

دليل عمليات ونشر OmniTWAG

OmniTouch أنشاء

هذا الدليل مخصص لمشغلي الشبكات، ومديري الأنظمة، والعملاء الذين يقومون بنشر OmniTWAG.

جدول المحتويات

1. مقدمة
2. WiFi ما هو تحميل
3. معمارية النشر
4. تدفق الشحن
5. تدفق المصادقة
6. دليل التكوين
7. إعداد نقطة الوصول
8. Hotspot 2.0 تكامل
9. المراقبة والإدارة
10. استكشاف الأخطاء وإصلاحها
11. الامتثال للمعايير

مقدمة

OmniTWAG هو تنفيذ متوافق مع المعايير لـ 3 (WiFi بوابة الوصول الموثوقة لشبكة) OmniTWAG الذي يمكن مشغلي الشبكات المحمولة من تحميل حركة مرور المشتركين من الشبكات بشكل آمن مع الحفاظ على المصادقة الآمنة المعتمدة على WiFi الخلوية إلى نقاط الوصول لشبكة SIM.

EAP-AKA الخاصة بهم عبر SIM باستخدام بيانات اعتماد WiFi بمصادقة مشتركي TWAG يقوم وهو نفس آلية المصادقة، (بروتوكول المصادقة القابل للتوسيع - المصادقة واتفاقية المفتاح) للمشاركين المتنقلين WiFi المستخدمة في الشبكات الخلوية. وهذا يوفر وصولاً سلساً وأمنًا لشبكة منفصلة WiFi دون الحاجة إلى كلمات مرور.

الفوائد الرئيسية

:للمستخدمين النهائيين

- متوافق SIM **عدم وجود تكوين**: يعمل مباشرة مع
- **تجربة سلسة**: اتصال تلقائي مثل الشبكات الخلوية
- (WPA2) مشفر WiFi **آمن**: يستخدم دائمًا
- SIM **لا كلمات مرور**: مصادقة تعتمد على

:لمشغلي الشبكات المحمولة

- **تخفيف سعة الشبكة**: يقلل الحمل على محطات القاعدة الخلوية
- **تحمّل متحكم فيه**: يمكن فقط للمشاركين المصرح لهم الاتصال
- عادةً عرض نطاق ترددي أعلى WiFi **تحسين تجربة المستخدم**: توفر
- التحتية أقل تكلفة من الخلوية WiFi **كفاءة التكلفة**: بنية
- والخلوية WiFi المستخدمة لـ IMSI **هوية متسقة**: نفس
- إذا رغبت WiFi **تكامل الفوترة**: يمكن شحن استخدام

:للمواقع/الشركات

- **أمان على مستوى المشغل**: لا خطر من مشاركة كلمات المرور
- **قابلية التوسع**: دعم لآلاف المستخدمين دون توفير يدوي
- WiFi **إدارة مبسطة**: لا حاجة لتوزيع كلمات مرور

WiFi؟ ما هو تحميل

لمشغلي الشبكات المحمولة بإعادة توجيه حركة بيانات المشاركين من الشبكات WiFi يسمح تحميل WiFi الخلوية المزدحمة إلى شبكات

التحميل TWAG كيف يمكن

كبوابة المصادقة بين TWAG يعمل:

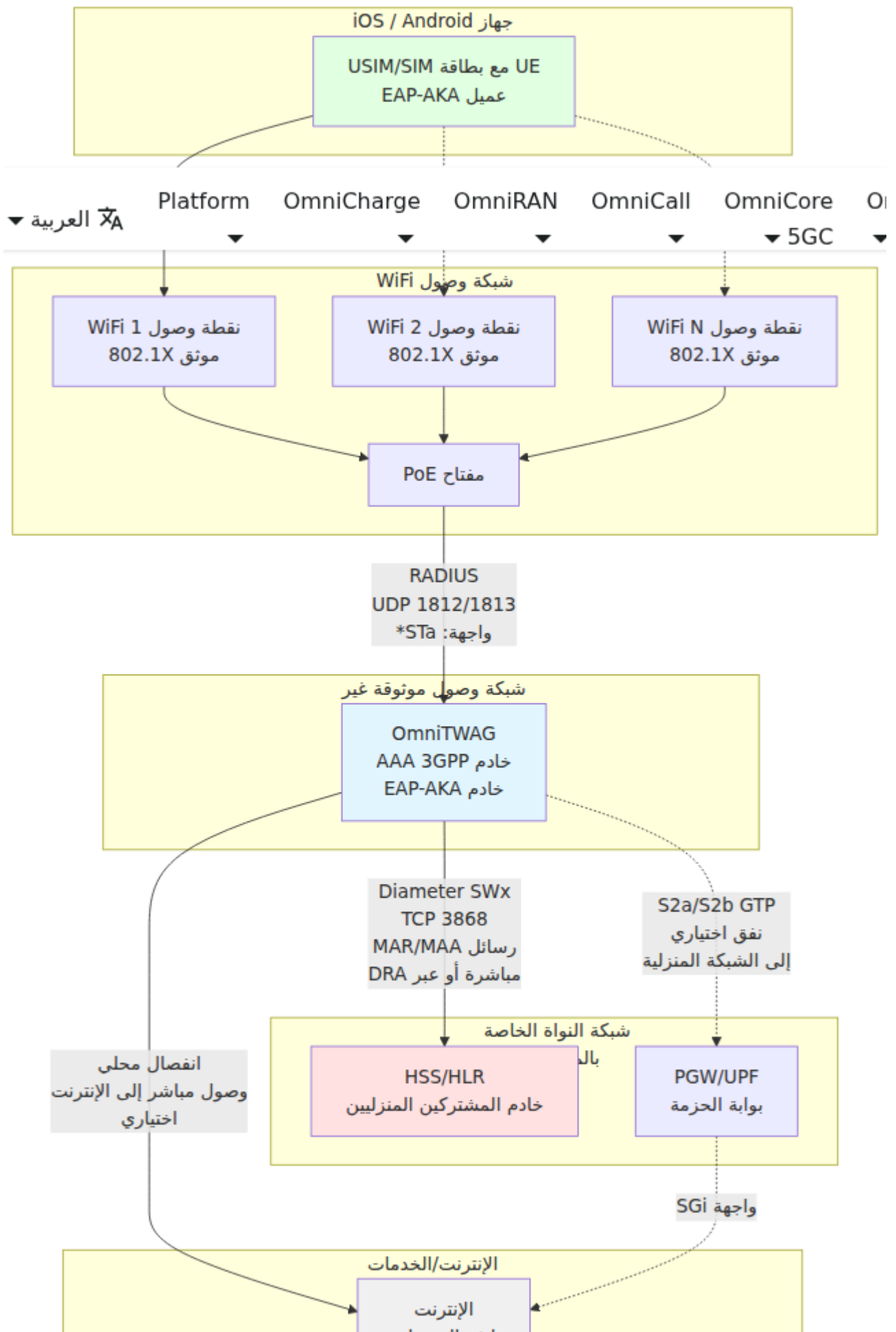
- **WiFi نقاط وصول** (RADIUS عبر بروتوكول)
- **شبكة النواة المحمولة** (Diameter SWx عبر واجهة) HSS/HLR

تم تكوينها للتحميل WiFi عندما يتصل جهاز المشترك بنقطة وصول:

1. (SIM من بطاقة) الخاص به IMSI يتعرف الجهاز على نفسه باستخدام
 2. RADIUS عبر TWAG بإرسال طلبات المصادقة إلى WiFi تقوم نقطة وصول
 3. الخاص بالمشغل لاسترجاع متجهات المصادقة HSS مع TWAG يتواصل
 4. TWAG بين الجهاز و EAP-AKA تحدث مصادقة التحدي-الاستجابة
 5. WiFi عند المصادقة الناجحة، يُمنح الجهاز وصول
 6. اختياريًا، يمكن أن يتم توجيه الحركة مرة أخرى إلى النواة المحمولة أو الانفصال محليًا
-

معمارية النشر

طوبولوجيا الشبكة

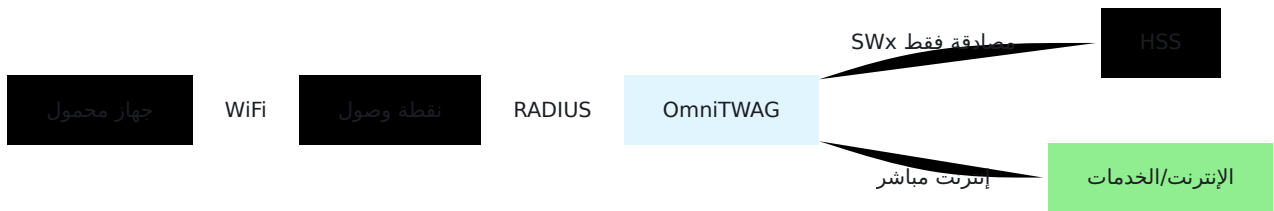


أسطورة الواجهة:

- **STa***: إلى GPP غير (3 TWAG و WiFi بين نقطة وصول RADIUS/Diameter واجهة: AAA)
- **SWx**: و HSS (AAA 3GPP خادم) بين Diameter واجهة
- **S2a/S2b**: للعودة إلى الشبكة المنزلية (اختياري) GTP واجهة نفق
- **SGi**: واجهة إلى الشبكات الخارجية لنقل البيانات (الإنترنت)
- **802.11**: WiFi واجهة راديو
- **EAPOL**: EAP عبر LAN (802.1 مصادقة X)

سيناريوهات النشر

السيناريو 1: الانفصال المحلي (موصى به للأداء)

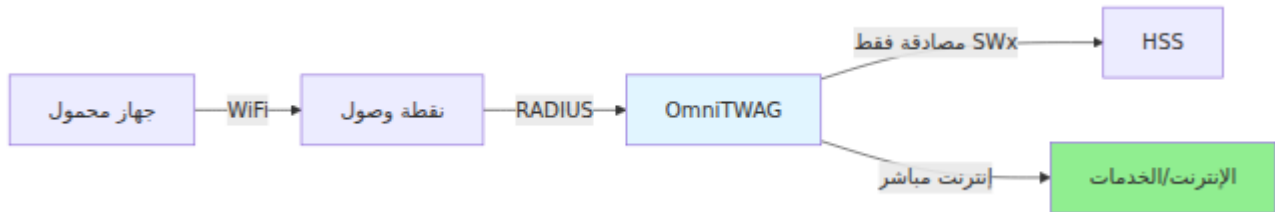


الفوائد:

- زمن انتقال أقل (لا إعادة توجيهه إلى النواة)

- تقليل الحمل على الشبكة الأساسية
- تجربة أفضل للمستخدمين في التطبيقات عالية النطاق
- توفير في سعة النقل

GTP نفق) السيناريو 2: توجيه الشبكة المنزلية

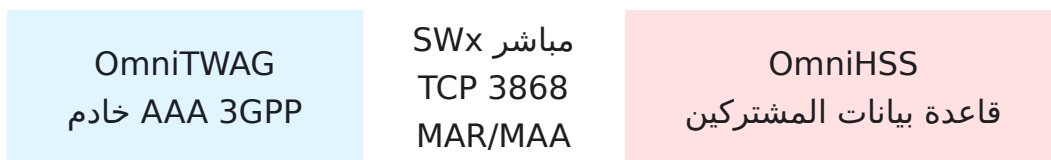


الفوائد:

- تنفيذ سياسة متسقة
- فوترة/محاسبة مركزية
- الأمان الخاصة بالشركات/VPN تطبيق سياسات
- والخلوية WiFi تنقل سلس بين

SWx خيارات اتصال

HSS الخيار 1: اتصال مباشر بـ

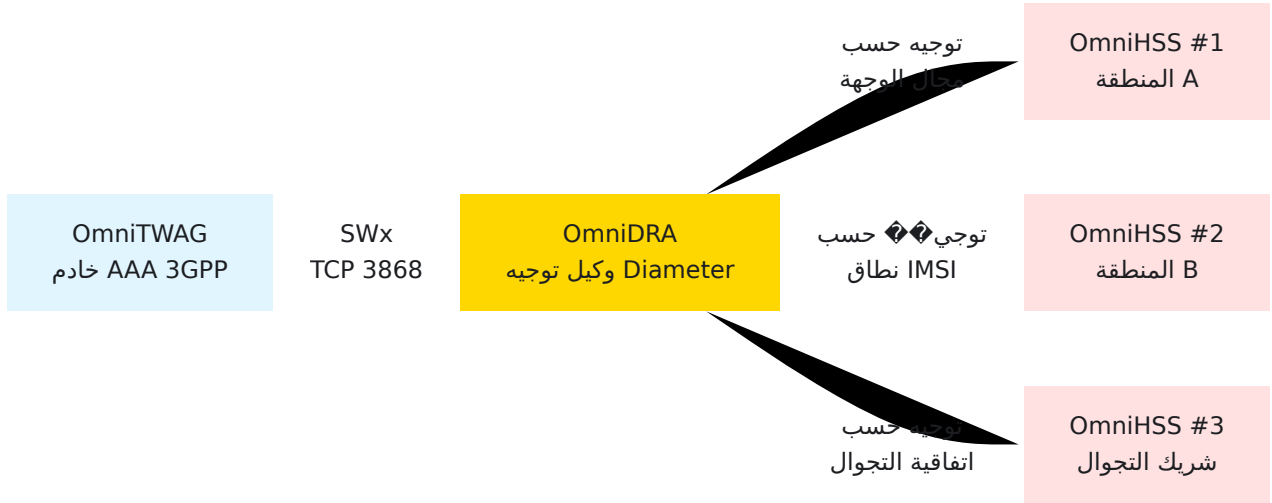


واحد HSS ، حالة الاستخدام: نشرات بسيطة، بيئات مختبرية

الفوائد:

- (DRA لا قفز عبر) زمن انتقال أقل
- تكوين مبسط
- سهولة استكشاف الأخطاء

Diameter وكيل توجيه) DRA الخيار 2: عبر



سيناريوهات التجوال، الشبكات الكبيرة، HSS حالة الاستخدام: نشرات متعددة

الفوائد:

- منطق توجيه مركزي
- متعددة HSS توازن الحمل عبر
- (المنزلية HSS توجيه إلى) دعم التجوال
- تكرار وفشل
- الالتصاق بالجلسة

تدفق الشحن

إلى نظام الشحن عبر Gy Diameter بالكامل لإرسال طلبات الشحن عبر TWAG يمكن تكامل (OCS) الإنترنت.

مقابل رصيد العميل، ويتم تسليمها عبر WiFi، يسمح ذلك بحاسبة جميع البيانات المستهلكة على DRA/OCS وإعادة توجيهها إلى TWAG بواسطة Gy وتحويلها إلى RADIUS على AP

TWAG في جميع الأوضاع، يتم تتبع الاستخدام بواسطة مقاييس

أوضاع الشحن

ثلاثة أوضاع شحن عبر الإنترنت TWAG يدعم:

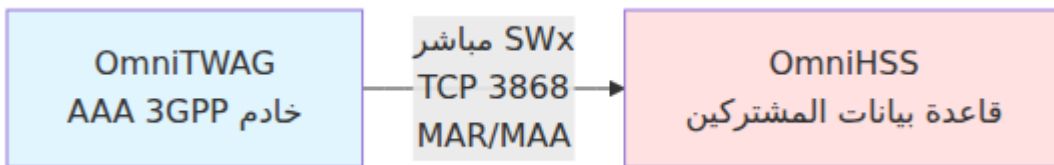
1. الشحن معطل

لا يتم إرسال طلبات التحكم في الائتمان. لا يتم إجراء تفويض للرصيد.

حالات الاستخدام:

- مفتوحة/مجانية WiFi شبكات
- بيئات مختبرية/اختبارية
- (إلى الفوترة RADIUS محاسبة) الشبكات التي تستخدم الشحن غير المتصل فقط

التدفق:



2. تفويض فقط

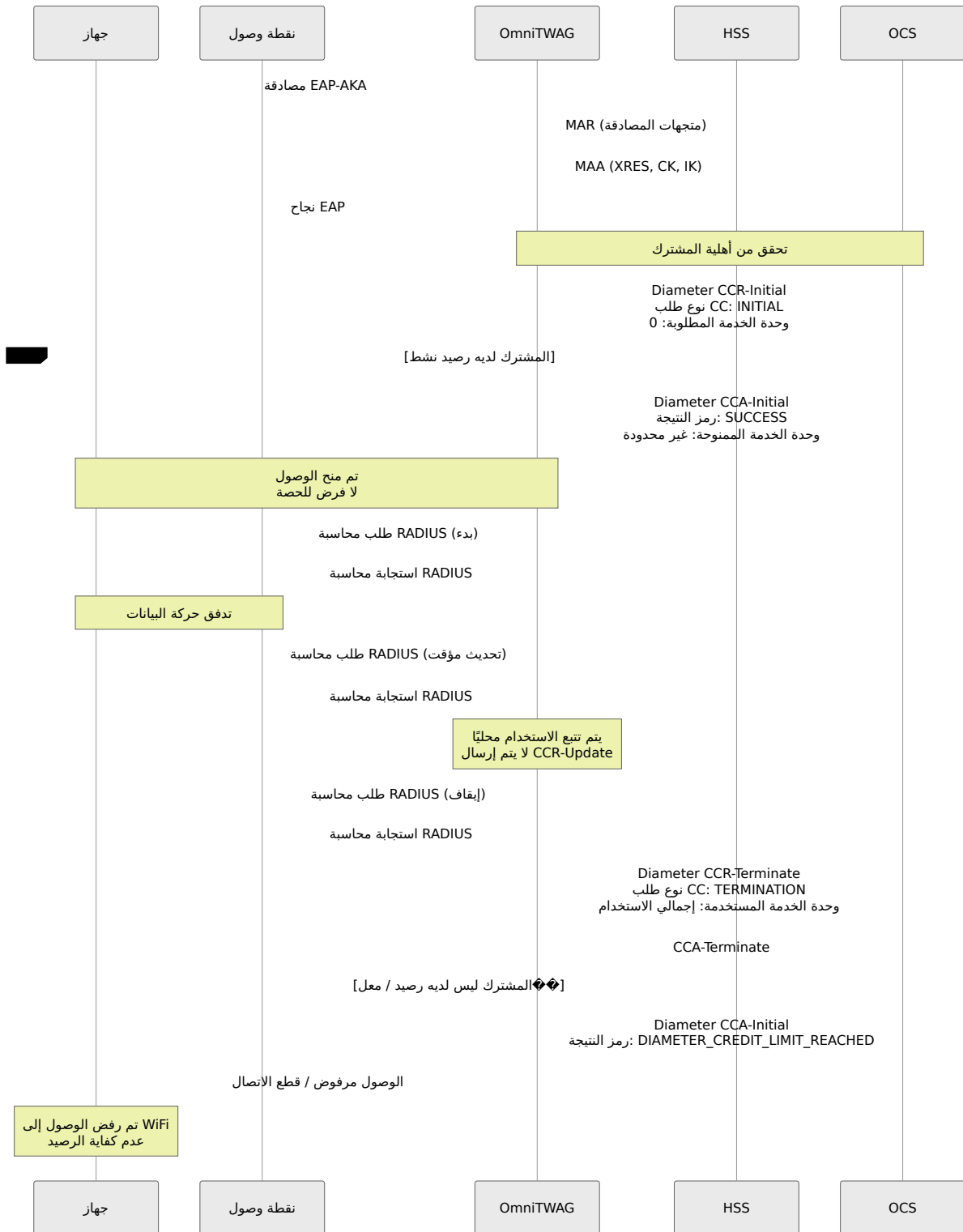
للتحقق من WiFi في بداية جلسة OCS إلى (طلب التحكم في الائتمان) CCR-Initial يتم إرسال أن المشترك لديه رصيد، ولكن لا يتم سحب الرصيد خلال الجلسة.

حالات الاستخدام:

- التحقق من أن المشترك لديه حساب/رصيد نشط

- للحسابات المعلقة WiFi منع الوصول إلى
- التحقق من أهلية الخدمة دون تتبع الحصة
- خدمة مكافأة/غير محدودة للعملاء الذين يدفعون WiFi السماح لـ

التدفق:



التكوين:

- (CCR-T) وعند الانتهاء (CCR-I) عند بدء الجلسة OCS يتم استعلام
- خلال الجلسة CCR-Update لا يتم إرسال رسائل
- يتم تفويض المشترك بناءً على حالة الحساب، وليس الحصة
- يتم الإبلاغ عن الاستخدام في نهاية الجلسة لأغراض إعلامية فقط

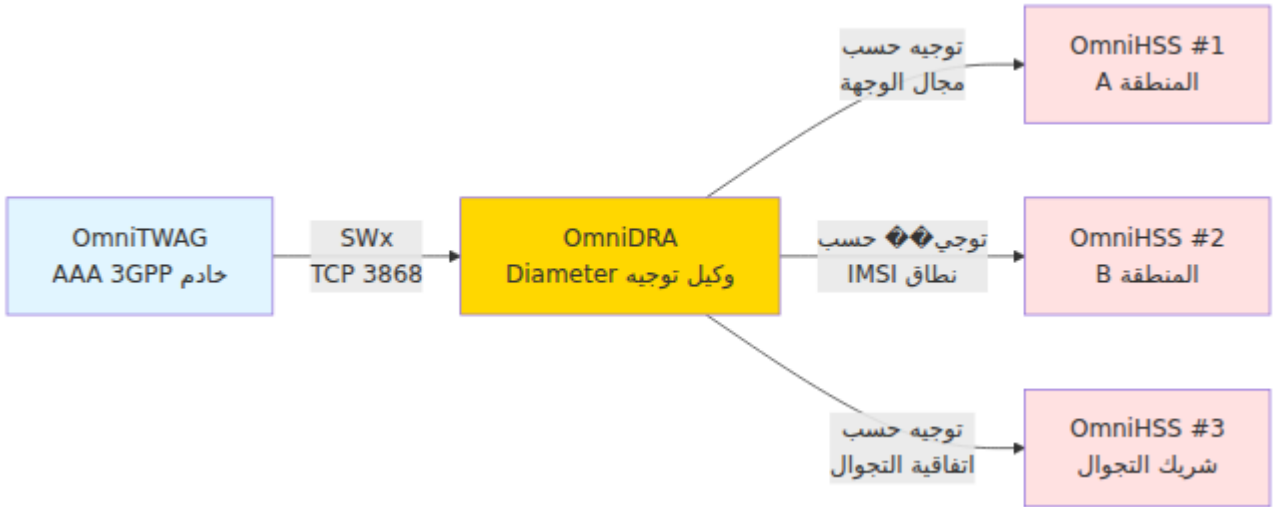
3. عبر الإنترنت بالكامل (تنفيذ كامل) Gy شحن

إلى WiFi يتم تمرير جميع الاستخدامات على GPP. يتم اتباع تدفق الشحن عبر الإنترنت القياسي 3 للشحن، ويتم قطع المشترك بمجرد تجاوزهم حصتهم OCS.

:حالات الاستخدام

- خدمات البيانات المدفوعة مسبقًا
- حسب الاستخدام WiFi
- (بدل شهري GB مثل، 10) خطط قائمة على الحصة
- شحن في الوقت الحقيقي وقطع الاتصال

:التدفق



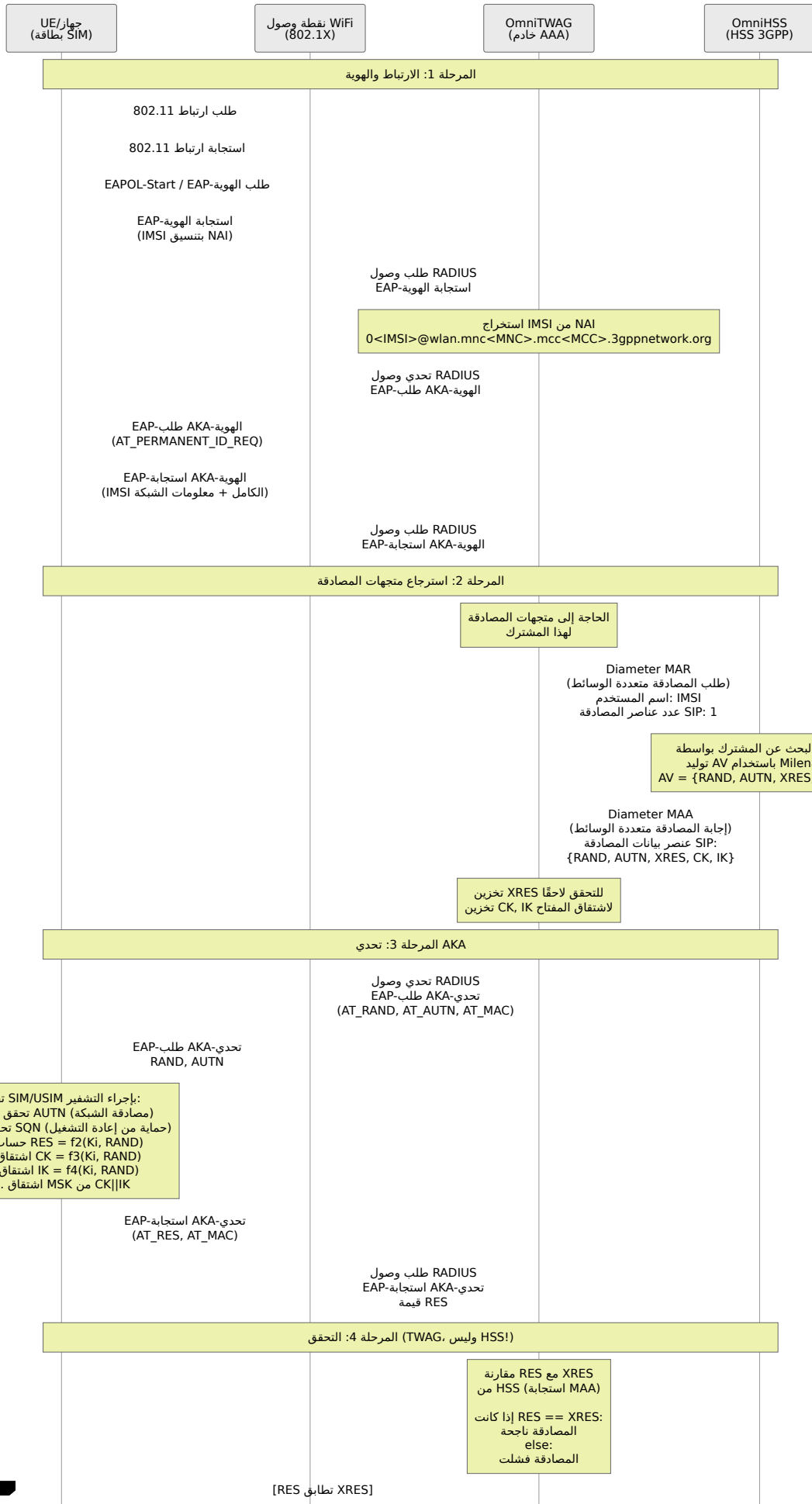
:التكوين

- وعند الانتهاء (CCR-U)، خلال الجلسة (CCR-I)، عند بدء الجلسة OCS يتم استعلام (CCR-T)
- (10 MB، 50MB، 100MB مثل، 10) يتم طلب الحصة في قطع قابلة للتكوين
- عند عتبة قابلة للتكوين (مثل، 80% من الحصة الممنوحة) CCR-Update يتم تفعيل
- يقوم مؤقت الصلاحية بتفعيل إعادة التفويض إذا لم يتم استنفاد الحصة
- قطع الاتصال القسري عند استنفاد الحصة

- خصم الرصيد في الوقت الحقيقي

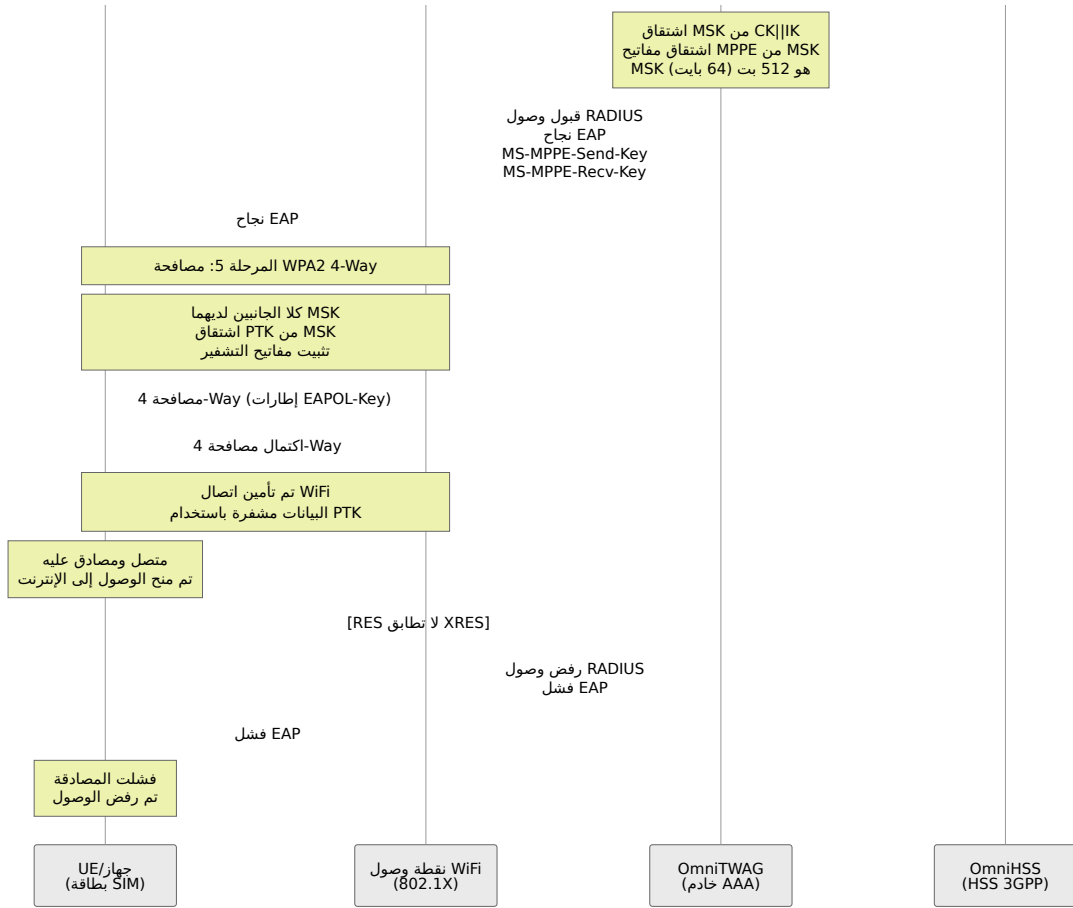
تدفق المصادقة

EAP-AKA تسلسل المصادقة الكامل



بإجراء التشفير SIM/USIM تقوم

1. (مصادقة الشبكة) AUTN تحقق من
2. (حماية من إعادة التشغيل) SQN تحقق من
3. حساب RES = f2(Ki, RAND)
4. اشتقاق CK = f3(Ki, RAND)
5. اشتقاق IK = f4(Ki, RAND)
6. اشتقاق MSK من CK||IK



النقاط الرئيسية في تدفق المصادقة

1. **MAR/MAA** هو نهاية الاتصال مع **HSS** بعد استلام **MAA** (إجابة المصادقة متعددة) مع **MAR/MAA**. جميع عمليات التحقق اللاحقة محليًا **TWAG** يتولى **XRES** مع (الوسائط).
2. **XRES** (الاستجابة المتوقعة **HSS** يوفر **RES** بإجراء التحقق من **TWAG** يقوم في هذه المقارنة **HSS** لا يشارك **UE** الفعلي من **RES** يقارنها مع **TWAG** لكن.
3. **HSS** هذا يختلف عن بعض المخططات التي تظهر **TWAG** تحدث المصادقة في **HSS** بإجراء **AAA** (TWAG) يقوم خادم **GPP** تقوم بالتحقق - في الهيكلية الفعلية لـ 3 المقارنة.

تنسيق الهوية

NAI: بتنسيق (IMSI) يستجيب الجهاز بهويته الدائمة

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

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

هو الهوية، وعادة ما يكون 0 ولكن قد يكون رقمًا آخر من رقم IMSI ملاحظة - الرقم الأول، قبل IMSI. الهواتف متعددة / SIM واحد لبطاقات

(MSK) مفتاح الجلسة الرئيسي

هو مفتاح تشفير بطول 512 بت (64 بايت) يتم اشتقاقه أثناء (MSK) مفتاح الجلسة الرئيسي WiFi. يعمل كمادة المفتاح الأساسية لتأمين اتصال EAP-AKA. مصادقة

اشتقاق MSK:

1. MSK بشكل مستقل باشتقاق نفس TWAG و UE يقوم كل من
2. SIM المحسوبة بواسطة CK/IK يشتق من UE
3. HSS المستلمة من CK/IK يشتق من TWAG
4. $MSK = PRF'(CK || IK, "Full Authentication", IMSI, \dots)$

استخدام MSK:

1. MSK أول 256 بت (32 بايت) من **PMK: اشتقاق**
2. PTK لاشتقاق PMK AP و UE يستخدم كل من **WPA2 4-Way مصادقة**
3. (TK) باستخدام المفتاح الزمني WiFi **تشفير البيانات**: يتم تشفير جميع إطارات بيانات من PTK

حاسم MSK لماذا:

- غير مشفرة WiFi ستكون حركة مرور، MSK **السرية**: بدون
- WiFi **السلامة**: يمنع التلاعب بإطارات
- WiFi بتشفير EAP **ربط المصادقة**: يربط مصادقة
- الجديد هجمات إعادة التشغيل MSK **حماية من إعادة التشغيل**: يمنع
- واحد على الآخرين MSK **سرية مثالية للأمام**: لا يؤثر اختراق

استعادة التزامن

:فإنه يبدأ عملية الاستعادة، (خارج التزامن SQN) إذا اكتشف الجهاز عدم تطابق في رقم التسلسل

1. (رمز المصادقة - التزامن) AUTS يحسب الجهاز
2. AT-AUTS مع EAP-AKA Synchronization-Failure يرسل
3. HSS إلى AUTS بإعادة توجيه TWAG يقوم

بإعادة تزامن رقم التسلسل وتوليد متجهات جديدة HSS يقوم 4.

تتم محاولة المصادقة مرة أخرى باستخدام متجهات جديدة 5.

هذا يكون شفافاً للمستخدم النهائي ولا يتطلب تدخل المشغل.

دليل التكوين

التكوين الرئيسي في وقت `config/` في دليل Elixir عبر ملفات تكوين TWAG يتم تكوين `config/runtime.exs` التشغيل موجود في

بالنسبة لنشر الإنتاج، يتم إدارة التكوين مركزياً. أدناه هو مرجع فقط، أي قيم تم تغييرها على عقدة الإنتاج ستفقد في المرة القادمة التي يتم فيها تشغيل التشغيل الآلي.

Diameter تكوين

موجود في `config :diameter_ex:`

```
config :diameter_ex,
  diameter: %{
    # اسم الخدمة لكتلة Diameter
    service_name: :omnitouch_twig,

    # Diameter المحلي لربط خدمة IP عنوان
    listen_ip: "10.5.198.200",

    # Diameter (القياسي هو 3868) المنفذ المحلي لاتصالات
    listen_port: 3868,

    # Diameter مضيف الأصل
    host: "omnitwig",

    # Diameter (يتطابق مع مجال شبكتك) مجال الأصل
    realm: "epc.mnc057.mcc505.3gppnetwork.org",

    # Diameter (HSS, DRA, خوادم AAA) أقران
    peers: [
      %{
        # Diameter مضيف الأصل للقرين
        host: "omni-hss01.epc.mnc057.mcc505.3gppnetwork.org",

        # Diameter مجال الأصل للقرين
        realm: "epc.mnc057.mcc505.3gppnetwork.org",

        # DRA مباشرة أو HSS (يمكن أن يكون) للقرين IP عنوان
        ip: "10.179.2.140",

        # المنفذ للقرين (القياسي هو 3868)
        port: 3868,

        # لآمان النقل TLS استخدام
        tls: false,

        # (:diameter_tcp أو :diameter_sctp) بروتوكول النقل
        transport: :diameter_tcp,

        # أو الانتظار حتى يتصل القرين (true) بدء الاتصال بالقرين
        (false)
        initiate_connection: true
      }
    ]
  }
}
```

```
]
}
```

3 يتبع **المجال** GPP TS 23.003تنسيق:

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

حيث:

- MNC = (057، مثل) رمز الشبكة المحمولة
- MCC = (505 لأستراليا) رمز الدولة المحمولة

للقرين للإشارة إلى IP قم بتكوين عنوان، OmniDRA لاستخدام **DRA ملاحظة حول استخدام** HSS بعد ذلك بتوجيه الرسائل إلى DRA سيقوم HSS بدلاً من الإشارة م❖❖ اشارة إلى DRA (إلخ، IMSI مجال الوجهة، نطاق) المناسب بناءً على قواعد التوجيه.

RADIUS تكوين

موجود في `config :omnitwag`:

```
config :omnitwag,  
  radius_config: %{\n    # RADIUS قائمة الشبكات الفرعية المسموح بها لمصادر عملاء  
    # قائمة فارغة = السماح للجميع (غير موصى به للإنتاج)  
    allowed_source_subnets: ["10.7.15.0/24", "192.168.1.0/24"],\n\n    # RADIUS السر المشترك لعملاء  
    # يجب أن تستخدم جميع نقاط الوصول هذا السر  
    secret: "YOUR_STRONG_SECRET_HERE"\n  }\n}
```

أفضل ممارسات الأمان:

- مشتركة قوية (+20 حرف) RADIUS استخدم أسرار
- AP لتقييد وصول `allowed_source_subnets` قم بتكوين
- استخدم قواعد جدار الحماية لتقييد الوصول إلى المنافذ 1812/1813

مثال على تكوين الشبكة الفرعية:

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

إذا كانت فارغة، يُسمح بجميع المصادر (مناسب فقط للمختبر/الاختبار).

Prometheus تكوين مراقبة

موجود في config :omnitwag:

```
config :omnitwag,  
  prometheus: %{\n    # Prometheus المنفذ لنقطة نهاية مقاييس  
    port: 9568\n  }\n}
```

الوصول إلى المقاييس على: <http://<twag-ip>:9568/metrics>

ملخص المنافذ

المنفذ	البروتوكول	الغرض
1812	UDP	RADIUS مصادقة
1813	UDP	RADIUS محاسبة
3868	TCP	Diameter (HSS/DRA إلى SWx)
443	TCP	HTTPS لوحة معلومات
8444	TCP	REST HTTPS واجهة برمجة التطبيقات
9568	TCP	Prometheus مقاييس

إعداد نقطة الوصول

نقاط الوصول المدعومة

تدعم WiFi مع أي نقطة وصول OmniTWAG يعمل:

- **WPA2-Enterprise** (802.1X مصادقة)
- **RADIUS** وظيفة عميل
- **EAP-AKA** طريقة المصادقة

نقاط الوصول المعتمدة، Cisco Aironet، Aruba، Ubiquiti UniFi، Ruckus، المنصات المختبرة على hostapd

العام AP متطلبات تكوين

1. **WPA2-Enterprise (802.1X)** وضع الأمان
2. **TWAG** ل IP يشير إلى عنوان **RADIUS** خادم
3. **RADIUS: 1812** منفذ مصادقة
4. **RADIUS: 1813** منفذ محاسبة (اختياري ولكن موصى به)
5. **RADIUS: السر المشترك ل** TWAG يجب أن يتطابق مع تكوين
6. **EAP: EAP-AKA** ("أو" الكل) طريقة

Cisco من AP مثال على تكوين

CLI: تكوين

```
! RADIUS تكوين خادم !  
radius-server host 10.5.198.200 auth-port 1812 acct-port 1813 key  
YOUR_SHARED_SECRET
```

```
! مع 802.1 SSID تكوين !  
dot11 ssid OPERATOR-WIFI  
    vlan 10  
    authentication open eap eap_methods  
    authentication network-eap eap_methods  
    authentication key-management wpa version 2
```

```
! بواجهة الراديو SSID ربط !  
interface Dot11Radio0  
    encryption mode ciphers aes-ccm  
    ssid OPERATOR-WIFI
```

واجهة الويب:

1. **RADIUS** خادم → **AAA** → انتقل إلى **الأمان**
2. مع السر المشترك **10.5.198.200:1812** أضف خادم RADIUS
3. **WLAN** انتقل إلى تكوين
4. **WPA2-Enterprise** اضبط الأمان على
5. أو الكل **EAP-AKA** على EAP اضبط طريقة
6. RADIUS قم بتعيين مجموعة خادم

hostapd مثال على تكوين

(الأنظمة المدمجة، OpenWrt) Linux للنقاط الوصول المعتمدة على

```
# /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

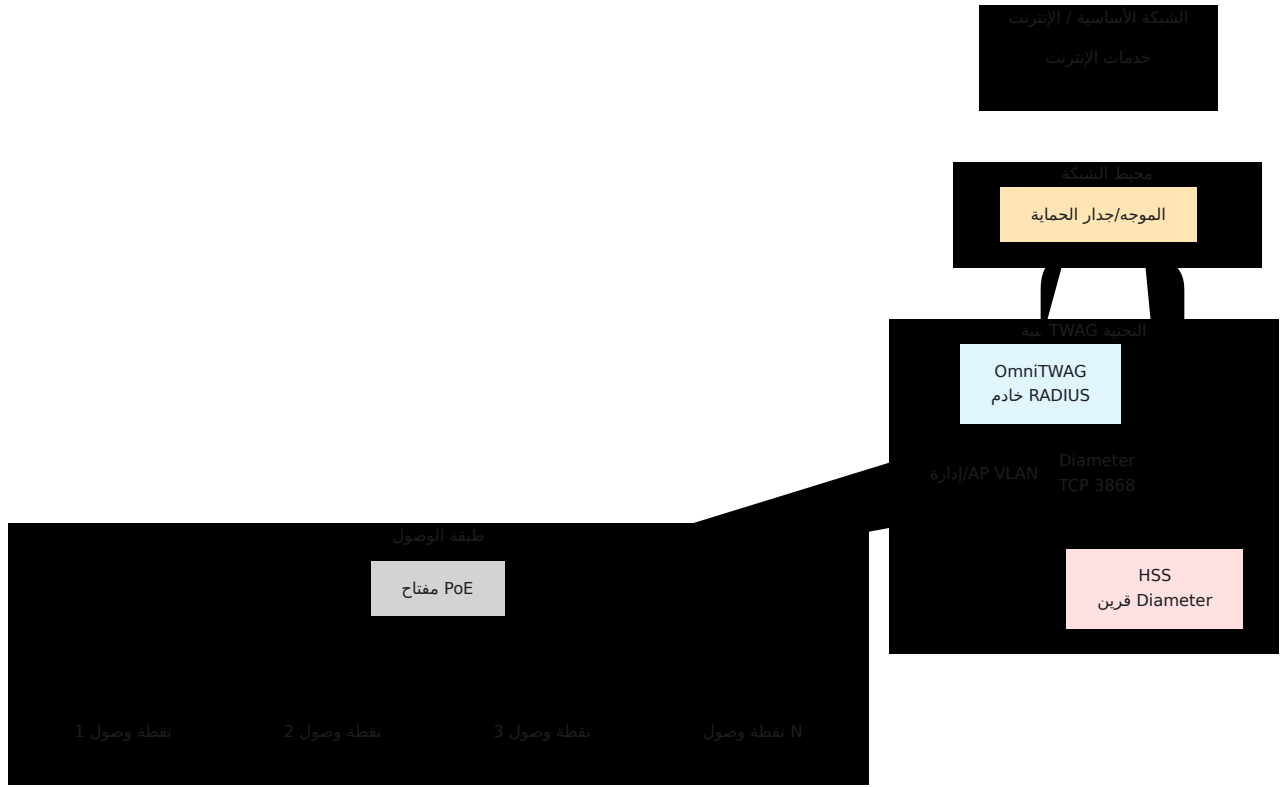
# تكوين RADIUS
auth_server_addr=10.5.198.200
auth_server_port=1812
auth_server_shared_secret=YOUR_SHARED_SECRET

acct_server_addr=10.5.198.200
acct_server_port=1813
acct_server_shared_secret=YOUR_SHARED_SECRET

# تكوين EAP
eap_server=0

# Hotspot 2.0 (اختياري - للتحميل التلقائي)
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
```

أفضل ممارسات بنية الشبكة



:في مقاطع شبكة موثوقة. استخدم قواعد جدار الحماية لـ TWAG و APS **مهم**: ضع

- TWAG 1812/1813 بالوصول إلى منافذ APS السماح فقط لـ
- HSS 3868 بالوصول إلى منفذ TWAG السماح لـ
- (المنفذ 443) TWAG تقييد الوصول الإداري إلى لوحة معلومات

Hotspot 2.0 تكامل

Hotspot 2.0 (Passpoint) نظرة عامة على

يمكن WiFi هو معيار من تحالف (أو 802.11 Passpoint المعروف أيضًا باسم) Hotspot 2.0 اكتشاف الشبكات اللاسلكية الآمنة والتوصيل التلقائي دون تدخل المستخدم. إنها التقنية الرئيسية السلس WiFi لتحميل.

:الميزات الرئيسية

- **اكتشاف الشبكة التلقائي**: يجد الجهاز الشبكات المتوافقة بناءً على المعايير
- دون إدخال المستخدم (EAP-AKA) SIM **المصادقة التلقائية**: يستخدم بيانات اعتماد

- للتزويد الآمن (OSU المصادقة فقط من خادم) OSEN: **الارتباط الأولي المشفر**
- **اتفاقيات التجوال**: تدعم الشبكات التي تمت زيارتها (مثل التجوال الخلوي)
- **الأولوية**: يفضل الجهاز الشبكات المملوكة للمشغل

Hotspot 2.0 لـ AP تكوين

AP متطلبات

1. ANQP قدرة استعلام/استجابة: **u دعم 802.11**
2. **WPA2-Enterprise**: 802.1X مصادقة
3. EAP-AKA يجب أن يدعم طريقة: **EAP-AKA دعم**
4. الإعلان عن معلومات المشغل الصحيحة: **ANQP تكوين**

hostapd المعتمد على AP) مثال على التكوين:

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

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

# تكوين مجال NAI
nai_realm=0,wlan.mnc057.mcc505.3gppnetwork.org,0,21[2:1][5:7]
# معرف- المصادقة: قيمة- [eap-التنسيق: <الترميز>, <المجال>, <طريقة
المصادقة]
# 21 = EAP-AKA
# 2:1 = نوع الاعتماد: SIM
# 5:7 = (مباشر EAP-AKA) الموجهة: لا شيء EAP طريقة
# اتحاد التجوال
roaming_consortium=505057
# MCC=505 (الولايات المتحدة), MNC=057 (محدد للمشغل)
# معلومات المكان (اختياري)
venue_group=1
venue_type=8
venue_name=eng: العامة للمشغل WiFi شبكة
# تكوين WPA2-Enterprise
wpa=2
wpa_key_mgmt=WPA-EAP
rsn_pairwise=CCMP
ieee8021x=1
# تكوين RADIUS (يشير إلى 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
```

```
# تكوين SSID
ssid=OperatorWiFi
utf8_ssid=1

# إشارة Hotspot 2.0
hs20=1
hs20_oper_friendly_name=eng:للمشغل WiFi شبكة
```

سلوك التحميل التلقائي

كيف يعمل التحميل التلقائي:

1. دوري WiFi بإجراء مسح Passpoint يقوم الجهاز الذي يحتوي على ملف تعريف
2. إلى نقاط الوصول المكتشفة ANQP يرسل استعلام
3. (اتحاد التجوال، MCC/MNC) تتطابق مع الملف الشخصي ANQP إذا كان استجابة:
 - تكون الأولوية عالية (◆◆) لشبكة المنزلية) أو متوسطة (شريك التجوال)
4. إذا كانت الأولوية \leq العتبة والإشارة $<$ الحد الأدنى:
 - تلقائية EAP-AKA مصادقة
5. إذا كانت المصادقة ناجحة والأولوية $<$ الاتصال الحالي:
 - قطع بيانات الخلوية، WiFi التحويل إلى
6. مراقبة جودة الإشارة والحفاظ على الاتصال

عوامل الأولوية:

1. (MCC/MNC مطابقة) **الشبكة المنزلية مقابل التجوال**: تفضل الشبكة المنزلية على التجوال
 2. **قوة الإشارة**: تفضل الإشارة الأقوى
 3. WPA2-PSK/على الشبكة المفتوحة WPA2-Enterprise **الأمان**: تفضل
 4. **السياسة**: يمكن للمشغل تكوين الشبكات المفضلة
 5. يدويًا أو تفضيل الخلوية WiFi **تجاوز المستخدم**: يمكن للمستخدم تعطيل
-

المراقبة والإدارة

لوحة المعلومات على الويب

الوصول إلى لوحة المراقبة في الوقت الحقيقي على <https://<twag-ip>/>

الميزات:

- المشتركين النشطين، حالة المصادقة، تفاصيل الجلسة: **RADIUS عرض عملاء**
- SSID عرض نقاط الوصول:** نقاط الوصول المتصلة، عدد العملاء، معلومات
- عرض استخدام العميل:** بيانات المحاسبة، وقت الجلسة، استخدام البيانات
- Diameter عرض أقران:** HSS/DRA حالة الاتصال بـ

Prometheus تكامل

TWAG لالتقاط مقاييس Prometheus قم بتكوين

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

المقاييس المتاحة:

RADIUS مقاييس خادم

- `radius_access_request_count` - المستلمة RADIUS إجمالي حزم طلب وصول
- `radius_access_accept_count` - إجمالي حزم قبول الوصول المرسله
- `radius_access_reject_count` - إجمالي حزم رفض الوصول المرسله
- `radius_access_challenge_count` - إجمالي حزم التحدي المرسله
- `radius_accounting_request_count{status_type}` - إجمالي حزم طلب المحاسبة (موسومة حسب الحالة: بدء، إيقاف، تحديث مؤقت، محاسبة قيد التشغيل، محاسبة متوقفة)

- `radius_active_clients_count` - العملاء المصادق عليهم حاليًا (يتم الاستطلاع - كل 5 ثوانٍ)
- `radius_access_points_count` - نقاط الوصول المسجلة (يتم الاستطلاع كل 5 ثوانٍ)

EAP-AKA: مقاييس مصادقة

- `eap_aka_identity_count` - EAP-AKA تبادلات هوية
- `eap_aka_challenge_count` - EAP-AKA تبادلات تحدي
- `eap_aka_sync_failure_count` - أحداث إعادة تزامن (حالات فشل التزامن - SQN)
- `eap_aka_auth_success_count` - المصادقات الناجحة
- `eap_aka_auth_reject_count` - المصادقات المرفوضة

Diameter: مقاييس بروتوكول

- `diameter_message_count{application, command, direction}` - إجمالي (موسومة حسب التطبيق، نوع الأمر، والاتجاه) رسائل Diameter

VM Erlang: مقاييس ذاكرة

- `vm_memory_total` - إجمالي كمية الذاكرة المخصصة (بايت)
- `vm_memory_processes` - Erlang الذاكرة المستخدمة بواسطة عمليات
- `vm_memory_processes_used` - Erlang الذاكرة المستخدمة بواسطة عمليات باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_system` - Erlang الذاكرة المستخدمة بواسطة نظام تشغيل
- `vm_memory_atom` - الذاكرة المستخدمة بواسطة الذرات (بايت)
- `vm_memory_atom_used` - الذاكرة المستخدمة بواسطة الذرات باستثناء الذاكرة المخصصة غير المستخدمة (بايت)
- `vm_memory_binary` - الذاكرة المستخدمة بواسطة الثنائيات (بايت)
- `vm_memory_code` - الذاكرة المستخدمة بواسطة الكود المحمل (بايت)
- `vm_memory_ets` - ETS الذاكرة المستخدمة بواسطة جداول (بايت)

VM Erlang: مقاييس نظام

- `vm_system_info_process_count` - Erlang العدد الحالي لعمليات
- `vm_system_info_port_count` - العدد الحالي للمنفذ

- `vm_system_info_atom_count` - العدد الحالي للذرات
- `vm_system_info_schedulers` - عدد خيوط الجدول
- `vm_system_info_schedulers_online` - عدد الجدولين المتصلين حاليًا

VM Erlang مقاييس جدول

- `vm_statistics_run_queue` - الطول الإجمالي لجميع قوائم التشغيل
- `vm_total_run_queue_lengths_total` - الطول الإجمالي لجميع قوائم التشغيل (المجدولين الإجماليين)
- `vm_total_run_queue_lengths_cpu` - الطول الإجمالي لقوائم تشغيل الجدول CPU
- `vm_total_run_queue_lengths_io` - IO الطول الإجمالي لقوائم تشغيل الجدول

جمع المقاييس:

- في الوقت الحقيقي عند حدوث الأحداث EAP-AKA و RADIUS يتم إصدار مقاييس
- يتم استطلاع عدد العملاء ونقاط الوصول النشطة كل 5 ثوانٍ
- Erlang كل 5 ثوانٍ من وقت تشغيل VM يتم استطلاع مقاييس
- على Prometheus يتم عرض جميع المقاييس بتنسيق `http://<twag-ip>:9568/metrics`

السجلات

.للتسجيل المنظم Elixir مسجل TWAG يستخدم

(systemd): عرض السجلات

```
# ذيل السجل في الوقت الحقيقي  
journalctl -u twag -f
```

```
# آخر 100 سطر  
journalctl -u twag -n 100
```

```
# السجلات منذ آخر تشغيل  
journalctl -u twag -b
```

```
# السجلات لفترة زمنية محددة  
journalctl -u twag --since "2025-10-12 10:00:00" --until "2025-10-12 11:00:00"
```

رسائل السجل الرئيسية:

- يستمع على المنفذ 1812 - بدء تشغيل الخادم RADIUS خادم
- AP من RADIUS تم استلام طلب الوصول - طلب {IP} من
- EAP المرحلة 1: استجابة الهوية - الهوية الأولية
- التحدي المرسل إلى الجهاز - AKA المرحلة 2: تحدي
- المصادقة مقبولة - المصادقة الناجحة
- المصادقة مرفوضة - فشلت المصادقة
- جديدة AP تم اكتشاف - {IP} : مسجلة AP

استكشاف الأخطاء وإصلاحها

فشل المصادقة

WiFi العرض: لا يمكن للعميل الاتصال بشبكة

خطوات التشخيص:

1. TWAG: تحقق من سجلات `journalctl -u twag -f`
2. TWAG و AP يتطابق بين RADIUS تحقق من أن السر المشترك لـ
3. TWAG إلى RADIUS تأكد من وصول حزم `tcpdump -i eth0 port 1812`
4. التكوين/HSS تحقق من توفير المشترك في

الأسباب الشائعة:

- غير صحيح RADIUS السر المشترك لـ
- جدار الحماية يمنع UDP 1812/1813
- (خاطئ HSS أو تكوين Ki) RES/XRES عدم تطابق
- خارج التزامن (يجب أن يتعافى تلقائيًا عبر إعادة التزامن) (SQN) رقم التسلسل
- AP و TWAG مشاكل الاتصال الشبكي بين

Diameter مشاكل اتصال

HSS/DRA Diameter العرض: عدم اتصال القرين

خطوات التشخيص:

1. تحقق من الاتصال الشبكي: `telnet <hss-ip> 3868`
2. (القرين IP، مضيف الأصل، مجال الأصل) Diameter تحقق من تكوين
3. لمحاولات الاتصال HSS/DRA راجع سجلات
4. TCP 3868 تحقق من أن جدار الحماية يسمح

الأسباب الشائعة:

- المنفذ غير صحيح للقرين في التكوين/IP
- جدار الحماية يمنع TCP 3868
- عدم تطابق مضيف الأصل/المجال
- TWAG لا تقبل الاتصال من HSS/DRA

مشاكل الأداء

العرض: مصادقة بطيئة (<5 ثوانٍ)

خطوات التشخيص:

1. HSS تحقق من وقت استجابة
2. قياس زمن الانتقال الشبكي: `ping <hss-ip>`, `mtr <hss-ip>`
3. TWAG مراقبة استخدام موارد: `top`, `htop`
4. Diameter مراجعة إعدادات مهلة طلب

الأسباب الشائعة:

- أو استجابة بطيئة HSS مهلة استعلام
- زمن انتقال شبكي مرتفع
- (ذاكرة/CPU) TWAG استنفاد موارد
- عدد كبير جدًا من المصادقات المتزامنة

أدوات التصحيح

التقاط الحزم

```
# RADIUS التقاط حركة مرور
tcpdump -i eth0 -n port 1812 or port 1813 -w radius.pcap

# Diameter التقاط حركة مرور
tcpdump -i eth0 -n port 3868 -w diameter.pcap

# محدد AP الالتقاط من
tcpdump -i eth0 -n host 10.7.15.72 and port 1812 -w radius-
ap1.pcap
```

(Diameter و RADIUS يدعم محللات) Wireshark تحليل باستخدام.

وحدة التحكم التفاعلية

الجاري للتصحيح المباشر TWAG الارتباط بـ:

```
# الجاري TWAG قشرة عن بُعد إلى
iex --sname debug --remsh twag@hostname --cookie <cookie>
```

من IEx وحدة التحكم:

```
# قائمة بجميع العملاء المصادق عليهم  
CryptoState.keys()
```

```
# الحصول على حالة عميل محدد  
CryptoState.get("0505338057900001867@wlan.mnc057.mcc505.3gppnetwork.c
```

```
# قائمة بجميع APs  
APState.list()
```

```
# قائمة بجلسات المحاسبة  
ClientUsage.list()
```

رسائل الخطأ الشائعة

رسالة الخطأ	المعنى	الحل
فشل التحقق من مصادق الرسالة	عدم تطابق السر المشترك	تحقق من أن السر المشترك AP يتطابق على RADIUS و TWAG
متوقع RES: فشل التحقق من <XRES>، حصلت على <RES>	استجابة المصادقة غير صحيحة	تحقق من SIM، Ki تحقق من HSS من توفير
Diameter مهلة اتصال القرين	لا يمكن الوصول إلى HSS	تحقق من الشبكة، جدار HSS الحماية، تكوين
EAP فشل في فك تشفير رسالة	EAP حزمة مشوهة	تحقق من البرنامج الثابت لـ AP قد تحتاج إلى تحديث، AP
غير معروف EAP-AKA نوع	EAP- AKA رسالة غير مدعومة	يستخدم الجهاز إصدار غير EAP-AKA قياسي من
يتطلب إعادة تزامن رقم التسلسل	خارج SQN التزامن	طبيعي، سيقوم الجهاز بإعادة التزامن تلقائيًا

الاستشارة للمعايير

IETF و GPP المواصفات التالية من 3 OmniTWAG يطبق:

- **3GPP TS 23.402:** GPP تحسينات المعمارية للوصول غير 3
- **3GPP TS 24.302:** GPP عبر الشبكات غير 3 EPC الوصول إلى
- **3GPP TS 29.273:** Diameter المعتمدة على SWx/SWm واجهات
- **3GPP TS 33.402:** GPP جوانب الأمان للوصول غير 3
- **3GPP TS 35.206:** Milenage مواصفة خوارزمية
- **RFC 2865:** RADIUS مصادقة
- **RFC 2866:** RADIUS محاسبة
- **RFC 3579:** RADIUS ل EAP دعم
- **RFC 4187:** EAP-AKA بروتوكول المصادقة
- **RFC 5448:** EAP-AKA' (الإصدار المحسن)

الملخص

3GPP WiFi حلاً كاملاً متوافقاً مع المعايير لتحميل، **Omnitouch** الذي أنشأته، OmniTWAG يوفر:

1. **نشر مرّن:** يدعم الانفصال المحلي أو حركة المرور الموجهة إلى المنزل.
2. **RADIUS و EAP-AKA و GPP SWx معتمد على المعايير:** ينفذ بروتوكولات 3.
3. **مع إعادة تزامن تلقائية SIM مصادقة آمنة:** مصادقة متبادلة تعتمد على.
4. **WPA2 توفر تشفير MSK تشفير قوي:** مفاتيح مشتقة من.
5. **يمكنّ التحميل التلقائي بالكامل بدون لمس: Hotspot 2.0 جاهز لـ.**
6. **تحكم المشغل:** يحافظ على الهوية، والسياسة، وخيار الفوترة.
7. **للتوجيه/توازن الحمل OmniDRA أو عبر HSS اتصال مرّن:** اتصال مباشر بـ.

حقوق WiFi بوابة الوصول الموثوقة لشبكة - OmniTWAG نسخة الوثيقة: 2.0 آخر تحديث: 2025
جميع الحقوق محفوظة. Omnitouch. الطبع والنشر © 2025