

# Поймите iWAG Решение для Мобильных данных 3G

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Акронимы](#)

[Пояснение используемой терминологии](#)

[Поймите сервисы мобильности \(3G/4G\)](#)

[Упрощенный поток вызовов 3G](#)

[Как WiFi помещается в сервисы мобильности \(iWAG решение\)](#)

[DHCP 3G обнаруживает поток вызовов \(часть 1\)](#)

[DHCP 3G обнаруживает поток вызовов \(часть 2\)](#)

## Введение

Этот документ описывает Интеллектуальный Шлюз беспроводного доступа (iWAG) решение и как это интегрирует технологию мобильности с Решением WiFi.

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Wireless
- Поток вызовов мобильности

### Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

## Общие сведения

Обычно для доступа к Интернету вы используете два типа интернет-сервисов:

- WiFi
- Мобильный Интернет (Сеть мобильной связи 3G/4G)

Комбинация этих двух технологий дает лучший опыт клиенту, и это - основная цель этого

решения.

iWAG решение включает комбинацию простых пользователей IP (традиционный ISG и WiFi) и пользователи Mobile IP (PMIPv6 или GTP, туннелирующий). Термин сервис мобильности использован для обращения или к сервису GTP или к сервису PMIPv6, применился к трафику пользователя. iWAG предоставляет сервисы мобильности пользователям Mobile IP, и в результате мобильный клиент может эффективно обратиться к 3G или сети мобильной связи 4G. Однако iWAG не предоставляет сервисы мобильности простым пользователям IP.

Поэтому простые пользователи IP могут обратиться к сети Public Wireless LAN (PWLAN) через Cisco ISG. Клиенты могут обратиться к Wi-Fi Интернету (общее радио), где когда-либо возможно. Однако, если WiFi не доступен, те же клиенты могут соединиться с интернет-сервисом с сетью мобильной связи 4G или 3G.

Поставщики услуг используют комбинацию WiFi, и мобильность предлагает разгружать их сети мобильной связи в области использования сервиса высокой концентрации. Это привело к развитию iWAG. iWAG предоставляет WiFi, разгружают опцию к 4G и поставщикам услуг 3G путем включения единого готового решения, которое предоставляет объединенную функциональность Мобильного IPv6 Прокси (PMIPv6) и Протокол туннелирования GPRS (GTP).

## Акронимы

GPRS - General Packet Radio Service

RNC - контроллер радиосети

SGSN - Сервисный узел поддержки GPRS

PDP - Протокол коммутации пакетов

GGSN - Gateway GPRS Support Node

APN - Название точки доступа

IMSI - международный идентификатор мобильного абонента

MSISDN - мобильная станция международный номер каталога абонента

HLR - домашний регистр местоположения

## Пояснение используемой терминологии

- Проксируйте мобильный IPv6

Сетевое управление мобильности добавляет ту же функциональность как Мобильный IP без любых модификаций к Стеку протоколов TCP/IP хоста. С PMIP хост может изменить свою точку подключения на Интернет без потребности изменить его IP-адрес. Противоречащий подходу Мобильного IP, эта функциональность внедрена сетью, которая ответственна, чтобы отследить перемещения хоста и инициировать требуемую мобильность, которая сигнализирует от своего лица. Однако в случае, если мобильность включает другие сетевые интерфейсы, хосту нужны модификации, подобные Мобильному IP для поддержания того

же IP-адреса через другие интерфейсы.

- Протокол туннелирования GPRS

GTP является группой на основе IP протоколов связи, используемых для переноса General Packet Radio Service (GPRS) в GSM, сетях UMTS и LTE.

- General Packet Radio Service

GPRS является ориентированным сервисом мобильных данных пакета на сотовой связи 3G и 2G.

- Контроллер радиосети

RNC является управляющим элементом в UMTS (3G) сеть радиодоступа (UTRAN).

- Сервисный узел поддержки GPRS

SGSN является основным компонентом сети GPRS, которая обрабатывает все данные с коммутацией пакетов в сети, например, управление мобильности и аутентификацию пользователей.

- Gateway GPRS Support Node

GGSN является частью базовой сети, которая подключает основанные на GSM сети 3G с Интернетом. GGSN, иногда известный как беспроводной маршрутизатор, работает в тандеме с SGSN для хранения мобильных пользователей связанными с Интернетом и на основе IP приложениями.

- Протокол коммутации пакетов

Контекст PDP является подарком структуры данных и на обслуживании узла поддержки GPRS (SGSN) и на узле Gateway GPRS Support Node (GGSN), который содержит информацию о сеанса абонента, когда у абонента есть активный сеанс.

- Название точки доступа

APN является названием для параметров настройки, которые ваш телефон читает для устанавливания соединения со шлюзом между сотовой сетью носителя и общедоступным Интернетом.

- Международный идентификатор мобильного абонента

IMSI используется для определения пользователя сотовой сети и является идентификационным идентификационным, привязанным ко всем сотовым сетям. Это сохранено как 64 битовых поля и передается телефоном сети.

- Мобильная станция международный номер каталога абонента

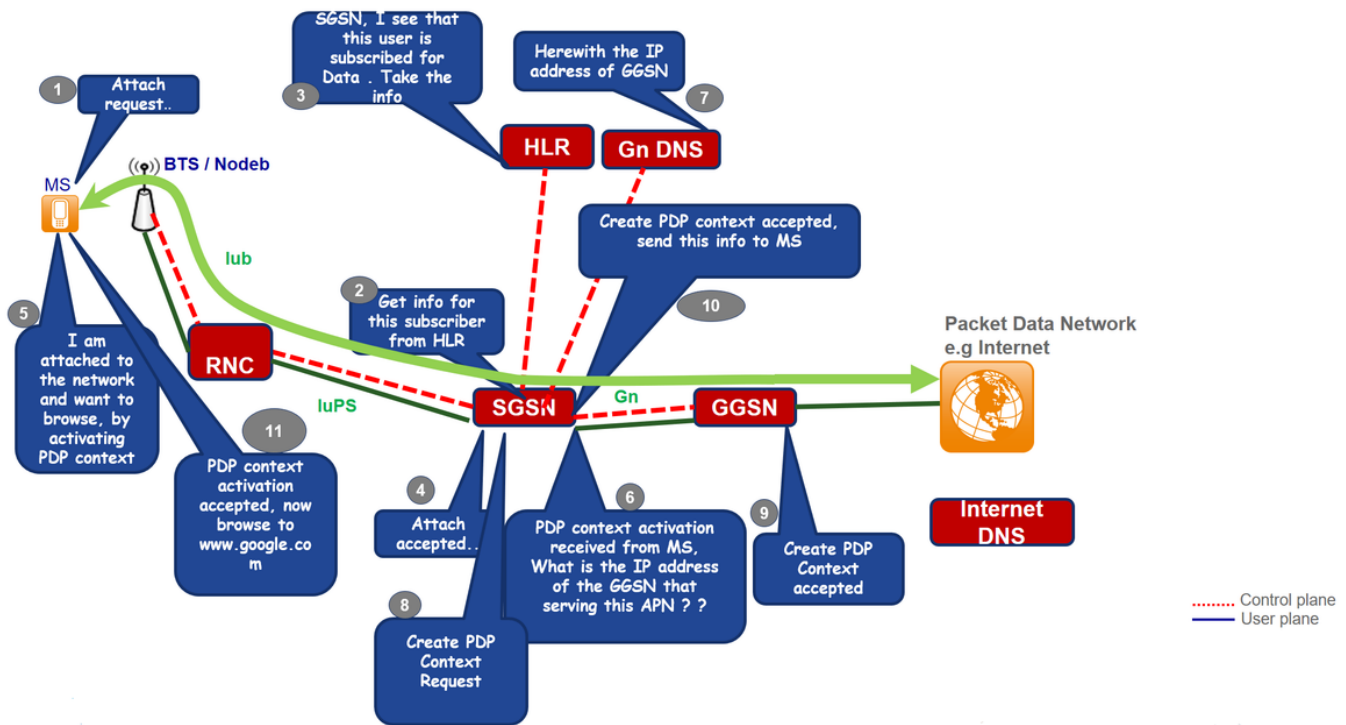
MSISDN является номером, используемым для определения номера мобильного телефона на международном уровне. MSISDN определен планом нумерации E.164. Этот номер включает код страны и Национальный код места назначения, который определяет оператора абонента.

- Домашний регистр местоположения

HLR является основной базой данных постоянных сведений об абоненте для сети мобильной связи.

# Поймите сервисы мобильности (3G/4G)

## Упрощенный поток вызовов 3G



Шаг 1. Мобильные помехи (MS) инициируют процедуру присоединения передачей сообщения Запроса Присоединения к SGSN.

Шаг 2. Если MS неизвестен на SGSN, SGSN отправляет Идентификационный Запрос к MS. MS отвечает Идентификационным Ответом, который включает IMSI MS.

Шаг 3. Если никакой контекст Менеджмента мобильности (MM) для MS не существует на SGSN (существующий сеанс), то аутентификация является обязательной. SGSN делает запрос HLR для получения информации для аутентификации мобильного телефона с Информацией для аутентификации Передачи и запрашивает, чтобы MS передал подлинную информацию путем передачи Аутентификации GPRS и Шифрования Запроса к мобильному телефону.

Шаг 4. . HLR передает Данные подписчиков Вставки к SGSN, который включает данные подписки мобильного телефона.

Шаг 5. . SGSN передает Присоединение, Принимают сообщение к MS.

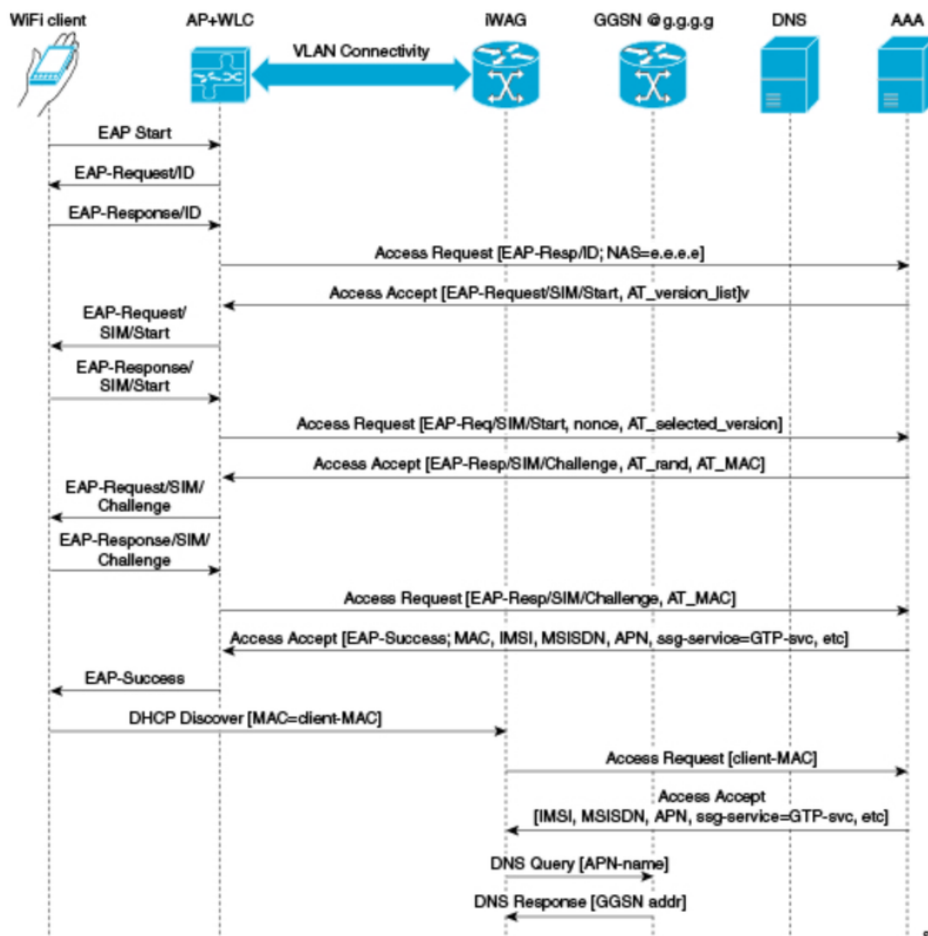
Шаг 6. MS подтверждает его путем возврата Сообщения о выполнении Присоединения к SGSN, и инициируйте контекст активации PDP, который получен SGSN, и это спрашивает DNS для IP-адреса GGSN.

Шаг 7. Создайте запрос PDP, передается GGSN после, принятие которого **Создают Контекст PDP, acceptedmessage** передается MS с пользовательским IP-адресом.

Шаг 8. Теперь MS может просмотреть Интернет.

# Как WiFi помещается в сервисы мобильности (iWAG решение)

## DHCP 3G обнаруживает поток вызовов (часть 1)



Шаг 1. Мобильное устройство автоматически привязано к идентификаторам наборов сервисов (SSID), переданным точками доступа, чтобы установить и поддержать возможность беспроводного подключения.

Шаг 2. AP или WLC запускают процесс Аутентификации eap путем передачи ID Запроса EAP к мобильному устройству.

Шаг 3. Мобильное устройство передает ответ, который принадлежит ID Запроса EAP назад к AP или WLC.

Шаг 4. . WLC отправляет Запрос ДОСТУПА К СЕРВЕРУ RADIUS к аутентификации, авторизации и учету (AAA) и просит , чтобы он аутентифицировал абонента.

Шаг 5. . После того, как абонент аутентифицируется, AAA-сервер кэширует свой весь профиль пользователя, который включает информацию о IMSI, MSISDN, APN и паре значение-атрибут Cisco , которая имеет ssg-service-info к GTP-сервису. Кэшированные данные также включают MAC-адрес клиента, который установлен как calling-station-ID во входящих сообщениях EAP.

Шаг 6. AAA-сервер передает ДОСТУП К СЕРВЕРУ RADIUS, Принимают сообщение к AP или WLC.

Шаг 7. Когда ДОСТУП К СЕРВЕРУ RADIUS Признает, что сообщение возвращается, соответствующий профиль пользователя, в котором определено использование GTP-сервиса, получен.

Шаг 8. WLC передает успешное сообщение Аутентификации ear к мобильному устройству.

Шаг 9. Мобильное устройство передает сообщение DHCP DISCOVER к iWAG. В ответ на это сообщение DHCP DISCOVER DHCP входит в новое состояние в состоянии ожидания для ожидания сигнализации на стороне MNO, которая будет завершена, который назначает IP-адрес на абонента. В ответ на это, сообщение DHCP DISCOVER, DHCP входит в новое состояние в состоянии ожидания для ожидания сигнализации на стороне MNO, которая будет завершена, который назначает IP-адрес на абонента.

Шаг 10. iWAG находит сеанс привязанным к MAC-адресу абонента и получает IP-адрес абонента из контекста сеанса.

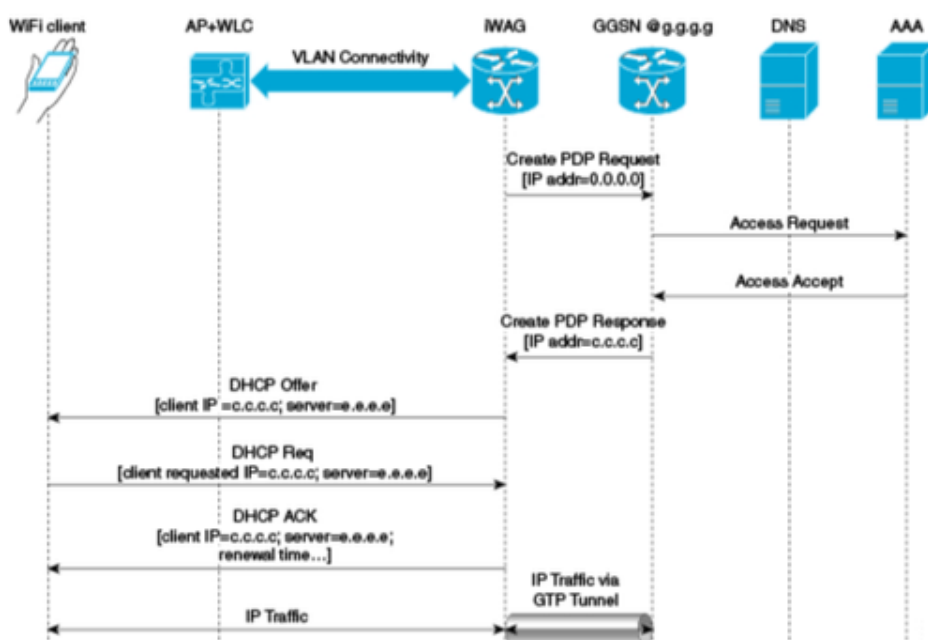
Шаг 11. iWAG отправляет Запрос ДОСТУПА К СЕРВЕРУ RADIUS к AAA-серверу и просит, чтобы он аутентифицировал абонента с использованием MAC-адреса в нем как calling-station-ID, в то время как это также предоставляет все другие известные сведения об абоненте, ID и IMSI в этом сообщении Запроса Доступа.

Шаг 12. Когда AAA-сервер передает ДОСТУП К СЕРВЕРУ RADIUS ОБРАТНО, Принимают сообщение к iWAG, профиль пользователя, в котором определено использование GTP-сервиса, получен.

Шаг 13. iWAG передает запрос к серверу DNS для решения данного Названия точки доступа (APN) к IP-адресу GGSN.

Шаг 14. Сервер DNS передает решенный DNS адрес GGSN обратно в iWAG.

## DHCP 3G обнаруживает поток вызовов (часть 2)



Шаг 15. После того, как это получает решенный DNS адрес GGSN, iWAG передает Создание Запроса Контекста PDP, в котором адрес контекста PDP установлен в 0 для запроса GGSN на присвоение IP-адреса.

Шаг 16. GGSN отправляет Запрос ДОСТУПА К СЕРВЕРУ RADIUS к AAA-серверу.

Шаг 17. На основе кэшируемой информации, полученной из аутентификации SIM EAP, ответы AAA-сервера с ДОСТУПОМ К СЕРВЕРУ RADIUS Принимают сообщение к GGSN.

Шаг 18. GGSN передает Создание Ответа Контекста PDP, который несет назначенный IP - адрес с . с . с для абонента, к iWAG.

Шаг 19. iWAG передает сообщение предложения DHCP к мобильному устройству.

Шаг 20. Мобильное устройство передает сообщение Запроса DHCP к iWAG, и iWAG подтверждает этот запрос путем передачи сообщения ACK DHCP к мобильному устройству.

Шаг 21. Трафик абонента WiFi теперь имеет путь данных, через который он может течь.