Guide d'Opérations et de Déploiement d'OmniTWAG

Créé par Omnitouch

Ce guide est destiné aux opérateurs de réseau, aux administrateurs système et aux clients déployant OmniTWAG.

Table des Matières

Introduction

OmniTWAG (Trusted WiFi Access Gateway) est une mise en œuvre conforme aux normes d'un TWAG 3GPP qui permet aux opérateurs de réseaux mobiles de décharger en toute sécurité le trafic des abonnés des réseaux cellulaires vers

des points d'accès WiFi tout en maintenant une authentification sécurisée basée sur la SIM.

Le TWAG authentifie les abonnés WiFi en utilisant leurs identifiants SIM via EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement), le même mécanisme d'authentification utilisé dans les réseaux cellulaires. Cela fournit un accès WiFi sécurisé et sans couture pour les abonnés mobiles sans nécessiter de mots de passe WiFi séparés.

Avantages Clés

Pour les Utilisateurs Finaux :

- **Configuration Zéro** : Fonctionne dès la sortie de la boîte avec une SIM compatible
- **Expérience Sans Couture** : Connexion automatique comme sur le cellulaire
- **Sécurisé** : Utilise toujours un WiFi crypté (WPA2)
- **Pas de Mots de Passe** : Authentification basée sur la SIM

Pour les Opérateurs Mobiles :

- **Soulagement de la Capacité du Réseau** : Réduit la charge sur les stations de base cellulaires
- **Déchargement Contrôlé** : Seuls les abonnés autorisés peuvent se connecter
- **Amélioration de l'Expérience Utilisateur** : Le WiFi offre généralement une bande passante plus élevée
- **Efficacité Coût** : L'infrastructure WiFi est moins coûteuse que celle du cellulaire
- **Identité Cohérente** : Même IMSI utilisée pour le WiFi et le cellulaire
- **Intégration de Facturation** : Peut facturer l'utilisation du WiFi si désiré

Pour les Lieux/Entreprises :

- **Sécurité de Niveau Opérateur** : Aucun risque de partage de mots de passe

- **Scalabilité** : Supporte des milliers d'utilisateurs sans provisionnement manuel
- **Gestion Simplifiée** : Pas besoin de distribuer des mots de passe WiFi

---

Qu'est-ce que le WiFi Offload ?

Le WiFi offload permet aux opérateurs de réseaux mobiles de rediriger le trafic de données des abonnés des réseaux cellulaires congestionnés vers des réseaux WiFi.

Comment le TWAG Permet le Déchargement

Le TWAG agit comme la passerelle d'authentification entre :

- **Points d'Accès WiFi** (via le protocole RADIUS)
- **Réseau Mobile Central** HSS/HLR (via l'interface Diameter SWx)

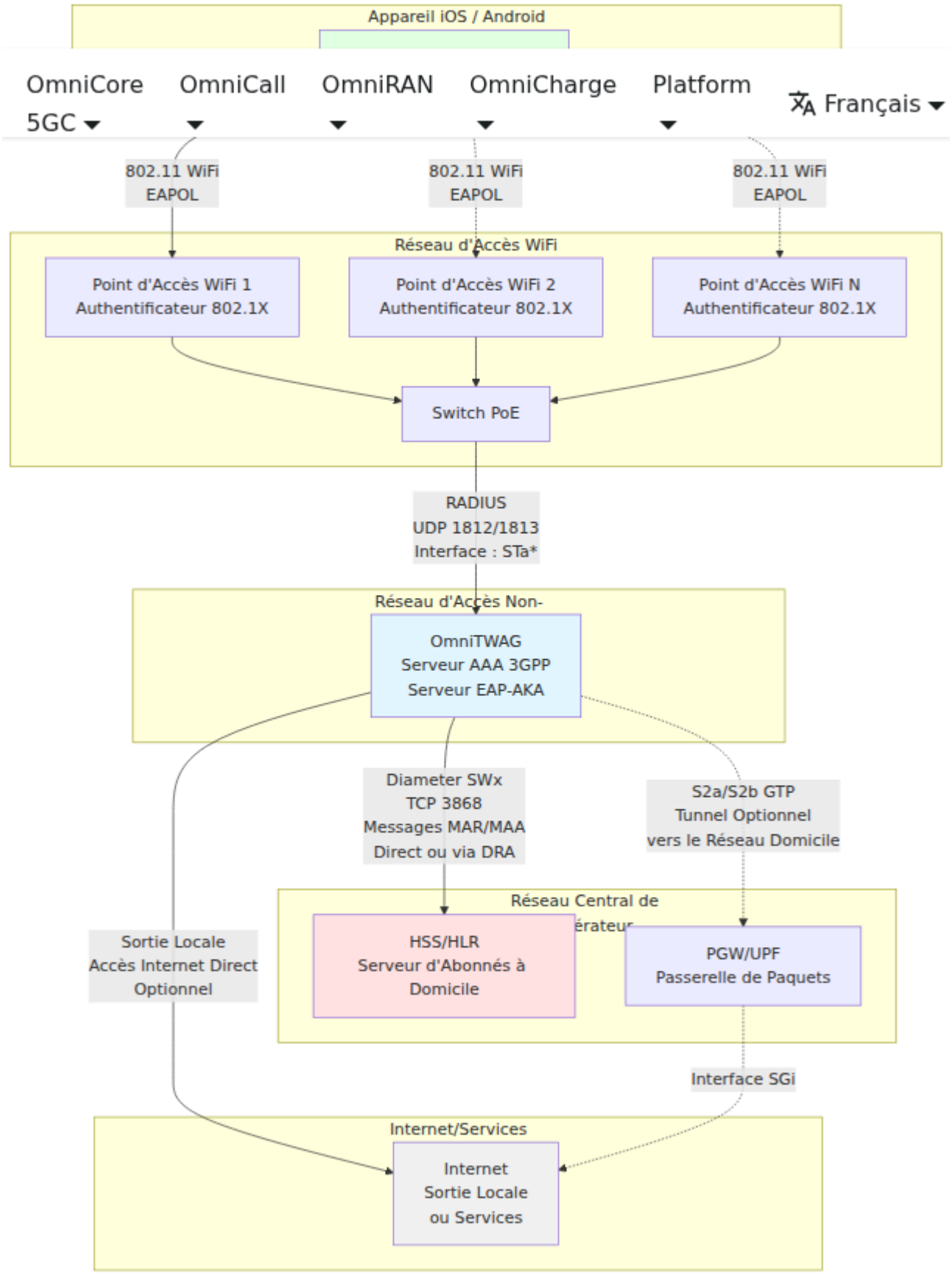
Lorsqu'un appareil d'abonné se connecte à un AP WiFi configuré pour le déchargement :

1. L'appareil s'identifie en utilisant son IMSI (de la carte SIM)
2. L'AP WiFi transmet les demandes d'authentification au TWAG via RADIUS
3. Le TWAG communique avec le HSS de l'opérateur pour récupérer les vecteurs d'authentification
4. L'authentification par défi-réponse EAP-AKA se produit entre l'appareil et le TWAG
5. Après une authentification réussie, l'appareil obtient l'accès au WiFi
6. En option, le trafic peut être tunnelé de retour vers le cœur mobile ou sortir localement

---

Architecture de Déploiement

Topologie du Réseau



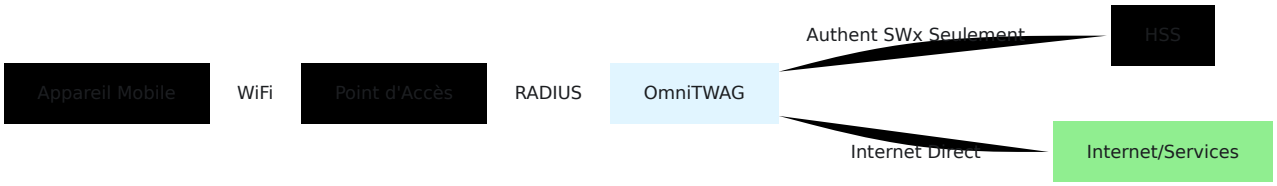
Légende des Interfaces :

- **STa*** : Interface RADIUS/Diameter entre l'AP WiFi et le TWAG (non-3GPP à AAA)

- **SWx** : Interface Diameter entre le TWAG (Serveur AAA 3GPP) et le HSS
- **S2a/S2b** : Interface de tunnel GTP pour le retour vers le réseau domicile (optionnel)
- **SGi** : Interface vers des réseaux de données de paquets externes (Internet)
- **802.11** : Interface radio WiFi
- **EAPOL** : EAP sur LAN (authentification 802.1X)

Scénarios de Déploiement

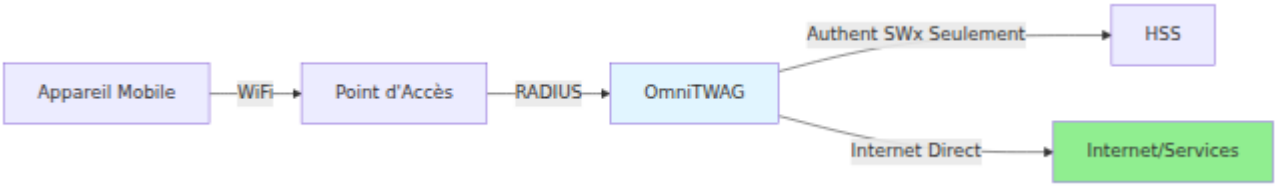
Scénario 1 : Sortie Locale (Recommandé pour la Performance)



Avantages :

- Latence plus faible (pas de retour au cœur)
- Charge réduite sur le réseau central
- Meilleure expérience utilisateur pour les applications à forte bande passante
- Économies sur la capacité de retour

Scénario 2 : Routage vers le Réseau Domicile (Tunnel GTP)



Avantages :

- Application cohérente des politiques
- Facturation/chargement centralisés
- Politiques de sécurité/VPN d'entreprise appliquées
- Mobilité transparente entre WiFi et cellulaire

Options de Connexion SWx

Option 1 : Connexion Directe au HSS

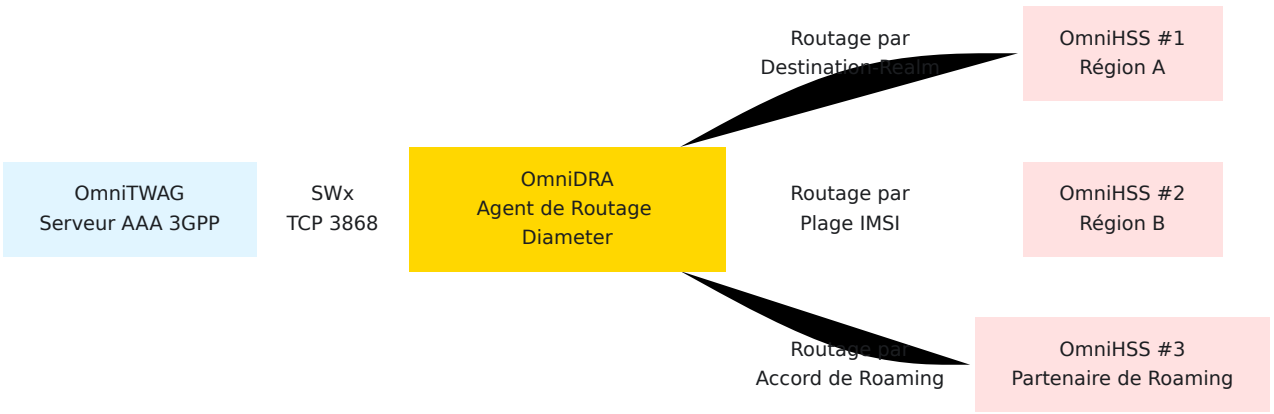
OmniTWAG Serveur AAA 3GPP	SWx Direct TCP 3868 MAR/MAA	OmniHSS Base de Données des Abonnés

Cas d'Utilisation : Déploiements simples, environnements de laboratoire, HSS unique

Avantages :

- Latence plus faible (pas de saut via DRA)
- Configuration simplifiée
- Dépannage plus facile

Option 2 : Via DRA (Agent de Routage Diameter)



Cas d'Utilisation : Déploiements multi-HSS, scénarios de roaming, réseaux à grande échelle

Avantages :

- Logique de routage centralisée
- Équilibrage de charge entre plusieurs HSS
- Support de roaming (routes vers le HSS domicile)
- Redondance et basculement
- Adhérence aux sessions

Flux de Facturation

Le TWAG peut être entièrement intégré pour envoyer des demandes de facturation en ligne basées sur Diameter `Gy` à un Système de Facturation en Ligne (OCS).

Cela permet de comptabiliser toutes les données consommées sur WiFi, par rapport au solde du client, et est livré via l'AP sur RADIUS et converti en `Gy` par le TWAG et transmis au DRA/OCS.

Dans tous les modes, l'utilisation est suivie par les métriques du TWAG.

Modes de Facturation

Le TWAG prend en charge trois modes de facturation en ligne :

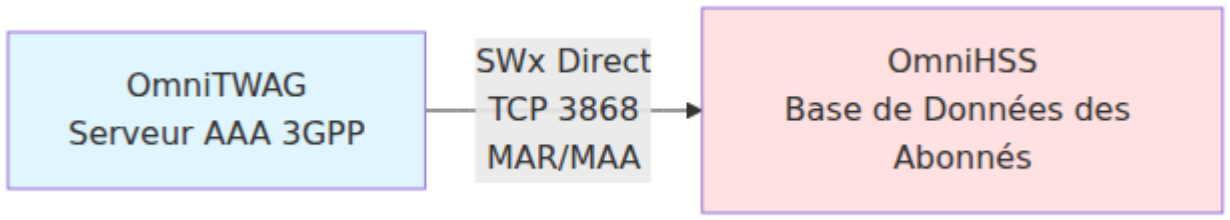
1. Facturation Désactivée

Aucune demande de contrôle de crédit n'est envoyée. Aucune autorisation de solde n'est effectuée.

Cas d'Utilisation :

- Réseaux WiFi ouverts/gratuits
- Environnements de laboratoire/test
- Réseaux avec facturation hors ligne uniquement (comptabilité RADIUS à la facturation)

Flux :



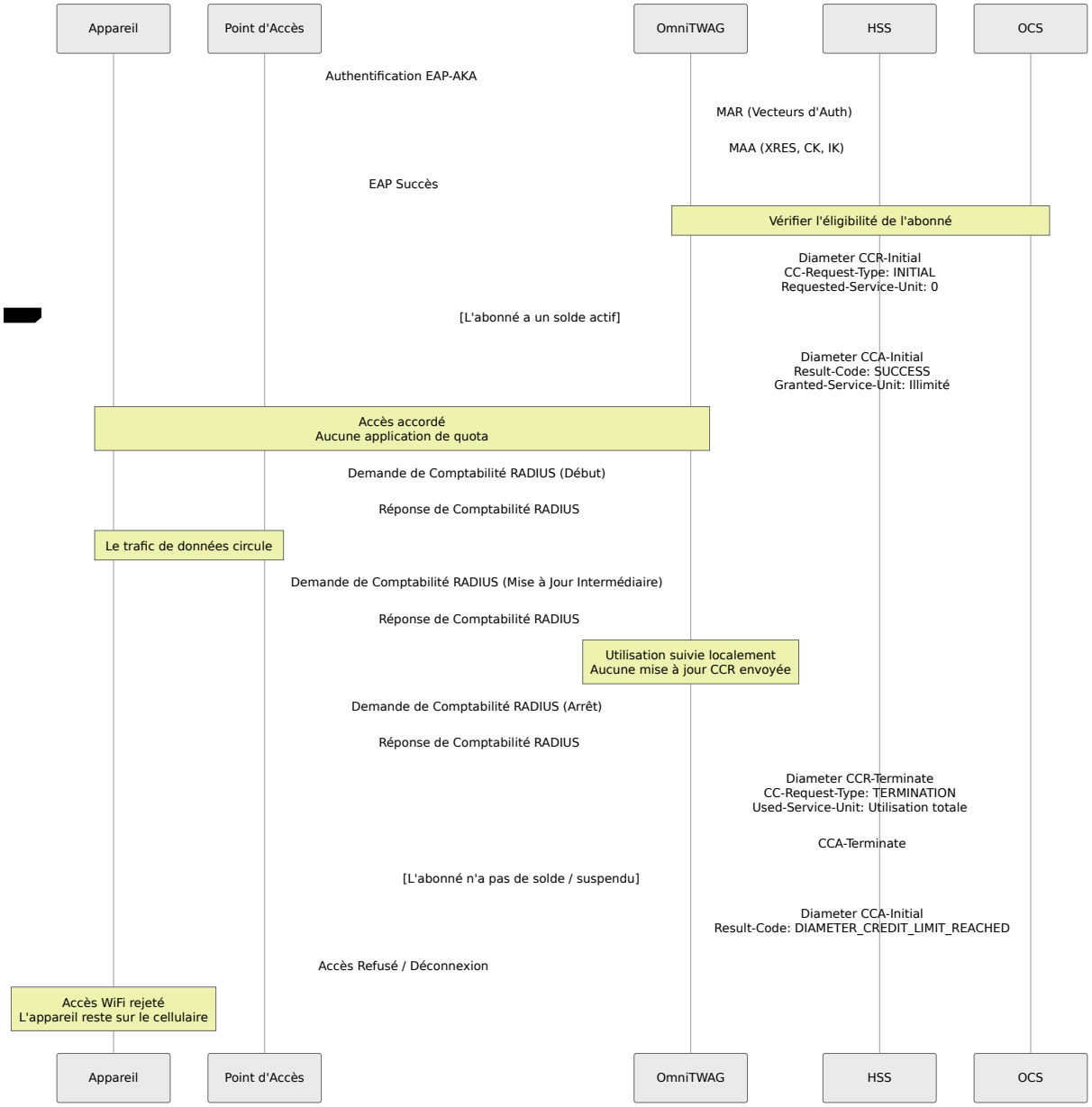
2. Autorisation Seulement

Une CCR-Initial (Demande de Contrôle de Crédit) est envoyée à l'OCS au début de la session WiFi pour valider que l'abonné a un solde, mais le solde n'est pas diminué pendant la session.

Cas d'Utilisation :

- Valider que l'abonné a un compte/solde actif
- Empêcher l'accès WiFi pour les comptes suspendus
- Vérifier l'éligibilité au service sans suivi de quota
- Autoriser le WiFi comme service bonus/illimité pour les clients payants

Flux :



Configuration :

- L'OCS est interrogé au début de la session (CCR-I) et à la fin (CCR-T)
- Aucun message CCR-Update envoyé pendant la session

- Abonné autorisé en fonction de l'état du compte, pas du quota
- Utilisation rapportée à la fin de la session à des fins d'information uniquement

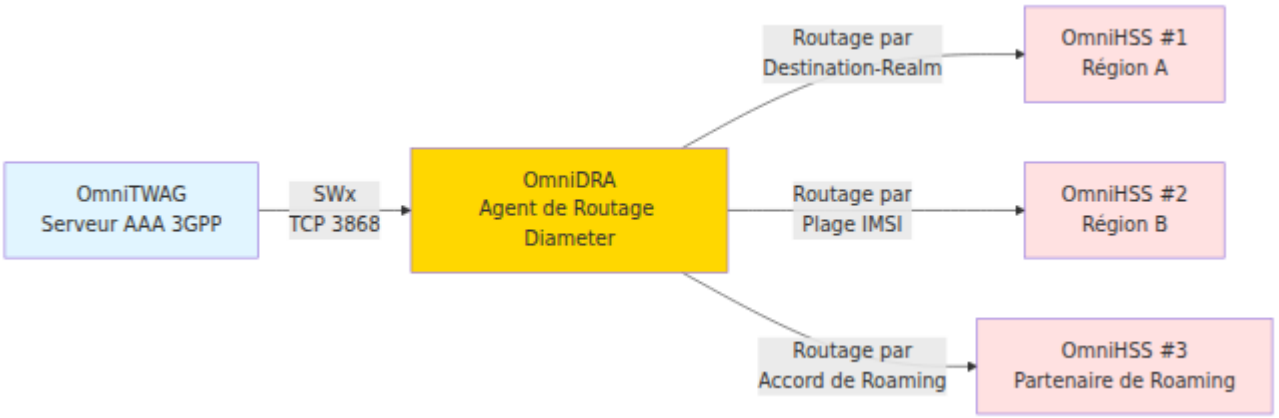
3. Facturation en Ligne Gy Complète (Implémentation Complète)

Le flux de facturation en ligne standard 3GPP est suivi. Toute utilisation sur WiFi est transmise à l'OCS pour facturation, l'abonné étant coupé une fois qu'il a dépassé son quota.

Cas d'Utilisation :

- Services de données prépayés
- WiFi à la demande
- Plans basés sur un quota (par exemple, 10 Go d'allocation mensuelle)
- Facturation et coupure en temps réel

Flux :



Configuration :

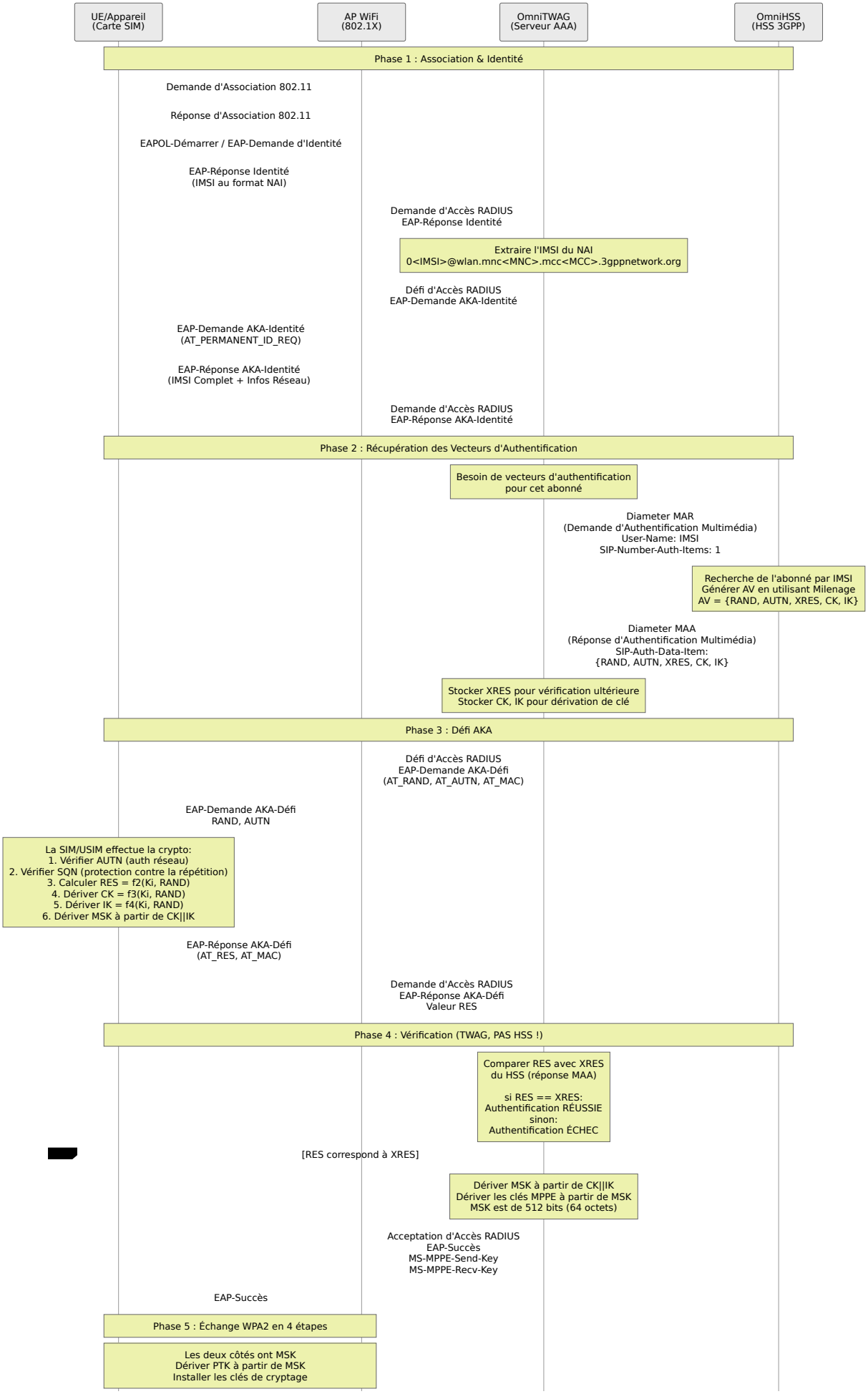
- OCS interrogé au début de la session (CCR-I), pendant la session (CCR-U), et à la fin (CCR-T)
- Quota demandé en morceaux configurables (par exemple, 10MB, 50MB, 100MB)
- CCR-Update déclenché à un seuil configurable (par exemple, 80% du quota accordé)
- Le minuteur de validité déclenche une ré-authentification si le quota n'est pas épuisé

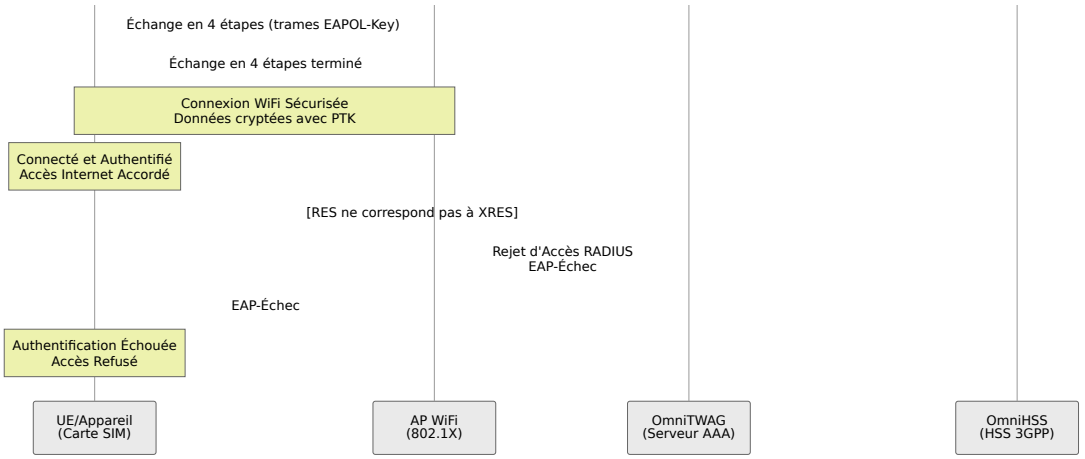
- Déconnexion forcée lorsque le quota est épuisé
- Déduction du solde en temps réel

Flux d'Authentification

Séquence Complète d'Authentification EAP-

AKA


UE/Appareil
(Carte SIM)
AP WiFi
(802.1X)
OmniTWAG
(Serveur AAA)
OmniHSS
(HSS 3GPP)
Phase 1 : Association & Identité
Demande d'Association 802.11
Réponse d'Association 802.11
EAPOL-Démarrer / EAP-Demande d'Identité
EAP-Réponse Identité
(IMSI au format NAI)
Demande d'Accès RADIUS
EAP-Réponse Identité
Extraire l'IMSI du NAI
0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org
Défi d'Accès RADIUS
EAP-Demande AKA-Identité
EAP-Demande AKA-Identité
(AT_PERMANENT_ID_REQ)
EAP-Réponse AKA-Identité
(IMSI Complet + Infos Réseau)
Demande d'Accès RADIUS
EAP-Réponse AKA-Identité
Phase 2 : Récupération des Vecteurs d'Authentification
Besoin de vecteurs d'authentification
pour cet abonné
Diameter MAR
(Demande d'Authentification Multimédia)
User-Name: IMSI
SIP-Number-Auth-Items: 1
Recherche de l'abonné par IMSI
Générer AV en utilisant Milenage
AV = {RAND, AUTN, XRES, CK, IK}
Diameter MAA
(Réponse d'Authentification Multimédia)
SIP-Auth-Data-Item:
{RAND, AUTN, XRES, CK, IK}
Stocker XRES pour vérification ultérieure
Stocker CK, IK pour dérivation de clé
Phase 3 : Défi AKA
Défi d'Accès RADIUS
EAP-Demande AKA-Défi
(AT_RAND, AT_AUTN, AT_MAC)
EAP-Demande AKA-Défi
RAND, AUTN
La SIM/USIM effectue la crypto:
1. Vérifier AUTN (auth réseau)
2. Vérifier SQN (protection contre la répétition)
3. Calculer RES = f2(Ki, RAND)
4. Dériver CK = f3(Ki, RAND)
5. Dériver IK = f4(Ki, RAND)
6. Dériver MSK à partir de CK||IK
EAP-Réponse AKA-Défi
(AT_RES, AT_MAC)
Demande d'Accès RADIUS
EAP-Réponse AKA-Défi
Valeur RES
Phase 4 : Vérification (TWAG, PAS HSS !)
Comparer RES avec XRES
du HSS (réponse MAA)
si RES == XRES:
Authentification RÉUSSIE
sinon:
Authentification ÉCHEC
[RES correspond à XRES]
Dériver MSK à partir de CK||IK
Dériver les clés MPPE à partir de MSK
MSK est de 512 bits (64 octets)
Acceptation d'Accès RADIUS
EAP-Succès
MS-MPPE-Send-Key
MS-MPPE-Recv-Key
EAP-Succès
Phase 5 : Échange WPA2 en 4 étapes
Les deux côtés ont MSK
Dériver PTK à partir de MSK
Installer les clés de cryptage



Points Clés dans le Flux d'Authentification

1. **MAR/MAA est la fin de la communication HSS** : Après avoir reçu le MAA (Réponse d'Authentification Multimédia) avec XRES, le TWAG gère toutes les vérifications suivantes localement.

2. **TWAG effectue la vérification RES** : Le HSS fournit la réponse attendue (XRES), mais le TWAG la compare à la RES réelle de l'UE. Le HSS n'est PAS impliqué dans cette comparaison.

3. **L'authentification se produit au TWAG** : Cela diffère de certains diagrammes qui montrent le HSS effectuant la vérification - dans l'architecture 3GPP réelle, le serveur AAA (TWAG) effectue la comparaison.

Format d'Identité

L'appareil répond avec son identité permanente (IMSI) au format NAI :

```
505570000000000001@wlan.mnc057.mcc505.3gppnetwork.org
```

Format : `0<IMSI>@wlan.mnc<MNC>.mcc<MCC>.3gppnetwork.org`

Note - Le premier chiffre, avant l'IMSI est l'identité, cela est généralement 0 mais peut être un autre chiffre unique pour les SIMs / appareils multi-IMSI.

Clé de Session Maître (MSK)

La Clé de Session Maître (MSK) est une clé cryptographique de 512 bits (64 octets) dérivée lors de l'authentification EAP-AKA. Elle sert de matériel clé racine pour sécuriser la connexion WiFi.

Dérivation de MSK :

1. À la fois l'UE et le TWAG dérivent indépendamment la même MSK
2. L'UE dérive de CK/IK calculé par la SIM
3. Le TWAG dérive de CK/IK reçu du HSS
4. MSK = PRF'(CK || IK, "Full Authentication", IMSI, ...)

Utilisation de MSK :

1. **Dérivation de PMK** : PMK = les premiers 256 bits (32 octets) de MSK
2. **Échange WPA2 en 4 étapes** : À la fois l'UE et l'AP utilisent PMK pour dériver PTK
3. **Cryptage des Données** : Tous les trames de données WiFi sont cryptées avec la Clé Temporelle (TK) dérivée de PTK

Pourquoi MSK est Critique :

- **Confidentialité** : Sans MSK, le trafic WiFi serait non crypté
- **Intégrité** : Empêche la falsification des trames WiFi
- **Liaison d'Authentification** : Lie l'authentification EAP à la cryptographie WiFi
- **Protection contre la Répétition** : Une MSK fraîche empêche les attaques par répétition
- **Confidentialité Avancée** : La compromission d'une MSK n'affecte pas les autres

Récupération de Resynchronisation

Si l'appareil détecte un décalage de numéro de séquence (SQN hors synchronisation), il initie une resynchronisation :

1. L'appareil calcule AUTS (Token d'Authentification - Synchronisation)

2. Envoie EAP-AKA Synchronization-Failure avec AT-AUTS
3. TWAG transmet AUTS au HSS
4. HSS resynchronise le numéro de séquence et génère de nouveaux vecteurs
5. L'authentification est réessayée avec de nouveaux vecteurs

Cela est transparent pour l'utilisateur final et ne nécessite aucune intervention de l'opérateur.

Guide de Configuration

Le TWAG est configuré via des fichiers de configuration Elixir dans le répertoire `config/`. La configuration principale à l'exécution se trouve dans `config/runtime.exs`.

Pour les déploiements en production, la configuration est gérée de manière centralisée. Ce qui suit est une référence uniquement, toute valeur modifiée sur un nœud de production sera perdue lors de la prochaine exécution de l'orchestration automatisée.

Configuration Diameter

Située dans `config :diameter_ex` :

```
config :diameter_ex,
  diameter: %{
    # Nom du service pour la pile Diameter
    service_name: :omnitouch_twag,

    # Adresse IP locale pour lier le service Diameter
    listen_ip: "10.5.198.200",

    # Port local pour les connexions Diameter (standard est 3868)
    listen_port: 3868,

    # Host d'Origine Diameter
    host: "omnitwag",

    # Realm d'Origine Diameter (correspond à votre domaine réseau)
    realm: "epc.mnc057.mcc505.3gppnetwork.org",

    # Pairs Diameter (HSS, DRA, serveurs AAA)
    peers: [
      %{
        # Host d'Origine Diameter du Pair
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

        # Realm d'Origine Diameter du Pair
        realm: "epc.mnc057.mcc505.3gppnetwork.org",

        # Adresse IP du Pair (peut être HSS directement ou DRA)
        ip: "10.179.2.140",

        # Port du Pair (standard est 3868)
        port: 3868,

        # Utiliser TLS pour la sécurité du transport
        tls: false,

        # Protocole de transport (:diameter_tcp ou :diameter_sctp)
        transport: :diameter_tcp,

        # Initier la connexion au pair (true) ou attendre que le
pair se connecte (false)
        initiate_connection: true
      }
```

```
    ]
  }
```

Format de Realm suit 3GPP TS 23.003 :

```
epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

Où :

- MNC = Code de Réseau Mobile (par exemple, 057)
- MCC = Code de Pays Mobile (par exemple, 505 pour l'Australie)

Remarque sur l'Utilisation de DRA : Pour utiliser OmniDRA, configurez l'adresse IP du pair pour pointer vers le DRA au lieu de directement vers le HSS. Le DRA acheminera ensuite les messages vers le HSS approprié en fonction des règles de routage (Destination-Realm, plage IMSI, etc.).

Configuration RADIUS

Située dans `config :omnitwag` :

```
config :omnitwag,
  radius_config: %{
    # Liste des sous-réseaux IP sources autorisées pour les
clients RADIUS
    # Liste vide = autoriser tout (non recommandé pour la
production)
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],

    # Secret partagé pour les clients RADIUS
    # Tous les AP doivent utiliser ce secret
    secret: "YOUR_STRONG_SECRET_HERE"
  }
```

Meilleures Pratiques de Sécurité :

- Utiliser des secrets partagés RADIUS forts (20+ caractères)
- Configurer `allowed_source_subnets` pour restreindre l'accès des AP
- Utiliser des règles de pare-feu pour restreindre davantage l'accès aux ports 1812/1813

Exemple de configuration de sous-réseau :

```
allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"]
```

Si vide, toutes les sources sont autorisées (uniquement adapté pour le laboratoire/test).

Configuration de Surveillance Prometheus

Située dans `config :omnitwag` :

```
config :omnitwag,
  prometheus: %{
    # Port pour le point de terminaison des métriques Prometheus
    port: 9568
  }
```

Accédez aux métriques à : `http://<twag-ip>:9568/metrics`

Résumé des Ports

Port	Protocole	But
1812	UDP	Authentification RADIUS
1813	UDP	Comptabilité RADIUS
3868	TCP	Diameter (SWx vers HSS/DRA)
443	TCP	Tableau de Bord Web HTTPS
8444	TCP	API REST HTTPS
9568	TCP	Métriques Prometheus

Configuration du Point d'Accès

Points d'Accès Supportés

OmniTWAG fonctionne avec n'importe quel AP WiFi qui prend en charge :

- **WPA2-Enterprise** (authentification 802.1X)
- Fonctionnalité **client RADIUS**
- Méthode d'authentification **EAP-AKA**

Plateformes testées : Cisco Aironet, Aruba, Ubiquiti UniFi, Ruckus, APs basés sur hostapd

Exigences Générales de Configuration des AP

1. Mode de sécurité **WPA2-Enterprise (802.1X)**
2. **Serveur RADIUS** pointant vers l'adresse IP du TWAG
3. **Port d'authentification RADIUS** : 1812
4. **Port de comptabilité RADIUS** : 1813 (optionnel mais recommandé)
5. **Secret partagé RADIUS** : Doit correspondre à la configuration du TWAG
6. **Méthode EAP** : EAP-AKA (ou "Tous")

Exemple de Configuration d'AP Cisco

Configuration CLI :

```
! Configurer le serveur RADIUS
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key
YOUR_SHARED_SECRET

! Configurer SSID avec 802.1X
dot11 ssid OPERATOR-WIFI
   vlan 10
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2

! Associer SSID avec l'interface radio
interface Dot11Radio0
   encryption mode ciphers aes-ccm
   ssid OPERATOR-WIFI
```

Interface Web :

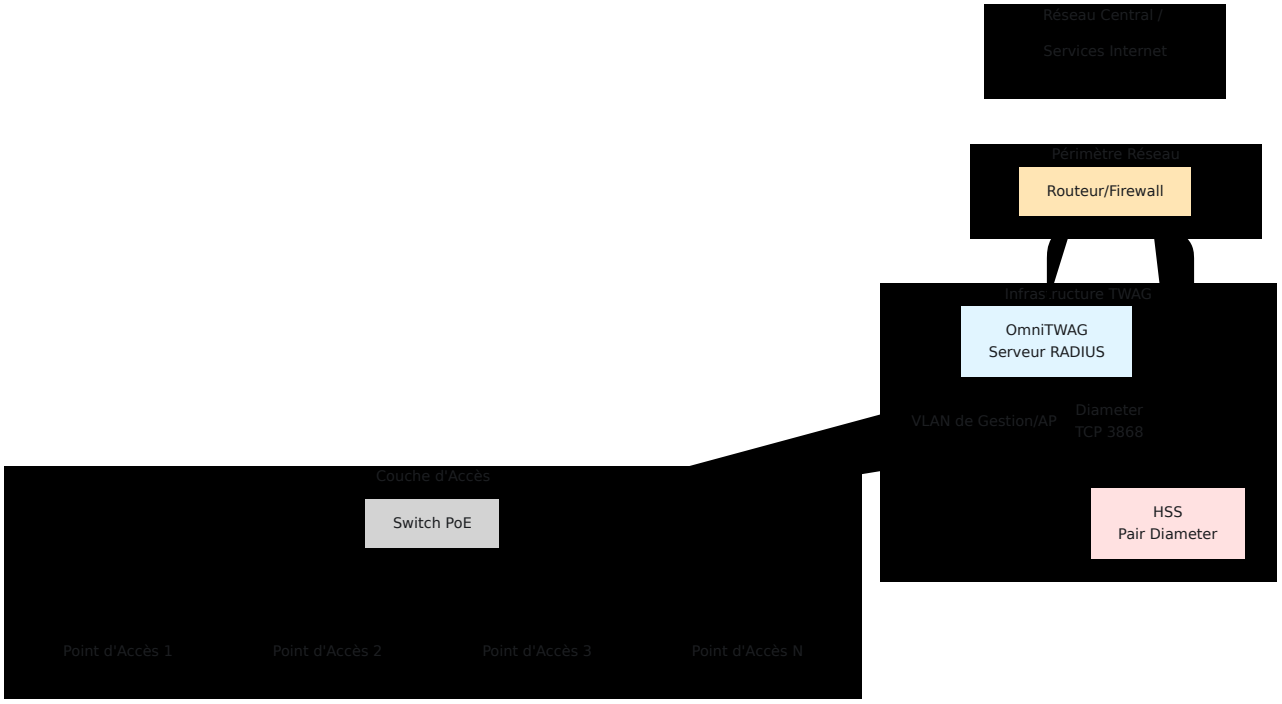
1. Naviguer vers **Sécurité → AAA → Serveur RADIUS**
2. Ajouter le serveur RADIUS : `10.5.198.200:1812` avec le secret partagé
3. Naviguer vers la configuration **WLAN**
4. Définir la Sécurité sur **WPA2-Enterprise**
5. Définir la méthode EAP sur **EAP-AKA** ou **Tous**
6. Assigner le groupe de serveur RADIUS

Exemple de Configuration hostapd

Pour les AP basés sur Linux (OpenWrt, systèmes embarqués) :

```
# /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
ssid=OPERATOR-WIFI

# WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
wpa_pairwise=CCMP
ieee8021x=1

# Configuration RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# Configuration EAP
eap_server=0

# Hotspot 2.0 (Optionnel - pour déchargement automatique)
interworking=1
internet=1
anqp_3gpp_cell_net=505,057
domain_name=wlan.mnc057.mcc505.3gppnetwork.org
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
roaming_consortium=505057
hs20=1
```

Meilleures Pratiques d'Architecture Réseau



Important : Placez les AP et le TWAG sur des segments de réseau de confiance. Utilisez des règles de pare-feu pour :

- Autoriser uniquement les AP à atteindre les ports 1812/1813 du TWAG
- Autoriser le TWAG à atteindre le port 3868 du HSS
- Restreindre l'accès de gestion au tableau de bord du TWAG (port 443)

Intégration Hotspot 2.0

Vue d'Ensemble de Hotspot 2.0 (Passpoint)

Hotspot 2.0 (également appelé Passpoint ou 802.11u) est une norme de la WiFi Alliance qui permet la découverte et la connexion automatique et sécurisée aux réseaux WiFi sans interaction de l'utilisateur. C'est la technologie clé pour un déchargement WiFi sans couture.

Caractéristiques Clés :

- **Découverte Automatique de Réseau** : L'appareil trouve des réseaux compatibles en fonction de critères

- **Authentification Automatique** : Utilise les identifiants SIM (EAP-AKA) sans saisie de l'utilisateur
- **Association Initiale Cryptée** : OSEN (Authentification uniquement par Serveur OSU) pour un provisionnement sécurisé
- **Accords de Roaming** : Supporte les réseaux visités (comme le roaming cellulaire)
- **Priorisation** : L'appareil préfère les réseaux appartenant à l'opérateur

Configuration AP Hotspot 2.0

Exigences pour l'AP :

1. **Support 802.11u** : Capacité de requête/réponse ANQP
2. **WPA2-Enterprise** : Authentification 802.1X
3. **Support EAP-AKA** : Doit prendre en charge la méthode EAP-AKA
4. **Configuration ANQP** : Annoncez les bonnes informations de l'opérateur

Exemple de Configuration (AP basé sur hostapd) :

```
# Configuration Hotspot 2.0 / Passpoint
interworking=1
internet=1
asra=0
esr=0
uesa=0

# Configuration ANQP
anqp_3gpp_cell_net=505,057
domain_name=omnitouchns.com,wlan.mnc057.mcc505.3gppnetwork.org

# Configuration de Realm NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# Format : <encodage>,<realm>,<méthode-eap>[auth-id:auth-val]
# 21 = EAP-AKA
# 2:1 = Type d'identifiant : SIM
# 5:7 = Méthode EAP Tunnelée : Aucune (EAP-AKA direct)

# Consortium de Roaming
roaming_consortium=505057
# MCC=505 (USA), MNC=057 (spécifique à l'opérateur)

# Informations sur le Lieu (optionnel)
venue_group=1
venue_type=8
venue_name=eng:Opérateur Public WiFi

# Configuration WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
rsn_pairwise=CCMP
ieee8021x=1

# Configuration RADIUS (pointe vers OmniTWAG)
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# Configuration SSID
```

```
ssid=OperatorWiFi
utf8_ssid=1

# Indication Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:Réseau WiFi de l'Opérateur
```

Comportement de Déchargement Automatique

Comment Fonctionne le Déchargement Automatique :

1. L'appareil avec un profil Passpoint effectue une analyse WiFi périodique
2. Envoie une requête ANQP aux AP détectés
3. Si la réponse ANQP correspond au profil (MCC/MNC, consortium de roaming) :
   - Priorité est ÉLEVÉE (réseau domicile) ou MOYENNE (partenaire de roaming)
4. Si la priorité ≥ seuil et le signal > minimum :
   - Authentification automatique EAP-AKA
5. Si l'authentification réussie et la priorité > connexion actuelle :
   - Passer au WiFi, déconnecter les données cellulaires
6. Surveiller la qualité du signal et maintenir la connectivité

Facteurs de Priorité :

1. **Domicile vs. Roaming** : Réseau domicile (correspondance MCC/MNC) préféré au roaming
2. **Force du Signal** : Signal plus fort préféré
3. **Sécurité** : WPA2-Enterprise préféré au WiFi ouvert/WPA2-PSK
4. **Politique** : L'opérateur peut configurer les réseaux préférés
5. **Surcharge Utilisateur** : L'utilisateur peut désactiver manuellement le WiFi ou préférer le cellulaire

---

Surveillance et Gestion

Tableau de Bord Web

Accédez au tableau de bord de surveillance en temps réel à : `https://<twag-ip>/`

Fonctionnalités :

- **Vue des Clients RADIUS** : Abonnés actifs, statut d'authentification, détails de session
- **Vue des Points d'Accès** : AP connectés, comptes clients, informations SSID
- **Vue de l'Utilisation des Clients** : Données de comptabilité, temps de session, utilisation des données
- **Vue des Pairs Diameter** : Statut de connexion HSS/DRA

Intégration Prometheus

Configurez Prometheus pour extraire les métriques du TWAG :

```
# prometheus.yml
scrape_configs:
  - job_name: 'omnitwag'
    static_configs:
      - targets: ['10.5.198.200:9568']
    metrics_path: '/metrics'
    scrape_interval: 15s
```

Métriques Disponibles :

Métriques du Serveur RADIUS :

- `radius_access_request_count` - Total des paquets RADIUS Access-Request reçus
- `radius_access_accept_count` - Total des paquets Access-Accept envoyés
- `radius_access_reject_count` - Total des paquets Access-Reject envoyés

- `radius_access_challenge_count` - Total des paquets Access-Challenge envoyés
- `radius_accounting_request_count{status_type}` - Total des paquets Accounting-Request (tagués par statut : start, stop, interim_update, accounting_on, accounting_off)
- `radius_active_clients_count` - Clients actuellement authentifiés (poll tous les 5 secondes)
- `radius_access_points_count` - Points d'accès enregistrés (poll tous les 5 secondes)

Métriques d'Authentification EAP-AKA :

- `eap_aka_identity_count` - Échanges d'identité EAP-AKA
- `eap_aka_challenge_count` - Échanges de défi EAP-AKA
- `eap_aka_sync_failure_count` - Échecs de synchronisation (événements de resynchronisation SQN)
- `eap_aka_auth_success_count` - Authentifications réussies
- `eap_aka_auth_reject_count` - Authentifications rejetées

Métriques du Protocole Diameter :

- `diameter_message_count{application, command, direction}` - Total des messages Diameter (tagués par application, type de commande, et direction)

Métriques de Mémoire de la VM Erlang :

- `vm_memory_total` - Total de la mémoire allouée (octets)
- `vm_memory_processes` - Mémoire utilisée par les processus Erlang (octets)
- `vm_memory_processes_used` - Mémoire utilisée par les processus Erlang excluant la mémoire allouée inutilisée (octets)
- `vm_memory_system` - Mémoire utilisée par le système d'exécution Erlang (octets)
- `vm_memory_atom` - Mémoire utilisée par les atomes (octets)
- `vm_memory_atom_used` - Mémoire utilisée par les atomes excluant la mémoire allouée inutilisée (octets)
- `vm_memory_binary` - Mémoire utilisée par les binaires (octets)

- `vm_memory_code` - Mémoire utilisée par le code chargé (octets)
- `vm_memory_ets` - Mémoire utilisée par les tables ETS (octets)

Métriques Système de la VM Erlang :

- `vm_system_info_process_count` - Nombre actuel de processus Erlang
- `vm_system_info_port_count` - Nombre actuel de ports
- `vm_system_info_atom_count` - Nombre actuel d'atomes
- `vm_system_info_schedulers` - Nombre de threads de planificateur
- `vm_system_info_schedulers_online` - Nombre de planificateurs actuellement en ligne

Métriques de Planificateur de la VM Erlang :

- `vm_statistics_run_queue` - Longueur totale de toutes les files d'attente d'exécution
- `vm_total_run_queue_lengths_total` - Longueur totale de toutes les files d'attente d'exécution (tous les planificateurs)
- `vm_total_run_queue_lengths_cpu` - Longueur totale des files d'attente d'exécution des planificateurs CPU
- `vm_total_run_queue_lengths_io` - Longueur totale des files d'attente d'exécution des planificateurs IO

Collecte de Métriques :

- Les métriques RADIUS et EAP-AKA sont émises en temps réel au fur et à mesure des événements
- Les comptes de clients actifs et de points d'accès sont pollés toutes les 5 secondes
- Les métriques de la VM sont pollées toutes les 5 secondes depuis l'exécution Erlang
- Toutes les métriques sont exposées au format Prometheus à `http://<twag-ip>:9568/metrics`

Journalisation

Le TWAG utilise le Logger d'Elixir pour la journalisation structurée.

Voir les Journaux (systemd) :

```
# Journal en temps réel
journalctl -u twag -f

# Dernières 100 lignes
journalctl -u twag -n 100

# Journaux depuis le dernier démarrage
journalctl -u twag -b

# Journaux pour une plage horaire spécifique
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-
12 11:00:00"
```

Messages Clés dans les Journaux :

- `Serveur RADIUS écoutant sur le port 1812` - Serveur démarré
- `De {IP} : Demande d'Accès reçue` - Demande RADIUS de l'AP
- `Phase 1 : Réponse d'Identité` - Identité EAP initiale
- `Phase 2 : Défi AKA` - Défi envoyé à l'appareil
- `Authentification ACCEPTÉE` - Authentification réussie
- `Authentification REJETÉE` - Authentification échouée
- `AP Enregistré : {IP}` - Nouvel AP détecté

Dépannage

Échecs d'Authentification

Symptôme : Le client ne peut pas se connecter au WiFi

Étapes de Diagnostic :

1. Vérifiez les journaux du TWAG : `journalctl -u twag -f`
2. Vérifiez que le secret partagé RADIUS correspond entre l'AP et le TWAG

3. Confirmez que les paquets RADIUS atteignent le TWAG : `tcpdump -i eth0 port 1812`
4. Vérifiez le provisionnement de l'abonné dans le HSS/configuration

Causes Courantes :

- Secret partagé RADIUS incorrect
- Pare-feu bloquant UDP 1812/1813
- Mismatch RES/XRES (mauvais Ki SIM ou configuration HSS)
- Numéro de séquence (SQN) hors synchronisation (devrait se rétablir automatiquement via resync)
- Problèmes de connectivité réseau entre l'AP et le TWAG

Problèmes de Connexion Diameter

Symptôme : Pair Diameter ne se connecte pas au HSS/DRA

Étapes de Diagnostic :

1. Vérifiez la connectivité réseau : `telnet <hss-ip> 3868`
2. Vérifiez la configuration Diameter (Host d'Origine, Realm d'Origine, IP du pair)
3. Consultez les journaux HSS/DRA pour les tentatives de connexion
4. Vérifiez que le pare-feu autorise TCP 3868

Causes Courantes :

- IP/port de pair incorrect dans la configuration
- Pare-feu bloquant TCP 3868
- Mismatch Host/Realm d'Origine
- HSS/DRA n'acceptant pas la connexion du TWAG

Problèmes de Performance

Symptôme : Authentification lente (>5 secondes)

Étapes de Diagnostic :

1. Vérifiez le temps de réponse du HSS
2. Mesurez la latence réseau : `ping <hss-ip>`, `mtr <hss-ip>`
3. Surveillez l'utilisation des ressources du TWAG : `top`, `htop`
4. Consultez les paramètres de délai d'attente des demandes Diameter

Causes Courantes :

- Délai d'attente de requête HSS ou réponse lente
- Latence réseau élevée
- Épuisement des ressources du TWAG (CPU/mémoire)
- Trop d'authentifications concurrentes

Outils de Débogage

Capture de Paquet

```
# Capturer le trafic RADIUS
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# Capturer le trafic Diameter
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# Capturer depuis un AP spécifique
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-
ap1.pcap
```

Analysez avec Wireshark (prend en charge les dissectors RADIUS et Diameter).

Console Interactive

Attachez-vous au TWAG en cours d'exécution pour un débogage en direct :

```
# Shell distant vers le TWAG en cours d'exécution
iex --sname debug --remsh twag@hostname --cookie <cookie>
```

Depuis la console IEx :

```
# Lister tous les clients authentifiés
CryptoState.keys()

# Obtenir l'état d'un client spécifique
CryptoState.get("050533805790000186 7@wlan.mnc057.mcc505.3gppnetwork.o

# Lister tous les AP
APState.list()

# Lister les sessions de comptabilité
ClientUsage.list()
```

Messages d'Erreur Courants

Message d'Erreur	Signification	Solution
`Échec de validation de Message-Authenticator`	Mismatch de secret partagé	Vérifiez que le secret RADIUS correspond sur l'AP et le TWAG
`Échec de vérification RES : attendu <XRES>, obtenu <RES>`	Réponse d'authentification incorrecte	Vérifiez Ki SIM, vérifiez le provisionnement HSS
`Délai d'attente de connexion du pair Diameter`	Impossible d'atteindre le HSS	Vérifiez le réseau, le pare-feu, la configuration HSS
`Échec de décodage du message EAP`	Paquet EAP malformé	Vérifiez le firmware de l'AP, peut nécessiter une mise à jour de l'AP
`Sous-type EAP-AKA inconnu`	Message EAP-AKA non pris en charge	L'appareil utilise une variante EAP-AKA non standard
`Synchronisation du numéro de séquence requise`	SQN hors synchronisation	Normal, l'appareil se resynchronisera automatiquement

---

Conformité aux Normes

OmniTWAG met en œuvre les spécifications 3GPP et IETF suivantes :

- **3GPP TS 23.402** : Améliorations de l'architecture pour les accès non-3GPP
- **3GPP TS 24.302** : Accès à EPC via des réseaux d'accès non-3GPP

- **3GPP TS 29.273** : Interfaces SWx/SWm basées sur Diameter
- **3GPP TS 33.402** : Aspects de sécurité des accès non-3GPP
- **3GPP TS 35.206** : Spécification de l'algorithme Milenage
- **RFC 2865** : Authentification RADIUS
- **RFC 2866** : Comptabilité RADIUS
- **RFC 3579** : Support RADIUS pour EAP
- **RFC 4187** : Protocole d'authentification EAP-AKA
- **RFC 5448** : EAP-AKA' (version améliorée)

Résumé

OmniTWAG, créé par Omnitouch, fournit une solution complète et conforme aux normes pour le déchargement WiFi 3GPP :

1. **Déploiement Flexible** : Supporte le déchargement local ou le trafic routé vers le domicile
2. **Basé sur des Normes** : Met en œuvre les protocoles 3GPP SWx, EAP-AKA, RADIUS
3. **Authentification Sécurisée** : Authentification mutuelle basée sur la SIM avec resync automatique
4. **Cryptage Fort** : Les clés dérivées de MSK fournissent un cryptage WPA2
5. **Prêt pour Hotspot 2.0** : Permet un déchargement entièrement automatique et sans contact
6. **Contrôle de l'Opérateur** : Maintient l'identité, la politique, et éventuellement la facturation
7. **Connectivité Flexible** : Connexion directe au HSS ou via OmniDRA pour le routage/l'équilibrage de charge

---

Version du Document : 2.0 Dernière Mise à Jour : 2025 OmniTWAG - Passerelle d'Accès WiFi de Confiance