

# Guia de Operações e Implantação do OmniTWAG

Criado por **Omnitouch**

Este guia é para operadores de rede, administradores de sistema e clientes que estão implantando o OmniTWAG.

## Índice

1. [Introdução](#)
  2. [O que é WiFi Offload?](#)
  3. [Arquitetura de Implantação](#)
  4. [Fluxo de Cobrança](#)
  5. [Fluxo de Autenticação](#)
  6. [Guia de Configuração](#)
  7. [Configuração do Ponto de Acesso](#)
  8. [Integração Hotspot 2.0](#)
  9. [Monitoramento e Gestão](#)
  10. [Solução de Problemas](#)
  11. [Conformidade com Padrões](#)
- 

## Introdução

OmniTWAG (Trusted WiFi Access Gateway) é uma implementação compatível com padrões de um 3GPP TWAG que permite que operadores de rede móvel descarreguem com segurança o tráfego de assinantes de redes celulares para pontos de acesso WiFi, mantendo a autenticação segura baseada em SIM.

O TWAG autentica assinantes WiFi usando suas credenciais SIM via EAP-AKA (Extensible Authentication Protocol - Authentication and Key Agreement), o mesmo mecanismo de autenticação usado em redes celulares. Isso proporciona acesso WiFi seguro e contínuo para assinantes móveis sem a necessidade de senhas WiFi separadas.

## Principais Benefícios

### Para Usuários Finais:

- **Zero Configuração:** Funciona imediatamente com SIM compatível
- **Experiência Sem Costura:** Conexão automática como celular
- **Seguro:** Sempre usa WiFi criptografado (WPA2)
- **Sem Senhas:** Autenticação baseada em SIM

### Para Operadores Móveis:

- **Alívio da Capacidade da Rede:** Reduz a carga nas estações base celulares
- **Descarregamento Controlado:** Apenas assinantes autorizados podem se conectar
- **Melhoria na Experiência do Usuário:** WiFi geralmente oferece maior largura de banda
- **Eficiência de Custos:** A infraestrutura WiFi é menos cara do que a celular
- **Identidade Consistente:** Mesmo IMSI usado para WiFi e celular
- **Integração de Cobrança:** Pode cobrar pelo uso de WiFi, se desejado

### Para Locais/Empresas:

- **Segurança de Nível Operador:** Sem risco de compartilhamento de senhas
  - **Escalabilidade:** Suporta milhares de usuários sem provisionamento manual
  - **Gestão Simplificada:** Sem necessidade de distribuir senhas WiFi
-

# O que é WiFi Offload?

WiFi offload permite que operadores de rede móvel redirecionem o tráfego de dados dos assinantes de redes celulares congestionadas para redes WiFi.

## Como o TWAG Habilita o Descarregamento

O TWAG atua como o gateway de autenticação entre:

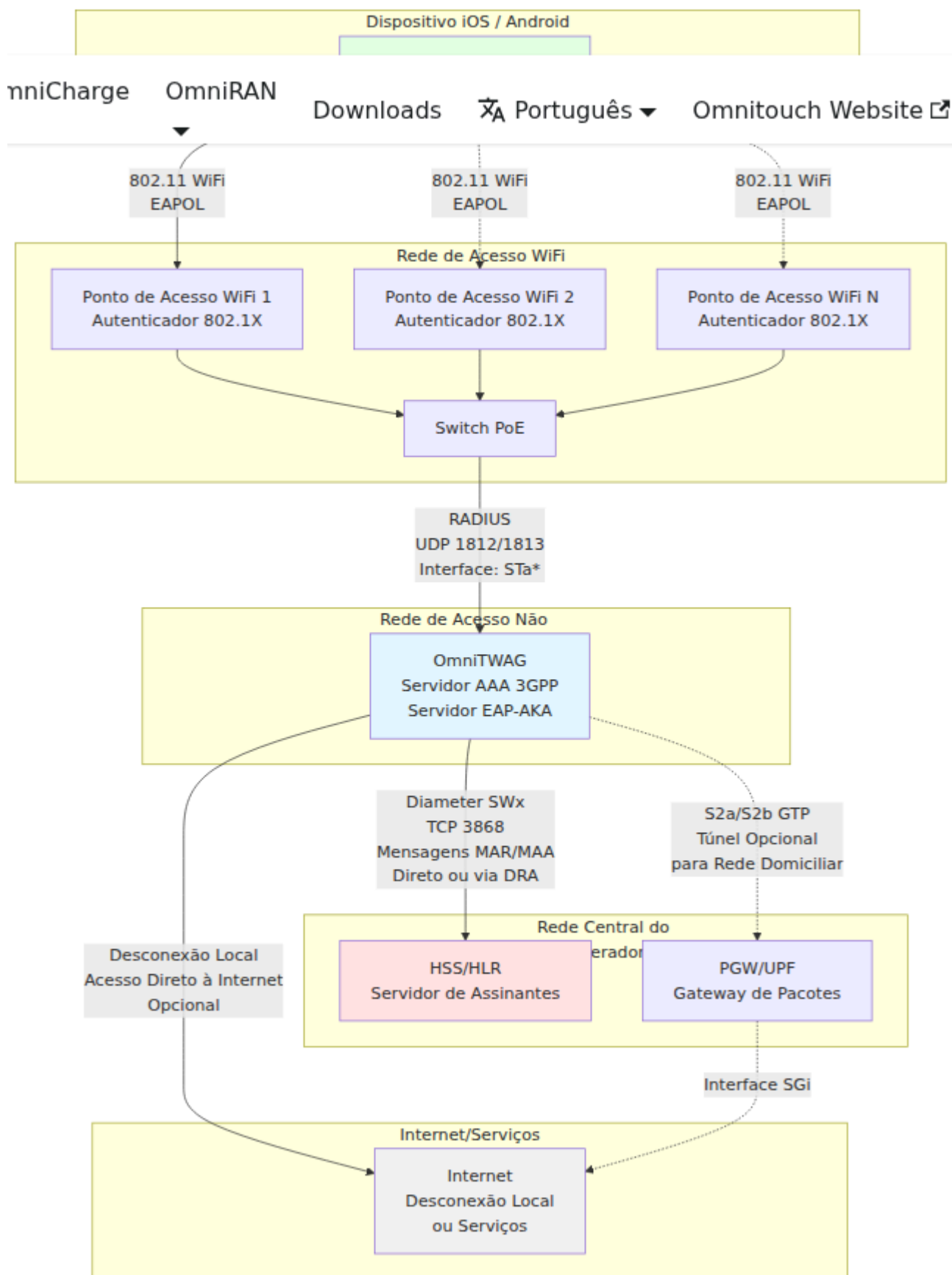
- **Pontos de Acesso WiFi** (via protocolo RADIUS)
- **Rede Central Móvel** HSS/HLR (via interface Diameter SWx)

Quando o dispositivo de um assinante se conecta a um AP WiFi configurado para descarregamento:

1. O dispositivo se identifica usando seu IMSI (do cartão SIM)
  2. O AP WiFi encaminha solicitações de autenticação para o TWAG via RADIUS
  3. O TWAG se comunica com o HSS do operador para recuperar vetores de autenticação
  4. A autenticação de desafio-resposta EAP-AKA ocorre entre o dispositivo e o TWAG
  5. Após a autenticação bem-sucedida, o dispositivo recebe acesso WiFi
  6. Opcionalmente, o tráfego pode ser encaminhado de volta para a rede central móvel ou ser desconectado localmente
-

# **Arquitetura de Implantação**

## **Topologia de Rede**

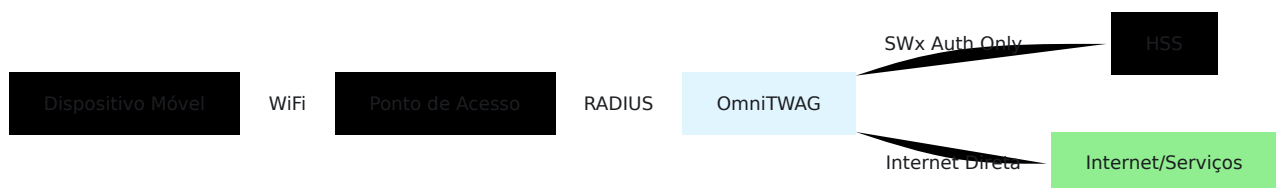


**Legenda de Interface:**

- **STa\***: Interface RADIUS/Diameter entre AP WiFi e TWAG (não 3GPP para AAA)
- **SWx**: Interface Diameter entre TWAG (Servidor AAA 3GPP) e HSS
- **S2a/S2b**: Interface de túnel GTP para retorno à rede doméstica (opcional)
- **SGi**: Interface para redes de dados de pacotes externas (Internet)
- **802.11**: Interface de rádio WiFi
- **EAPOL**: EAP sobre LAN (autenticação 802.1X)

## Cenários de Implantação

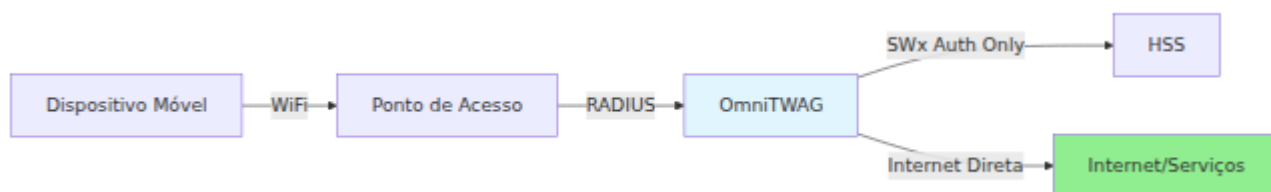
### Cenário 1: Desconexão Local (Recomendado para Desempenho)



#### Benefícios:

- Menor latência (sem retorno para o núcleo)
- Carga reduzida na rede central
- Melhor experiência do usuário para aplicações de alta largura de banda
- Economia de custos na capacidade de retorno

### Cenário 2: Roteamento da Rede Domiciliar (Túnel GTP)



## Benefícios:

- Aplicação consistente de políticas
- Cobrança/ faturamento centralizados
- Políticas de segurança/VPN corporativa aplicáveis
- Mobilidade contínua entre WiFi e celular

## Opções de Conexão SWx

### Opção 1: Conexão Direta ao HSS

OmniTWAG  
Servidor AAA 3GPP

SWx Direto  
TCP 3868  
MAR/MAA

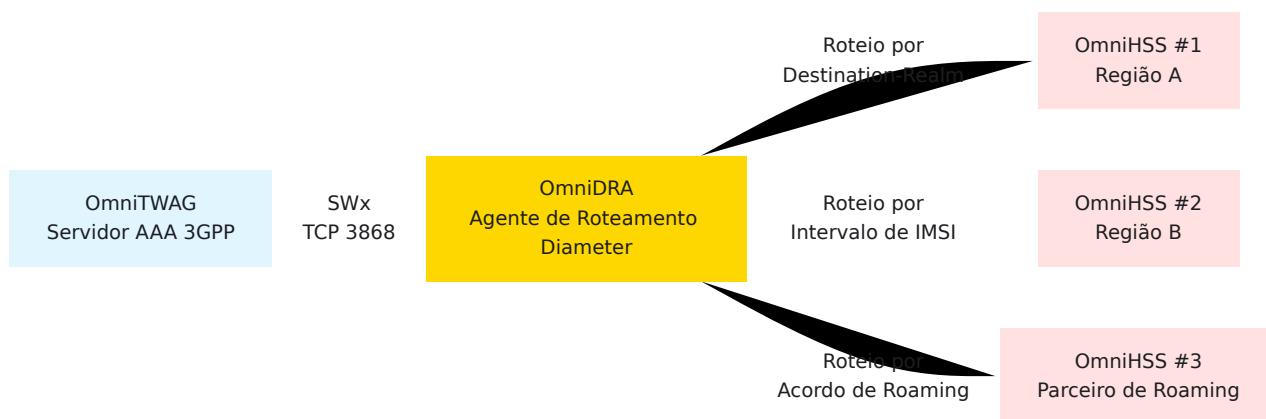
OmniHSS  
Banco de Dados de  
Assinantes

**Caso de Uso:** Implantações simples, ambientes de laboratório, único HSS

## Benefícios:

- Menor latência (sem salto através do DRA)
- Configuração simplificada
- Solução de problemas mais fácil

### Opção 2: Via DRA (Agente de Roteamento Diameter)



**Caso de Uso:** Implantações multi-HSS, cenários de roaming, redes de grande escala

### Benefícios:

- Lógica de roteamento centralizada
- Balanceamento de carga entre múltiplos HSS
- Suporte a roaming (roteia para HSS doméstico)
- Redundância e failover
- Persistência de sessão

---

## Fluxo de Cobrança

O TWAG pode ser totalmente integrado para enviar solicitações de cobrança online baseadas em Diameter Gy para um Sistema de Cobrança Online (OCS).

Isso permite a contabilidade de todos os dados consumidos no WiFi, em relação ao saldo do cliente, e é entregue via AP no RADIUS e convertido para Gy pelo TWAG e encaminhado para o DRA/OCS.

Em todos os modos, o uso é rastreado pelas métricas do TWAG.



## Modos de Cobrança

O TWAG suporta três modos de cobrança online:

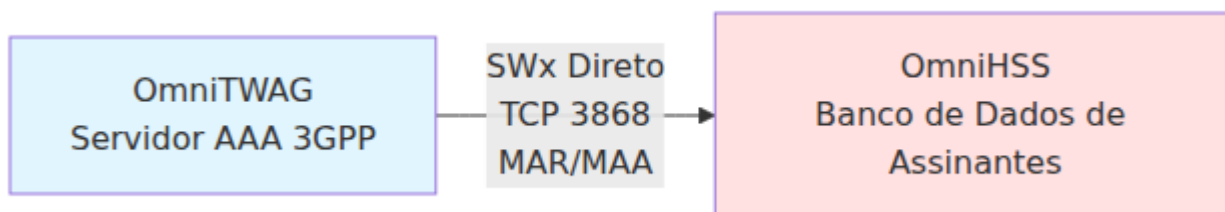
### 1. Cobrança Desativada

Nenhum pedido de controle de crédito é enviado. Nenhuma autorização de saldo é realizada.

#### Casos de Uso:

- Redes WiFi abertas/gratuitas
- Ambientes de laboratório/teste
- Redes com cobrança offline apenas (contabilidade RADIUS para faturamento)

#### Fluxo:



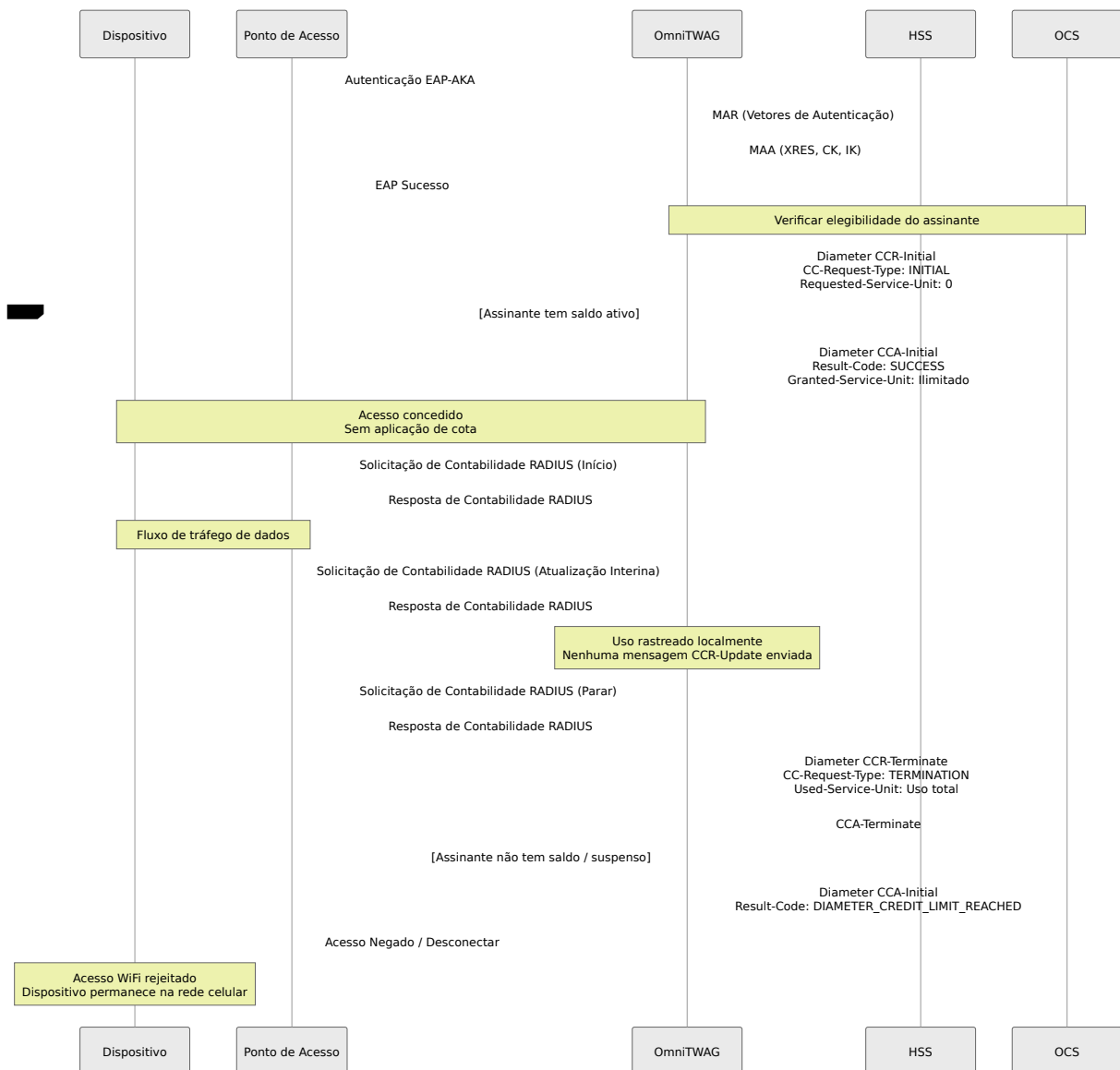
### 2. Apenas Autorização

Um CCR-Initial (Credit-Control-Request) é enviado para o OCS no início da sessão WiFi para validar se o assinante tem saldo, mas o saldo não é descontado durante a sessão.

## Casos de Uso:

- Validar se o assinante tem conta/saldo ativo
- Impedir acesso WiFi para contas suspensas
- Verificar elegibilidade de serviço sem rastreamento de cota
- Permitir WiFi como serviço bônus/ilimitado para clientes pagantes

## Fluxo:



## Configuração:

- OCS é consultado no início da sessão (CCR-I) e no final (CCR-T)
- Nenhuma mensagem CCR-Update enviada durante a sessão
- Assinante autorizado com base no status da conta, não na cota

- Uso relatado no final da sessão apenas para fins informativos

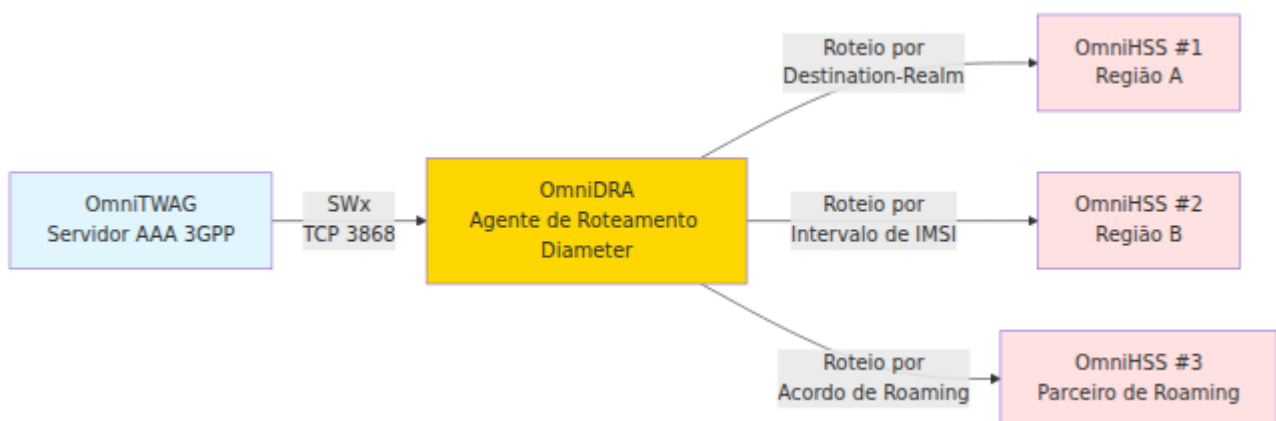
### 3. Cobrança Online Gy Completa (Implementação Completa)

O fluxo de cobrança online padrão 3GPP é seguido. Todo o uso no WiFi é passado para o OCS para cobrança, com o assinante sendo desconectado uma vez que excedeu sua cota.

#### Casos de Uso:

- Serviços de dados pré-pagos
- WiFi pago por uso
- Planos baseados em cota (ex: 10GB de limite mensal)
- Cobrança em tempo real e desconexão

#### Fluxo:

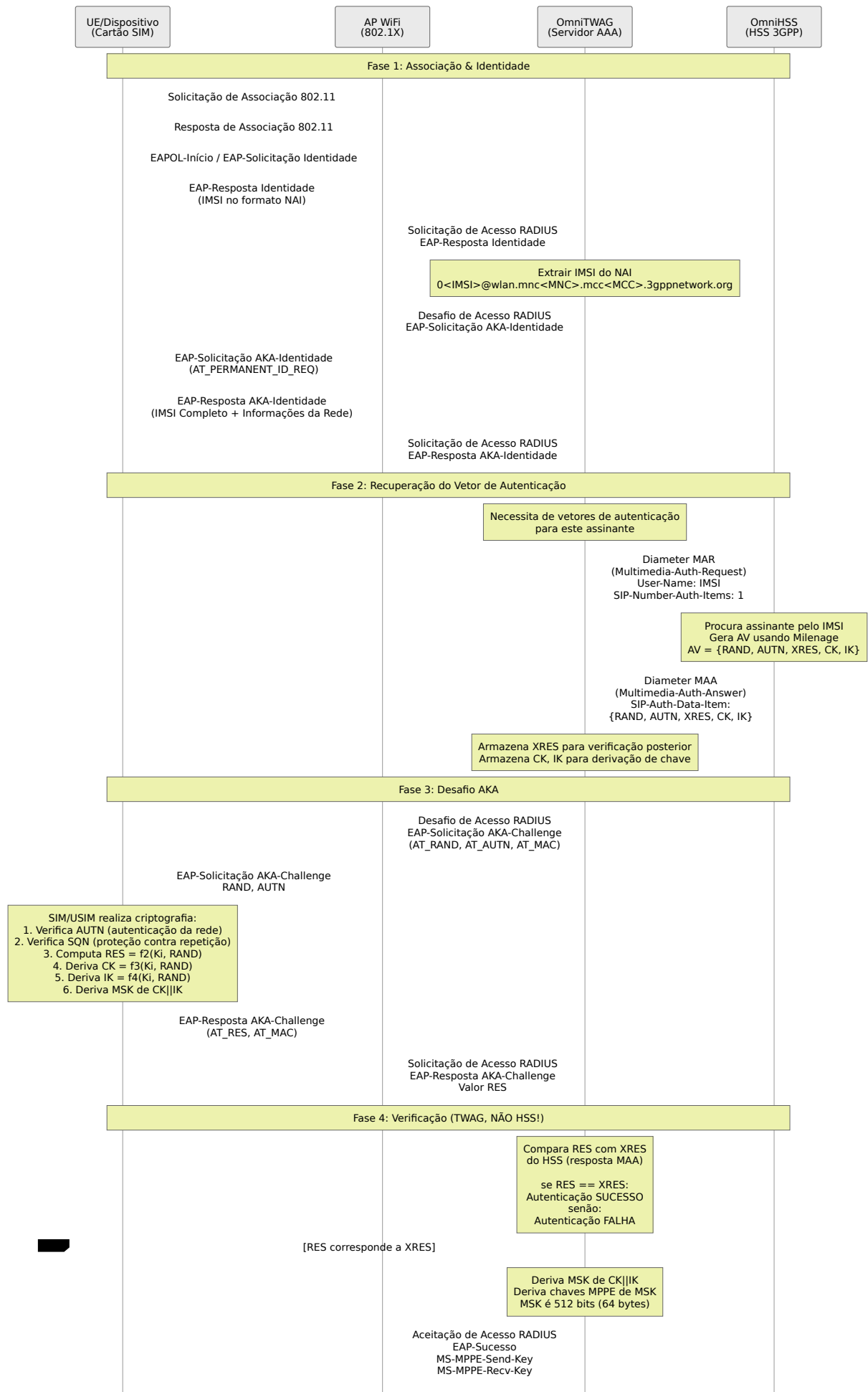


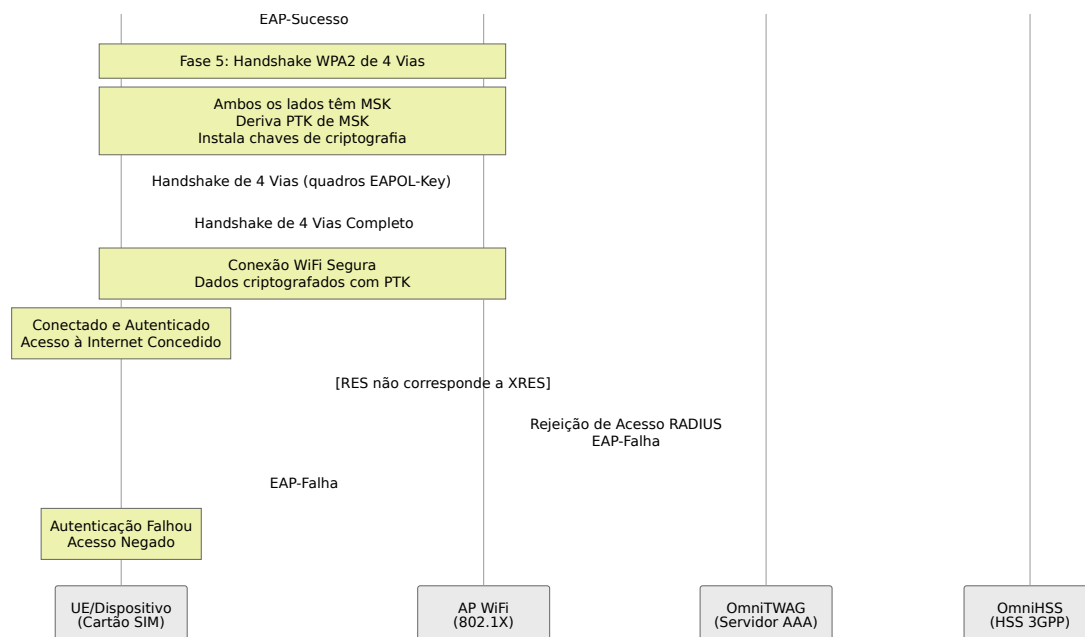
#### Configuração:

- OCS consultado no início da sessão (CCR-I), durante a sessão (CCR-U) e no final (CCR-T)
- Cota solicitada em partes configuráveis (ex: 10MB, 50MB, 100MB)
- CCR-Update acionado em um limite configurável (ex: 80% da cota concedida)
- Temporizador de validade aciona re-autorização se a cota não for esgotada
- Desconexão forçada quando a cota é esgotada
- Dedução de saldo em tempo real

# **Fluxo de Autenticação**

## **Sequência Completa de Autenticação EAP-AKA**





## Pontos-Chave no Fluxo de Autenticação

1. **MAR/MAA é o fim da comunicação com o HSS:** Após receber o MAA (Multimedia-Auth-Answer) com XRES, o TWAG lida com toda a verificação subsequente localmente.
2. **TWAG realiza a verificação de RES:** O HSS fornece a resposta esperada (XRES), mas o TWAG a compara com o RES real do UE. O HSS NÃO está envolvido nesta comparação.
3. **A autenticação ocorre no TWAG:** Isso é diferente de alguns diagramas que mostram o HSS realizando a verificação — na arquitetura 3GPP real, o servidor AAA (TWAG) realiza a comparação.

## Formato de Identidade

O dispositivo responde com sua identidade permanente (IMSI) no formato NAI:

```
50557000000000000001@wlan.mnc057.mcc505.3gppnetwork.org
```

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

Nota - O primeiro dígito, antes do IMSI, é a identidade, geralmente é 0, mas pode ser outro número de um único dígito para SIMs / dispositivos multi-IMSI.

# Chave de Sessão Mestre (MSK)

A Chave de Sessão Mestre (MSK) é uma chave criptográfica de 512 bits (64 bytes) derivada durante a autenticação EAP-AKA. Ela serve como o material de chave raiz para proteger a conexão WiFi.

## Derivação da MSK:

1. Tanto o UE quanto o TWAG derivam independentemente a mesma MSK
2. UE deriva de CK/IK computados pelo SIM
3. TWAG deriva de CK/IK recebidos do HSS
4.  $MSK = PRF'(CK || IK, \text{"Full Authentication"}, IMSI, \dots)$

## Uso da MSK:

1. **Derivação da PMK:** PMK = primeiros 256 bits (32 bytes) da MSK
2. **Handshake WPA2 de 4 Vias:** Tanto UE quanto AP usam PMK para derivar PTK
3. **Criptografia de Dados:** Todos os quadros de dados WiFi criptografados com Chave Temporal (TK) da PTK

## Por que a MSK é Crítica:

- **Confidencialidade:** Sem MSK, o tráfego WiFi seria não criptografado
- **Integridade:** Impede a adulteração dos quadros WiFi
- **Vinculação de Autenticação:** Liga a autenticação EAP à criptografia WiFi
- **Proteção contra Repetição:** MSK nova impede ataques de repetição
- **Perfeita Segurança de Encaminhamento:** Comprometimento de uma MSK não afeta outras

# Recuperação de Resincronização

Se o dispositivo detectar uma discrepância no número de sequência (SQN fora de sincronia), ele inicia a resincronização:

1. O dispositivo computa AUTS (Token de Autenticação - Sincronização)
2. Envia EAP-AKA Synchronization-Failure com AT-AUTS
3. TWAG encaminha AUTS para HSS

4. HSS resincroniza o número de sequência e gera novos vetores
5. Autenticação é tentada novamente com vetores frescos

Isso é transparente para o usuário final e não requer intervenção do operador.

---

## Guia de Configuração

O TWAG é configurado através de arquivos de configuração Elixir no diretório `config/`. A configuração principal em tempo de execução está em `config/runtime.exs`.

Para implantações em produção, a configuração é gerenciada centralmente. O abaixo é apenas uma referência, quaisquer valores alterados em um nó de produção serão perdidos na próxima vez que a orquestração automatizada for executada.

### Configuração Diameter

Localizado em `config :diameter_ex:`



```
config :diameter_ex,  
  diameter: %{  
    # Nome do serviço para a pilha Diameter  
    service_name: :omnitouch_twig,  
  
    # Endereço IP local para vincular o serviço Diameter  
    listen_ip: "10.5.198.200",  
  
    # Porta local para conexões Diameter (padrão é 3868)  
    listen_port: 3868,  
  
    # Host de Origem Diameter  
    host: "omnitwig",  
  
    # Realm de Origem Diameter (corresponde ao seu realm de rede)  
    realm: "epc.mnc057.mcc505.3gppnetwork.org",  
  
    # Pares Diameter (HSS, DRA, servidores AAA)  
    peers: [  
      %{  
        # Host de Origem Diameter do par  
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",  
  
        # Realm de Origem Diameter do par  
        realm: "epc.mnc057.mcc505.3gppnetwork.org",  
  
        # Endereço IP do par (pode ser HSS diretamente ou DRA)  
        ip: "10.179.2.140",  
  
        # Porta do par (padrão é 3868)  
        port: 3868,  
  
        # Usar TLS para segurança de transporte  
        tls: false,  
  
        # Protocolo de transporte (:diameter_tcp ou  
:diameter_sctp)  
        transport: :diameter_tcp,  
  
        # Iniciar conexão com o par (verdadeiro) ou esperar o par  
se conectar (falso)  
        initiate_connection: true  
      }  
    ]  
  }
```

```
]
}
```

**Formato de Realm** segue 3GPP TS 23.003:

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

Onde:

- MNC = Código da Rede Móvel (ex: 057)
- MCC = Código do País Móvel (ex: 505 para Austrália)

**Nota sobre o Uso do DRA:** Para usar OmniDRA, configure o IP do par para apontar para o DRA em vez de diretamente para o HSS. O DRA então roteará mensagens para o HSS apropriado com base nas regras de roteamento (Destination-Realm, intervalo de IMSI, etc.).

## Configuração RADIUS

Localizado em `config :omnitwag:`

```
config :omnitwag,  
  radius_config: %{  
    # Lista de sub-redes IP de origem permitidas para clientes  
    RADIUS  
    # Lista vazia = permite todos (não recomendado para produção)  
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],  
  
    # Segredo compartilhado para clientes RADIUS  
    # Todos os APs devem usar este segredo  
    secret: "YOUR_STRONG_SECRET_HERE"  
  }  
}
```

### Melhores Práticas de Segurança:

- Use segredos compartilhados RADIUS fortes (20+ caracteres)
- Configure `allowed_source_subnets` para restringir o acesso dos APs
- Use regras de firewall para restringir ainda mais o acesso às portas 1812/1813

### Exemplo de configuração de sub-rede:

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

Se vazio, todas as fontes são permitidas (apenas adequado para laboratório/teste).

# Configuração de Monitoramento Prometheus

Localizado em `config :omnitwag`:

```
config :omnitwag,  
  prometheus: %{  
    # Porta para o endpoint de métricas do Prometheus  
    port: 9568  
  }
```

Acesse as métricas em: `http://<twag-ip>:9568/metrics`

## Resumo de Portas

Porta	Protocolo	Propósito
1812	UDP	Autenticação RADIUS
1813	UDP	Contabilidade RADIUS
3868	TCP	Diameter (SWx para HSS/DRA)
443	TCP	Painel Web HTTPS
8444	TCP	API REST HTTPS
9568	TCP	Métricas Prometheus

---

## Configuração do Ponto de Acesso

### Pontos de Acesso Suportados

OmniTWAG funciona com qualquer AP WiFi que suporte:

- **WPA2-Enterprise** (autenticação 802.1X)
- Funcionalidade de **cliente RADIUS**
- Método de autenticação **EAP-AKA**

Plataformas testadas: Cisco Aironet, Aruba, Ubiquiti UniFi, Ruckus, APs baseados em hostapd

## Requisitos Gerais de Configuração do AP

1. Modo de segurança **WPA2-Enterprise (802.1X)**
2. **Servidor RADIUS** apontando para o endereço IP do TWAG
3. **Porta de autenticação RADIUS:** 1812
4. **Porta de contabilidade RADIUS:** 1813 (opcional, mas recomendado)
5. **Segredo compartilhado RADIUS:** Deve corresponder à configuração do TWAG
6. **Método EAP:** EAP-AKA (ou "Todos")

## Exemplo de Configuração do AP Cisco

### Configuração CLI:

```
! Configurar servidor RADIUS
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key
YOUR_SHARED_SECRET

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

! Associar SSID com a interface de rádio
interface Dot11Radio0
    encryption mode ciphers aes-ccm
    ssid OPERATOR-WIFI
```

### Interface Web:

1. Navegue até **Segurança → AAA → Servidor RADIUS**
2. Adicione o servidor RADIUS: `10.5.198.200:1812` com segredo compartilhado
3. Navegue até a configuração **WLAN**
4. Defina a Segurança como **WPA2-Enterprise**
5. Defina o método EAP como **EAP-AKA** ou **Todos**
6. Atribua o grupo de servidor RADIUS

## Exemplo de Configuração do hostapd

Para APs baseados em Linux (OpenWrt, sistemas embarcados):

```
# /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

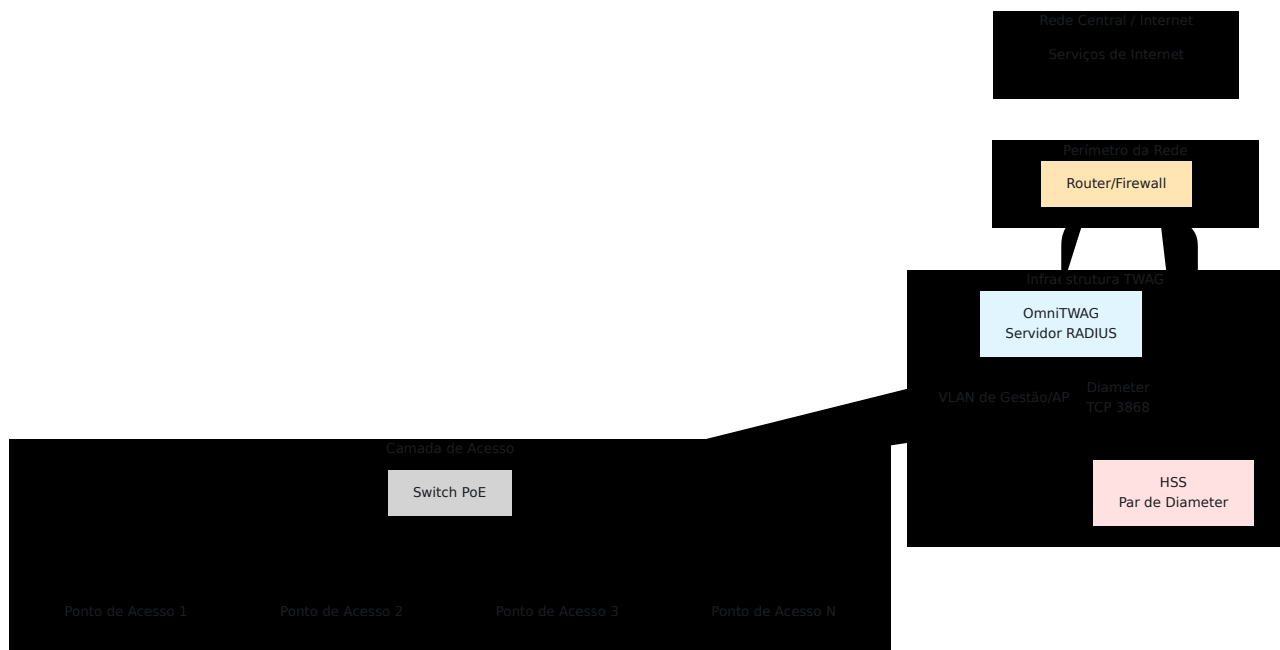
# Configuração RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# Configuração EAP
eap_server=0

# Hotspot 2.0 (Opcional - para descarregamento automático)
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
```

# Melhores Práticas de Arquitetura de Rede



**Importante:** Coloque os APs e o TWAG em segmentos de rede confiáveis. Use regras de firewall para:

- Permitir apenas que os APs acessem as portas 1812/1813 do TWAG
- Permitir que o TWAG acesse a porta 3868 do HSS
- Restringir o acesso de gestão ao painel do TWAG (porta 443)

---

## Integração Hotspot 2.0

### Visão Geral do Hotspot 2.0 (Passpoint)

Hotspot 2.0 (também chamado de Passpoint ou 802.11u) é um padrão da WiFi Alliance que permite a descoberta e conexão automática e segura de redes WiFi sem interação do usuário. É a tecnologia chave para descarregamento WiFi contínuo.

#### Principais Recursos:

- **Descoberta Automática de Redes:** O dispositivo encontra redes compatíveis com base em critérios



- **Autenticação Automática:** Usa credenciais SIM (EAP-AKA) sem entrada do usuário
- **Associação Inicial Criptografada:** OSEN (OSU Server-only Authentication) para provisionamento seguro
- **Acordos de Roaming:** Suporta redes visitadas (como roaming celular)
- **Priorização:** O dispositivo prefere redes de propriedade do operador

## Configuração do AP Hotspot 2.0

### Requisitos para o AP:

1. Suporte a **802.11u**: Capacidade de consulta/resposta ANQP
2. **WPA2-Enterprise**: Autenticação 802.1X
3. Suporte a **EAP-AKA**: Deve suportar o método EAP-AKA
4. Configuração ANQP: Anunciar informações corretas do operador

### Exemplo de Configuração (AP baseado em hostapd):

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

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

# Configuração do Realm NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# Formato: <encoding>,<realm>,<eap-method>[auth-id:auth-val]
# 21 = EAP-AKA
# 2:1 = Tipo de Credencial: SIM
# 5:7 = Método EAP Tunnelado: Nenhum (EAP-AKA direto)

# Consórcio de Roaming
roaming_consortium=505057
# MCC=505 (EUA), MNC=057 (específico do operador)

# Informações do Local (opcional)
venue_group=1
venue_type=8
venue_name=eng:Rede WiFi Pública do Operador

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

# Configuração RADIUS (aponta para 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

# Configuração SSID
```

```
ssid=OperatorWiFi
utf8_ssid=1

# Indicação Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:Rede WiFi do Operador
```

## Comportamento de Descarregamento Automático

### Como Funciona o Descarregamento Automático:

1. Dispositivo com perfil Passpoint realiza varredura WiFi periódica
2. Envia consulta ANQP para APs detectados
3. Se a resposta ANQP corresponder ao perfil (MCC/MNC, consórcio de roaming):
  - Prioridade é ALTA (rede doméstica) ou MÉDIA (parceiro de roaming)
4. Se a prioridade  $\geq$  limite e o sinal  $>$  mínimo:
  - Autenticação automática EAP-AKA
5. Se a autenticação for bem-sucedida e a prioridade  $>$  conexão atual:
  - Muda para WiFi, desconecta dados celulares
6. Monitora qualidade do sinal e mantém conectividade

### Fatores de Prioridade:

1. **Doméstico vs. Roaming:** Rede doméstica (correspondência MCC/MNC) preferida sobre roaming
  2. **Força do Sinal:** Sinal mais forte preferido
  3. **Segurança:** WPA2-Enterprise preferido sobre aberto/WPA2-PSK
  4. **Política:** O operador pode configurar redes preferidas
  5. **Sobrescrição do Usuário:** O usuário pode desativar manualmente o WiFi ou preferir celular
-

# Monitoramento e Gestão

## Painel Web

Acesse o painel de monitoramento em tempo real em: `https://<twag-ip>/`

### Recursos:

- **Visualização de Clientes RADIUS:** Assinantes ativos, status de autenticação, detalhes da sessão
- **Visualização de Pontos de Acesso:** APs conectados, contagens de clientes, informações do SSID
- **Visualização de Uso do Cliente:** Dados de contabilidade, tempo de sessão, uso de dados
- **Visualização de Pares Diameter:** Status de conexão HSS/DRA

## Integração Prometheus

Configure o Prometheus para coletar métricas do TWAG:

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

### Métricas Disponíveis:

#### Métricas do Servidor RADIUS:

- `radius_access_request_count` - Total de pacotes RADIUS Access-Request recebidos
- `radius_access_accept_count` - Total de pacotes Access-Accept enviados
- `radius_access_reject_count` - Total de pacotes Access-Reject enviados

- `radius_access_challenge_count` - Total de pacotes Access-Challenge enviados
- `radius_accounting_request_count{status_type}` - Total de pacotes Accounting-Request (marcados por status: início, parar, atualização interina, contabilidade ativada, contabilidade desativada)
- `radius_active_clients_count` - Clientes atualmente autenticados (consultados a cada 5 segundos)
- `radius_access_points_count` - Pontos de acesso registrados (consultados a cada 5 segundos)

### **Métricas de Autenticação EAP-AKA:**

- `eap_aka_identity_count` - Trocas de Identidade EAP-AKA
- `eap_aka_challenge_count` - Trocas de Desafio EAP-AKA
- `eap_aka_sync_failure_count` - Falhas de sincronização (eventos de resync SQN)
- `eap_aka_auth_success_count` - Autenticações bem-sucedidas
- `eap_aka_auth_reject_count` - Autenticações rejeitadas

### **Métricas do Protocolo Diameter:**

- `diameter_message_count{application, command, direction}` - Total de mensagens Diameter (marcadas por aplicação, tipo de comando e direção)

### **Métricas de Memória do VM Erlang:**

- `vm_memory_total` - Total de memória alocada (bytes)
- `vm_memory_processes` - Memória usada por processos Erlang (bytes)
- `vm_memory_processes_used` - Memória usada por processos Erlang excluindo memória alocada não utilizada (bytes)
- `vm_memory_system` - Memória usada pelo sistema de execução Erlang (bytes)
- `vm_memory_atom` - Memória usada por átomos (bytes)
- `vm_memory_atom_used` - Memória usada por átomos excluindo memória alocada não utilizada (bytes)
- `vm_memory_binary` - Memória usada por binários (bytes)
- `vm_memory_code` - Memória usada por código carregado (bytes)

- `vm_memory_ets` - Memória usada por tabelas ETS (bytes)

### Métricas do Sistema VM Erlang:

- `vm_system_info_process_count` - Número atual de processos Erlang
- `vm_system_info_port_count` - Número atual de portas
- `vm_system_info_atom_count` - Número atual de átomos
- `vm_system_info_schedulers` - Número de threads de agendamento
- `vm_system_info_schedulers_online` - Número de agendadores atualmente online

### Métricas do Agendador VM Erlang:

- `vm_statistics_run_queue` - Comprimento total de todas as filas de execução
- `vm_total_run_queue_lengths_total` - Comprimento total de todas as filas de execução (todos os agendadores)
- `vm_total_run_queue_lengths_cpu` - Comprimento total das filas de execução do agendador de CPU
- `vm_total_run_queue_lengths_io` - Comprimento total das filas de execução do agendador de IO

### Coleta de Métricas:

- Métricas RADIUS e EAP-AKA são emitidas em tempo real à medida que os eventos ocorrem
- Contagens de clientes ativos e pontos de acesso são consultadas a cada 5 segundos
- Métricas do VM são consultadas a cada 5 segundos a partir do tempo de execução Erlang
- Todas as métricas são expostas no formato Prometheus em `http://<twag-ip>:9568/metrics`

## Registro

O TWAG usa o Logger do Elixir para registro estruturado.

## Visualizar Logs (systemd):

```
# Registro em tempo real
journalctl -u twag -f

# Últimas 100 linhas
journalctl -u twag -n 100

# Logs desde a última inicialização
journalctl -u twag -b

# Logs para intervalo de tempo específico
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00"
```

## Mensagens de Log Chave:

- Servidor RADIUS ouvindo na porta 1812 - Servidor iniciado
  - De {IP}: Solicitação de Acesso recebida - Solicitação RADIUS do AP
  - Fase 1: Resposta de Identidade - Identidade EAP inicial
  - Fase 2: Desafio AKA - Desafio enviado para o dispositivo
  - Autenticação ACEITA - Autenticação bem-sucedida
  - Autenticação REJEITADA - Autenticação falhada
  - AP Registrado: {IP} - Novo AP detectado
- 

# Solução de Problemas

## Falhas de Autenticação

**Sintoma:** Cliente não consegue se conectar ao WiFi

### Etapas de Diagnóstico:

1. Verifique os logs do TWAG: `journalctl -u twag -f`
2. Verifique se o segredo compartilhado RADIUS corresponde entre o AP e o TWAG

3. Confirme se os pacotes RADIUS estão chegando ao TWAG: `tcpdump -i eth0 port 1812`
4. Verifique o provisionamento do assinante no HSS/configuração

### **Causas Comuns:**

- Segredo compartilhado RADIUS incorreto
- Firewall bloqueando UDP 1812/1813
- Desvio RES/XRES (Ki do SIM errado ou configuração do HSS)
- Número de sequência (SQN) fora de sincronia (deve se recuperar automaticamente via resync)
- Problemas de conectividade de rede entre o AP e o TWAG

## **Problemas de Conexão Diameter**

**Sintoma:** Par de Diameter não se conectando ao HSS/DRA

### **Etapas de Diagnóstico:**

1. Verifique a conectividade de rede: `telnet <hss-ip> 3868`
2. Verifique a configuração Diameter (Host de Origem, Realm de Origem, IP do par)
3. Revise os logs do HSS/DRA para tentativas de conexão
4. Verifique se o firewall permite TCP 3868

### **Causas Comuns:**

- IP/porta do par incorretos na configuração
- Firewall bloqueando TCP 3868
- Desvio de Host/Realm
- HSS/DRA não aceitando conexão do TWAG

## **Problemas de Desempenho**

**Sintoma:** Autenticação lenta (>5 segundos)

### **Etapas de Diagnóstico:**



1. Verifique o tempo de resposta do HSS
2. Meça a latência da rede: `ping <hss-ip>`, `mtr <hss-ip>`
3. Monitore o uso de recursos do TWAG: `top`, `htop`
4. Revise as configurações de tempo limite de solicitação Diameter

### Causas Comuns:

- Tempo limite de consulta HSS ou resposta lenta
- Alta latência de rede
- Exaustão de recursos do TWAG (CPU/memória)
- Muitas autenticações simultâneas

## Ferramentas de Depuração

### Captura de Pacotes

```
# Capturar tráfego RADIUS
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# Capturar tráfego Diameter
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# Capturar de um AP específico
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-ap1.pcap
```

Analise com Wireshark (suporta dissectores RADIUS e Diameter).

### Console Interativo

Anexe-se ao TWAG em execução para depuração ao vivo:

```
# Shell remoto para o TWAG em execução
iex --sname debug --remsh twag@hostname --cookie <cookie>
```

Do console IEx:

```
# Listar todos os clientes autenticados  
CryptoState.keys()
```

```
# Obter estado de cliente específico  
CryptoState.get("0505338057900001867@wlan.mnc057.mcc505.3gppnetwork.c
```

```
# Listar todos os APs  
APState.list()
```

```
# Listar sessões de contabilidade  
ClientUsage.list()
```

## Mensagens de Erro Comuns

Mensagem de Erro	Significado	Solução
Validação do Message-Authenticator falhou	Desvio de segredo compartilhado	Verifique se o segredo RADIUS corresponde no AP e no TWAG
Verificação de RES falhou: esperado <XRES>, obteve <RES>	Resposta de autenticação incorreta	Verifique Ki do SIM, verifique o provisionamento do HSS
Tempo limite de conexão do par Diameter	Não consegue alcançar o HSS	Verifique a rede, firewall, configuração do HSS
Falha ao decodificar mensagem EAP	Pacote EAP malformatado	Verifique o firmware do AP, pode precisar de atualização do AP
Subtipo EAP-AKA desconhecido	Mensagem EAP-AKA não suportada	Dispositivo usando variante EAP-AKA não padrão
Requerida sincronização do número de sequência	SQN fora de sincronia	Normal, o dispositivo irá resincronizar automaticamente

## Conformidade com Padrões

OmniTWAG implementa as seguintes especificações 3GPP e IETF:

- **3GPP TS 23.402:** Melhorias de arquitetura para acessos não 3GPP
- **3GPP TS 24.302:** Acesso ao EPC via redes de acesso não 3GPP

- **3GPP TS 29.273:** Interfaces SWx/SWm baseadas em Diameter
  - **3GPP TS 33.402:** Aspectos de segurança de acessos não 3GPP
  - **3GPP TS 35.206:** Especificação do algoritmo Milenage
  - **RFC 2865:** Autenticação RADIUS
  - **RFC 2866:** Contabilidade RADIUS
  - **RFC 3579:** Suporte RADIUS para EAP
  - **RFC 4187:** Protocolo de autenticação EAP-AKA
  - **RFC 5448:** EAP-AKA' (versão aprimorada)
- 

## Resumo

OmniTWAG, criado por **Omnitouch**, fornece uma solução completa e compatível com padrões para descarregamento WiFi 3GPP:

1. **Implantação Flexível:** Suporta desconexão local ou tráfego roteado para casa
  2. **Baseado em Padrões:** Implementa 3GPP SWx, EAP-AKA, protocolos RADIUS
  3. **Autenticação Segura:** Autenticação mútua baseada em SIM com resync automático
  4. **Criptografia Forte:** Chaves derivadas de MSK fornecem criptografia WPA2
  5. **Pronto para Hotspot 2.0:** Permite descarregamento totalmente automático e sem toque
  6. **Controle do Operador:** Mantém identidade, política e opcionalmente cobrança
  7. **Conectividade Flexível:** Conexão direta ao HSS ou via OmniDRA para roteamento/balanceamento de carga
- 

*Versão do Documento: 2.0 Última Atualização: 2025 OmniTWAG - Trusted WiFi Access Gateway Copyright © 2025 Omnitouch. Todos os direitos reservados.*