# Comprendre la solution iWAG pour les données mobiles 3G

## Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Acronymes](#)
[Explication de la terminologie utilisée](#)
[Comprendre les services de mobilité (3G/4G)](#)
[Flux d'appels 3G simplifié](#)
[Fonctionnement du Wi-Fi dans les services de mobilité (solution iWAG)](#)
[Flux d'appels de découverte DHCP 3G (Partie 1)](#)
[Flux d'appels de découverte DHCP 3G (Partie 2)](#)

## Introduction

Ce document décrit la solution de passerelle d'accès sans fil intelligente (iWAG) et comment elle intègre la technologie de mobilité à la solution WiFi.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès sans fil
- Flux d'appels de mobilité

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

## Informations générales

Normalement, pour accéder à Internet, vous utilisez deux types de services Internet :

- WiFi
- Internet mobile (réseau de mobilité 3G/4G)

La combinaison de ces deux technologies offre une meilleure expérience au client et c'est le principal objectif de cette solution.

La solution iWAG inclut une combinaison d'utilisateurs IP simples (ISG et WiFi traditionnels) et d'utilisateurs IP mobiles (tunnellisation PMIPv6 ou GTP). Le terme service de mobilité est utilisé pour désigner le service GTP ou le service PMIPv6 appliqué au trafic utilisateur. L'iWAG fournit des services de mobilité aux utilisateurs IP mobiles et, par conséquent, un client mobile peut accéder en toute transparence à un réseau de mobilité 3G ou 4G. Cependant, l'iWAG ne fournit pas de services de mobilité aux utilisateurs IP simples.

Par conséquent, les utilisateurs IP simples peuvent accéder au réseau de réseau local sans fil public (PWLAN) via Cisco ISG. Les clients peuvent accéder à Internet WiFi (sans fil public), dans la mesure du possible. Toutefois, si le Wi-Fi n'est pas disponible, les mêmes clients peuvent se connecter au service Internet à l'aide d'un réseau de mobilité 3G ou 4G.
Les fournisseurs de services utilisent une combinaison d'offres Wi-Fi et de mobilité pour décharger leurs réseaux de mobilité dans le domaine de l'utilisation de services à forte concentration. Cela a conduit à l'évolution de l'iWAG. L'iWAG offre une option de déchargement WiFi aux fournisseurs de services 4G et 3G en activant une solution unique qui offre la fonctionnalité combinée de Proxy Mobile IPv6 (PMIPv6) et GPRS Tunneling Protocol (GTP).

# Acronymes

GPRS - General Packet Radio Service

RNC - Contrôleur de réseau radio

SGSN - Noeud de prise en charge du service GPRS

PDP - Packet Data Protocol

GGSN - Noeud de prise en charge GPRS de passerelle

APN - Nom du point d'accès

IMSI - Identité de l'abonné mobile international

MSISDN - Numéro de répertoire de l'abonné international de la station mobile

HLR - Registre du site d'accueil

# Explication de la terminologie utilisée

- Proxy Mobile IPv6

La gestion de la mobilité basée sur le réseau offre les mêmes fonctionnalités que Mobile IP, sans aucune modification de la pile de protocoles TCP/IP de l'hôte. Avec PMIP, l’hôte peut modifier son point de connexion à Internet sans avoir à modifier son adresse IP. Contrairement à l'approche IP mobile, cette fonctionnalité est mise en oeuvre par le réseau, qui est chargé de suivre les mouvements de l'hôte et d'initier la mobilité requise qui signale en son nom. Cependant, si la mobilité implique différentes interfaces réseau, l'hôte doit être modifié de la même manière que l'IP mobile afin de conserver la même adresse IP sur différentes interfaces.

- Protocole de tunnellisation GPRS

GTP est un groupe de protocoles de communication IP utilisés pour transporter le service GPRS

(General Packet Radio Service) dans les réseaux GSM, UMTS et LTE.

- Service général de radio par paquets

GPRS est un service de données mobiles orienté paquets sur les communications cellulaires 2G et 3G.

- Contrôleur de réseau radio

RNC est un élément de gouvernance du réseau d'accès radio UMTS (3G) (UTRAN).

- Noeud d'assistance GPRS de service

Le SGSN est un composant principal du réseau GPRS, qui gère toutes les données à commutation de paquets au sein du réseau, par exemple la gestion de la mobilité et l'authentification des utilisateurs.

- Noeud de prise en charge GPRS de passerelle

GGSN fait partie du réseau principal qui connecte des réseaux 3G GSM à Internet. Le GGSN, parfois appelé routeur sans fil, fonctionne en tandem avec le SGSN pour maintenir les utilisateurs mobiles connectés à Internet et aux applications IP.

- Protocole de données de paquets

Le contexte PDP est une structure de données présente sur le noeud de support GPRS (SGSN) et le noeud de support GPRS de passerelle (GGSN) qui contient les informations de session de l'abonné lorsque l'abonné a une session active.

- Nom du point d'accès

L'APN est le nom des paramètres lus par votre téléphone pour configurer une connexion à la passerelle entre le réseau cellulaire de votre opérateur et l'Internet public.

- Identité de l'abonné mobile international

L'IMSI est utilisé pour identifier l'utilisateur d'un réseau cellulaire et est une identification unique associée à tous les réseaux cellulaires. Il est stocké en tant que champ 64 bits et est envoyé par le téléphone au réseau.

- Numéro de répertoire de l'abonné international de la station mobile

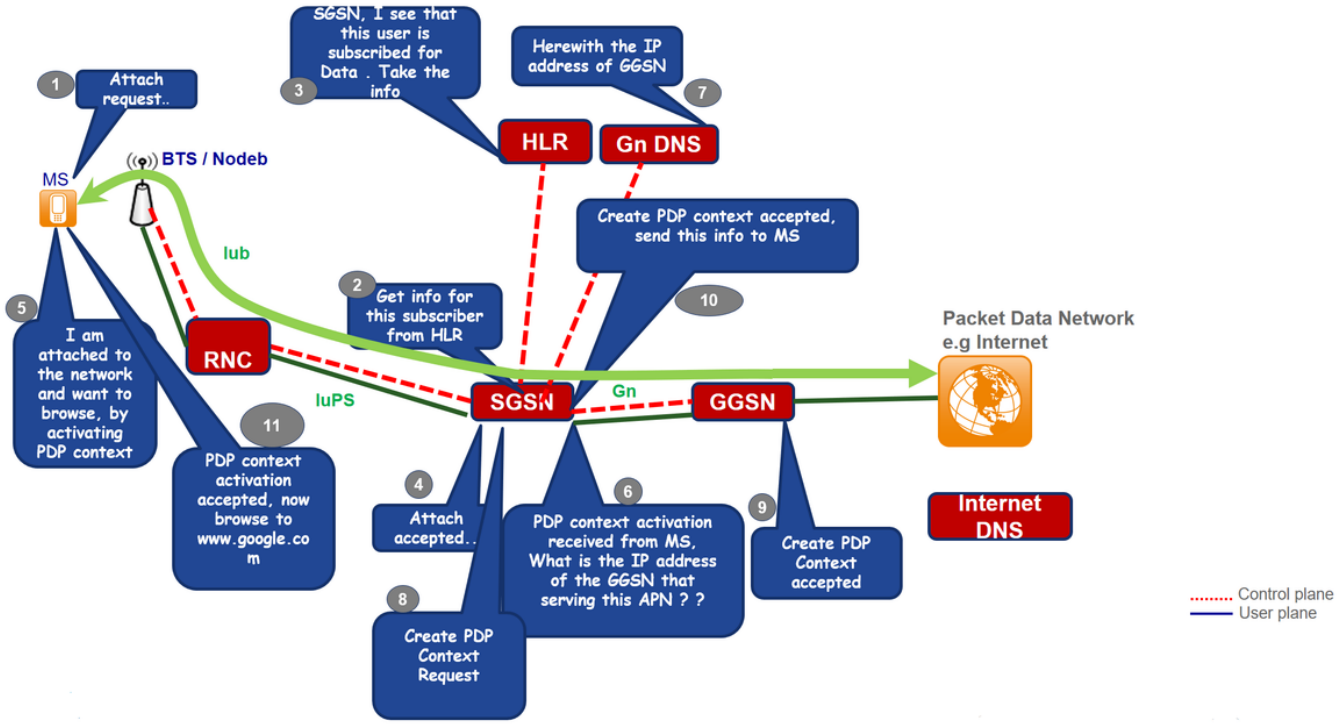
Le RNIS est un numéro utilisé pour identifier un numéro de téléphone mobile à l'échelle internationale. Le RNIS est défini par le plan de numérotation E.164. Ce numéro comprend un code de pays et un code de destination national qui identifie l'opérateur de l'abonné.

- Registre du site personnel

Le HLR est la base de données principale des informations permanentes des abonnés pour un réseau mobile.

# Comprendre les services de mobilité (3G/4G)

## Flux d'appels 3G simplifié




Étape 1. Le service Mobile Static (MS) initie la procédure d'attachement en transmettant un message Attach Request au SGSN.

Étape 2. Si le SGSN est inconnu sur le SGSN, le SGSN envoie une demande d'identité à la MS. L'ÉM répond par une réponse d'identité, qui comprend l'IMSI de l'ÉM.

Étape 3. Si aucun contexte de gestion de la mobilité (MM) pour le MS n'existe sur le SGSN (session existante), l'authentification est obligatoire. Le SGSN interroge le HLR pour obtenir les informations d'authentification du mobile avec une information d'authentification d'envoi et demande que le MS envoie des informations d'authentification en envoyant une demande d'authentification et de chiffrement GPRS au mobile.

Étape 4. Le HLR envoie des données d'abonné Insert au SGSN, qui inclut les données d'abonnement du mobile.

Étape 5. Le SGSN envoie un message Attach Accept au MS.

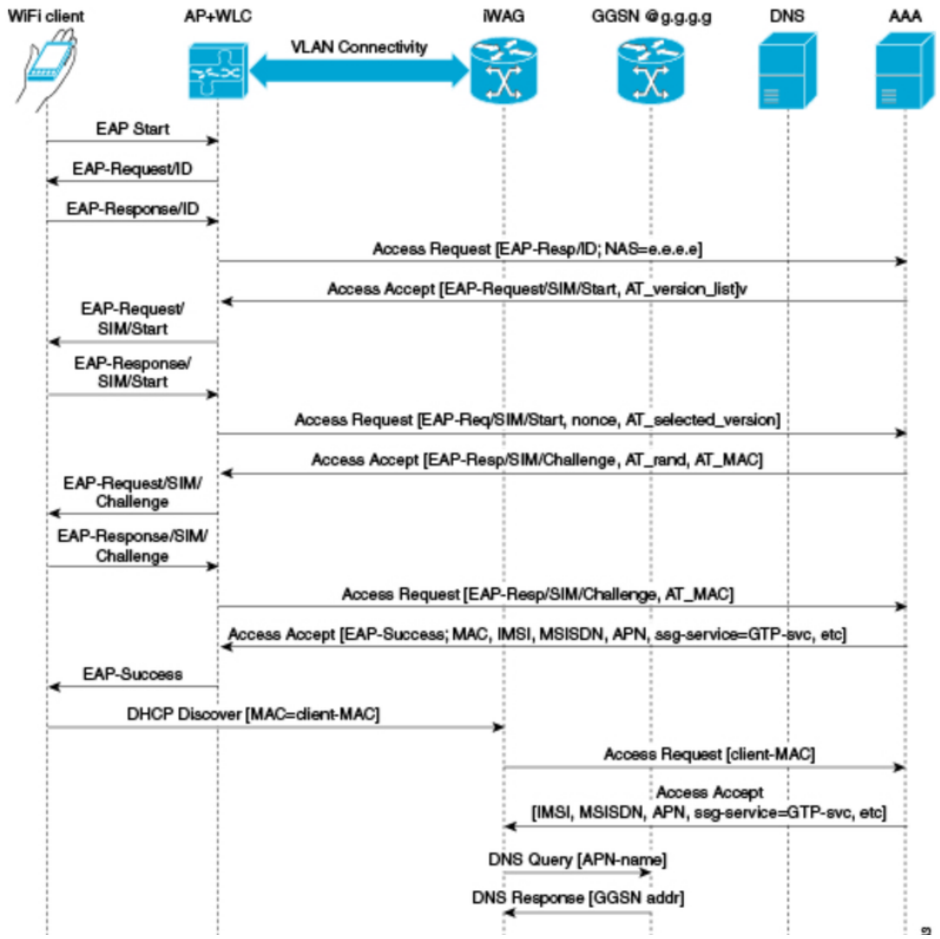
Étape 6. MS le reconnaît en renvoyant un message Attach Complete au SGSN et en initiant le contexte d'activation PDP qui est reçu par le SGSN et il demande au DNS l'adresse IP du GGSN.

Étape 7. La demande Create PDP est envoyée au GGSN après acceptation du message **Create PDP Context** accepté envoyé à MS avec l'adresse IP de l'utilisateur.

Étape 8. Maintenant, MS peut naviguer sur Internet.

# Fonctionnement du Wi-Fi dans les services de mobilité (solution iWAG)

## Flux d'appels de découverte DHCP 3G (Partie 1)




Étape 1. L'appareil mobile est automatiquement associé au SSID (Service Set Identifier) diffusé par les points d'accès pour établir et maintenir la connectivité sans fil.

Étape 2. L'AP ou le WLC démarre le processus d'authentification EAP en envoyant un ID de demande EAP à l'appareil mobile.

Étape 3. L'appareil mobile envoie une réponse qui se rapporte à l'ID de requête EAP au point d'accès ou au WLC.

Étape 4. Le WLC envoie une demande d'accès RADIUS au serveur Authentication, Authorization, and Accounting (AAA) et lui demande d'authentifier l'abonné.

Étape 5. Une fois l'abonné authentifié, le serveur AAA met en cache l'intégralité de son profil utilisateur, qui inclut les informations relatives à IMSI, MSISDN, APN et à la paire AV Cisco dont ssg-service-info est défini sur GTP-service. Les données mises en cache incluent également l'adresse MAC du client, définie comme ID de station appelante dans les messages EAP entrants.

Étape 6. Le serveur AAA envoie le message d'acceptation d'accès RADIUS au point d'accès ou au WLC.

Étape 7. Lorsque le message d'acceptation d'accès RADIUS revient, le profil utilisateur correspondant dans lequel l'utilisation du service GTP est identifiée est obtenu.

Étape 8. Le WLC envoie le message d'authentification EAP réussi à l'appareil mobile.

Étape 9. L'appareil mobile envoie un message de détection DHCP à l'iWAG. En réponse à ce message de détection DHCP, le DHCP passe dans un nouvel état en attente pour attendre la fin de la signalisation côté MNO, qui attribue une adresse IP à l'abonné. En réponse à ce message,

DHCP Discover, DHCP passe dans un nouvel état en attente pour attendre que la signalisation côté MNO soit terminée, qui attribue une adresse IP à l'abonné.

Étape 10. L'iWAG recherche une session associée à l'adresse MAC de l'abonné et extrait l'adresse IP de l'abonné du contexte de session.

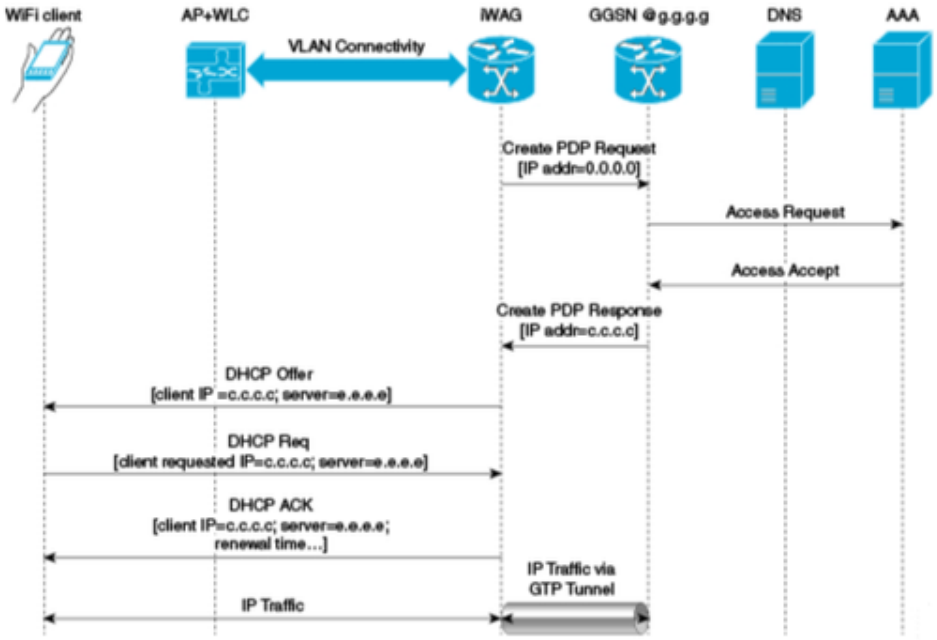
Étape 11. L'iWAG envoie une demande d'accès RADIUS au serveur AAA et lui demande d'authentifier l'abonné en utilisant l'adresse MAC qu'il contient comme ID de station d'appel, tout en fournissant toutes les autres informations d'abonné, ID et IMSI connus dans ce message de demande d'accès.

Étape 12. Lorsque le serveur AAA renvoie le message d'acceptation d'accès RADIUS à l'iWAG, le profil utilisateur dans lequel l'utilisation du service GTP est identifiée est obtenu.

Étape 13. L'iWAG envoie une requête au serveur DNS pour résoudre un nom de point d'accès (APN) donné en une adresse IP GGSN.

Étape 14. Le serveur DNS renvoie l'adresse GGSN résolue par DNS à l'iWAG.

## Flux d'appels de découverte DHCP 3G (Partie 2)




Étape 15. Après avoir reçu l'adresse GGSN résolue par DNS, l'iWAG envoie la requête de création de contexte PDP, dans laquelle l'adresse de contexte PDP est définie sur 0, afin de demander au GGSN d'attribuer une adresse IP.

Étape 16. Le GGSN envoie une requête d'accès RADIUS au serveur AAA.

Étape 17. Sur la base des informations mises en cache obtenues à partir de l'authentification EAP-SIM, le serveur AAA répond avec un message d'acceptation d'accès RADIUS au GGSN.

Étape 18. Le GGSN envoie la réponse contextuelle Create PDP qui transporte l'adresse IP c.c.c.c

attribuée à l'abonné, vers l'iWAG.

Étape 19. L'iWAG envoie un message d'offre DHCP à l'appareil mobile.

Étape 20. L'appareil mobile envoie un message de requête DHCP à l'iWAG et l'iWAG accuse réception de cette requête en envoyant un message ACK DHCP à l'appareil mobile.

Étape 21. Le trafic des abonnés WiFi dispose désormais d'un chemin de données par lequel il peut circuler.