iWAG-Lösung für mobile 3G-Daten

Inhalt

Einführung

Dieses Dokument beschreibt die iWAG-Lösung (Intelligent Wireless Access Gateway) und die Integration der Mobilitätstechnologie in die WiFi-Lösung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Wireless
- Mobility-Anruffluss

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Hintergrundinformationen

Normalerweise nutzen Sie für den Internetzugang zwei Internet-Services:

- WiFi
- Mobiles Internet (3G/4G Mobility Network)

Die Kombination dieser beiden Technologien bietet dem Kunden ein besseres Erlebnis, und dies ist der Hauptzweck dieser Lösung.

Die iWAG-Lösung umfasst eine Kombination aus einfachen IP-Benutzern (klassisches ISG und

WiFi) und mobilen IP-Benutzern (PMIPv6 oder GTP-Tunneling). Der Begriff "Mobility-Service" bezieht sich entweder auf den GTP-Service oder den auf Benutzerdatenverkehr angewendeten PMIPv6-Service. Die iWAG stellt Mobility-Services für mobile IP-Benutzer bereit, sodass mobile Clients nahtlos auf ein 3G- oder 4G-Mobilitätsnetzwerk zugreifen können. Die iWAG stellt jedoch keine Mobilitätsdienste für einfache IP-Benutzer bereit.

Aus diesem Grund können einfache IP-Benutzer über die Cisco ISG auf das öffentliche Wireless LAN (PWLAN)-Netzwerk zugreifen. Clients können, wo immer möglich, auf das WiFi-Internet (öffentliches Wireless) zugreifen. Wenn WiFi jedoch nicht verfügbar ist, können dieselben Clients eine Verbindung zum Internetdienst über ein 3G- oder 4G-Mobilitätsnetzwerk herstellen. Service Provider nutzen eine Kombination aus Wi-Fi- und Mobilitätsangeboten, um ihre Mobilitätsnetzwerke im Bereich der Nutzung von Diensten mit hoher Konzentration auszulagern. Dies führte zur Weiterentwicklung der iWAG. Die iWAG stellt 4G- und 3G-Service Providern eine Wi-Fi-Offload-Option zur Verfügung, indem sie eine Paketlösung bereitstellt, die die kombinierte Funktionalität von Proxy Mobile IPv6 (PMIPv6) und GPRS Tunneling Protocol (GTP) bietet.

Akronyme

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 - Nummer des internationalen Teilnehmerverzeichnisses für Mobilgeräte

HLR = Home Location Register

Erläuterung der verwendeten Terminologie

- Mobile Proxy-IPv6

Das netzwerkbasierte Mobilitätsmanagement bietet dieselben Funktionen wie Mobile IP, ohne dass Änderungen am TCP/IP-Protokoll-Stack des Hosts erforderlich sind. Mit PMIP kann der Host seine Verbindungspunkte im Internet ändern, ohne seine IP-Adresse ändern zu müssen. Im Gegensatz zum Mobile IP-Ansatz wird diese Funktionalität vom Netzwerk implementiert, das die Bewegungen des Hosts nachverfolgt und die erforderliche Mobilität initiiert, die in seinem Namen Signale aussendet. Falls die Mobilität jedoch verschiedene Netzwerkschnittstellen umfasst, benötigt der Host ähnliche Änderungen wie Mobile IP, um dieselbe IP-Adresse über verschiedene Schnittstellen hinweg zu erhalten.

- GPRS Tunneling Protocol

GTP ist eine Gruppe von IP-basierten Kommunikationsprotokollen, die zur Übertragung des

allgemeinen Paket-Funkdienstes (GPRS) in GSM-, UMTS- und LTE-Netzwerken verwendet werden.

- Allgemeiner Paketfunk

GPRS ist ein paketorientierter mobiler Datendienst auf 2G- und 3G-Mobilfunkverbindungen.

- Funknetzwerkcontroller

RNC ist ein Element des UMTS (3G)-Funkzugangsnetzwerks (UTRAN).

- Service GPRS Support-Knoten

SGSN ist eine Hauptkomponente des GPRS-Netzwerks, das alle paketvermittelten Daten innerhalb des Netzwerks verarbeitet, z. B. das Mobilitätsmanagement und die Authentifizierung der Benutzer.

- Gateway-GPRS-Support-Knoten

GGSN ist Teil des Kernnetzwerks, das GSM-basierte 3G-Netzwerke mit dem Internet verbindet. Das GGSN, manchmal auch als Wireless-Router bezeichnet, arbeitet mit dem SGSN zusammen, um mobile Benutzer mit dem Internet und IP-basierten Anwendungen zu verbinden.

- Paketdatenprotokoll

Der PDP-Kontext ist eine Datenstruktur, die sowohl auf dem Server-GPRS-Support-Knoten (SGSN) als auch auf dem Gateway-GPRS-Support-Knoten (GGSN) vorhanden ist, der die Sitzungsinformationen des Teilnehmers enthält, wenn der Teilnehmer eine aktive Sitzung hat.

- Name des Access Points

Die APN ist der Name für die Einstellungen, die Ihr Telefon liest, um eine Verbindung zum Gateway zwischen dem Mobilfunknetz Ihres Mobilfunkanbieters und dem öffentlichen Internet einzurichten.

- Internationale Identität mobiler Teilnehmer

Der IMSI wird verwendet, um den Benutzer eines Mobilfunknetzes zu identifizieren und ist eine eindeutige Identifizierung, die mit allen Mobilfunknetzen verknüpft ist. Sie wird als 64-Bit-Feld gespeichert und vom Telefon an das Netzwerk gesendet.

- Nummer des internationalen Teilnehmerverzeichnisses für Mobilgeräte

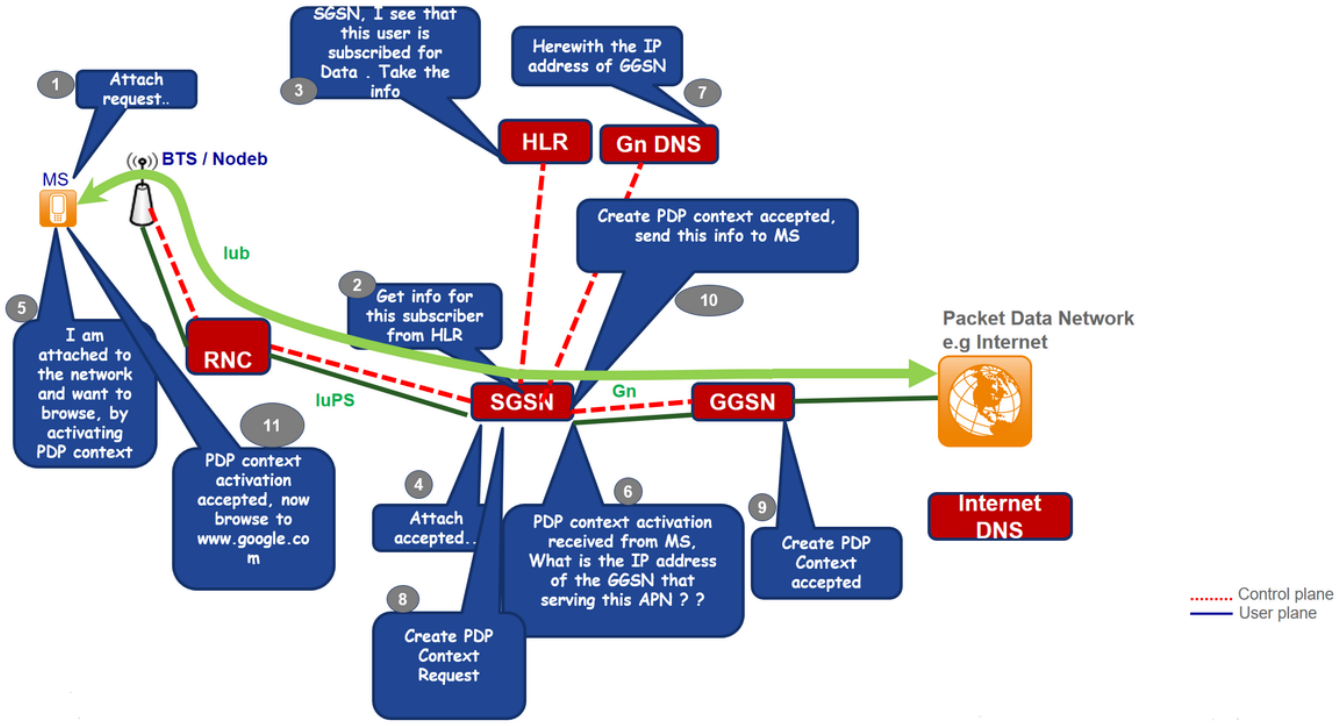
MSISDN ist eine Nummer, die zur internationalen Identifizierung einer Mobiltelefonnummer verwendet wird. MSISDN ist im E.164-Nummernplan definiert. Diese Nummer enthält eine Ländervorwahl und einen nationalen Zielcode zur Identifizierung des Teilnehmerbetreibers.

- Registrierung des Home Location

Das HLR ist die Hauptdatenbank von permanenten Teilnehmerinformationen für ein Mobilfunknetz.

Kenntnis der Mobilitätsdienste (3G/4G)

Vereinfachter 3G-Anruffluss



Schritt 1: Der Mobile Static (MS) initiiert das Anfügeverfahren, indem eine Attach Request-Nachricht an den SGSN gesendet wird.

Schritt 2: Wenn der MS im SGSN unbekannt ist, sendet der SGSN eine Identitätsanforderung an den MS. Der MS reagiert mit Identity Response, zu dem auch der IMSI der MS gehört.

Schritt 3: Wenn im SGSN (vorhandene Sitzung) kein Mobility Management (MM)-Kontext für die MS vorhanden ist, ist eine Authentifizierung erforderlich. Das SGSN fragt das HLR nach den Authentifizierungsinformationen des Mobilgeräts mit einer Send Authentication Information ab und fordert die MS auf, Autoreninformationen zu senden, indem sie eine GPRS Authentication and Ciphering Request an das Mobiltelefon sendet.

Schritt 4: Das HLR sendet Insert Subscriber Data an das SGSN, das auch die Abonnementdaten des Mobiltelefons enthält.

Schritt 5: Der SGSN sendet eine Meldung zur Anrufannahme an den MS.

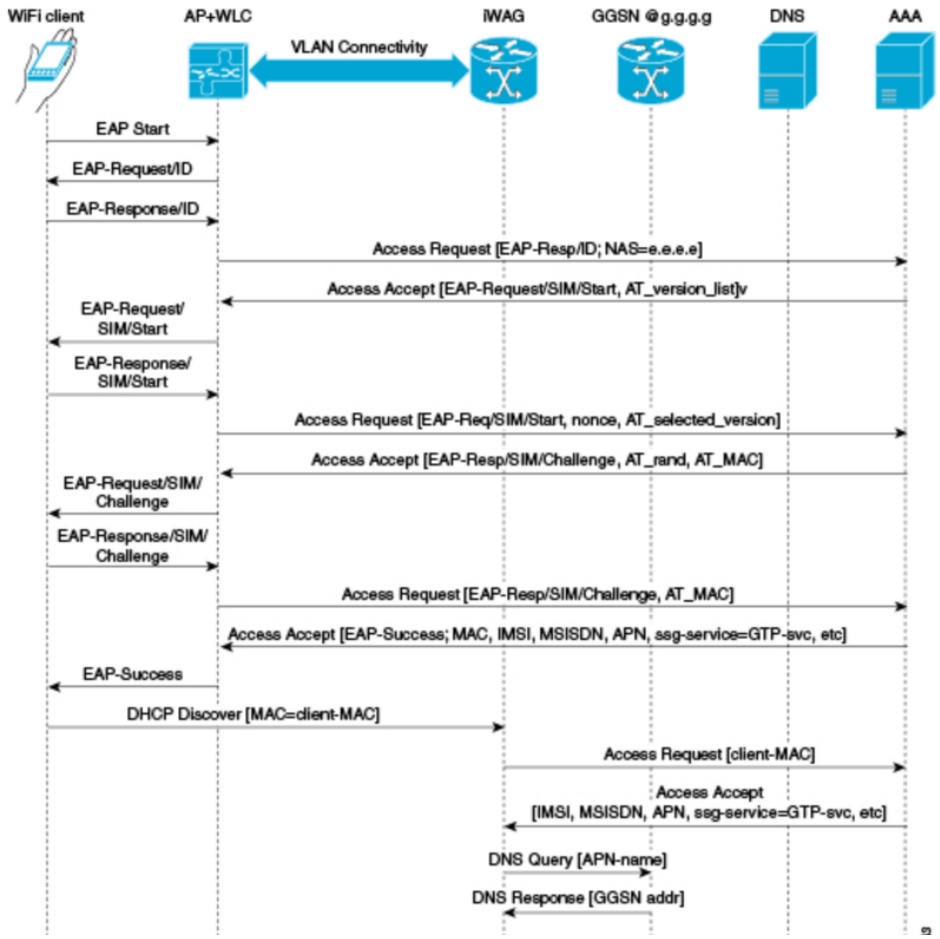
Schritt 6: MS bestätigt dies, indem es eine "Attach Complete"-Nachricht an den SGSN zurücksendet und den PDP-Aktivierungskontext initiiert, der vom SGSN empfangen wird, und DNS nach der GGSN-IP-Adresse fragt.

Schritt 7: Die Erstellung der PDP-Anfrage wird an GGSN gesendet, nachdem die **Create PDP Context** Accepted Message an MS mit der Benutzer-IP-Adresse gesendet wurde.

Schritt 8: MS kann jetzt im Internet surfen.

Wie Wi-Fi bei Mobility-Services (iWAG-Lösung) funktioniert

3G DHCP Discover Call Flow (Anruffluss für 3G-DHCP ermitteln) (Teil 1)



Schritt 1: Das Mobilgerät wird automatisch mit dem Service Set Identifier (SSID)-Broadcast von den Access Points verknüpft, um eine Wireless-Verbindung herzustellen und aufrechtzuerhalten.

Schritt 2: Der AP oder der WLC startet den EAP-Authentifizierungsprozess, indem er eine EAP-Anfrage-ID an das mobile Gerät sendet.

Schritt 3: Das Mobilgerät sendet eine Antwort, die sich auf die EAP-Anfrage-ID bezieht, an den AP oder den WLC zurück.

Schritt 4: Der WLC sendet eine RADIUS Access Request an den Server Authentication, Authorization, Accounting (AAA) und fordert ihn auf, den Teilnehmer zu authentifizieren.

Schritt 5: Nachdem der Abonnent authentifiziert wurde, speichert der AAA-Server sein gesamtes Benutzerprofil, das Informationen über IMSI, MSISDN, APN und das Cisco AV-Paar enthält, für das ssg-service-info auf GTP-Service festgelegt ist. Zu den zwischengespeicherten Daten gehört auch die MAC-Adresse des Clients, die in den eingehenden EAP-Nachrichten als Calling-Station-ID festgelegt ist.

Schritt 6: Der AAA-Server sendet die RADIUS Access Accept-Nachricht an den AP oder den WLC.

Schritt 7: Wenn die Meldung RADIUS Access Accept (RADIUS Access Accept) zurückgegeben wird, wird das entsprechende Benutzerprofil abgerufen, in dem der GTP-Service verwendet wird.

Schritt 8: Der WLC sendet die erfolgreiche EAP-Authentifizierungsmeldung an das Mobilgerät.

Schritt 9. Das Mobilgerät sendet eine DHCP Discover-Nachricht an die iWAG. Als Antwort auf diese DHCP Discover-Meldung wechselt der DHCP in einen neuen ausstehenden Zustand, um

auf die Beendigung der Signalisierung auf der MNO-Seite zu warten, die dem Teilnehmer eine IP-Adresse zuweist. Als Antwort auf diese DHCP Discover-Nachricht wechselt DHCP in einen neuen ausstehenden Zustand, um auf die Beendigung der Signalisierung auf der MNO-Seite zu warten, die dem Teilnehmer eine IP-Adresse zuweist.

Schritt 10: Die iWAG findet eine Sitzung, die der MAC-Adresse des Teilnehmers zugeordnet ist, und ruft die Teilnehmer-IP-Adresse aus dem Sitzungskontext ab.

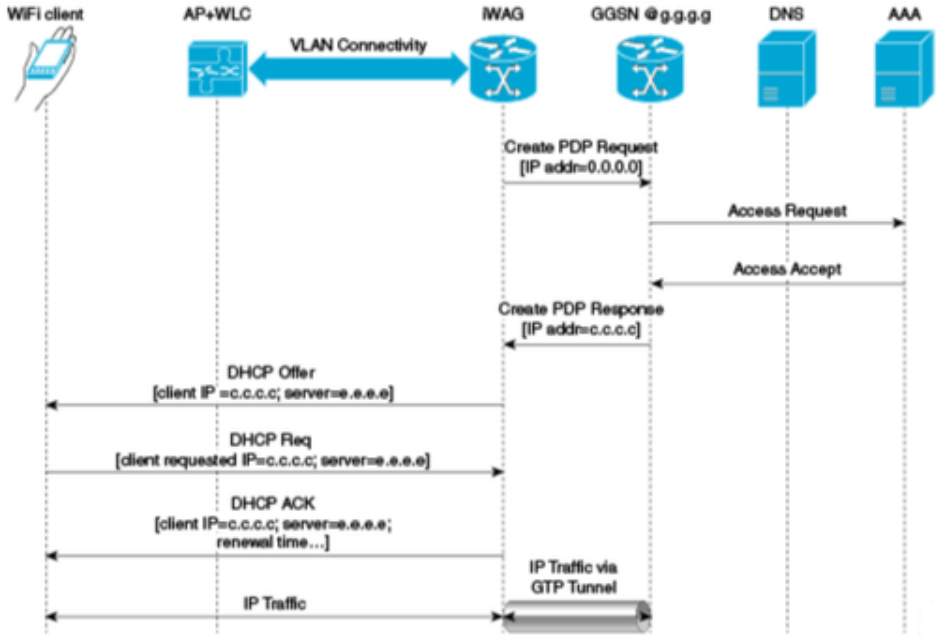
Schritt 11: Die iWAG sendet eine RADIUS-Zugriffsanfrage an den AAA-Server und fordert diesen auf, den Teilnehmer mithilfe der darin enthaltenen MAC-Adresse als Anrufer-Station-ID zu authentifizieren, während sie in dieser Zugriffsanfrage auch alle anderen bekannten Abonnenten-Informationen, IDs und IMSI bereitstellt.

Schritt 11: Wenn der AAA-Server die RADIUS Access Accept-Nachricht an die iWAG zurücksendet, wird das Benutzerprofil abgerufen, in dem der GTP-Service verwendet wird.

Schritt 13: Die iWAG sendet eine Abfrage an den DNS-Server, um einen bestimmten Access Point Name (APN) an eine GGSN-IP-Adresse aufzulösen.

Schritt 14: Der DNS-Server sendet die DNS-aufgelöste GGSN-Adresse zurück an die iWAG.

3G DHCP Discover Call Flow (Anruffluss für 3G-DHCP ermitteln) (Teil 2)



Schritt 15: Nachdem die DNS-aufgelöste GGSN-Adresse empfangen wurde, sendet die iWAG die Create PDP Context Request (PDP-Kontextanforderung erstellen), in der die PDP-Kontextadresse auf 0 gesetzt ist, um das GGSN für eine IP-Adresszuweisung anzufordern.

Schritt 16: Der GGSN sendet eine RADIUS Access Request an den AAA-Server.

Schritt 17: Basierend auf den zwischengespeicherten Informationen, die aus der EAP-SIM-Authentifizierung abgerufen wurden, antwortet der AAA-Server mit einer RADIUS Access Accept-

Nachricht an den GGSN.

Schritt 17: Der GGSN sendet die Create PDP Context Response, die die zugewiesene IP-Adresse c.c.c für den Abonnenten enthält, an die iWAG.

Schritt 19. Die iWAG sendet eine DHCP Offer-Nachricht an das mobile Gerät.

Schritt 20: Das Mobilgerät sendet eine DHCP-Anfrage-Nachricht an die iWAG, und die iWAG bestätigt diese Anforderung durch das Senden einer DHCP-ACK-Nachricht an das Mobilgerät.

Schritt 21: Der WiFi-Teilnehmerdatenverkehr hat nun einen Datenpfad, über den er fließen kann.