

Comprender la solución iWAG para datos móviles 3G

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Acrónimos](#)

[Explicación de la terminología utilizada](#)

[Comprender los servicios de movilidad \(3G/4G\)](#)

[Flujo de llamadas 3G simplificado](#)

[Cómo encaja WiFi en los servicios de movilidad \(solución iWAG\)](#)

[Flujo de llamadas de detección de DHCP 3G \(parte 1\)](#)

[Flujo de llamadas de detección de DHCP 3G \(parte 2\)](#)

Introducción

Este documento describe la solución Intelligent Wireless Access Gateway (iWAG) y cómo integra la tecnología de movilidad con la solución WiFi.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Tecnología inalámbrica
- Flujo de llamadas de movilidad

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Antecedentes

Normalmente para acceder a Internet se utilizan dos tipos de servicios de Internet:

- WiFi
- Internet móvil (red móvil 3G/4G)

La combinación de estas dos tecnologías ofrece una mejor experiencia al cliente y este es el

objetivo principal de esta solución.

La solución iWAG incluye una combinación de usuarios IP simples (ISG tradicional y WiFi) y usuarios IP móviles (tunelación PMIPv6 o GTP). El término servicio de movilidad se utiliza para hacer referencia al servicio GTP o al servicio PMIPv6 aplicado al tráfico de usuarios. iWAG proporciona servicios de movilidad a los usuarios de IP móviles y, como resultado, un cliente móvil puede acceder sin problemas a una red de movilidad 3G o 4G. Sin embargo, iWAG no proporciona servicios de movilidad a usuarios IP simples.

Por lo tanto, los usuarios IP simples pueden acceder a la red LAN inalámbrica pública (PWLAN) a través de Cisco ISG. Los clientes pueden acceder a Internet WiFi (red inalámbrica pública) siempre que sea posible. Sin embargo, si no hay WiFi disponible, los mismos clientes pueden conectarse al servicio de Internet con una red móvil 3G o 4G.

Los proveedores de servicios utilizan una combinación de ofertas de Wi-Fi y movilidad para descargar sus redes de movilidad en el área de uso de servicios de alta concentración. Esto llevó a la evolución del iWAG. El iWAG proporciona una opción de descarga WiFi a los proveedores de servicios 4G y 3G al habilitar una solución de paquete único que proporciona la funcionalidad combinada de Proxy Mobile IPv6 (PMIPv6) y GPRS Tunneling Protocol (GTP).

Acrónimos

GPRS - Servicio General de Radio de Paquetes

RNC - Controlador de red de radio

SGSN - Nodo de soporte de GPRS de servicio

PDP - Protocolo de datos de paquetes

GGSN - Nodo de soporte GPRS de gateway

APN - Nombre del punto de acceso

IMSI - Identidad de suscriptor móvil internacional

MSISDN - Número de directorio del suscriptor internacional de la estación móvil

HLR - Registro de ubicación en casa

Explicación de la terminología utilizada

- Proxy Mobile IPv6

La gestión de movilidad basada en red permite la misma funcionalidad que la IP móvil, sin ninguna modificación en la pila de protocolo TCP/IP del host. Con PMIP, el host puede cambiar su punto de conexión a Internet sin necesidad de cambiar su dirección IP. A diferencia del enfoque de IP móvil, esta funcionalidad es implementada por la red, que es responsable de realizar el seguimiento de los movimientos del host e iniciar la movilidad necesaria que indica en su nombre. Sin embargo, en caso de que la movilidad involucre diferentes interfaces de red, el host necesita modificaciones similares a Mobile IP para mantener la misma dirección IP en diferentes interfaces.

- Protocolo de túnel GPRS

GTP es un grupo de protocolos de comunicación basados en IP que se utilizan para transportar el servicio de radio de paquetes general (GPRS) dentro de las redes GSM, UMTS y LTE.

- Servicio general de radio de paquetes

GPRS es un servicio de datos móviles orientado a paquetes en la comunicación móvil 2G y 3G.

- Controlador de red de radio

RNC es un elemento rector de la red de acceso a radio (UTRAN) UMTS (3G).

- Nodo de soporte de GPRS de servicio

SGSN es un componente principal de la red GPRS, que gestiona todos los datos de paquetes conmutados dentro de la red, por ejemplo, la gestión de la movilidad y la autenticación de los usuarios.

- Nodo de soporte GPRS de gateway

GGSN forma parte de la red principal que conecta redes 3G basadas en GSM a Internet. El GGSN, a veces conocido como router inalámbrico, funciona junto con el SGSN para mantener a los usuarios móviles conectados a Internet y a las aplicaciones basadas en IP.

- Protocolo de datos de paquetes

El contexto PDP es una estructura de datos presente tanto en el nodo de soporte GPRS (SGSN) de servicio como en el nodo de soporte GPRS de gateway (GGSN) que contiene la información de sesión del suscriptor cuando el suscriptor tiene una sesión activa.

- Nombre del punto de acceso

El APN es el nombre de la configuración que se indica en el teléfono para configurar una conexión a la puerta de enlace entre la red móvil de la portadora y la Internet pública.

- Identidad de suscriptor móvil internacional

El IMSI se utiliza para identificar al usuario de una red móvil y es una identificación única asociada con todas las redes móviles. Se almacena como un campo de 64 bits y el teléfono lo envía a la red.

- Número de directorio del suscriptor internacional de la estación móvil

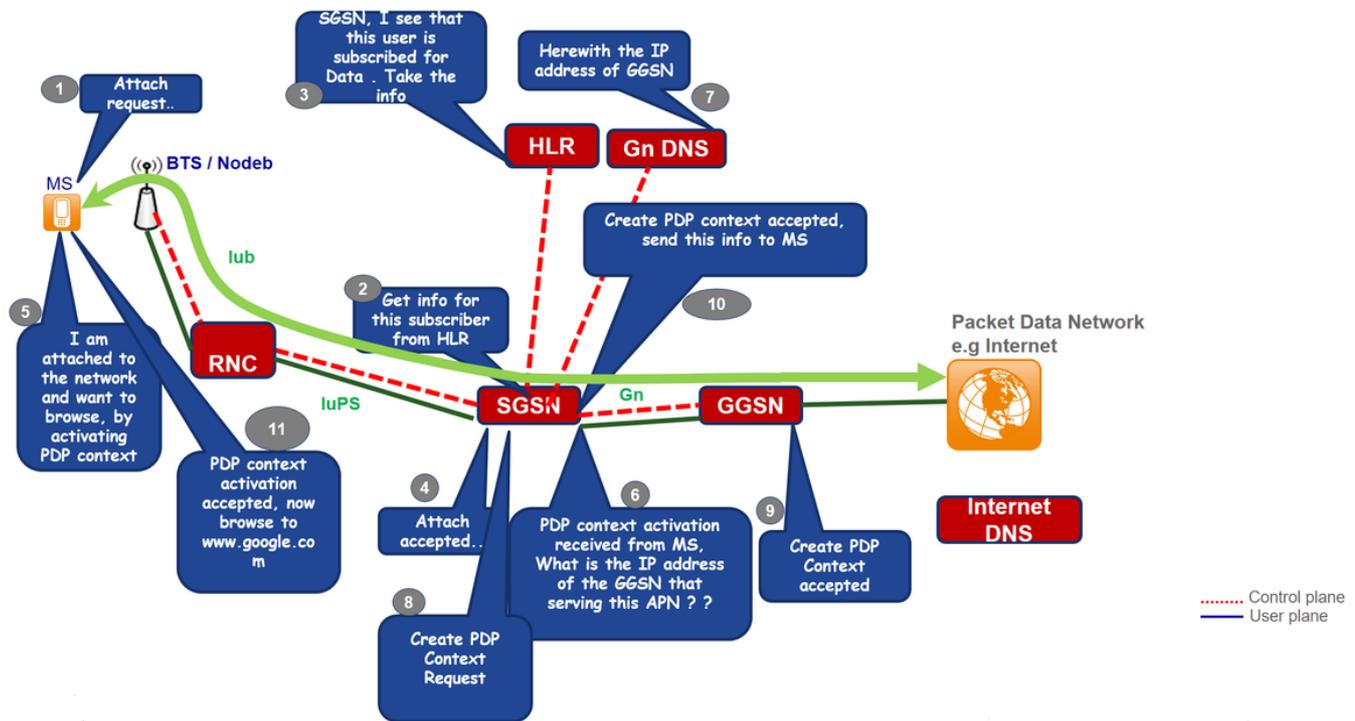
MSISDN es un número utilizado para identificar un número de teléfono móvil internacionalmente. MSISDN está definido por el plan de numeración E.164. Este número incluye un código de país y un código nacional de destino que identifica al operador del suscriptor.

- Registro de ubicación en casa

La HLR es la base de datos principal de información permanente del suscriptor para una red móvil.

Comprender los servicios de movilidad (3G/4G)

Flujo de llamadas 3G simplificado



Paso 1. El Mobile Station (MS) inicia el procedimiento de adhesión mediante la transmisión de un mensaje de solicitud de adhesión al SGSN.

Paso 2. Si se desconoce el MS en el SGSN, el SGSN envía una solicitud de identidad al MS. MS responde con Identity Response, que incluye el IMSI de los EM.

Paso 3. Si no existe un contexto de gestión de movilidad (MM) para MS en la SGSN (sesión existente), la autenticación es obligatoria. El SGSN solicita al HLR la información de autenticación del móvil con una Información de autenticación de envío y solicita que MS envíe la información de autenticación enviando una Solicitud de autenticación y cifrado de GPRS al móvil.

Paso 4. La HLR envía los datos de inserción del suscriptor al SGSN, que incluye los datos de suscripción del móvil.

Paso 5. El SGSN envía un mensaje Attach Accept al MS.

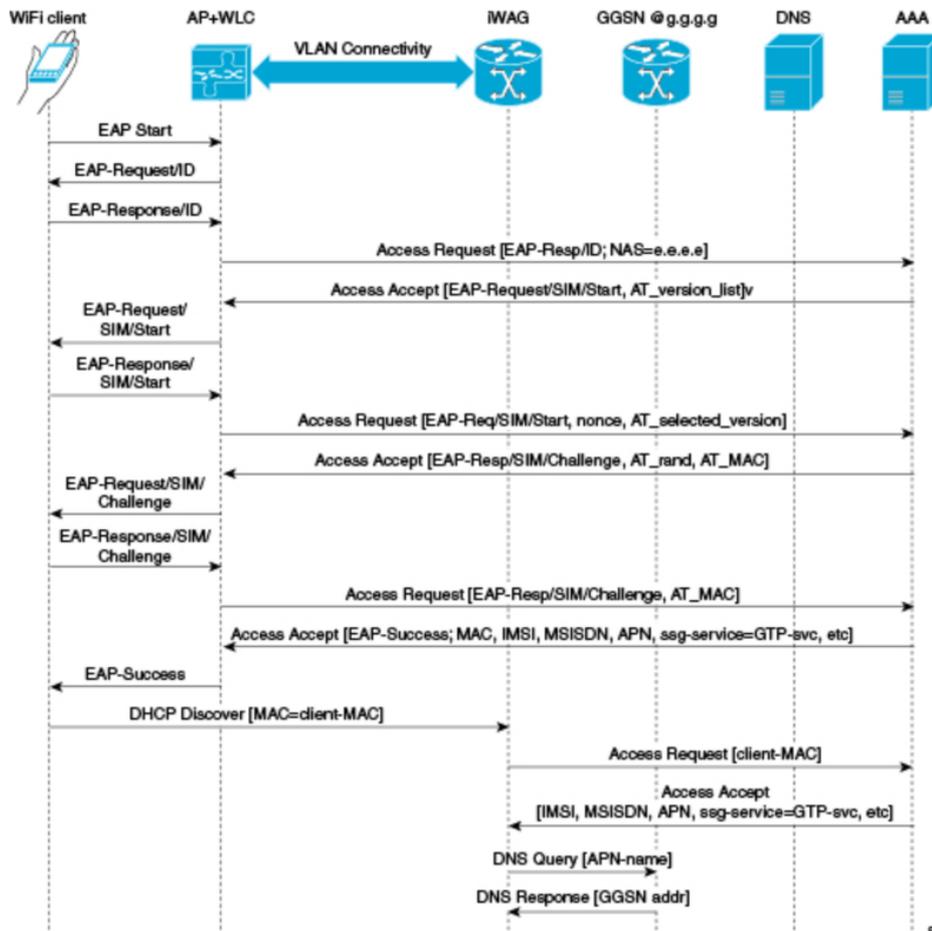
Paso 6. MS lo reconoce devolviendo un mensaje Attach Complete (Adjuntar mensaje completo) a SGSN e inicie el contexto de activación PDP que recibe SGSN y solicita DNS para la dirección IP GGSN.

Paso 7. La solicitud de creación de PDP se envía a GGSN después de la aceptación del mensaje **Create PDP Context accept** se envía a MS con la dirección IP del usuario.

Paso 8. Ahora MS puede navegar por Internet.

Cómo encaja WiFi en los servicios de movilidad (solución iWAG)

Flujo de llamadas de detección de DHCP 3G (parte 1)



- Paso 1. El dispositivo móvil se asocia automáticamente al identificador de conjunto de servicios (SSID) que transmiten los puntos de acceso para establecer y mantener la conectividad inalámbrica.
- Paso 2. El AP o el WLC inicia el proceso de autenticación EAP al enviar un ID de solicitud EAP al dispositivo móvil.
- Paso 3. El dispositivo móvil envía una respuesta que pertenece al ID de solicitud EAP de regreso al AP o al WLC.
- Paso 4. El WLC envía una solicitud de acceso RADIUS al servidor de autenticación, autorización y contabilidad (AAA) y le pide que autentique al suscriptor.
- Paso 5. Después de autenticar al suscriptor, el servidor AAA almacena en memoria caché todo su perfil de usuario que incluye la información sobre IMSI, MSISDN, APN y el par AV de Cisco que tiene ssg-service-info configurado en GTP-service. Los datos almacenados en caché también incluyen la dirección MAC del cliente, que se establece como el call-station-ID en los mensajes EAP entrantes.
- Paso 6. El servidor AAA envía el mensaje RADIUS Access Accept al AP o al WLC.
- Paso 7. Cuando vuelve el mensaje RADIUS Access Accept, se obtiene el perfil de usuario correspondiente en el que se identifica el uso del servicio GTP.
- Paso 8. El WLC envía el mensaje de autenticación EAP exitoso al dispositivo móvil.
- Paso 9. El dispositivo móvil envía un mensaje DHCP Discover al iWAG. En respuesta a este mensaje DHCP Discover, el DHCP pasa a un nuevo estado pendiente para esperar a que la

señalización del lado MNO se complete, que asigna una dirección IP al suscriptor. En respuesta a esto, el mensaje DHCP Discover, DHCP entra en un nuevo estado pendiente para esperar a que la señalización en el lado MNO se complete, que asigna una dirección IP al suscriptor.

Paso 10. El iWAG encuentra una sesión asociada con la dirección MAC del suscriptor y recupera la dirección IP del suscriptor del contexto de sesión.

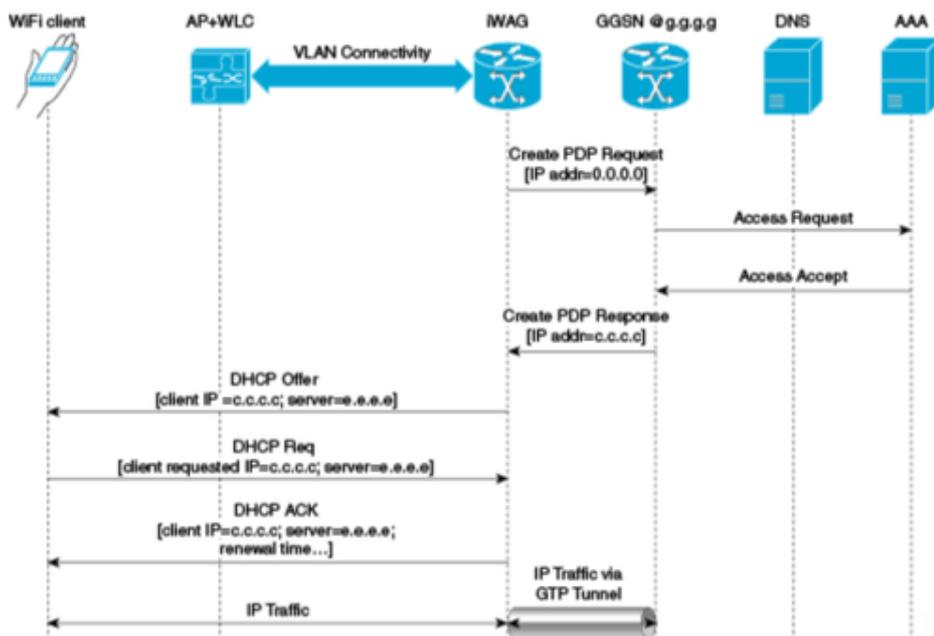
Paso 11. El iWAG envía una solicitud de acceso RADIUS al servidor AAA y le pide que autentique al suscriptor con el uso de la dirección MAC en ella como el ID de estación de llamada, mientras que también proporciona toda la información de suscriptor conocida, ID e IMSI en este mensaje de solicitud de acceso.

Paso 12. Cuando el servidor AAA devuelve el mensaje RADIUS Access Accept al iWAG, se obtiene el perfil de usuario en el que se identifica el uso del servicio GTP.

Paso 13. El iWAG envía una consulta al servidor DNS para resolver un nombre de punto de acceso (APN) dado a una dirección IP GGSN.

Paso 14. El servidor DNS envía la dirección GGSN resuelta por DNS nuevamente al iWAG.

Flujo de llamadas de detección de DHCP 3G (parte 2)



Paso 15. Después de recibir la dirección GGSN resuelta por DNS, iWAG envía la solicitud de contexto de creación PDP, en la que la dirección de contexto PDP se establece en 0, para solicitar al GGSN una asignación de dirección IP.

Paso 16. El GGSN envía una solicitud de acceso RADIUS al servidor AAA.

Paso 17. Según la información almacenada en la memoria caché obtenida de la autenticación EAP-SIM, el servidor AAA responde con un mensaje RADIUS Access Accept al GGSN.

Paso 18. El GGSN envía la respuesta de contexto de creación de PDP que transporta la dirección IP c.c.c asignada para el suscriptor, al iWAG.

Paso 19. El iWAG envía un mensaje de oferta DHCP al dispositivo móvil.

Paso 20. El dispositivo móvil envía un mensaje de solicitud DHCP al iWAG y el iWAG reconoce esta solicitud enviando un mensaje ACK DHCP al dispositivo móvil.

Paso 21. El tráfico del suscriptor WiFi ahora tiene una ruta de datos a través de la cual puede fluir.