

Compreenda a solução do iWAG para dados do móbil 3G

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Acrônimos](#)

[Explicação da terminologia usada](#)

[Compreenda os Serviços de mobilidade \(3G/4G\)](#)

[Fluxo de chamadas 3G simplificado](#)

[Como ajustes de WiFi nos Serviços de mobilidade \(solução do iWAG\)](#)

[3G DHCP descobrem o fluxo de chamadas \(parte 1\)](#)

[3G DHCP descobrem o fluxo de chamadas \(parte 2\)](#)

Introdução

Este documento descreve a solução inteligente do gateway do acesso Wireless (iWAG) e como integra a tecnologia da mobilidade com solução de WiFi.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Tecnologia Wireless
- Fluxo de chamadas da mobilidade

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

Informações de Apoio

Para alcançar normalmente o Internet você usa dois tipos de serviços de Internet:

- WiFi
- Internet móvel (rede da mobilidade 3G/4G)

A combinação destas duas Tecnologias dá uma experiência melhor ao cliente e este é o propósito principal desta solução.

A solução do iWAG inclui uma combinação de usuários simples IP (ISG tradicional e WiFi) e de usuários IP Móveis (Tunelamento PMIPv6 ou GTP). O serviço da mobilidade do termo é usado para referir o serviço GTP ou o serviço PMIPv6 aplicado ao tráfego de usuário. O iWAG proporciona Serviços de mobilidade aos usuários IP Móveis e em consequência, um cliente móvel pode continuamente alcançar a rede de uma mobilidade 3G ou 4G. Contudo, o iWAG não proporciona Serviços de mobilidade aos usuários simples IP.

Conseqüentemente, os usuários simples IP podem alcançar a rede pública do Wireless LAN (PWLAN) através do ISG de Cisco. Os clientes podem alcançar o Internet de WiFi (Sem fio público), onde sempre possível. Contudo, se WiFi não está disponível, os mesmos clientes podem conectar ao serviço de Internet com a rede de uma mobilidade 3G ou 4G.

Os provedores de serviços usam uma combinação de WiFi e a mobilidade oferece offload suas redes da mobilidade na área do uso do serviço da alto-concentração. Isto conduziu à evolução do iWAG. O iWAG fornece WiFi offload a opção aos provedores de serviços 4G e 3G permitindo uma solução da único-caixa que forneça a funcionalidade combinada do IPv6 móvel do proxy (PMIPv6) e do protocolo de tunelamento GPRS (GTP).

Acrônimos

GPRS - General Packet Radio Service

RNC - Controlador da rede de rádio

SGSN - Preste serviços de manutenção ao nó de suporte GPRS

PDP - Protocolo de dados de pacote

GGSN - Gateway GPRS Support Node

APN - Nome do Access point

IMSI - Identidade internacional do assinante de celular

MSISDN - Número de diretório de assinante internacional da estação móvel

HLR - Registro de lugar home

Explicação da terminologia usada

- IPv6 do móbil do proxy

O Gerenciamento de mobilidade Com base na rede permite a mesma funcionalidade que o IP Móvel, sem nenhuma alteração à pilha de protocolos TCP/IP do host. Com PMIP, o host pode mudar seu ponto de conexão ao Internet sem a necessidade de mudar seu endereço IP de Um ou Mais Servidores Cisco ICM NT. O contrário à aproximação IP Móvel, esta funcionalidade é executado pela rede, que é responsável seguir os movimentos do host e iniciar a mobilidade exigida que sinaliza em seu nome. Contudo, caso que a mobilidade envolve interfaces de rede diferentes, o host precisa as alterações similares ao IP Móvel a fim manter o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT através das relações diferentes.

- Protocolo de tunelamento GPRS

GTP é um grupo de protocolos de comunicações com base em IP usados para levar o General Packet Radio Service (GPRS) dentro das redes GS, UMTS e LTE.

- General Packet Radio Service

O GPRS é um serviço dos dados móvel orientado pacote na comunicação 2G e 3G celular.

- Controlador da rede de rádio

RNC é um elemento de governo na rede de acesso do rádio UMTS (3G) (UTRAN).

- Preste serviços de manutenção ao nó de suporte GPRS

SGSN é um componente principal da rede de GPRS, que segura todos os dados comutáveis por blocos dentro da rede, por exemplo o Gerenciamento de mobilidade e a autenticação dos usuários.

- Gateway GPRS Support Node

O GGSN é parte da rede central que conecta as redes 3G GS-baseadas ao Internet. O GGSN, conhecido às vezes como um roteador Wireless, trabalha com o SGSN para manter usuários móveis conectados ao Internet e aos aplicativos com base em IP.

- Protocolo de dados de pacote

O contexto PDP é uma estrutura de dados atual no nó de suporte servindo GPRS (SGSN) e no Gateway GPRS Support Node (GGSN) que contém a informação de sessão do subscritor quando o subscritor tem uma sessão ativa.

- Nome do Access point

O APN é o nome para os ajustes que seu telefone lê para estabelecer uma conexão ao gateway entre a rede celular do seu portador e os Internet públicas.

- Identidade internacional do assinante de celular

O IMSI é usado para identificar o usuário de uma rede celular e é uma identificação exclusiva associada com todas as redes celulares. É armazenado como uns 64 campo de bit e enviado pelo telefone à rede.

- Número de diretório de assinante internacional da estação móvel

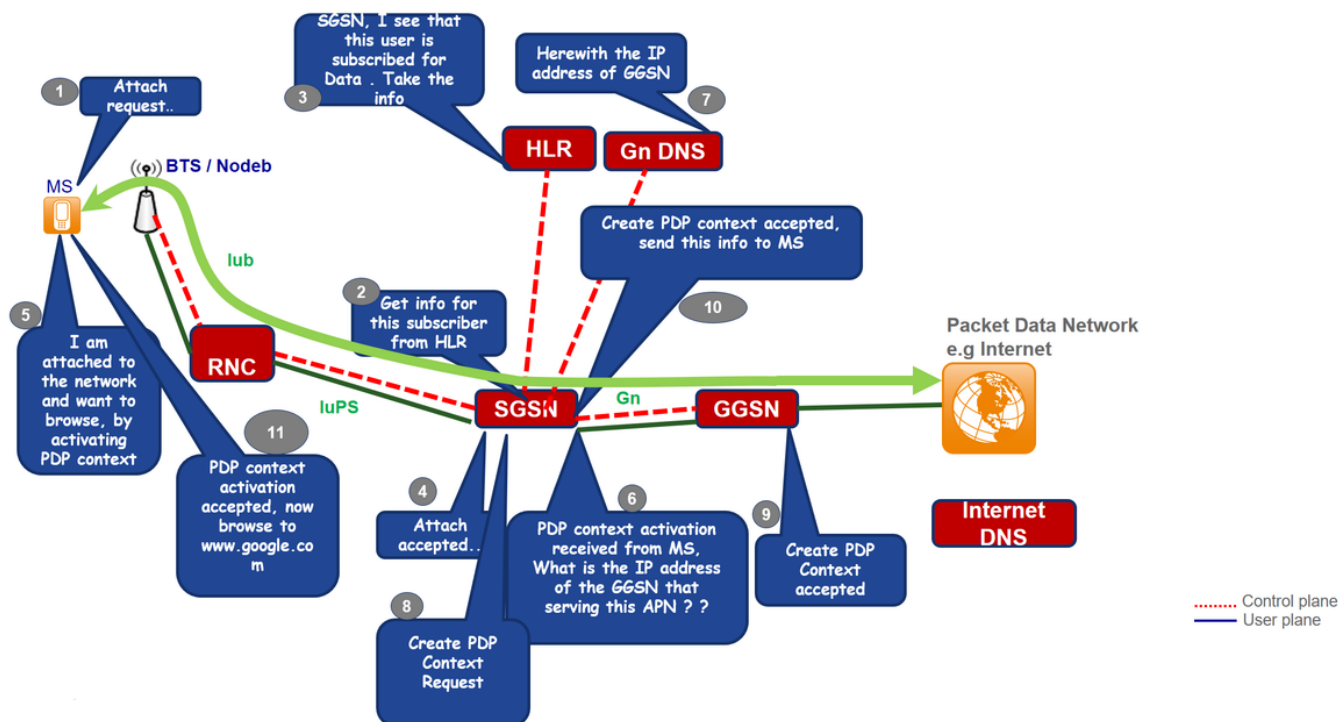
O MSISDN é um número usado para identificar internacionalmente um número de telefone celular. MSISDN é definido pelo plano de numeração E.164. Este número inclui um código de país e um código de destino nacional que identifique o operador do subscritor.

- Registro de lugar home

O HLR é o base de dados principal da informação de assinante permanente para uma rede móvel.

Compreenda os Serviços de mobilidade (3G/4G)

Fluxo de chamadas 3G simplificado



Etapa 1. A estática móvel (MS) inicia o procedimento do anexo pela transmissão de um mensagem request do anexo ao SGSN.

Etapa 2. Se o MS é desconhecido no SGSN, o SGSN envia um pedido da identidade ao MS. O MS responde com resposta da identidade, que inclui o IMSI do MS.

Etapa 3. Se nenhum contexto do Gerenciamento de mobilidade (MM) para o MS existe no SGSN (sessão existente), a seguir a autenticação é imperativa. O SGSN pergunta o HLR para a informação da autenticação do móbil com uma informação da autenticação da emissão, e pede que o MS envie a informação do AUTH enviando uma autenticação GPRS e calculando o pedido ao móbil.

Etapa 4. O HLR envia dados do subscritor da inserção ao SGSN, que inclui os dados da assinatura do móbil.

Etapa 5. O SGSN envia um anexo aceita a mensagem ao MS.

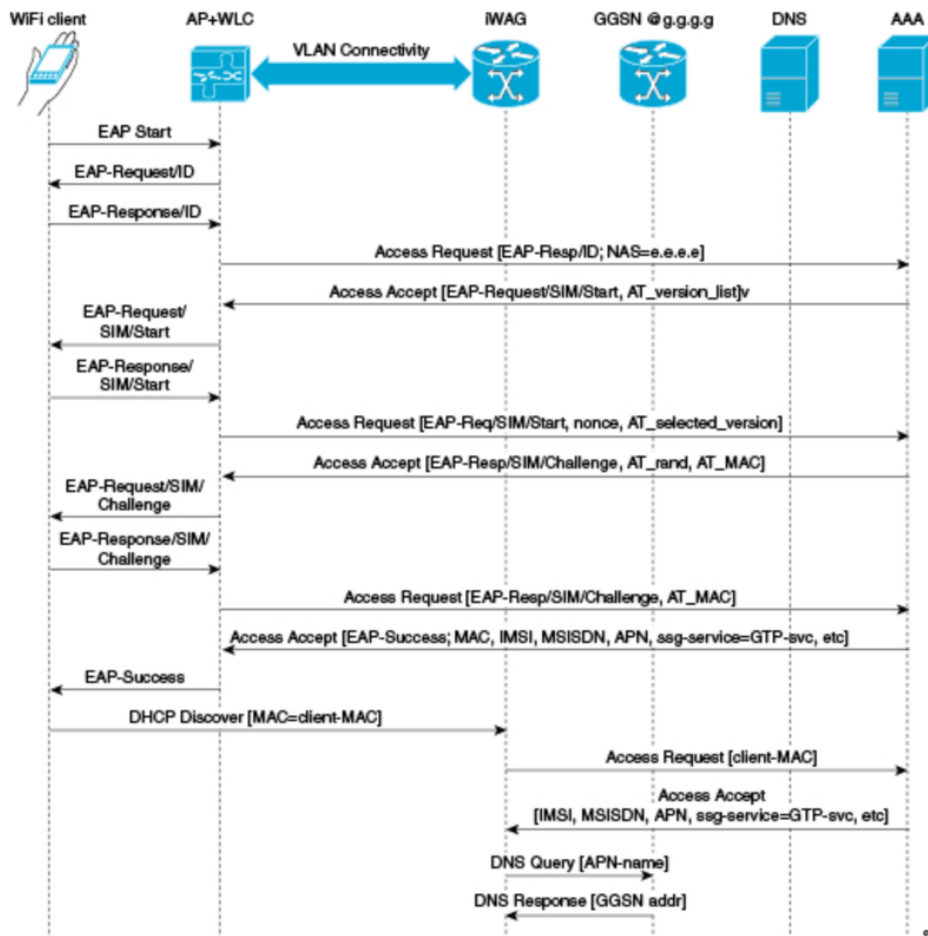
Etapa 6. O MS reconhece-a retornando um mensagem completa do anexo ao SGSN & inicia-o o contexto da ativação PDP que é recebido por SGSN & inquire o DNS para o endereço IP de Um ou Mais Servidores Cisco ICM NT GGSN.

Etapa 7. Crie o pedido PDP é enviado ao GGSN após a aceitação de que **crie o acceptedmessage do contexto PDP** é enviado ao MS com endereço IP de Um ou Mais Servidores Cisco ICM NT do usuário.

Etapa 8. Agora o MS pode consultar o Internet.

Como ajustes de WiFi nos Serviços de mobilidade (solução do iWAG)

3G DHCP descobrem o fluxo de chamadas (parte 1)



Etapa 1. O dispositivo móvel é associado automaticamente à transmissão do Service Set Identifier (SSID) pelos Access point para estabelecer e manter a conectividade Wireless.

Etapa 2. O AP ou o WLC começam o processo de autenticação de EAP enviando um pedido ID EAP ao dispositivo móvel.

Etapa 3. O dispositivo móvel envia uma resposta que se refira ao pedido ID EAP de volta ao AP ou ao WLC.

Etapa 4. O WLC envia um pedido do acesso radius ao server do Authentication, Authorization, and Accounting (AAA) e pede que autentique o subscritor.

Etapa 5. Depois que o subscritor é autenticado, o servidor AAA põe em esconderijo seu perfil de usuário inteiro que inclui a informação sobre IMSI, MSISDN, APN, e o par do AV Cisco que tem o GTP-serviço ajustado SSG-serviço-informação. Os dados postos em esconderijo igualmente incluem o MAC address do cliente, que é ajustado como o chamar-estação-ID nos mensagens EAP entrantes.

Etapa 6. O servidor AAA envia o acesso radius aceita a mensagem ao AP ou ao WLC.

Etapa 7. Quando o acesso radius aceita a mensagem volta, o perfil de usuário correspondente em que o uso do GTP-serviço é identificado é obtido.

Etapa 8. O WLC envia a mensagem bem sucedida da autenticação de EAP ao dispositivo móvel.

Etapa 9. O dispositivo móvel envia um mensagem DISCOVER DHCP ao iWAG. Em resposta a este mensagem DISCOVER DHCP, o DHCP entra em um novo durante o estado esperar a sinalização no lado MNO a ser terminado, que atribui um endereço IP de Um ou Mais Servidores Cisco ICM NT ao subscritor. Em resposta a isto, o mensagem DISCOVER DHCP, DHCP entra em um novo durante o estado esperar a sinalização no lado MNO a ser terminado, que atribui um endereço IP de Um ou Mais Servidores Cisco ICM NT ao subscritor.

Etapa 10. O iWAG encontra uma sessão associada com o MAC address do subscritor e recupera o endereço IP de Um ou Mais Servidores Cisco ICM NT do subscritor do contexto da sessão.

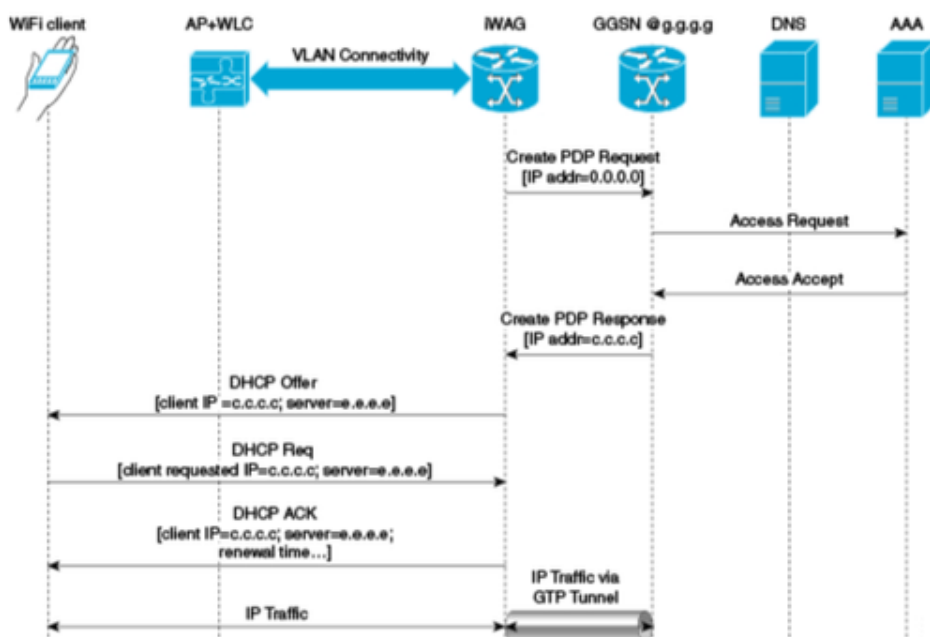
Etapa 11. O iWAG envia um pedido do acesso radius ao servidor AAA e pede que autentique o subscritor com o uso do MAC address nele como o chamar-estação-ID, quando igualmente fornecer todos informação de assinante, ID, e IMSI conhecidos restantes neste mensagem request do acesso.

Etapa 12. Quando o servidor AAA envia para trás o acesso radius aceite a mensagem ao iWAG, o perfil de usuário em que o uso do GTP-serviço é identificado é obtido.

Etapa 13. O iWAG envia uma pergunta ao servidor DNS para resolver um nome dado do Access point (APN) a um endereço IP de Um ou Mais Servidores Cisco ICM NT GGSN.

Etapa 14. O servidor DNS envia o endereço DNS-resolved GGSN de volta ao iWAG.

3G DHCP descobrem o fluxo de chamadas (parte 2)



Etapa 15. Depois que recebe o endereço DNS-resolved GGSN, o iWAG envia o pedido do contexto da criação PDP, em que o endereço do contexto PDP é ajustado a 0, a fim pedir o GGSN para uma atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT.

Etapa 16. O GGSN envia um pedido do acesso radius ao servidor AAA.

Etapa 17. Baseado na informação posta em esconderijo obtida da autenticação EAP-SIM, as respostas do servidor AAA com um acesso radius aceitam a mensagem ao GGSN.

Etapa 18. O GGSN envia a resposta do contexto da criação PDP que leva o endereço IP atribuído c.c.c.c para o subscritor, ao iWAG.

Etapa 19. O iWAG envia uma mensagem da oferta de DHCP ao dispositivo móvel.

Etapa 20. O dispositivo móvel envia um mensagem REQUEST DHCP ao iWAG, e o iWAG reconhece este pedido enviando um mensagem de reconhecimento DHCP ao dispositivo móvel.

Etapa 21. O tráfego de assinante de WiFi tem agora um trajeto de dados por que pode passar.