Understand iWAG Solution for 3G Mobile Data

Contents

Introduction

This document describes Intelligent Wireless Access Gateway (iWAG) solution and how it integrates mobility technology with WiFi Solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Wireless
- Mobility call flow

Components Used

This document is not restricted to specific software and hardware versions.

Background Information

Normally to access internet you use two types of internet services:

- WiFi
- Mobile Internet (3G/4G Mobility network)

The combination of these two technologies gives a better experience to the customer and this is the main purpose of this solution.

The iWAG solution includes a combination of simple IP users (traditional ISG and WiFi) and mobile IP users (PMIPv6 or GTP tunneling). The term mobility service is used to refer to either the GTP service or the PMIPv6 service applied to user traffic. The iWAG provides mobility services to mobile IP users and as a result, a mobile client can seamlessly access a 3G or 4G mobility network. However, the iWAG does not provide mobility services to simple IP users.

Therefore, simple IP users can access the Public Wireless LAN (PWLAN) network through the Cisco ISG. Clients can access WiFi Internet (public wireless), where ever possible. However, if WiFi is not available, the same clients can connect to the Internet service with a 3G or 4G mobility network.
Service providers use a combination of WiFi and mobility offers to offload their mobility networks in the area of high-concentration service usage. This led to the evolution of the iWAG. The iWAG provides a WiFi offload option to 4G and 3G service providers by enabling a single-box solution that provides the combined functionality of Proxy Mobile IPv6 (PMIPv6) and GPRS Tunneling Protocol (GTP).

Acronyms

GPRS - General Packet Radio Service

RNC - Radio Network Controller

SGSN - Service GPRS Support Node

PDP - Packet Data Protocol

GGSN - Gateway GPRS Support Node

APN - Access Point Name

IMSI - International Mobile Subscriber Identity

MSISDN -Mobile Station International Subscriber Directory Number

HLR - Home Location Register

Explanation of Terminology Used

- Proxy Mobile IPv6

Network-based mobility management enables the same functionality as Mobile IP, without any modifications to the host's TCP/IP Protocol stack. With PMIP, the host can change its point-of-attachment to the Internet without the need to change its IP address. Contrary to Mobile IP approach, this functionality is implemented by the network, which is responsible to track the movements of the host and initiate the required mobility which signals on its behalf. However, in case the mobility involves different network interfaces, the host needs modifications similar to Mobile IP in order to maintain the same IP address across different interfaces.

- GPRS Tunneling Protocol

GTP is a group of IP-based communications protocols used to carry general packet radio service (GPRS) within GSM, UMTS and LTE networks.

- General Packet Radio Service

GPRS is a packet oriented mobile data service on the 2G and 3G cellular communication.

- Radio Network Controller

RNC is a governing element in the UMTS (3G) radio access network (UTRAN).

- Service GPRS Support Node

SGSN is a main component of the GPRS network, which handles all packet switched data within the network, e.g. the mobility management and authentication of the users.

- Gateway GPRS Support Node

GGSN is part of the core network that connects GSM-based 3G networks to the Internet. The GGSN, sometimes known as a wireless router, works in tandem with the SGSN to keep mobile users connected to the Internet and IP-based applications.

- Packet Data Protocol

The PDP context is a data structure present on both the serving GPRS support node (SGSN) and the gateway GPRS support node (GGSN) which contains the subscriber's session information when the subscriber has an active session.

- Access Point Name

The APN is the name for the settings your phone reads to set up a connection to the gateway between your carrier's cellular network and the public Internet.

- International Mobile Subscriber Identity

The IMSI is used to identify the user of a cellular network and is a unique identification associated with all cellular networks. It is stored as a 64 bit field and is sent by the phone to the network.

- Mobile Station International Subscriber Directory Number

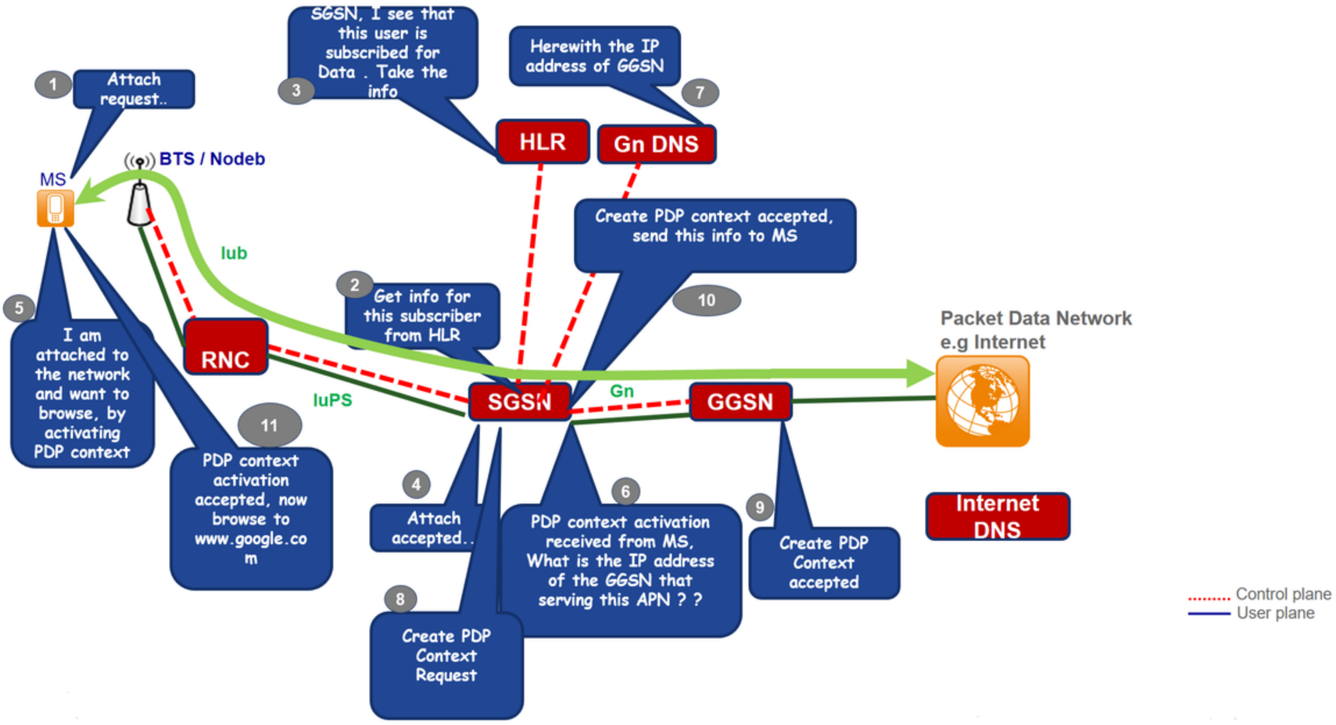
The MSISDN is a number used to identify a mobile phone number internationally. MSISDN is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code which identifies the subscriber's operator.

- Home Location Register

The HLR is the main database of permanent subscriber information for a mobile network.

Understand Mobility Services (3G/4G)

Simplified 3G Call Flow


1
Attach request..
SGSN, I see that this user is subscribed for Data . Take the info
3
Herewith the IP address of GGSN
7
HLR
Gn DNS
BTS / Nodeb
MS
Iub
Create PDP context accepted, send this info to MS
10
2
Get info for this subscriber from HLR
5
I am attached to the network and want to browse, by activating PDP context
RNC
Packet Data Network e.g Internet
IuPS
SGSN
Gn
GGSN
11
PDP context activation accepted, now browse to www.google.com
4
Attach accepted..
6
PDP context activation received from MS, What is the IP address of the GGSN that serving this APN ? ?
9
Create PDP Context accepted
Internet DNS
8
Create PDP Context Request
Control plane
User plane

Step 1. The Mobile Static (MS) initiates the attach procedure by the transmission of an Attach Request message to the SGSN.

Step 2. If the MS is unknown on the SGSN, the SGSN sends an Identity Request to the MS. The MS responds with Identity Response, which includes the MS’s IMSI.

Step 3. If no Mobility Management (MM) context for the MS exists on the SGSN (existing session), then authentication is mandatory. The SGSN queries the HLR for the mobile’s authentication information with a Send Authentication Information, and requests that the MS send auth info by sending a GPRS Authentication and Ciphering Request to the mobile.

Step 4. The HLR sends Insert Subscriber Data to the SGSN, which includes the mobile’s subscription data.

Step 5. The SGSN sends an Attach Accept message to the MS.

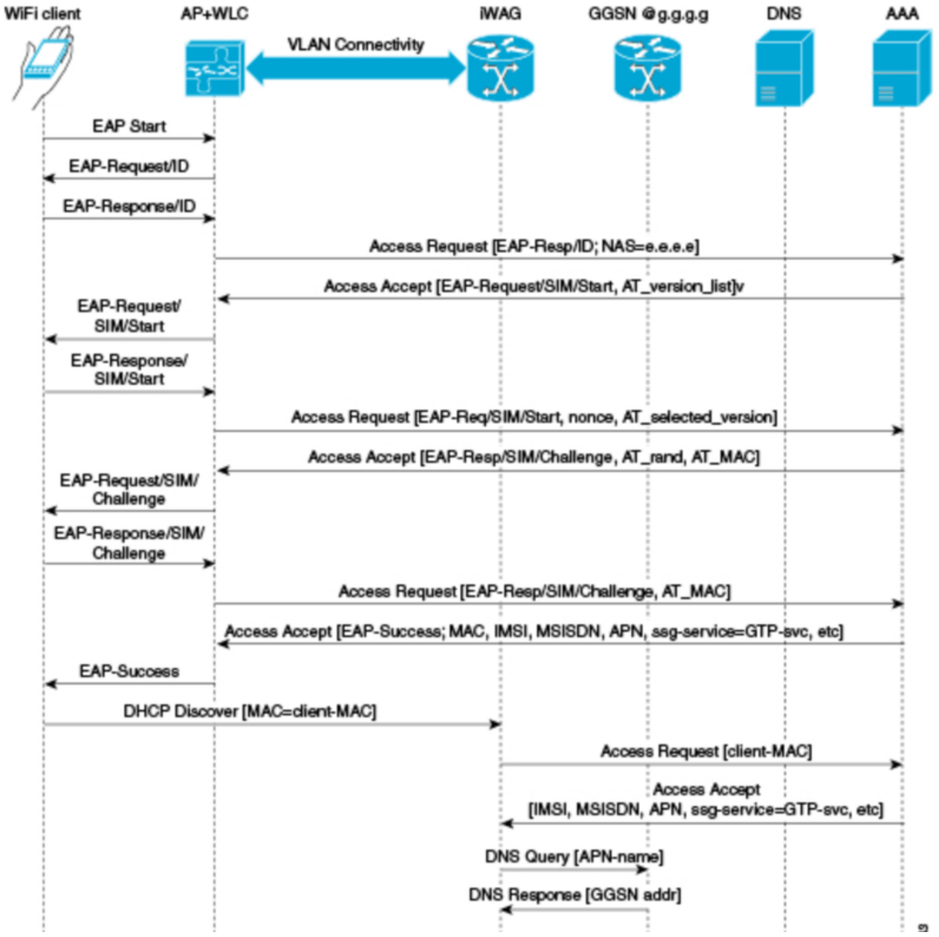
Step 6. MS acknowledges it by returning an Attach Complete message to the SGSN & initiate PDP activation context which is received by SGSN & it enquire DNS for GGSN IP address.

Step 7. Create PDP request is sent to GGSN after acceptance of which **Create PDP Context accepted**message is sent to MS with user IP address.

Step 8. Now MS can browse internet.

How WiFi Fits in Mobility Services (iWAG Solution)

3G DHCP Discover Call Flow (Part 1)


WiFi client
AP+WLC
IWAG
GGSN @g.g.g.g
DNS
AAA
VLAN Connectivity
EAP Start
EAP-Request/ID
EAP-Response/ID
Access Request [EAP-Resp/ID; NAS=e.e.e.e]
Access Accept [EAP-Request/SIM/Start, AT_version_list]v
EAP-Request/ SIM/Start
EAP-Response/ SIM/Start
Access Request [EAP-Req/SIM/Start, nonce, AT_selected_version]
Access Accept [EAP-Resp/SIM/Challenge, AT_rand, AT_MAC]
EAP-Request/SIM/ Challenge
EAP-Response/SIM/ Challenge
Access Request [EAP-Resp/SIM/Challenge, AT_MAC]
Access Accept [EAP-Success; MAC, IMSI, MSISDN, APN, ssg-service=GTP-svc, etc]
EAP-Success
DHCP Discover [MAC=client-MAC]
Access Request [client-MAC]
Access Accept [IMSI, MSISDN, APN, ssg-service=GTP-svc, etc]
DNS Query [APN-name]
DNS Response [GGSN addr]

Step 1. The mobile device is automatically associated to the Service Set Identifier (SSID) broadcast by the access points to establish and maintain wireless connectivity.

Step 2. The AP or the WLC starts the EAP authentication process by sending an EAP Request ID to the mobile device.

Step 3. The mobile device sends a response which pertains to the EAP Request ID back to the AP or the WLC.

Step 4. The WLC sends a RADIUS Access Request to the Authentication, Authorization, and Accounting (AAA) server and asks it to authenticate the subscriber.

Step 5. After the subscriber is authenticated, the AAA server caches its entire user profile that includes the information about IMSI, MSISDN, APN, and the Cisco AV pair that has ssg-service-info set to GTP-service. The cached data also includes the client's MAC address, which is set as the calling-station-ID in the incoming EAP messages.

Step 6. The AAA server sends the RADIUS Access Accept message to the AP or the WLC.

Step 7. When the RADIUS Access Accept message comes back, the corresponding user profile in which the use of GTP-service is identified is obtained.

Step 8. The WLC sends the successful EAP authentication message to the mobile device.

Step 9. The mobile device sends a DHCP Discover message to the iWAG. In response to this DHCP Discover message, the DHCP goes into a new pending state to wait for the signaling on the MNO side to be completed, which assigns an IP address to the subscriber. In response to this, DHCP Discover message, DHCP goes into a new pending state to wait for the signaling on the

MNO side to be completed, which assigns an IP address to the subscriber.

Step 10. The iWAG finds a session associated with the subscriber MAC address and retrieves the subscriber IP address from the session context.

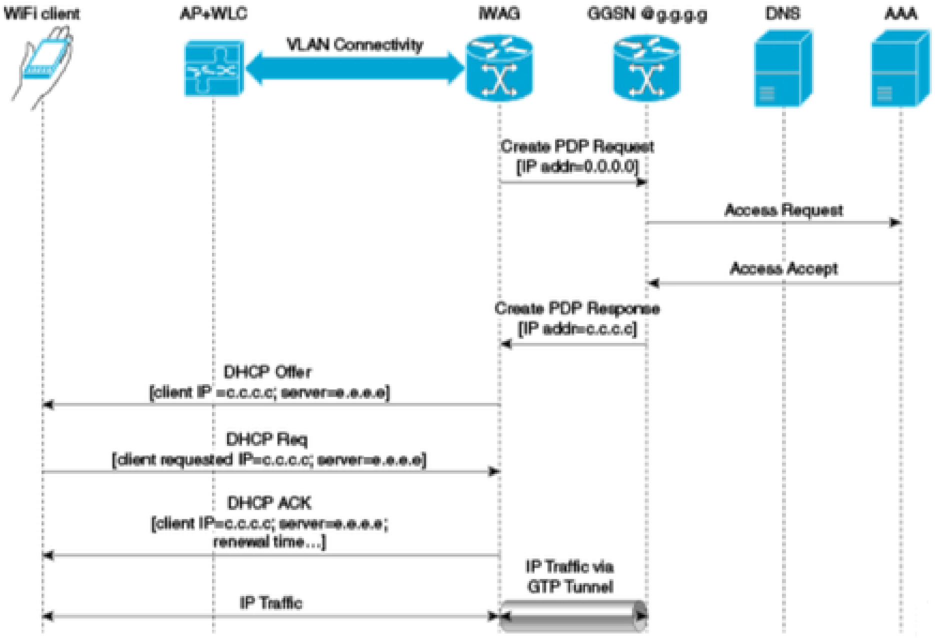
Step 11. The iWAG sends a RADIUS Access Request to the AAA server and asks it to authenticate the subscriber with the use of the MAC address in it as the calling-station-ID, while it also provides all other known subscriber information, IDs, and IMSI in this Access Request message.

Step 12. When the AAA server sends back the RADIUS Access Accept message to the iWAG, the user profile in which the use of GTP-service is identified is obtained.

Step 13. The iWAG sends a query to the DNS server to resolve a given Access Point Name (APN) to a GGSN IP address.

Step 14. The DNS server sends the DNS-resolved GGSN address back to the iWAG.

3G DHCP Discover Call Flow (Part 2)



Step 15. After it receives the DNS-resolved GGSN address, the iWAG sends the Create PDP Context Request, in which the PDP context address is set to 0, in order to request the GGSN for an IP address assignment.

Step 16. The GGSN sends a RADIUS Access Request to the AAA server.

Step 17. Based on the cached information obtained from the EAP-SIM authentication, the AAA server replies with a RADIUS Access Accept message to the GGSN.

Step 18. The GGSN sends the Create PDP Context Response that carries the assigned IP address c.c.c.c for the subscriber, to the iWAG.

Step 19. The iWAG sends a DHCP Offer message to the mobile device.

Step 20. The mobile device sends a DHCP Request message to the iWAG, and the iWAG acknowledges this request by sending a DHCP ACK message to the mobile device.

Step 21. The WiFi subscriber traffic now has a data path through which it can flow.