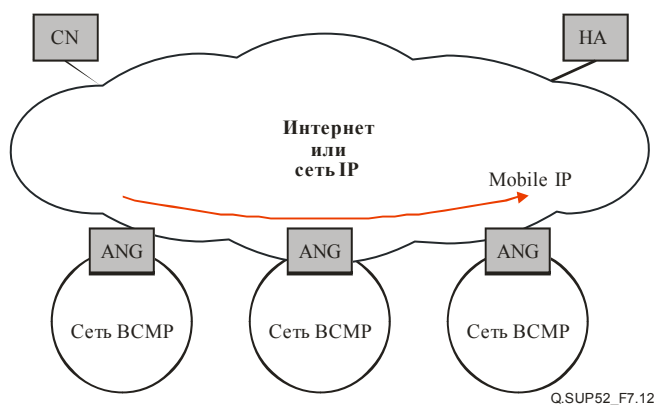


Рисунок 7.12 – Архитектура VMCP с MIP для MM

Когда МТ входит в район действия ВСМР, оно получает адрес IP, используя процедуры сети доступа для ВСМР, и затем может использовать его для совмещенного передаваемого адреса (ССоА) в условиях действия MIP. Последующие регистрационные сообщения внутреннего агента, который может находиться в любом месте в сети Интернет или сети IP, или обновления подключения, например для оптимизации маршрута, совершенно прозрачны. Внутри сети ВСМР перемещение управляется с помощью протокола ВСМР. При перемещении МТ в другой домен ВСМР оно обязано снова провести регистрацию в MIP.

7.7.3 Протокол ВСМР с SIP для MM

На рисунке 7.13 представлена архитектура, основанная на сочетании SIP и ВСМР.

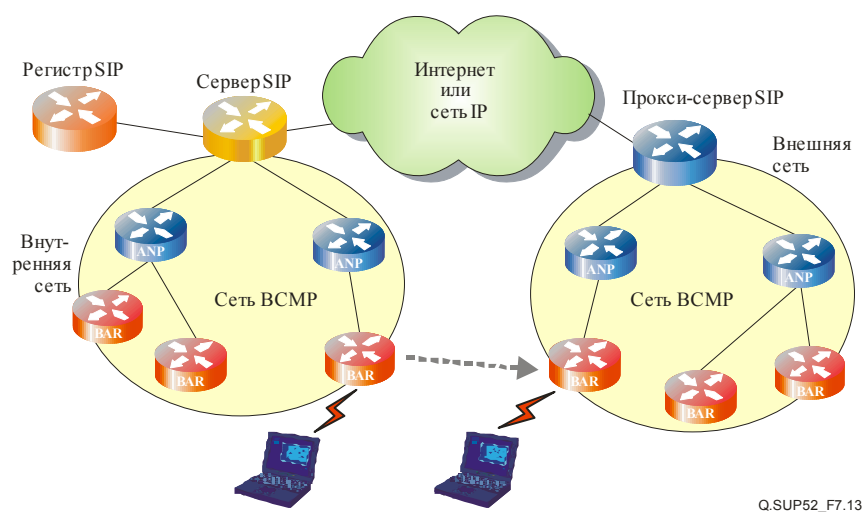


Рисунок 7.13 – Архитектура VMCP с SIP для MM

Таким способом можно поддерживать мобильность SIP. Показанная на рисунке 7.13 система SIP состоит из регистратора SIP, сервера и прокси-сервера. На рисунке показаны точки ANP и BAR, которые составляют сеть ВСМР. Сервер SIP и прокси-сервер SIP используются для управления перемещением МТ во внутренней и внешней сетях. Оба они действуют как ANG, то есть шлюзы ВСМР. Для обеспечения бесшовной мобильности в домене ВСМР используется протокол ВСМР.

MT приобретает адрес IP при соединении с сетью BCMP, и этот адрес затем используется при регистрации на выбранном сервере SIP, который может находиться в любом месте глобальной сети. Из этой точки сеть BCMP "видит" сообщения о согласовании сеансов и пакеты данных в виде пакетов IP, и они не требуют никакой специальной обработки.

7.7.4 Резюме

BCMP представляет собой протокол для внутрисетевого MM. Этот протокол в сочетании с MIP и SIP можно использовать как возможное решение для межсетевого MM.

8 Анализ существующих протоколов MM для SBI2K

В этом разделе проведено сравнение на высоком уровне существующих MMP, которые рассмотрены в данном документе.

8.1 Обзор существующих MMP

Ниже в таблице приведена краткая сводка обобщенных характеристик существующих протоколов MM, которые были описаны в разделе 7.

Таблица 8.1 – Особенности существующих протоколов MM

Название	Характеристики протоколов MM
MIP	<ul style="list-style-type: none"> – Протокол уровня сети. – Обеспечивает функции определения местоположения и ограниченного управления хендовером. – Требует агентов мобильности, таких как HA, FA (MIPv4). – Поддерживает оптимизацию маршрута. – Стандартизован в IETF. – Для поддержки бесшовного хендовера требуются расширения MIP.
MIP с расширениями	<ul style="list-style-type: none"> – Протокол уровня сети. – Поддерживает все функции MIP в дополнение к следующим функциям: <ul style="list-style-type: none"> • Обеспечивает управление бесшовным хендовером; • NMIP требует агентов мобильности, таких как GFA (MIPv4), MAP (MIPv4); FMIP требует расширенных AR. • NMIP снижает нагрузки трафика сигнализации. • Находится на стадии разработки.
SIP	<ul style="list-style-type: none"> – Протокол прикладного уровня. – Обеспечивает функции определения местоположения. – Не требует оптимизации маршрута. – Стандартизован в IETF. – Может использоваться с SIP, MIP (с расширениями MIP или без них), mSCTP для управления хендовером.
CIP	<ul style="list-style-type: none"> – Протокол уровня сети. – Обеспечивает управление хендовером и ограниченное определение местоположения. – Требует узлы CIP для маршрутизации и шлюз CIP для межсетевого взаимодействия. – Не требует оптимизации маршрута. – Находится на стадии разработки. – Может использоваться с MIP и SIP для определения местоположения.
mSCTP	<ul style="list-style-type: none"> – Протокол уровня транспортировки. – Обеспечивает управление хендовером. Не требует поддержки сети. – Не требует оптимизации маршрута. – Находится на стадии разработки. – Может использоваться с MIP и SIP для определения местоположения.

Таблица 8.1 – Особенности существующих протоколов ММ

Название	Характеристики протоколов ММ
3GPP ММ	<ul style="list-style-type: none"> – Обеспечивает управление хендовером и определение местоположения. – Требуется SGSN, GGSN для пакетного обслуживания. – Стандартизован в 3GPP. – Связан с технологией радиодоступа для 3GPP. – Может дополнительно поддерживать МIP.
3GPP2 ММ	<ul style="list-style-type: none"> – Обеспечивает управление хендовером и определение местоположения. – Требуется HA, FA/PDSN. – Стандартизован в 3GPP2. – Должен поддерживать МIP.
BCMP	<ul style="list-style-type: none"> – Протокол уровня сети. – Обеспечивает управление хендовером и ограниченное определение местоположения. – Требуется специальных маршрутизаторов для BCMP, таких как ANP, BAR и шлюзы ANG. – Не требует оптимизации маршрута. – Находится на стадии разработки. – Требуется межсетевое взаимодействие с другими протоколами ММ, такими как SIP и МIP.

8.2 Возможные протоколы управления мобильностью для управления мобильностью

SIP и BCMP могут не подходить для протоколов межсетевого ММ в SBI2K, поскольку они главным образом предназначены для внутрисетевого ММ. Протокол mSCTP также может не годиться для межсетевого ММ, поскольку это комплексное решение. Кроме того, все возможные расширения, включая расширение МIP, на этот раз не рассматриваются в качестве возможных протоколов для ММ, поскольку они все еще находятся на стадии разработки.

Надо также отметить, что ММ системы 3GPP2 основано на МIP для услуг пакетных данных, и поэтому его нельзя отнести к одной категории с МIP.

Поэтому среди существующих протоколов ММ протоколы МIP, SIP и 3GPP ММ могут рассматриваться как возможные протоколы для ММ в SBI2K.

В этом разделе проведен анализ возможных протоколов ММ (МIP, SIP и 3GPP ММ) в свете требований к протоколам ММ для SBI2K.

Таблица 8.2 – Возможные протоколы для MM

Требования	MIP (используется 3GPP2 MM)	SIP (используется IMS)	3GPP MM
Независимость от используемых в сети технологий доступа	☒	☒	ρ
Согласование с базовыми сетями на основе IP	☒	☒	ρ
Физическое разделение трафика управления и транспортировки	ρ	ρ	☒
Логическое разделение трафика управления и транспортировки	☒	☒	☒
Определение местоположения	☒	☒	☒
Идентификация пользователей/оконечных устройств	☒	☒	☒
Взаимодействие с AAA и схемами защиты	☒	☒	☒
Передача контекста	ρ	ρ	☒
Взаимодействие с внутрисетевым MM	☒	ρ	☒
Конфиденциальность местоположения	☒ (Если не используется RO)	ρ	☒
Поддержка "перемещающейся сети"	ρ	ρ	ρ
Поддержка пейджинга	ρ	ρ	☒
Поддержка как IP-версии 4, так и IP-версии 6	☒	☒	☒
Управление бесшовным хендвером	ρ	ρ	☒
ПРИМЕЧАНИЕ. – ☒ (поддержка), ρ (возможна поддержка)			

- *MIP*

MIP является решением для уровня сети на основе IP и не зависит от используемых технологий сети доступа. Его можно хорошо согласовать с базовыми сетями на основе IP, поскольку он основан на IP. MIP поддерживает функцию определения местоположения и ограниченное управление хендвером. В настоящее время в IETF разрабатываются передача контекста и поддержка перемещающейся сети на основе MIP. Ожидается, что возможна и поддержка пейджинга. MIP поддерживает как IP-версию 4, так и IP-версию 6.

Однако он зависит от версии IP, как показано в MIPv4 и MIPv6. Для сетей Ipv4 и Ipv6, сосуществующих в SBI2K, потребуется взаимодействие между MIPv4 и MIPv6 для обеспечения бесшовной мобильности. Основных технических требований к MIP недостаточно для обеспечения управления бесшовным хендвером для приложений в реальном масштабе времени или чувствительных к потерям, и поэтому требуется усиление или расширение MIP, такое как FMIP и NMIP.

- *SIP*

SIP является протоколом сигнализации между равноправными узлами и предназначен для поддержки управления сеансом в мультимедийных сеансах на основе IP, а также широко применяется в других сетях. SIP может обеспечить функцию определения местоположения с помощью регистратора SIP. Его можно хорошо согласовать с базовыми сетями на основе IP. Следует также отметить, что для большинства будущих систем, включая SBI2K, SIP рассматривается как протокол сигнализации. Он также может работать независимо от используемых технологий доступа. SIP не зависит от версии IP, так как он является решением для прикладного уровня.

Однако SIP не может поддерживать управление бесшовным хендвером, и поэтому требуется дальнейшее совершенствование.

- *3GPP MM*

MM системы 3GPP может обеспечивать управление хендовером и определение местоположения и может удовлетворять большинству требований к MM. Однако он может потребовать дальнейшего усовершенствования для поддержки различных сетей с неоднородным доступом.

8.3 Заключительные замечания

В настоящем документе определен ряд требований к MM для систем, разрабатываемых после IMT-2000 (SBI2K). На основе этих требований были рассмотрены и изучены существующие протоколы или схемы MM, включая Mobile IP, SIP, Cellular IP, mSCTP, BCMP, 3GPP MM и 3GPP2 MM. Следует отметить, что эти протоколы включают все варианты от находящихся в процессе разработки до уже стандартизованных.

В настоящем документе также рассмотрено, какие из существующих протоколов MM можно использовать для MM в среде SBI2K, и требует ли новая концепция или протокол для MM разработки с точки зрения SBI2K. По данным этого анализа, в качестве возможных для протокола MM считаются следующие протоколы: MIP, SIP и 3GPP MM.

Однако обнаружено, что ни один отдельный протокол из существующих протоколов MM не может поддерживать все требования для MM в SBI2K. В связи с этим может потребоваться определить новую концепцию для MM и функциональную архитектуру для SBI2K. За этим последует разработка функциональной модели MM и соответствующих потоков сообщений для нее. Эта концепция будет также включать или расширять существующие протоколы MM, чтобы она смогла обеспечить MM для ныне существующих и появляющихся базовых сетей и сетей доступа.

БИБЛИОГРАФИЯ

Указанные ниже документы приведены в качестве ссылок, не имеющих нормативного характера.

- [1] ITU-T Recommendation M.3100 (1995), "Generic network information model"
- [2] ITU-T Recommendation E.164 (1997), "The international public telecommunication numbering plan"
- [3] ITU-T Recommendation E.212 (1998), "The international identification plan for mobile terminals and mobile users"
- [4] ITU-T Recommendation Q.1290 (1998), "Glossary of terms used in the definition of intelligent networks"
- [5] ITU-T Recommendation Q.1400 (1993), "Architecture framework for the development of signalling and OA&M protocols using OSI concepts"
- [6] ITU-T Recommendation Q.1701 (1999), "Framework for IMT-2000 networks"
- [7] ITU-T Recommendation Q.1702 (2002), "Long-term vision of network aspects for systems beyond IMT-2000"
- [8] ITU-T Recommendation Q.1703 (2004), "Service and Network Capabilities Framework of Network Aspects for Systems Beyond IMT-2000"
- [9] ITU-T Recommendation Q.1711 (1999), "Network functional model for IMT-2000"
- [10] ITU-T Recommendation Q.1721 (2000), "Information flows for IMT-2000 capability set 1"
- [11] ITU-T Recommendation Q.1741.1 (2002), "IMT-2000 References to Release 1999 of GSM Evolved UMTS Core Network with UTRAN Access Network"
- [12] ITU-T Recommendation Q.1741.2 (2002), "IMT-2000 References to Release 4 of GSM evolved UMTS Core Network with UTRAN Access Network"
- [13] ITU-T Recommendation Q.1741.3 (2003), "IMT-2000 References to Release 5 of GSM evolved UMTS Core Network"
- [14] ITU-T Recommendation Q.1742.1 (2002), "IMT-2000 References to ANSI-41 evolved Core Network with cdma2000 Access Network"
- [15] ITU-T Recommendation Q.1742.2 (2003), "IMT-2000 References (approved as of 11 July 2002) to ANSI-41 Evolved Core Network with cdma2000 Access Network"
- [16] ITU-T Recommendation Q.1742.3 (2004), "IMT-2000 References (approved as of 30 June 2003) to ANSI-41 Evolved Core Network with cdma2000 Access Network"
- [17] ITU-T Recommendation Q.1761 (2004), "Principles and requirements for convergence of fixed and existing IMT-2000 systems"
- [18] ITU-R Recommendation M.687-2 (1997), "International Mobile Telecommunications-2000 (IMT-2000)"
- [19] ITU-R Recommendation M.816-1 (1997), "Framework for services supported on International Mobile Telecommunications-2000 (IMT-2000)"
- [20] ITU-R Recommendation M.1034-1 (1997), "Requirements for the radio interface(s) for International Mobile Telecommunications-2000 (IMT-2000)"
- [21] ITU-R Recommendation M.1168 (1995), "Framework of International Mobile Telecommunications-2000 (IMT-2000)"

- [22] ITU-R Recommendation M.1224 (1997), "Vocabulary of terms for International Mobile Telecommunications-2000 (IMT-2000) "
- [23] ITU-R Recommendation M.1645 (2003), "Vision framework and overall objectives of the future development of IMT-2000 and of systems beyond IMT-2000"
- [24] 3GPP TR 21.902 (2003), "Evolution of 3GPP System"
- [25] 3GPP TS 23.221 (2002), "Architectural requirements"
- [26] 3GPP TS 29.002 (2004), "Mobile Application Part (MAP) specification"
- [27] IETF RFC 2003 (1996), "IP Encapsulation within IP"
- [28] IETF RFC 2004 (1996), "Minimal Encapsulation within IP"
- [29] IETF RFC 2005 (1996), "Applicability Statement for IP Mobility Support"
- [30] IETF RFC 2006 (1996), "The Definitions of Managed Objects for IP Mobility Support using SMIv2"
- [31] IETF RFC 2460 (1998), "Internet Protocol version 6 (IPv6) specification"
- [32] IETF RFC 2461 (1998), "Neighbour Discovery for IP version 6"
- [33] IETF RFC 2462 (1998), "IPv6 Stateless Address Autoconfiguration"
- [34] IETF RFC 2794 (2000), "Mobile IP Network Access Identifier Extension for IPv4"
- [35] IETF RFC 2960 (2000), "Stream Control Transmission Protocol"
- [36] IETF RFC 2977 (2000), "Mobile IP Authentication, Authorization, and Accounting Requirements"
- [37] IETF RFC 3012 (2000), "Mobile IP Challenge/Response Extensions"
- [38] IETF RFC 3024 (2001), "Reverse Tunnelling for Mobile IP"
- [39] IETF RFC 3115 (2001), "Mobile IP Vendor/Organization-Specific Extensions"
- [40] IETF RFC 3257 (2002), "SCTP Applicability Statement"
- [41] IETF RFC 3261 (2002), "SIP: Session Initiation Protocol"
- [42] IETF RFC 3262 (2002), "SIP: Locating SIP Servers"
- [43] IETF RFC 3361 (2002), "DHCP Option for SIP Servers"
- [44] IETF RFC 3344 (2002), "IP Mobility Support for IPv4"
- [45] IETF RFC 3775 (2004), "Mobility Support in IPv6"
- [46] IETF draft-ietf-mobileip-cellularip-00.txt (1999), "Cellular IP"
- [47] IETF draft-ietf-tsvwg-addip-sctp-09.txt (2004), "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration"

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия В	Средства выражения: определения, символы, классификация
Серия С	Общая статистика электросвязи
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	TMN и техническое обслуживание сетей: международные системы передачи, телефонные, телеграфные, факсимильные и арендованные каналы
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных и взаимосвязь открытых систем
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевых протоколов и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи