Comprenez la solution d'iWAG pour des données du mobile 3G

Contenu

Introduction

Ce document décrit la solution Sans fil intelligente de passerelle d'Access (iWAG) et comment il intègre la technologie de mobilité avec la solution de WiFi.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Radio
- Écoulement d'appel de mobilité

Composants utilisés

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

Informations générales

Accéder à normalement l'Internet vous utilisez deux types de services Internet :

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

La combinaison de ces deux Technologies donne une meilleure expérience au client et c'est le but principal de cette solution.

La solution d'iWAG inclut une combinaison des utilisateurs simples IP (ISG traditionnel et WiFi) et des utilisateurs d'IP mobile (Tunnellisation PMIPv6 ou GTP). Le service de mobilité de terme est utilisé pour se rapporter au service GTP ou au service PMIPv6 appliqué au trafic d'utilisateur. L'iWAG fournit des Services de mobilité aux utilisateurs d'IP mobile et en conséquence, un client mobile peut sans faille accéder au réseau d'une mobilité 3G ou 4G. Cependant, l'iWAG ne fournit pas des Services de mobilité aux utilisateurs simples IP.

Par conséquent, les utilisateurs simples IP peuvent accéder au réseau Sans fil public du RÉSEAU LOCAL (PWLAN) par l'ISG de Cisco. Les clients peuvent accéder à l'Internet de WiFi (radio publique), où toujours possible. Cependant, si le WiFi n'est pas disponible, les mêmes clients peuvent se connecter au service Internet au réseau d'une mobilité 3G ou 4G.
Les fournisseurs de services utilisent une combinaison de WiFi et la mobilité offre de débarquer leurs réseaux de mobilité dans le domaine de l'utilisation de service de forte concentration. Ceci a mené à l'évolution de l'iWAG. L'iWAG fournit un WiFi débarquent l'option aux fournisseurs de services 4G et 3G en activant une solution d'unique qui fournit la fonctionnalité combinée de l'IPv6 mobile de proxy (PMIPv6) et du GPRS Tunneling Protocol (GTP).

Acronymes

GPRS - Service général de radiocommunication par paquets

RNC - Contrôleur de réseau radio

SGSN - Noeud de support du service GPRS

PDP - Données de paquets Protocol

GGSN - Noeud de support de la passerelle GPRS

APN - Nom de Point d'accès

IMSI - Identité d'abonné mobile internationale

MSISDN - Nombre de répertoire d'abonné international de poste mobile

HLR - Registre d'emplacement de la maison

Explication de terminologie utilisée

- IPv6 de mobile de proxy

La gestion de la mobilité Fondé(e) sur le réseau n'active la même fonctionnalité que l'IP mobile, sans aucune modification à la pile de protocoles TCP/IP de l'hôte. Avec PMIP, l'hôte peut changer sa point-de-connexion à l'Internet sans nécessité de changer son adresse IP. Le contraire à l'approche d'IP mobile, cette fonctionnalité est mis en application par le réseau, qui est responsable pour dépister les mouvements de l'hôte et pour initier la mobilité exigée qui signale en son nom. Cependant, au cas où la mobilité impliquerait différentes interfaces réseau, l'hôte a besoin de modifications semblables à l'IP mobile afin de mettre à jour la même adresse IP à travers différentes interfaces.

- GPRS perçant un tunnel Protocol

GTP est un groupe de protocoles de transmissions basés sur IP utilisés pour porter le Service général de radiocommunication par paquets (GPRS) dans des réseaux GSM, UMTS et LTE.

- Service général de radiocommunication par paquets

GPRS est un service de données mobile orienté par paquet sur la transmission 2G et 3G cellulaire.

- Contrôleur de réseau radio

RNC est un élément de gouvernement dans le réseau d'accès de radio UMTS (3G) (UTRAN).

- Noeud de support du service GPRS

SGSN est un composant principal du réseau GPRS, qui traite toutes les données de commutation de paquets dans le réseau, par exemple la gestion de la mobilité et l'authentification des utilisateurs.

- Noeud de support de la passerelle GPRS

GGSN fait partie du principal réseau qui connecte les réseaux 3G basés sur GSM à l'Internet. Le GGSN, parfois connu sous le nom de routeur Sans fil, fonctionne en tandem avec le SGSN pour maintenir des utilisateurs nomades connectés à l'Internet et aux applications basées sur IP.

- Données de paquets Protocol

Le contexte PDP est une structure de données actuelle sur le les deux le noeud servant de support GPRS (SGSN) et le Gateway GPRS Support Node (GGSN) qui contient les informations de session de l'abonné quand l'abonné a une session active.

- Nom de Point d'accès

L'APN est le nom pour les configurations que votre téléphone indique pour installer une connexion à la passerelle entre le réseau cellulaire de votre transporteur et l'Internet public.

- Identité d'abonné mobile internationale

L'IMSI est utilisé pour identifier l'utilisateur d'un réseau cellulaire et est une seule identification associée avec tous les réseaux cellulaires. Il est enregistré comme champ de 64 bits et est envoyé par le téléphone au réseau.

- Nombre de répertoire d'abonné international de poste mobile

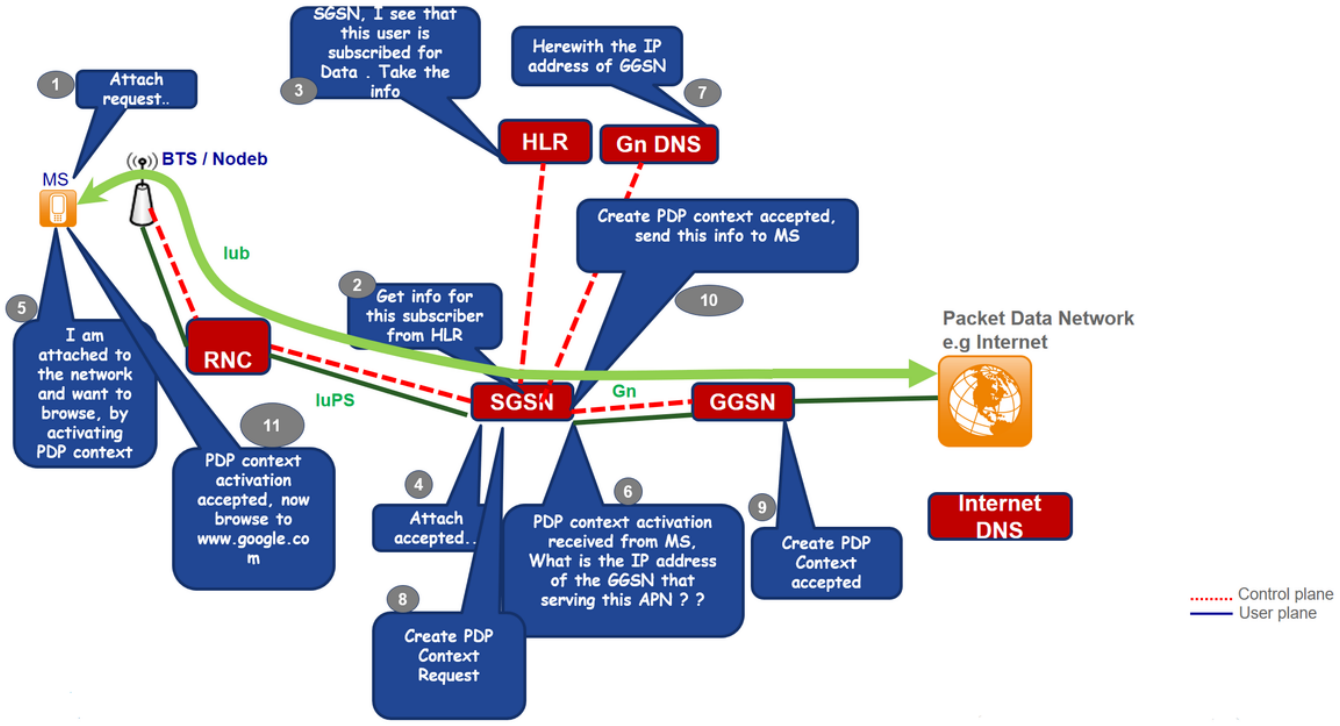
Le MSISDN est un nombre utilisé pour identifier un nombre de téléphone portable internationalement. MSISDN est défini par le plan du numérotage E.164. Ce nombre inclut code de pays et un code de destination national qui identifie l'opérateur de l'abonné.

- Registre d'emplacement de la maison

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

Comprenez les Services de mobilité (3G/4G)

Écoulement simplifié de l'appel 3G



Étape 1. La charge statique mobile (MS) initie la procédure d'attache par la transmission d'un message de demande d'attache au SGSN.

Étape 2. Si le MS est inconnu sur le SGSN, le SGSN envoie une demande d'identité au MS. Le MS répond avec la réponse d'identité, qui inclut l'IMSI de la milliseconde.

Étape 3. Si aucun contexte de la gestion de la mobilité (millimètre) pour le MS n'existe sur le SGSN (session existante), alors l'authentification est obligatoire. Le SGSN questionne le HLR pour les informations d'authentification du mobile avec des informations d'authentification d'envoi, et demande que le MS envoient les informations authentiques en envoyant une authentification GPRS et en chiffrant la demande au mobile.

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

Étape 5. Le SGSN envoie une attache reçoit le message au MS.

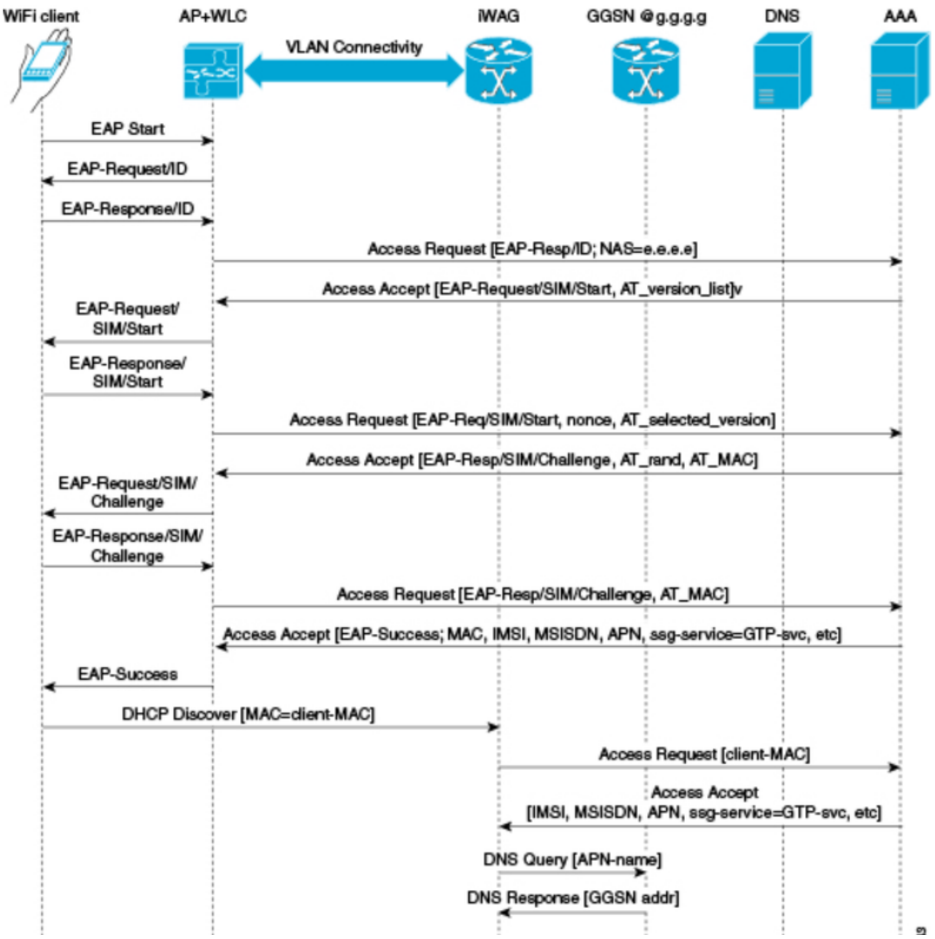
Étape 6. Le MS la reconnaît en renvoyant un message complet d'attache au SGSN et le contexte initié de lancement PDP qui est reçu par SGSN et lui s'enquièrent des DN pour l'adresse IP GGSN.

Étape 7. Créez la demande PDP est envoyé à GGSN après acceptation dont **créez l'acceptedmessage de contexte PDP** est envoyé au MS avec l'adresse IP d'utilisateur.

Étape 8. Maintenant le MS peut parcourir l'Internet.

Comment adaptations de WiFi aux Services de mobilité (solution d'iWAG)

DHCP 3G découvrent l'écoulement d'appel (partie 1)



Étape 1. Le périphérique mobile est automatiquement associé à l'émission d'Identifiant SSID (Service Set Identifier) par les Points d'accès pour établir et mettre à jour la connexion sans fil.

Étape 2. AP ou le WLC commence le procédé d'authentification EAP par envoyer un ID de demande d'EAP au périphérique mobile.

Étape 3. Le périphérique mobile envoie une réponse qui concerne l'ID de demande d'EAP de nouveau à AP ou au WLC.

Étape 4. Le WLC envoie une demande d'Access de RAYON au serveur d'Authentification, autorisation et comptabilité (AAA) et lui demande d'authentifier l'abonné.

Étape 5. Après que l'abonné soit authentifié, le serveur d'AAA cache son profil utilisateur entier qui inclut les informations sur IMSI, MSISDN, APN, et la paire AV de Cisco qui a le GTP-service du positionnement ssg-service-information. Les données cachées incluent également l'adresse MAC du client, qui est placée comme calling-station-id dans les messages entrants d'EAP.

Étape 6. Le serveur d'AAA envoie le RAYON Access reçoivent le message à AP ou au WLC.

Étape 7. Quand le RAYON Access reçoivent le message revient, le profil utilisateur correspondant dans lequel l'utilisation du GTP-service est identifiée est obtenue.

Étape 8. Le WLC envoie le message réussi d'authentification EAP au périphérique mobile.

Étape 9. Le périphérique mobile envoie un DHCP découvrent le message à l'iWAG. En réponse à ce DHCP découvrez le message, le DHCP entre dans un nouveau en attendant l'état pour attendre la signalisation du côté MNO à terminer, qui assigne une adresse IP à l'abonné. En réponse à ceci, le DHCP découvrent le message, DHCP entre dans un nouveau en attendant

l'état pour attendre la signalisation du côté MNO à terminer, qui assigne une adresse IP à l'abonné.

Étape 10. L'iWAG trouve une session associée avec l'adresse MAC d'abonné et récupère l'adresse IP d'abonné du contexte de session.

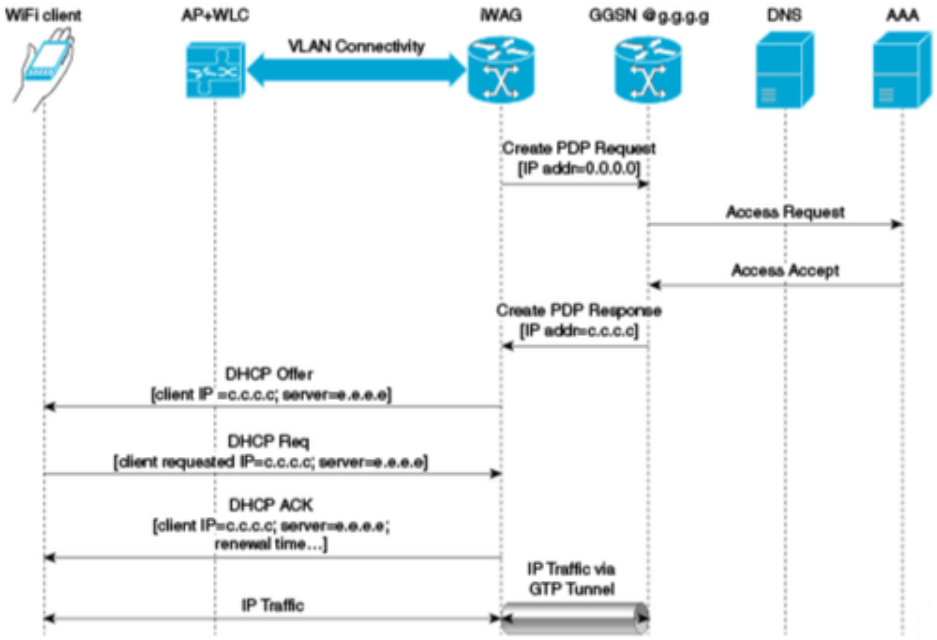
Étape 11. L'iWAG envoie une demande d'Access de RAYON au serveur d'AAA et lui demande d'authentifier l'abonné avec l'utilisation de l'adresse MAC dans lui comme calling-station-id, alors qu'il fournit également tous autres informations, id, et IMSI connus d'abonné dans ce message de demande d'Access.

Étape 12. Quand le serveur d'AAA renvoie le RAYON Access recevez le message à l'iWAG, le profil utilisateur dans lequel l'utilisation du GTP-service est identifiée est obtenue.

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

Étape 14. Le serveur DNS envoie l'adresse Dn-résolue GGSN de nouveau à l'iWAG.

DHCP 3G découvrent l'écoulement d'appel (partie 2)



Étape 15. Après qu'il reçoive l'adresse Dn-résolue GGSN, l'iWAG envoie la demande de contexte de la création PDP, dans laquelle l'adresse de contexte PDP est placée à 0, afin de demander le GGSN pour une affectation d'adresse IP.

Étape 16. Le GGSN envoie une demande d'Access de RAYON au serveur d'AAA.

Étape 17. Basé sur les informations en cache obtenues de l'authentification EAP-SIM, les réponses de serveur d'AAA avec un RAYON Access reçoivent le message au GGSN.

Étape 18. Le GGSN envoie la réponse de contexte de la création PDP qui porte l'adresse IP

assignée c.c.c.c pour l'abonné, à l'iWAG.

Étape 19. L'iWAG envoie un message d'offre DHCP au périphérique mobile.

Étape 20. Le périphérique mobile envoie un message de requête DHCP à l'iWAG, et l'iWAG reconnaît cette demande en envoyant un message DHCP ACK au périphérique mobile.

Étape 21. Le trafic d'abonné de WiFi a maintenant un chemin de données par lequel il peut circuler.