Guía de Operaciones y Despliegue de OmniTWAG

Creado por Omnitouch

Esta guía es para operadores de red, administradores de sistemas y clientes que despliegan OmniTWAG.

Tabla de Contenidos

Introducción

OmniTWAG (Trusted WiFi Access Gateway) es una implementación conforme a las normas de un 3GPP TWAG que permite a los operadores de redes móviles descargar de manera segura el tráfico de suscriptores de redes celulares a puntos de acceso WiFi mientras mantiene una autenticación segura basada en SIM.

El TWAG autentica a los suscriptores de WiFi utilizando sus credenciales SIM a través de EAP-AKA (Protocolo de Autenticación Extensible - Acuerdo de Clave de Autenticación), el mismo mecanismo de autenticación utilizado en redes celulares. Esto proporciona acceso WiFi seguro y sin interrupciones para suscriptores móviles sin requerir contraseñas WiFi separadas.

Beneficios Clave

Para los Usuarios Finales:

- **Cero Configuración**: Funciona directamente con SIM compatible
- **Experiencia Sin Interrupciones**: Conexión automática como en celular
- **Seguro**: Siempre utiliza WiFi encriptado (WPA2)
- **Sin Contraseñas**: Autenticación basada en SIM

Para los Operadores Móviles:

- **Alivio de Capacidad de Red**: Reduce la carga en estaciones base celulares
- **Descarga Controlada**: Solo los suscriptores autorizados pueden conectarse
- **Mejora de la Experiencia del Usuario**: WiFi generalmente ofrece mayor ancho de banda
- **Eficiencia de Costos**: La infraestructura WiFi es menos costosa que la celular
- **Identidad Consistente**: Mismo IMSI utilizado para WiFi y celular
- **Integración de Facturación**: Puede cobrar por el uso de WiFi si se desea

Para Lugares/Empresas:

- **Seguridad de Grado Operador**: Sin riesgo de compartir contraseñas
- **Escalabilidad**: Soporta miles de usuarios sin aprovisionamiento manual
- **Gestión Simplificada**: No es necesario distribuir contraseñas WiFi

---

¿Qué es la descarga de WiFi?

La descarga de WiFi permite a los operadores de redes móviles redirigir el tráfico de datos de suscriptores de redes celulares congestionadas a redes WiFi.

Cómo Habilita el TWAG la Descarga

El TWAG actúa como la puerta de autenticación entre:

- **Puntos de Acceso WiFi** (a través del protocolo RADIUS)
- **Red Central Móvil** HSS/HLR (a través de la interfaz Diameter SWx)

Cuando el dispositivo de un suscriptor se conecta a un AP WiFi configurado para la descarga:

1. El dispositivo se identifica utilizando su IMSI (de la tarjeta SIM)
2. El AP WiFi reenvía las solicitudes de autenticación al TWAG a través de RADIUS
3. El TWAG se comunica con el HSS del operador para recuperar vectores de autenticación
4. Ocurre la autenticación de desafío-respuesta EAP-AKA entre el dispositivo y el TWAG
5. Tras una autenticación exitosa, se concede acceso WiFi al dispositivo
6. Opcionalmente, el tráfico puede ser tunelizado de vuelta a la red central móvil o salir localmente

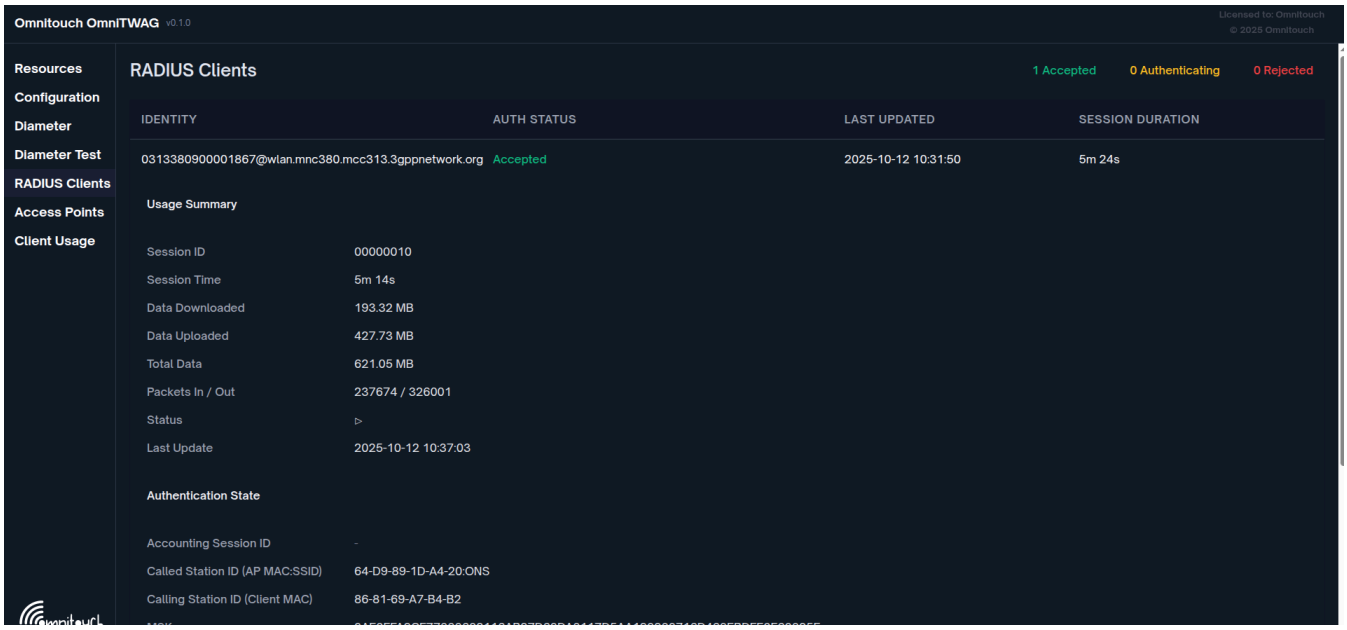
---

Arquitectura de Despliegue

Topología de Red

Leyenda de Interfaces:

- **STa***: Interfaz RADIUS/Diameter entre el AP WiFi y el TWAG (no 3GPP a AAA)
- **SWx**: Interfaz Diameter entre el TWAG (Servidor AAA 3GPP) y el HSS
- **S2a/S2b**: Interfaz de túnel GTP para el retorno a la red local (opcional)
- **SGi**: Interfaz a redes de datos de paquetes externas (Internet)
- **802.11**: Interfaz de radio WiFi
- **EAPOL**: EAP sobre LAN (autenticación 802.1X)



Escenarios de Despliegue

Escenario 1: Salida Local (Recomendado para Rendimiento)

Beneficios:

- Menor latencia (sin retorno a la central)
- Carga reducida en la red central
- Mejor experiencia para aplicaciones de alto ancho de banda
- Ahorros en capacidad de retorno

Escenario 2: Enrutamiento de Red Local (Túnel GTP)

Beneficios:

- Aplicación consistente de políticas
- Facturación/contabilidad centralizada
- Aplicación de políticas de VPN/seguridad corporativa
- Movilidad sin interrupciones entre WiFi y celular

Opciones de Conexión SWx

Opción 1: Conexión Directa al HSS

Caso de Uso: Despliegues simples, entornos de laboratorio, un solo HSS

Beneficios:

- Menor latencia (sin salto a través de DRA)
- Configuración simplificada
- Solución de problemas más fácil

Opción 2: A través de DRA (Agente de Enrutamiento Diameter)

Caso de Uso: Despliegues multi-HSS, escenarios de roaming, redes a gran escala

Beneficios:

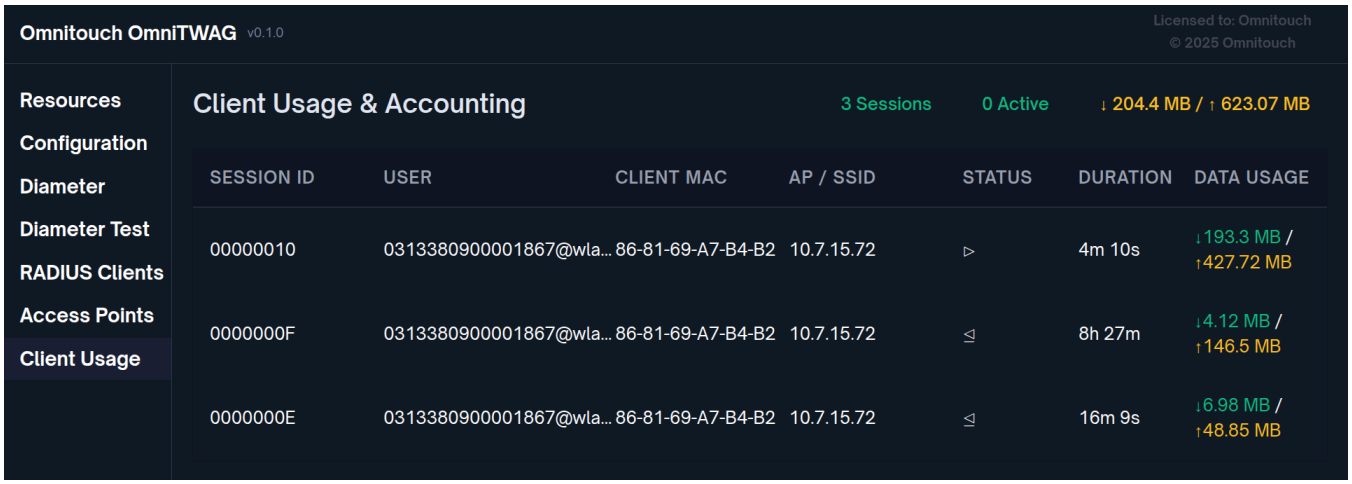
- Lógica de enrutamiento centralizada
- Balanceo de carga entre múltiples HSS
- Soporte de roaming (rutas al HSS local)
- Redundancia y conmutación por error
- Persistencia de sesión

Flujo de Carga

El TWAG puede integrarse completamente para enviar solicitudes de carga en línea basadas en Diameter `Gy` a un Sistema de Carga en Línea (OCS).

Esto permite contabilizar todos los datos consumidos en WiFi, contra el saldo del cliente, y se entrega a través del AP en RADIUS y se convierte a `Gy` por el TWAG y se reenvía al DRA/OCS.

En todos los modos, el uso es rastreado por las métricas del TWAG.



Modos de Carga

El TWAG soporta tres modos de carga en línea:

1. Carga Desactivada

No se envían solicitudes de control de crédito. No se realiza autorización de saldo.

Casos de Uso:

- Redes WiFi abiertas/gratuitas
- Entornos de laboratorio/pruebas
- Redes con carga solo fuera de línea (contabilidad RADIUS a facturación)

Flujo:

2. Solo Autorización

Se envía un CCR-Inicial (Solicitud de Control de Crédito) al OCS al inicio de la sesión de WiFi para validar que el suscriptor tiene saldo, pero el saldo no se reduce durante la sesión.

Casos de Uso:

- Validar que el suscriptor tiene cuenta/saldo activo
- Prevenir acceso WiFi para cuentas suspendidas
- Verificar elegibilidad del servicio sin seguimiento de cuotas
- Permitir WiFi como servicio de bonificación/sin límite para clientes que pagan

Flujo:

Configuración:

- Se consulta al OCS al inicio de la sesión (CCR-I) y al final (CCR-T)
- No se envían mensajes CCR-Actualización durante la sesión
- Suscriptor autorizado basado en el estado de la cuenta, no en la cuota
- Uso reportado al final de la sesión solo con fines informativos

3. Carga en Línea Gy Completa (Implementación Completa)

Se sigue el flujo de carga en línea estándar 3GPP. Todo el uso en WiFi se pasa al OCS para la carga, con el suscriptor desconectado una vez que ha excedido su cuota.

Casos de Uso:

- Servicios de datos prepagados
- WiFi de pago por uso
- Planes basados en cuotas (por ejemplo, 10GB de asignación mensual)
- Carga y corte en tiempo real

Flujo:

Configuración:

- Se consulta al OCS al inicio de la sesión (CCR-I), durante la sesión (CCR-U) y al final (CCR-T)
- Se solicita cuota en bloques configurables (por ejemplo, 10MB, 50MB, 100MB)
- CCR-Actualización se activa en un umbral configurable (por ejemplo, 80% de la cuota concedida)
- Temporizador de validez activa re-autorización si la cuota no se ha agotado
- Desconexión forzada cuando la cuota se agota
- Deducción de saldo en tiempo real

Flujo de Autenticación

Secuencia Completa de Autenticación EAP-AKA

Puntos Clave en el Flujo de Autenticación

1. **MAR/MAA es el final de la comunicación con el HSS**: Después de recibir el MAA (Respuesta de Autenticación Multimedia) con XRES, el TWAG maneja todas las verificaciones posteriores localmente.
2. **El TWAG realiza la verificación de RES**: El HSS proporciona la respuesta esperada (XRES), pero el TWAG la compara con el RES real del UE. El HSS NO está involucrado en esta comparación.
3. **La autenticación ocurre en el TWAG**: Esto es diferente de algunos diagramas que muestran al HSS realizando la verificación; en la arquitectura 3GPP real, el servidor AAA (TWAG) realiza la comparación.

Formato de Identidad

El dispositivo responde con su identidad permanente (IMSI) en formato NAI:

```
0505700000000000001@wlan.mnc057.mcc505.3gppnetwork.org
```

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

Nota - El primer dígito, antes del IMSI, es la identidad, generalmente es 0, pero puede ser otro número de un solo dígito para SIMs / dispositivos multi-IMSI.

Clave de Sesión Maestra (MSK)

La Clave de Sesión Maestra (MSK) es una clave criptográfica de 512 bits (64 bytes) derivada durante la autenticación EAP-AKA. Sirve como el material clave raíz para asegurar la conexión WiFi.

Derivación de MSK:

1. Tanto el UE como el TWAG derivan independientemente la misma MSK
2. El UE deriva de CK/IK calculado por la SIM
3. El TWAG deriva de CK/IK recibido del HSS
4. MSK = PRF'(CK || IK, "Autenticación Completa", IMSI, ...)

Uso de MSK:

1. **Derivación de PMK**: PMK = primeros 256 bits (32 bytes) de MSK
2. **Intercambio de 4 Vías WPA2**: Tanto el UE como el AP utilizan PMK para derivar PTK
3. **Encriptación de Datos**: Todos los tramas de datos WiFi encriptados con la Clave Temporal (TK) de PTK

Por qué MSK es Crítico:

- **Confidencialidad**: Sin MSK, el tráfico WiFi estaría sin encriptar

- **Integridad**: Previene la manipulación de tramas WiFi
- **Vinculación de Autenticación**: Vincula la autenticación EAP a la encriptación WiFi
- **Protección contra Repetición**: MSK fresca previene ataques de repetición
- **Secreto Perfecto hacia Adelante**: La compromisión de una MSK no afecta a otras

Recuperación de Resincronización

Si el dispositivo detecta un desajuste en el número de secuencia (SQN fuera de sincronización), inicia la resincronización:

1. El dispositivo calcula AUTS (Token de Autenticación - Sincronización)
2. Envía EAP-AKA Fallo de Sincronización con AT-AUTS
3. El TWAG reenvía AUTS al HSS
4. El HSS resincroniza el número de secuencia y genera nuevos vectores
5. La autenticación se reintenta con nuevos vectores

Esto es transparente para el usuario final y no requiere intervención del operador.

Guía de Configuración

El TWAG se configura a través de archivos de configuración de Elixir en el directorio `config/`. La configuración principal en tiempo de ejecución está en `config/runtime.exs`.

Para despliegues en producción, la configuración se gestiona de manera centralizada. Lo siguiente es solo una referencia, cualquier valor cambiado en un nodo de producción se perderá la próxima vez que se ejecute la orquestación automatizada.

Configuración de Diameter

Ubicado en `config :diameter_ex`:

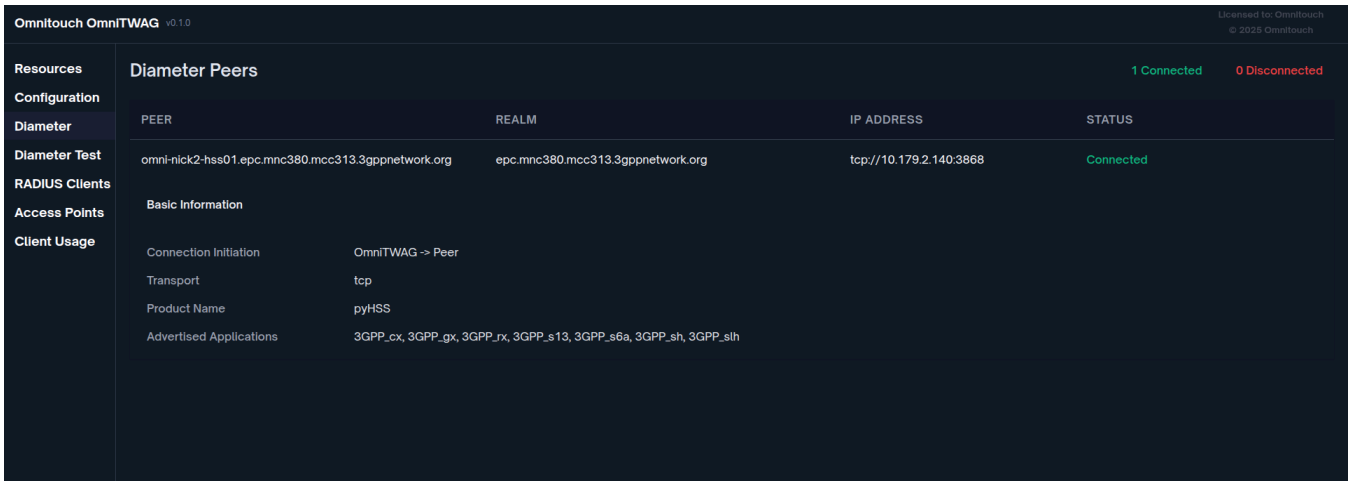
```
config :diameter_ex,
  diameter: %{
    # Nombre del servicio para la pila Diameter
    service_name: :omnitouch_twag,

    # Dirección IP local para vincular el servicio Diameter
    listen_ip: "10.5.198.200",

    # Puerto local para conexiones Diameter (el estándar es 3868)
    listen_port: 3868,

    # Host de Origen Diameter
    host: "omnitwag",

    # Dominio de Origen Diameter (coincide con el dominio de su red)
    realm: "epc.mnc057.mcc505.3gppnetwork.org",

    # Pares Diameter (HSS, DRA, servidores AAA)
    peers: [
      %{
        # Host de Origen Diameter del par
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

        # Dominio de Origen Diameter del par
        realm: "epc.mnc057.mcc505.3gppnetwork.org",

        # Dirección IP del par (puede ser HSS directamente o DRA)
        ip: "10.179.2.140",

        # Puerto del par (el estándar es 3868)
        port: 3868,

        # Usar TLS para seguridad en el transporte
        tls: false,

        # Protocolo de transporte (:diameter_tcp o :diameter_sctp)
        transport: :diameter_tcp,

        # Iniciar conexión con el par (true) o esperar a que el par se conecte (false)
        initiate_connection: true
      }
    ]
  }
```

Formato de Dominio sigue 3GPP TS 23.003:

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

Donde:

- MNC = Código de Red Móvil (por ejemplo, 057)
- MCC = Código de País Móvil (por ejemplo, 505 para Australia)

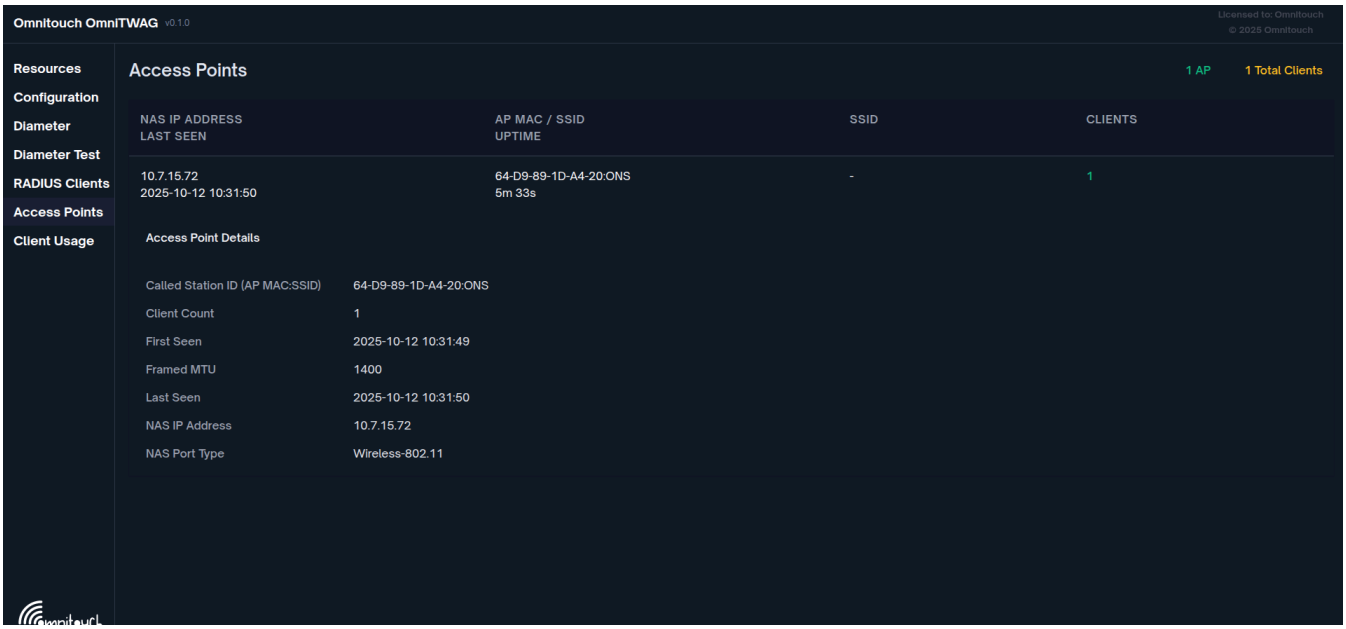


Nota sobre el Uso de DRA: Para usar OmniDRA, configure la IP del par para apuntar al DRA en lugar de directamente al HSS. El DRA luego enrutará los mensajes al HSS apropiado basado en las reglas de enrutamiento (Dominio de Destino, rango de IMSI, etc.).

Configuración de RADIUS

Ubicado en `config :omnitwag`:

```
config :omnitwag,
  radius_config: %{
    # Lista de subredes IP de origen permitidas para clientes RADIUS
    # Lista vacía = permitir todos (no recomendado para producción)
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],

    # Secreto compartido para clientes RADIUS
    # Todos los APs deben usar este secreto
    secret: "YOUR_STRONG_SECRET_HERE"
  }
```



Mejores Prácticas de Seguridad:

- Usar secretos compartidos RADIUS fuertes (más de 20 caracteres)
- Configurar `allowed_source_subnets` para restringir el acceso de AP
- Usar reglas de firewall para restringir aún más el acceso a los puertos 1812/1813

Ejemplo de configuración de subred:

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

Si está vacío, se permiten todas las fuentes (solo adecuado para laboratorio/pruebas).

Configuración de Monitoreo de Prometheus

Ubicado en `config :omnitwag`:

```
config :omnitwag,
  prometheus: %{
    # Puerto para el endpoint de métricas de Prometheus
    port: 9568
  }
```

Acceda a las métricas en: `http://<twag-ip>:9568/metrics`

Resumen de Puertos

Puerto	Protocolo	Propósito
1812	UDP	Autenticación RADIUS
1813	UDP	Contabilidad RADIUS
3868	TCP	Diameter (SWx a HSS/DRA)
443	TCP	Panel de Control Web HTTPS
8444	TCP	API REST HTTPS
9568	TCP	Métricas de Prometheus

Configuración del Punto de Acceso

Puntos de Acceso Soportados

OmniTWAG funciona con cualquier AP WiFi que soporte:

- **WPA2-Enterprise** (autenticación 802.1X)
- Funcionalidad de **cliente RADIUS**
- Método de autenticación **EAP-AKA**

Plataformas probadas: Cisco Aironet, Aruba, Ubiquiti UniFi, Ruckus, APs basados en hostapd

Requisitos Generales de Configuración del AP

1. Modo de seguridad **WPA2-Enterprise (802.1X)**
2. **Servidor RADIUS** apuntando a la dirección IP del TWAG
3. **Puerto de autenticación RADIUS**: 1812
4. **Puerto de contabilidad RADIUS**: 1813 (opcional pero recomendado)
5. **Secreto compartido RADIUS**: Debe coincidir con la configuración del TWAG
6. **Método EAP**: EAP-AKA (o "Todos")

Ejemplo de Configuración de AP Cisco

Configuración CLI:

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

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

! Asociar SSID con la interfaz de radio
interface Dot11Radio0
   encryption mode ciphers aes-ccm
   ssid OPERATOR-WIFI
```

Interfaz Web:

1. Navegar a **Seguridad → AAA → Servidor RADIUS**
2. Agregar servidor RADIUS: `10.5.198.200:1812` con secreto compartido
3. Navegar a la configuración de **WLAN**
4. Establecer Seguridad en **WPA2-Enterprise**
5. Establecer método EAP en **EAP-AKA** o **Todos**
6. Asignar grupo de servidores RADIUS

Ejemplo de Configuración de hostapd

Para APs basados en Linux (OpenWrt, sistemas embebidos):

```
# /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

# Configuración 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

# Configuración EAP
eap_server=0

# Hotspot 2.0 (Opcional - para descarga automática)
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
```

Mejores Prácticas de Arquitectura de Red

Importante: Coloque los APs y el TWAG en segmentos de red confiables. Use reglas de firewall para:

- Permitir solo a los APs alcanzar los puertos 1812/1813 del TWAG
- Permitir que el TWAG alcance el puerto 3868 del HSS
- Restringir el acceso de gestión al panel de control del TWAG (puerto 443)

Integración de Hotspot 2.0

Visión General de Hotspot 2.0 (Passpoint)

Hotspot 2.0 (también llamado Passpoint o 802.11u) es un estándar de la Alianza WiFi que permite el descubrimiento y la conexión automática y segura a redes WiFi sin interacción del usuario. Es la tecnología clave para la descarga de WiFi sin interrupciones.

Características Clave:

- **Descubrimiento Automático de Redes**: El dispositivo encuentra redes compatibles según criterios
- **Autenticación Automática**: Utiliza credenciales SIM (EAP-AKA) sin entrada del usuario
- **Asociación Inicial Encriptada**: OSEN (Autenticación Solo del Servidor OSU) para aprovisionamiento seguro
- **Acuerdos de Roaming**: Soporta redes visitadas (como roaming celular)
- **Priorización**: El dispositivo prefiere redes de operador

Configuración del AP para Hotspot 2.0

Requisitos para el AP:

1. **Soporte 802.11u**: Capacidad de consulta/respuesta ANQP
2. **WPA2-Enterprise**: Autenticación 802.1X
3. **Soporte EAP-AKA**: Debe soportar el método EAP-AKA
4. **Configuración ANQP**: Anunciar la información correcta del operador

Ejemplo de Configuración (AP basado en hostapd):

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

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

# Configuración de Dominio NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# Formato: <codificación>,<dominio>,<método-eap>[auth-id:auth-val]
# 21 = EAP-AKA
# 2:1 = Tipo de Credencial: SIM
# 5:7 = Método EAP Tunelado: Ninguno (EAP-AKA directo)

# Consorcio de Roaming
roaming_consortium=505057
# MCC=505 (EE.UU.), MNC=057 (específico del operador)

# Información del Lugar (opcional)
venue_group=1
venue_type=8
venue_name=eng:Red WiFi Pública del Operador

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

# Configuración RADIUS (apunta a 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

# Configuración SSID
ssid=OperatorWiFi
utf8_ssid=1

# Indicación de Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:Red WiFi del Operador
```

Comportamiento de Descarga Automática

Cómo Funciona la Descarga Automática:

1. Dispositivo con perfil Passpoint realiza un escaneo WiFi periódico
2. Envía consulta ANQP a los APs detectados
3. Si la respuesta ANQP coincide con el perfil (MCC/MNC, consorcio de roaming):
    - La prioridad es ALTA (red local) o MEDIA (socio de roaming)
4. Si la prioridad ≥ umbral y la señal > mínima:
    - Autenticación automática EAP-AKA
5. Si la autenticación es exitosa y la prioridad > conexi��n actual:
    - Cambiar a WiFi, desconectar datos celulares
6. Monitorear calidad de señal y mantener conectividad

Factores de Prioridad:

1. **Local vs. Roaming**: La red local (coincidencia MCC/MNC) se prefiere sobre el roaming
2. **Fuerza de Señal**: Se prefiere una señal más fuerte
3. **Seguridad**: WPA2-Enterprise se prefiere sobre abierto/WPA2-PSK
4. **Política**: El operador puede configurar redes preferidas
5. **Anulación del Usuario**: El usuario puede desactivar manualmente WiFi o preferir celular

Monitoreo y Gestión

Panel de Control Web

Acceda al panel de monitoreo en tiempo real en: `https://<twag-ip>/`

Características:

- **Vista de Clientes RADIUS**: Suscriptores activos, estado de autenticación, detalles de sesión
- **Vista de Puntos de Acceso**: APs conectados, conteos de clientes, información de SSID
- **Vista de Uso del Cliente**: Datos de contabilidad, tiempo de sesión, uso de datos
- **Vista de Pares Diameter**: Estado de conexión HSS/DRA

Integración de Prometheus

Configure Prometheus para recopilar métricas del TWAG:

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

Métricas Disponibles:

Métricas del Servidor RADIUS:

- `radius_access_request_count` - Total de paquetes RADIUS Access-Request recibidos
- `radius_access_accept_count` - Total de paquetes Access-Accept enviados
- `radius_access_reject_count` - Total de paquetes Access-Reject enviados
- `radius_access_challenge_count` - Total de paquetes Access-Challenge enviados
- `radius_accounting_request_count{status_type}` - Total de paquetes Accounting-Request (etiquetados por estado: inicio, detener, actualización interina, contabilidad activa, contabilidad inactiva)
- `radius_active_clients_count` - Clientes actualmente autenticados (sondeados cada 5 segundos)
- `radius_access_points_count` - Puntos de acceso registrados (sondeados cada 5 segundos)

Métricas de Autenticación EAP-AKA:

- `eap_aka_identity_count` - Intercambios de Identidad EAP-AKA
- `eap_aka_challenge_count` - Intercambios de Desafío EAP-AKA
- `eap_aka_sync_failure_count` - Fallos de sincronización (eventos de resincronización SQN)
- `eap_aka_auth_success_count` - Autenticaciones exitosas
- `eap_aka_auth_reject_count` - Autenticaciones rechazadas

Métricas del Protocolo Diameter:

- `diameter_message_count{application, command, direction}` - Total de mensajes Diameter (etiquetados por aplicación, tipo de comando y dirección)

Métricas de Memoria de la VM de Erlang:

- `vm_memory_total` - Cantidad total de memoria asignada (bytes)
- `vm_memory_processes` - Memoria utilizada por procesos Erlang (bytes)
- `vm_memory_processes_used` - Memoria utilizada por procesos Erlang excluyendo memoria asignada no utilizada (bytes)
- `vm_memory_system` - Memoria utilizada por el sistema de tiempo de ejecución Erlang (bytes)
- `vm_memory_atom` - Memoria utilizada por átomos (bytes)
- `vm_memory_atom_used` - Memoria utilizada por átomos excluyendo memoria asignada no utilizada (bytes)
- `vm_memory_binary` - Memoria utilizada por binarios (bytes)
- `vm_memory_code` - Memoria utilizada por código cargado (bytes)
- `vm_memory_ets` - Memoria utilizada por tablas ETS (bytes)

Métricas del Sistema de la VM de Erlang:

- `vm_system_info_process_count` - Número actual de procesos Erlang
- `vm_system_info_port_count` - Número actual de puertos
- `vm_system_info_atom_count` - Número actual de átomos
- `vm_system_info_schedulers` - Número de hilos de programador
- `vm_system_info_schedulers_online` - Número de programadores actualmente en línea

Métricas del Programador de la VM de Erlang:

- `vm_statistics_run_queue` - Longitud total de todas las colas de ejecución
- `vm_total_run_queue_lengths_total` - Longitud total de todas las colas de ejecución (programadores totales)
- `vm_total_run_queue_lengths_cpu` - Longitud total de colas de ejecución del programador de CPU
- `vm_total_run_queue_lengths_io` - Longitud total de colas de ejecución del programador de IO

Recopilación de Métricas:

- Las métricas de RADIUS y EAP-AKA se emiten en tiempo real a medida que ocurren eventos
- Los conteos de clientes activos y puntos de acceso se sondean cada 5 segundos
- Las métricas de la VM se sondean cada 5 segundos desde el tiempo de ejecución Erlang
- Todas las métricas se exponen en formato Prometheus en `http://<twag-ip>:9568/metrics`

Registro

El TWAG utiliza el Logger de Elixir para el registro estructurado.

Ver Registros (systemd):

```
# Registro en tiempo real
journalctl -u twag -f

# Últimas 100 líneas
journalctl -u twag -n 100

# Registros desde el último arranque
journalctl -u twag -b

# Registros para un rango de tiempo específico
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00"
```

Mensajes Clave en el Registro:

- `Servidor RADIUS escuchando en el puerto 1812` - Servidor iniciado
- `Desde {IP}: Solicitud de Acceso recibida` - Solicitud RADIUS del AP
- `Fase 1: Respuesta de Identidad` - Identidad EAP inicial
- `Fase 2: Desafío AKA` - Desafío enviado al dispositivo
- `Autenticación ACEPTADA` - Autenticación exitosa
- `Autenticación RECHAZADA` - Autenticación fallida
- `AP Registrado: {IP}` - Nuevo AP detectado

Solución de Problemas

Fallos de Autenticación

Síntoma: El cliente no puede conectarse a WiFi

Pasos de Diagnóstico:

1. Verifique los registros del TWAG: `journalctl -u twag -f`
2. Verifique que el secreto compartido de RADIUS coincida entre el AP y el TWAG
3. Confirme que los paquetes RADIUS lleguen al TWAG: `tcpdump -i eth0 port 1812`
4. Verifique el aprovisionamiento del suscriptor en HSS/configuración

Causas Comunes:

- Secreto compartido de RADIUS incorrecto
- Firewall bloqueando UDP 1812/1813
- Desajuste RES/XRES (Ki de SIM incorrecto o configuración de HSS)
- Número de secuencia (SQN) fuera de sincronización (debería recuperarse automáticamente a través de la resincronización)
- Problemas de conectividad de red entre el AP y el TWAG

Problemas de Conexión Diameter

Síntoma: El par Diameter no se conecta al HSS/DRA

Pasos de Diagnóstico:

1. Verifique la conectividad de red: `telnet <hss-ip> 3868`
2. Verifique la configuración de Diameter (Host de Origen, Dominio de Origen, IP del par)
3. Revise los registros del HSS/DRA para intentos de conexión
4. Verifique que el firewall permita TCP 3868

Causas Comunes:

- IP/puerto del par incorrecto en la configuración
- Firewall bloqueando TCP 3868
- Desajuste de Host/Dominio
- HSS/DRA no acepta conexión desde el TWAG

Problemas de Rendimiento

Síntoma: Autenticación lenta (>5 segundos)

Pasos de Diagnóstico:

1. Verifique el tiempo de respuesta del HSS
2. Mida la latencia de la red: `ping <hss-ip>`, `mtr <hss-ip>`
3. Monitoree el uso de recursos del TWAG: `top`, `htop`
4. Revise la configuración de tiempo de espera de solicitudes Diameter

Causas Comunes:

- Tiempo de espera de consulta HSS o respuesta lenta
- Alta latencia de red
- Agotamiento de recursos del TWAG (CPU/memoria)
- Demasiadas autenticaciones concurrentes

Herramientas de Depuración

Captura de Paquetes

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

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

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

Analizar con Wireshark (soporta disectores RADIUS y Diameter).

Consola Interactiva

Conéctese al TWAG en ejecución para depuración en vivo:

```
# Shell remoto al TWAG en ejecución
iex --sname debug --remsh twag@hostname --cookie <cookie>
```

Desde la consola IEx:

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

# Obtener estado de cliente específico
CryptoState.get("050533805790000l867@wlan.mnc057.mcc505.3gppnetwork.org")

# Listar todos los APs
APState.list()

# Listar sesiones de contabilidad
ClientUsage.list()
```

Mensajes de Error Comunes

Mensaje de Error	Significado	Solución
`Validación del Autenticador de Mensaje fallida`	Desajuste de secreto compartido	Verifique que el secreto RADIUS coincida en el AP y el TWAG
`Verificación de RES fallida: se esperaba <XRES>, se obtuvo <RES>`	Respuesta de autenticación incorrecta	Verifique Ki de SIM, verifique aprovisionamiento de HSS
`Tiempo de espera de conexión del par Diameter`	No se puede alcanzar el HSS	Verifique la red, firewall, configuración de HSS
`Error al decodificar el mensaje EAP`	Paquete EAP mal formado	Verifique el firmware del AP, puede necesitar actualización del AP
`Subtipo EAP-AKA desconocido`	Mensaje EAP-AKA no soportado	Dispositivo usando variante EAP-AKA no estándar
`Se requiere sincronización del número de secuencia`	SQN fuera de sincronización	Normal, el dispositivo se resincronizará automáticamente

---

Cumplimiento de Normas

OmniTWAG implementa las siguientes especificaciones de 3GPP e IETF:

- **3GPP TS 23.402**: Mejoras de arquitectura para accesos no 3GPP
- **3GPP TS 24.302**: Acceso a EPC a través de redes de acceso no 3GPP
- **3GPP TS 29.273**: Interfaces SWx/SWm basadas en Diameter
- **3GPP TS 33.402**: Aspectos de seguridad de accesos no 3GPP
- **3GPP TS 35.206**: Especificación del algoritmo Milenage
- **RFC 2865**: Autenticación RADIUS
- **RFC 2866**: Contabilidad RADIUS
- **RFC 3579**: Soporte RADIUS para EAP
- **RFC 4187**: Protocolo de autenticación EAP-AKA
- **RFC 5448**: EAP-AKA' (versión mejorada)

Resumen

OmniTWAG, creado por Omnitouch, proporciona una solución completa y conforme a las normas para la descarga de WiFi 3GPP:

1. **Despliegue Flexible**: Soporta salida local o tráfico enrutado a casa
2. **Basado en Normas**: Implementa protocolos 3GPP SWx, EAP-AKA, RADIUS
3. **Autenticación Segura**: Autenticación mutua basada en SIM con resincronización automática
4. **Fuerte Encriptación**: Claves derivadas de MSK proporcionan encriptación WPA2
5. **Listo para Hotspot 2.0**: Permite descarga completamente automática y sin intervención
6. **Control del Operador**: Mantiene identidad, políticas y opcionalmente facturación
7. **Conectividad Flexible**: Conexión directa al HSS o a través de OmniDRA para enrutamiento/balanceo de carga

---