بنية OmniTWAG

نظرة عامة

OmniTWAG هو بوابة وصول WLAN موثوقة (TWAG) 3 وفقًا لمعيار 3GPP TS 23.402 القسم 16. تقوم بربط نقاط الوصول WLAN الموثوقة في النواة المتطورة للحزم (EPC)، مقدمةً المصادقة، إدارة الجلسات، ونفق البيانات.

جدول المحتويات

- بنية المكونات والعمليات
- شجرة الإشراف
- مرجع المكونات
- أنماط التشغيل
- تكامل AP (نفق GRE)
- سلوك DHCP
- المصادقة
- دورة حياة الجلسة (موجهة للمنزل)
- واجهات Diameter
- ملخص التكوين
- اشتقاق المفاتيح
- صفحات ذات صلة

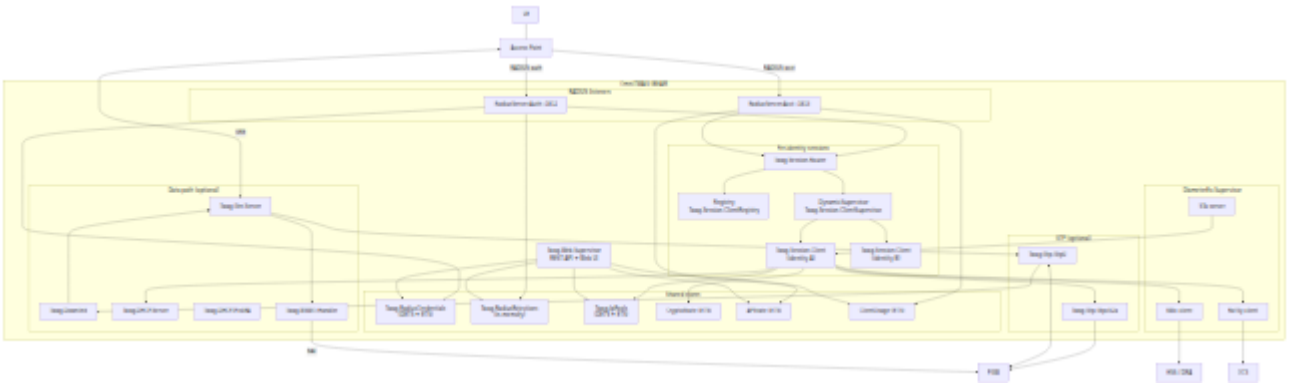
بنية المكونات والعمليات

يعمل OmniTWAG كتطبيق BEAM (Erlang VM) واحد. يبدأ المشرف الأعلى مجموعة ثابتة من الخدمات المشتركة، وبناءً على التكوين، مجموعة من الأطفال الاختياريين لمسار البيانات والواجهة. تعيش حالة كل مشترك في GenServer واحد لكل هوية، يتم إنشاؤه عند الطلب.

المجموعات الرئيسية هي:

- **الويب وإدارة العمليات**: واجهة برمجة التطبيقات REST وواجهة الويب (`Twag.Web.Supervisor`).

- **الجلسات حسب الهوية**: GenServer واحد `Twag.Session.Client` لكل مشترك، يتم العثور عليه من خلال `Registry` ويبدأ بواسطة `DynamicSupervisor`. يقوم `Twag.Session.Router` بعملية البحث أو الإنشاء.
- **المخازن المشتركة**: `Twag.RadiusCredentials` (أسرار مشتركة دائمة)، `Twag.RadiusRejections` (مصادر مرفوضة في الذاكرة)، `Twag.IpPools` (مجموعات العناوين)، و `ClientUsage` و `APState` و `CryptoState` المدعومة بـ ETS.
- **مستمعي RADIUS**: `RadiusServer.Auth` (المنفذ 1812) و `RadiusServer.Acct` (المنفذ 1813).
- **Diameter**: `DiameterEx.Supervisor` يحمل أقران SWx (متجهات المصادقة)، STa (إعادة المصادقة والإلغاء)، و Ro/Gy (الشحن عبر الإنترنت).
- **GTP**: `Twag.Gtp.GtpU` (نائرة المستخدم)، و `Twag.Gtp.GtpcS2a` (التحكم) تبدأ فقط عندما تكون `gtp.enabled` صحيحة.
- **مسار البيانات**: `Twag.Gre.Server`، `Twag.Downlink`، `Twag.DHCP.Server`، `Twag.DHCP.IPv6RA`، و `Twag.NSWO.Handler`، كل منها يبدأ فقط عندما يتم تمكين كتلة تكوينه.



شجرة الإشراف

يستخدم المشرف الجذري استراتيجية `:one_for_one` (60 إعادة تشغيل في 10 ثانية). تبدأ الأطفال بهذا الترتيب، بحيث يتم حل الأسرار حسب عنوان المصدر قبل وصول IP أول حزمة RADIUS:



الأطفال المميزون بـ `*` يبدأون فقط عندما يتم تمكين كتلة تكوينهم (انظر ملخص التكوين).

مرجع المكونات

المكون	النوع	يبدأ عند
`Twag.Web.Supervisor`	مشرف	دائمًا
`DiameterEx.Supervisor`	مشرف	دائمًا
`Twag.Session.ClientRegistry`	سجل	دائمًا
`Twag.Session.ClientSupervisor`	DynamicSupervisor	دائمًا
`Twag.Session.Router`	وحدة	عند الطلب
`Twag.Session.Client`	GenServer	حسب الهوية
`Twag.RadiusCredentials`	GenServer	دائمًا
`Twag.RadiusRejections`	GenServer	دائمًا

المكون	النوع	يبدأ عند
`Twag.IpPools`	GenServer	دائمًا
`RadiusServer.Auth`	GenServer	دائمًا
`RadiusServer.Acct`	GenServer	دائمًا
`CryptoState`	GenServer (ETS)	دائمًا
`APState`	GenServer (ETS)	دائمًا
`ClientUsage`	GenServer (ETS)	دائمًا
`Twag.Gtp.GtpcS2a`	GenServer	`gtp.enabled`

المكون	النوع	يبدأ عند
`Twag.Gtp.GtpU`	GenServer	`gtp.enabled`
`Twag.Downlink`	GenServer	`downlink.enabled`
`Twag.Gre.Server`	GenServer	`gre.enabled`
`Twag.DHCP.Server`	GenServer	`dhcp.enabled`
`Twag.DHCP.IPv6RA`	GenServer	`ipv6_ra.enabled`
`Twag.NSWO.Handler`	GenServer	`nswo.enabled`

أنماط التشغيل

يدعم OmniTWAG اعتماد AP نمطين لطائرة البيانات. يتم حل النمط المستخدم لجلسة من بيانات المطابقة (انظر أسرار RADIUS المشتركة)، مع تكوين `gtp` / `nswo` العالمي كافتراضي.

نمط موجه للمنزل (نفق GTP)

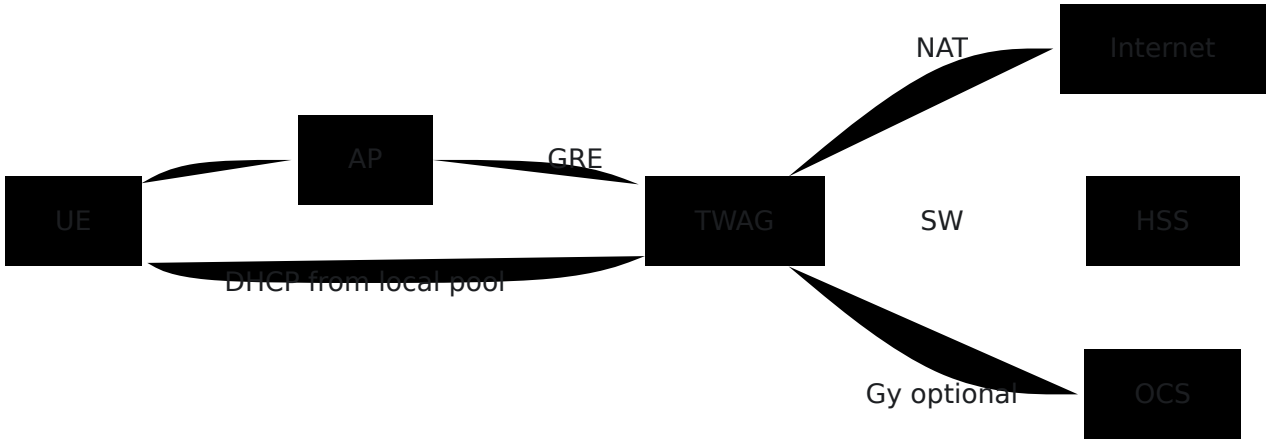
يتم نفق الحركة عبر GTP-C/GTP-U (واجهة S2a) إلى PGW. يقوم PGW بتخصيص عنوان IP لـ UE، ويطبق السياسة/الشحن، ويوفر الوصول إلى الإنترنت.



- **عنوان UE IP**: يتم تخصيصه بواسطة PGW في استجابة إنشاء الجلسة (PAA IE).
- **تسليم IP**: يقدم TWAG DHCP إلى UE عبر GRE، معطياً عنوان PGW المخصص.
- **الرفع**: يرسل AP حركة UE عبر GRE. يقوم TWAG بتغليفها في GTP-U إلى PGW.
- **الانخفاض**: يرسل PGW عبر GTP-U. يقوم TWAG بفك التغليف ويرسل عبر GRE إلى AP، ثم إلى UE.
- **الشحن**: يتم التعامل معه بواسطة PGW (PCEF) عبر Gy إلى OCS.
- **التكوين**: `gtp.enabled: true`، `gre.enabled: true`.

نمط الانفصال المحلي (NSWO)

تخرج الحركة مباشرة من TWAG إلى الإنترنت. لا يشارك PGW. يقوم TWAG بتنفيذ NAT/تخفي ويقوم اختياراً بإجراء شحنه عبر الإنترنت عبر Gy.



- **عنوان UE IP**: يتم تخصيصه من مجموعة IP المحلية لـ TWAG (`Twag.IpPools`).
- **تسليم IP**: يقدم TWAG DHCP إلى UE عبر GRE، من المجموعة.
- **الرفع**: يرسل AP عبر GRE. يقوم TWAG بتطبي NAT إلى الإنترنت.
- **الانخفاض**: يعود مسار الإنترنت عبر NAT TWAG، ثم GRE إلى AP، ثم إلى UE.
- **الشحن**: يعمل TWAG كـ PCEF عبر Gy إلى OCS (اختياري، معطل بشكل افتراضي). انظر الشحن عبر الإنترنت.
- **التكوين**: `nswo.enabled: true`، `gtp.enabled: false`.

يتم اختيار الانفصال المحلي عن طريق تعيين `nswo.enabled: true` (مع `gtp.enabled: false`)، أو لكل AP بواسطة بيانات الاعتماد `breakout_type`. عند التمكين، يتم بدء معالج PGW، ويتم رفع NSWO، ويتم منح الجلسات عنوانًا من مجموعة محلية بدلاً من عنوان مخصص من NAT/تخفي مباشرة إلى الإنترنت. انظر طائرة المستخدم ومسار البيانات لتفاصيل مسار البيانات.

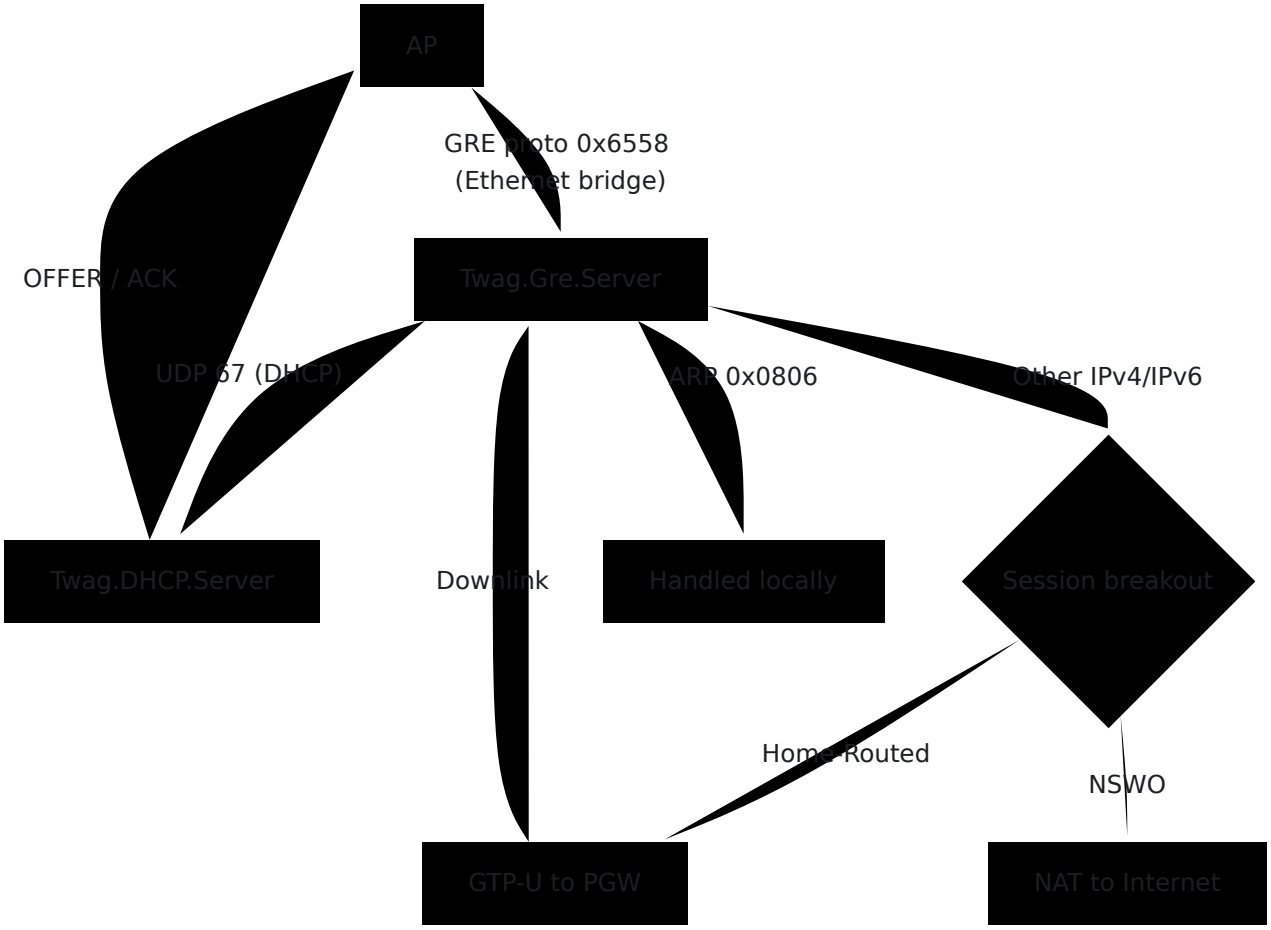
تكامل AP (نفق GRE)

يقوم AP بنفق إطارات L2 الخاصة بـ UE إلى TWAG عبر GRE (بروتوكول IP 47). يوفر هذا الرابط المطلوب بين UE وTWAG وفقًا لمعيار TS 23.402 16.1.2 القسم.

تكوين AP من Cisco

```
dot11 ssid ons
   tunnel CWAG
   authentication open eap eap_methods
   authentication key-management wpa
   accounting acct_methods

dot11 tunnel CWAG
    type gre
    source {AP_IP}
    destination {TWAG_IP}
    mss 1410
    mtu 1500
```

تدفق بيانات GRE



سلوك DHCP

النمط	مصدر IP	خادم DHCP	ملاحظات
موجه للمنزل	PGW (PAA في استجابة إنشاء الجلسة)	يقوم TWAG مسبقًا بتخصيص عنوان PGW، ويقدمه عبر DHCP عبر GRE	DNS من PGW PCO
الانفصال المحلي	مجموعة محلية لـ TWAG (`Twag.IpPools`)	يقوم TWAG بالتخصيص من المجموعة المرتبطة عند DISCOVER (توزيع المجموعة)	DNS من تكوين المجموعة

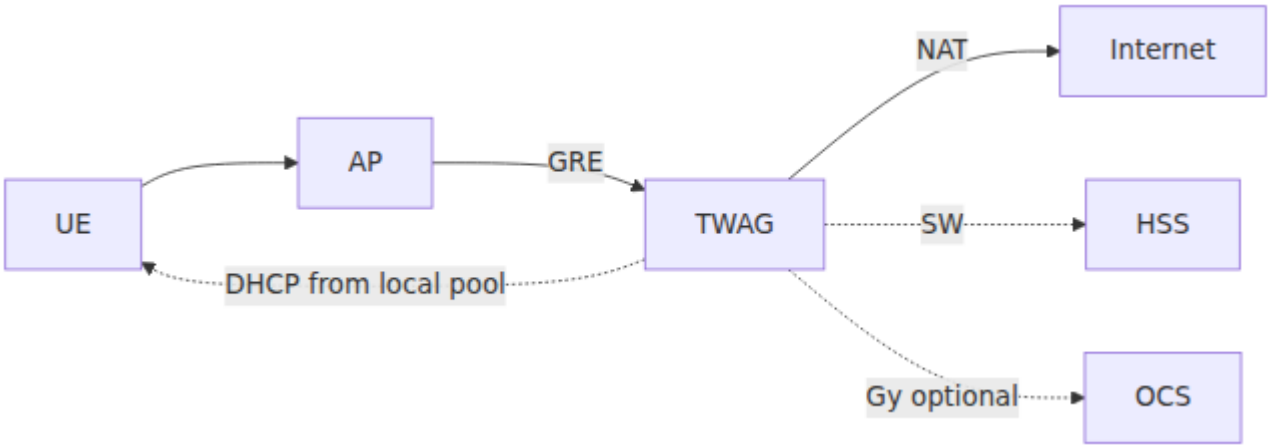
يعمل خادم DHCP الخاص بـ TWAG على:

1. استلام DISCOVER DHCP من UE عبر نفق GRE.
2. تقديم OFFER. عنوان IP المخصص من PGW في نمط موجه للمنزل، يكون هذا هو عنوان MAC مرتبطًا الذي تم تخصيصه مسبقًا للجلسة. في نمط الانفصال المحلي، عندما يكون بمجموعة، يقوم الخادم بتوزيع عنوان جديد من المجموعة.
3. التعامل مع REQUEST/ACK لإكمال التبادل.
4. تمرير جميع حركة مرور DHCP عبر نفق GRE إلى ومن AP.

المصادقة

يعمل OmniTWAG كخادم TWAG ومزود AAA 3 لـ3GPP، يقوم بإجراء مصادقة EAP-AKA محليًا لكل مشترك داخل EAP تعمل آلة حالة. وجلب متجهات المصادقة من HSS عبر Diameter SWx. الخاص به `Twag.Session.Client`.

تدفق المصادقة



المصدر مقابل IP بتفويض RADIUS قبل معالجة أي حزمة، يقوم مستمع `Twag.RadiusCredentials`. يتم إسقاط المصدر الذي لا يطابق شبكة بيانات الاعتماد ويتم تسجيله كـ `unauthorized_source`. يتم تسجيل المصدر الذي يتطابق ولكنه يفشل في التحقق من Message-Authenticator كـ `bad_secret`. رفض انظر RADIUS.

أوضاع المصادقة

النمط	التكوين	مصدر المتجه	معالجة EAP
`:swx`	`auth_mode: :swx`	SWx MAR/MAA عبر HSS	محلي (TWAG)
`:local`	`auth_mode: :local`	مفاتيح اختبار محلية (Milenage)	محلي (TWAG)

طريقة EAP

يمكن تكوينها عبر `eap_method`. الافتراضي هو `:eap_aka`. إذا قام UE برفض الطريقة المعروضة، يقوم TWAG بالتفاوض إلى الطريقة المدعومة المفضلة لـ UE. يتم دعم EAP-SIM وإعادة المصادقة EAP (ERP) أيضًا. انظر المصادقة.

دورة حياة الجلسة (موجهة للمنزل)



EAP Auth -> Access-Accept (MSK to AP)

AP sends Accounting-Start

Post-accept on Twag.Session.Client

GTP-C Create Session Request -> PGW

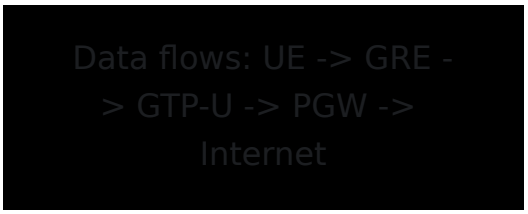
PGW allocates IP, Create Session Response

Register GTP-U tunnel (local + remote TEIDs)

Pre-allocate PGW IP in DHCP for UE MAC

UE DHCP Discover ->







يتم إنهاء الجلسة لأحد الأسباب العديدة، كل منها مسجل في مقياس `twag.session.teardown`: `accounting_stop`، `admin_disconnect`، `network_disconnect` (STa ASR)، `identity_timeout` (تم بدء المصادقة ولكن لم تكتمل أبدًا)، و `liveness_timeout`. انظر مرجع المقاييس و الجلسات.

واجهات Diameter

الواجهة	معرف التطبيق	الاتجاه	الغرض
SWx	16777265	TWAG -> HSS	جلب متجه المصادقة (MAR/MAA)
STa	16777250	وارد إلى TWAG	RAR (إعادة المصادقة)، ASR (الإلغاء)، STR (إنهاء)
Ro/Gy	4	TWAG -> OCS	الشحن عبر الإنترنت (NSWO فقط)

توجيه DRA

يجب على DRA توجيه SWx إلى HSS:

```
%{rule_name: "swx_to_hss", match: :all,
  filters: [{:application_id, 16777265}, {:avp, {296, "
{realm}"}}],
  route: %{peers: ["{hss_host}"]}}
```

ملخص التكوين

يتم توثيق كل معلمة في الجدول الذي يلي الكتلة.

```
config :omnitwag,
  auth_mode: :swx,
  eap_method: :eap_aka,
  identity_timeout_ms: 600_000,

  gtp: %{
    enabled: true,
    pgw_ip: "10.179.1.21",
    local_ip: "10.179.1.41",
    pgw_port: 2123,
    gtpu_port: 2152,
    echo_enabled: true
  },

  gre: %{
    enabled: true,
    local_ip: "10.179.1.41"
  },

  downlink: %{
    enabled: true
  },

  dhcp: %{
    enabled: true,
    interface: "gre"
  },

  ipv6_ra: %{
    enabled: false
  },

  nswo: %{
    enabled: false,
    local_pool: "10.100.0.0/16",
    nat_interface: "eth0"
  },

  online_charging: %{
    mode: :disabled
  },

  rate_limit: %{
```

```
    max_failures: 10,
    window_ms: 60_000
  },

  prometheus: %{
    port: 9568
  }
```

المعلمة	الافتراضي	الوصف
`auth_mode`	`:swx`	يجلب المتجهات `:swx` من HSS؛ `:local` يستخدم مفاتيح اختبار Milenage المحلية.
`eap_method`	`:eap_aka`	طريقة EAP المعروضة (`:eap_aka` أو `:eap_aka_prime`).
`identity_timeout_ms`	`600000`	الوقت الذي يمكن أن تبقى فيه الجلسة في مرحلة الهوية قبل أن يتم إنهاؤها (سبب الإنهاء `identity_timeout`).
`gtp.enabled`	`true`	بدء الأطفال GTP-C/GTP-U (نمط موجه للمنزل).
`gtp.pgw_ip`	`127.0.0.1`	عنوان PGW لـ GTP-C/GTP-U.
`gtp.local_ip`	لا شيء	عنوان TWAG المحلي لـ GTP.
`gtp.pgw_port`	`2123`	منفذ GTP-C لـ PGW.
`gtp.gtpu_port`	`2152`	المنفذ المحلي لـ GTP-U.
`gtp.echo_enabled`	`true`	إرسال نبضات GTP إلى PGW.
`gre.enabled`	`false`	بدء خادم GRE لنفق AP.

المعلمة	الافتراضي	الوصف
`gre.local_ip`	`0.0.0.0`	العنوان المحلي الذي يرتبط به خادم GRE.
`downlink.enabled`	`true`	بدء موصل الانخفاض.
`dhcp.enabled`	`false`	بدء خادم DHCPv4.
`dhcp.interface`	لا شيء	لوضع النفق، أو `"gre"` اسم NIC للتسليم المباشر.
`ipv6_ra.enabled`	`false`	بدء إعلانات الموجهات IPv6 وDHCPv6.
`nswo.enabled`	`false`	بدء معالج الانفصال المحلي NSWO.
`nswo.local_pool`	لا شيء	احتياطي لتوجيه CIDR الانفصال المحلي.
`nswo.nat_interface`	لا شيء	NIC للخروج لـ NAT/ تخفي.
`online_charging.mode`	`:disabled`	وضع Gy: `:disabled`، `:authorize_only`، أو `:online_charging`.
`rate_limit.max_failures`	`10`	فشل المصادقة لكل NAS في النافذة قبل إسقاط طلبات الوصول.
`rate_limit.window_ms`	`60000`	نافذة تحديد المعدل بالميلي ثانية.

المعلمة	الافتراضي	الوصف
`prometheus.port`	`9568`	منفذ مقاييس Prometheus.
`radius_config.acct_interim_interval`	`300`	فترة المحاسبة المؤقتة (بالثواني) المعلن عنها لـ AP في Access-Accept.

اشتقاق المفاتيح

لـ EAP-AKA'، 3 وفقًا لـ GPP TS 33.402 والملحق 6.2 البند A.2، و RFC 5448:

الخطوة	العقدة (`:swx` mode)	النتيجة
1	TWAG	SWx MAR مع `SIP-Authentication-Scheme` = `EAP-AKA'` و `ANID` = اسم الشبكة
2	HSS	RAND، AUTN مع بت فصل AMF 1، XRES
3	HSS	`CK'`، `IK'` = KDF(`CK`، `IK`، FC 0x20، اسم الشبكة، SQN XOR AK)
4	TWAG	`MK` = PRF'(`IK'`، `CK'`، "EAP-AKA'"، الهوية)
5	TWAG	`K_aut`، `MSK`، `EMSK` من `MK`

بتشغيل الخطوتين 2 و3 أيضًا، مع مفاتيح الاختبار المكونة. انظر TWAG يقوم في وضع `:local` المصادقة للاشتقاق الكامل.

لـ EAP-AKA (RFC 4187):

```
HSS provides: RAND, AUTN, XRES, CK, IK
TWAG derives: MK = SHA1(Identity || IK || CK)
              K_encr, K_aut, MSK, EMSK from PRF(MK)
```

اسم الشبكة (ANID) هو `WLAN` من 8.1.1.2 وفقًا للبند TS 24.302. انظر اسم الشبكة.

صفحات ذات صلة

- المصادقة
- أسرار RADIUS المشتركة
- رفض RADIUS
- مجموعات IP
- الجلسات
- محاسبة لكل AP
- طائرة المستخدم ومسار البيانات
- الشحن عبر الإنترنت
- مرجع المقاييس

نظرة عامة

المصادقة (EAP-AKA / EAP-AKA' / EAP-SIM)

نظرة عامة

يقوم OmniTWAG بمصادقة كل مشترك باستخدام طريقة EAP تعمل عبر RADIUS بين نقطة الوصول و TWAG. يعمل TWAG كخادم AAA مدمج لـ TWAG 3GPP. يقوم بتشغيل آلة حالة EAP، ويحصل على متجهات المصادقة من HSS عبر Diameter SWx، أو من مفاتيح اختبار محلية. عند النجاح، يقوم TWAG بتسليم مفتاح الجلسة الرئيسي (MSK) كمفاتيح إلى نقطة الوصول ثم تكمل نقطة الوصول مصافحة 802.11 ذات الأربع خطوات مع المشترك. MPPE داخل RADIUS Access-Accept.

للحصول على سياق النظام الأوسع، انظر العمارة. لمعرفة كيفية حل السر المشترك لـ RADIUS تعمل المصادقة أولاً. يتم تطبيق سياسة RADIUS لكل نقطة وصول، انظر الأسرار المشتركة لـ بعد نجاح المصادقة. لجلسة المصادقة ودورة حياتها، انظر الجلسات. AP الانفصال والتحميل لكل لجلسة S2a GTP-C بعد المصادقة، انظر TWAG التي ينشئها S2a GTP-C. بالنسبة للتحميل الذي يتبع المصادقة الناجحة، انظر التحميل عبر الإنترنت (Gy).

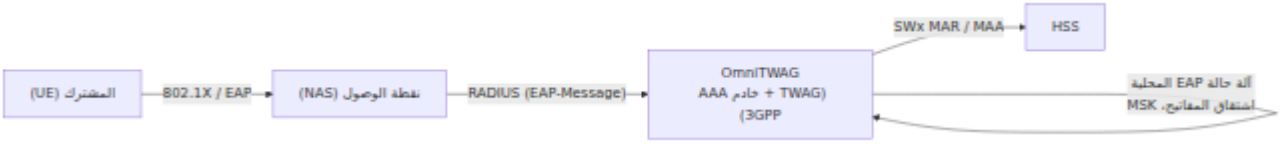
جدول المحتويات

- نظرة عامة
- طرق EAP المدعومة
- آلة حالة EAP والمراحل
- تسلسل المصادقة
- مصادر متجهات المصادقة
- معالجة الهوية و NAI
- اشتقاق المفاتيح والتسليم
- إعادة التزامن
- إعادة المصادقة السريعة (ERP)
- معالجة الأخطاء ورموز النتائج
- التكوين
- الرؤية
- استكشاف الأخطاء وإصلاحها

نظرة عامة

تبدأ نقطة الوصول تبادل EAP IEEE 802.1X مع المشترك. تقوم نقطة الوصول بتغليف كل رسالة EAP في سمة RADIUS `EAP-Message` وترسلها إلى TWAG. يقوم TWAG بتشغيل آلة حالة EAP مصادقة واحدة لكل هوية مشترك. تدفع آلة الحالة تبادل EAP إلى نتيجة، ثم تعيد واحدة من ثلاث نتائج إلى طبقة RADIUS.

النتيجة	رد RADIUS	المعنى
تحدي	`Access-Challenge`	يحتاج التبادل إلى جولة EAP أخرى.
قبول	`Access-Accept`	نجحت المصادقة. يحمل الرد MSK كمفاتيح MPPE.
رفض	`Access-Reject`	فشلت المصادقة. يحمل الرد EAP-Failure.



يمتلك TWAG حالة تشفير لكل هوية. يحتفظ بالاستجابة المتوقعة (XRES)، ومفتاح المصادقة (`K_aut`)، وRAND، وMSK، وEMSK (المفتاح الموسع) بين جولات EAP. بعد أن يقوم TWAG بتسليم مفاتيح MPPE، يقوم TWAG بتصفير المواد الحساسة للمفاتيح.

طرق EAP المدعومة

يدعم TWAG ثلاث طرق EAP. تستخدم كل طريقة نفس تنسيق سمة EAP ولكن قيمة نوع TLV، مختلفة وهرمية مفاتيح مختلفة.

الطريقة	نوع EAP	المواصفة	المتجهات	K_aut	MAC	اشتقاق المفتاح
EAP-AKA'	50 (`0x32`)	RFC 5448	quintet UMTS	32 بايت	HMAC-SHA-256، مقطوع إلى 16 بايت	`CK'`/`IK'` ثم PRF' (HMAC-SHA-256)
EAP-AKA	23 (`0x17`)	RFC 4187	quintet UMTS	16 بايت	HMAC-SHA1، مقطوع إلى 16 بايت	`MK = SHA1(Identit | IK | CK)` م FIPS 186-2 PRF
EAP-SIM	18 (`0x12`)	RFC 4186	2 3 أو triplets GSM	16 بايت	HMAC-SHA1، مقطوع إلى 16 بايت	`MK = SHA1(Identit | Kc... | NONCE_MT | version)` ثم FIPS 186-2 PRF

اختيار الطريقة والتفاوض

يقدم TWAG طريقة افتراضية. قم بتعيين الطريقة باستخدام مفتاح التكوين `eap_method`. الافتراضي هو `:eap_aka_prime` (EAP-AKA').

أنواع NAK تسرد (نوع EAP 3). يمكن للمشترك رفض الطريقة المعروضة باستخدام هذه الأنواع القائمة TWAG. يقرأ EAP التي يفضلها المشترك ويختار أول نوع يدعمه. يدعم TWAG في NAK: `50` (EAP-AKA')، `23` (EAP-AKA)، `18` و(EAP-SIM).

- إذا كانت NAK تسرد نوعًا مدعومًا، يقوم TWAG بإعادة بدء التبادل بتلك الطريقة. يرسل TWAG طلب AKA-Identity مع EAP-AKA، و EAP-AKA' بالنسبة لـ `AT_PERMANENT_ID_REQ`. يرسل TWAG طلب EAP-SIM بالنسبة لـ EAP-SIM/Start.

- إذا كانت NAK لا تسرد أي نوع مدعوم، يرفض TWAG المشترك.

آلة حالة EAP والمراحل

يعمل TWAG على تشغيل آلة حالة واحدة لكل هوية مشترك، داخل عملية عميل لكل هوية. تتعقب آلة الحالة مرحلة EAP. وأي بيانات استشعار TWAG تدفع المرحلة الرسالة التالية التي يتوقعها يخرجها.

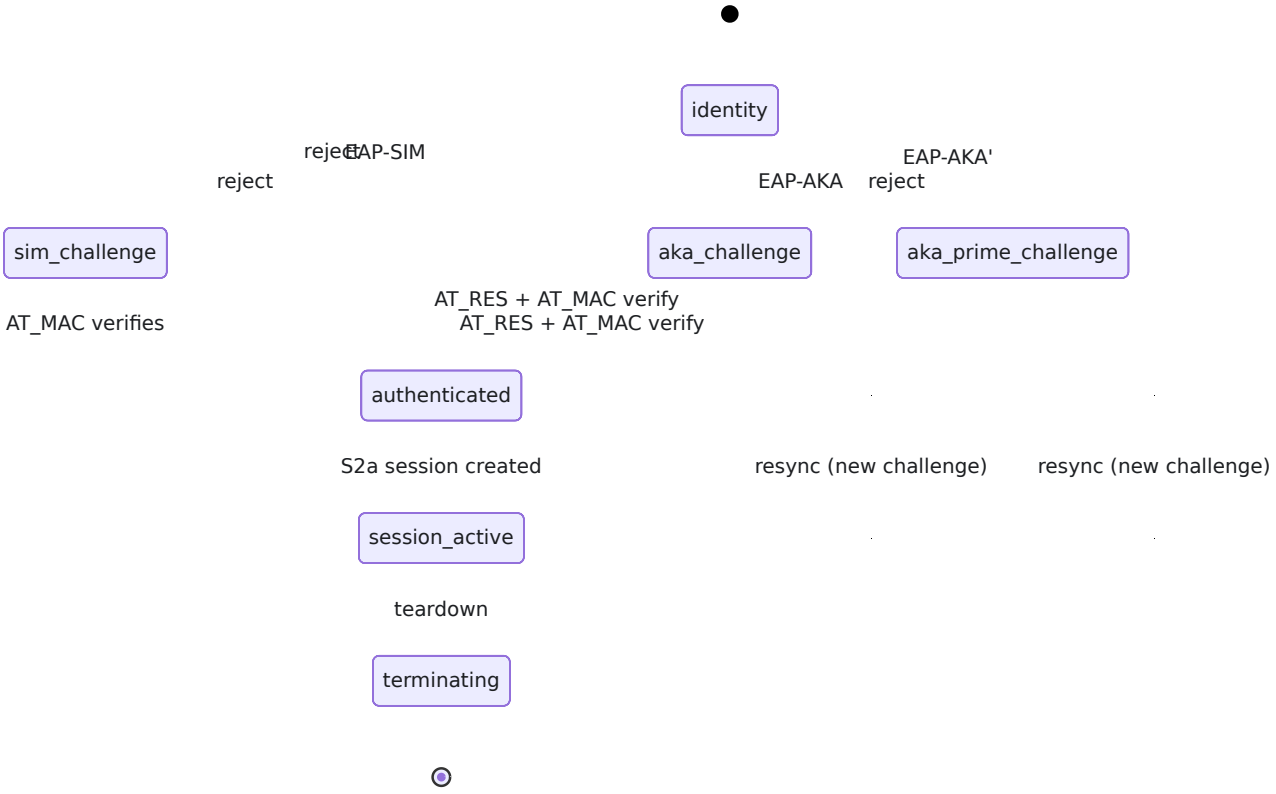
المرحلة (`eap_phase`)	المعنى
`identity`	المرحلة الأولية. يتوقع TWAG EAP-Identity، أو الجولة الأولى تعيد الجولة الفاشلة الحالة EAP-SIM/Start أو AKA-Identity إلى `identity`.
`aka_challenge`	أرسل TWAG تحدي EAP-AKA وينتظر استجابة AKA-Challenge.
`aka_prime_challenge`	أرسل TWAG تحدي EAP-AKA' وينتظر استجابة AKA-Challenge.
`sim_challenge`	أرسل TWAG تحدي EAP-SIM وينتظر استجابة SIM/Challenge.
`authenticated`	نجح تبادل EAP. يمتلك TWAG MSK وهو على وشك إنشاء جلسة S2a.
`session_active`	الجلسة S2a نشطة. يمكن للمشترك تمرير بيانات المستخدم. يمكن أيضًا أن يرفع حساب RADIUS جلسة إلى هذه المرحلة.

توجد قيمتان إضافيتان للمرحلة في الكود:

- `resyncing` محجوزة كمرحلة مصادقة قيد التقدم. في الممارسة العملية، تعيد جولة إعادة التزامن بناء التحدي وتعيد المرحلة إلى `aka_challenge` أو `aka_prime_challenge`، لذا لا تستقر الحالة على `resyncing`.
- `terminating` تشير إلى جلسة يتم إنهاؤها.

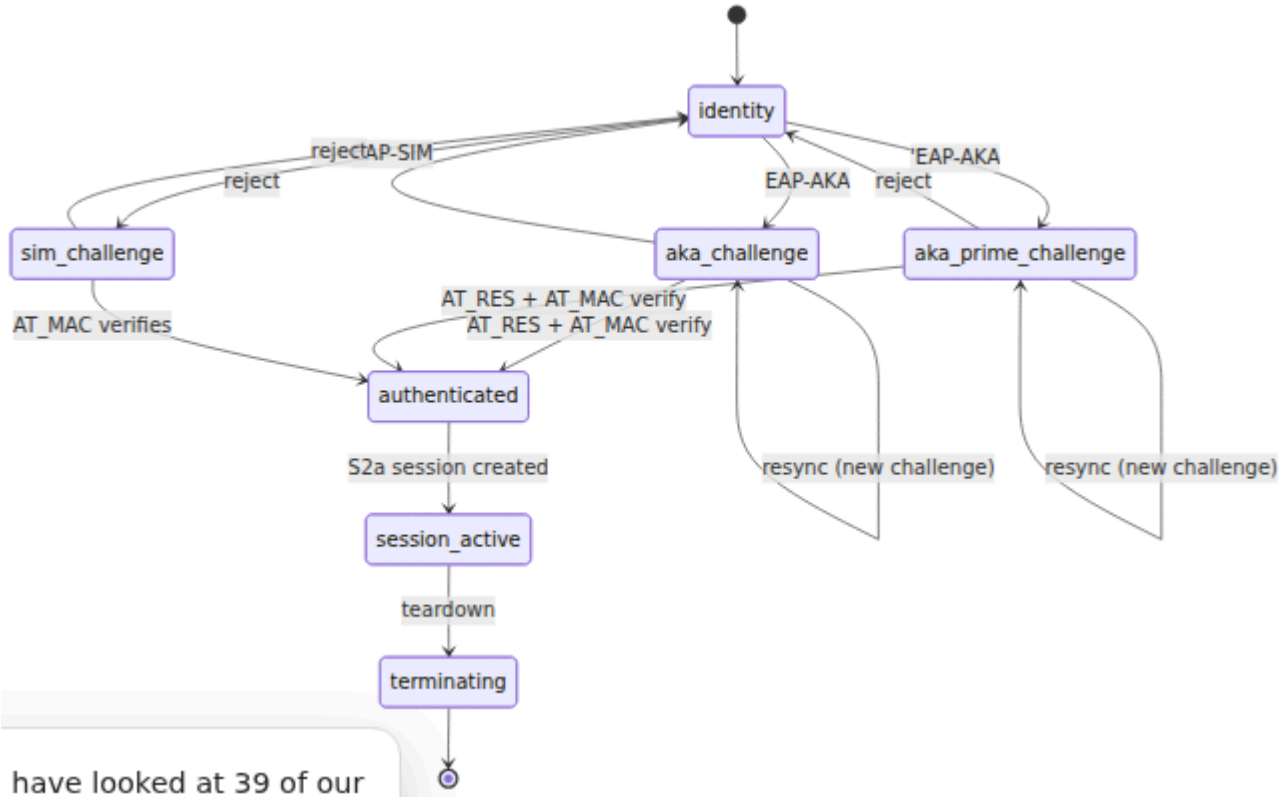
تتم إزالة الجلسة التي تبقى في مرحلة مصادقة قيد التقدم (`identity`، `aka_challenge`، `aka_prime_challenge`، `sim_challenge`، أو `resyncing`) بعد انتهاء مهلة الهوية. قم بتعيين المهلة باستخدام `identity_timeout_ms`. انظر التكوين.

تقوم صفحة الجلسات بربط هذه المراحل بحالة مصادقة الجلسة المعروضة في واجهة المستخدم وAPI.



تسلسل المصادقة

يتضمن التسلسل الكامل مرحلة الهوية ومرحلة التحدي. المثال أدناه يظهر EAP-AKA'. EAP-AKA بدلاً من جولة Start جولة EAP-SIM له نفس الشكل. يستخدم AKA-Identity، ولا يرسل `AT_RES`.



مرحلة الهوية

1. يرسل المشترك استجابة EAP-Identity تحمل معرف الوصول إلى الشبكة (NAI).
2. بالنسبة لـ EAP-AKA' أو EAP-AKA، يرد TWAG بطلب AKA-Identity يحمل `AT_PERMANENT_ID_REQ`. يطلب هذا من المشترك الهوية الدائمة.
3. بالنسبة لـ EAP-SIM، يرد TWAG بطلب EAP-SIM/Start يحمل `AT_VERSION_LIST` (الإصدار 1 فقط).
4. يعيد المشترك الهوية الدائمة (AKA-Identity مع `AT_IDENTITY`)، أو استجابة Start مع `AT_NONCE_MT` لـ EAP-SIM.

مرحلة التحدي

1. يستخرج TWAG IMSI من الهوية ويحصل على متجهات المصادقة. انظر مصادر متجهات المصادقة.
2. يقوم TWAG باشتقاق مفاتيح الجلسة، بما في ذلك MSK. انظر اشتقاق المفاتيح والتسليم.
3. يبني TWAG بالنسبة لـ EAP-AKA' التحدي. يحمل التحدي `AT_RAND`، `AT_AUTN`، `AT_KDF_INPUT` (اسم الشبكة)، `AT_KDF`، `AT_BIDDING`، و`AT_MAC`. بالنسبة لـ EAP-AKA يحمل التحدي `AT_RAND`، `AT_AUTN`، و`AT_MAC`. بالنسبة لـ EAP-SIM يحمل التحدي `AT_RAND` (2 أو 3 RANDs) و`AT_MAC`.

4. يتحقق المشترك من الشبكة (AUTN) وMAC، ثم يعيد الاستجابة.
5. يتحقق TWAG من الاستجابة. انظر التحقق من الاستجابة.
6. عند النجاح، يعيد TWAG EAP-Success وMSK. عند الفشل، يعيد TWAG EAP-Failure.

التحقق من الاستجابة

يتحقق TWAG من استجابة التحدي بترتيب ثابت. الترتيب هو نفسه لـ EAP-AKA وEAP-AKA'.

1. **تحقق الحالة.** إذا كانت `K_aut` أو XRES المخزنة مفقودة، يرفض TWAG.
2. **تحقق السمة.** إذا كانت `AT_MAC` أو `AT_RES` مفقودة، يرفض TWAG.
3. **تحقق MAC.** يقوم TWAG بتصفير حقل `AT_MAC`، وإعادة حساب MAC على الحزمة، ويقارن. يستخدم EAP-AKA HMAC-SHA1. يستخدم EAP-AKA' HMAC-SHA-256. كلاهما مقطوع إلى 16 بايت. باستخدام `K_aut`.
4. **تحقق الاستجابة.** يقارن TWAG `AT_RES` مع XRES **زمن** المخزنة. المقارنة هي **ثابت** زمن ثابت TWAG تحقق الطول ومقارنة بايت لمنع هجمات الزمن. يستخدم.
5. **النتيجة.** إذا تطابق كل من MAC والاستجابة، يقبل TWAG. خلاف ذلك، يرفض TWAG.

هو الدليل الوحيد على أن `AT_MAC` تحقق. `AT_RES` لا يرسل المشترك، بالنسبة لـ EAP-SIM، يقبل TWAG. المشترك يحمل المفاتيح الصحيحة. إذا تم التحقق من MAC،

مصادر متجهات المصادقة

يحصل TWAG على متجهات المصادقة من أحد مصدرين. قم بتعيين المصدر باستخدام مفتاح التكوين `auth_mode`.

الوضع	`auth_mode`	مصدر المتجه	الاستخدام
SWx	`:swx`	HSS، عبر Diameter SWx (MAR/MAA)	الإنتاج
محلي	أي قيمة غير `:swx` (افتراضي `:local`)	محلي من مفاتيح Milenage اختبار موفرة	الاختبار

في كلا الوضعين، يقوم TWAG بتشغيل آلة حالة EAP بأي قيمة مصدر المتجه. يختلف فقط مصدر المتجه محليًا. تختار مسار Milenage المحلي `:swx` ليست `auth_mode`.

> توصيل حمولات `Twag.Auth.StaAuth` **هو مسار منفصل.** يمكن لمزود **تمرير STa** الخام إلى خادم EAP عبر Diameter STa (DER/DEA)، بحيث يقوم خادم AAA 3GPP بتشغيل تبادل EAP-AKA ويعيد MSK. هذا المزود موجود ولكنه ليس على مسار المصادقة المباشر. يقوم المسار المباشر بجلب المتجهات باستخدام RADIUS `:local` أو `:swx` ويشغل آلة حالة EAP على TWAG.

SWx إلى HSS

في وضع `:swx`، يرسل TWAG طلب مصادقة وسائط متعددة (MAR) إلى HSS عبر واجهة SWx (3GPP TS 29.273، `16777265` معرف التطبيق). يحمل MAR:

- `User-Name`: IMSI.
- `SIP-Auth-Data-Item` مع `SIP-Authentication-Scheme` تم تعيينه إلى طريقة EAP المستخدمة: `EAP-AKA'` أو `EAP-AKA`. بالنسبة لإعادة التزامن، يحمل العنصر أيضًا `SIP-Authorization`. يحمل هذا RAND متبوعًا بـ AUTS.
- `SIP-Number-Auth-Items`: 1.
- `ANID`: اسم الشبكة. الافتراضي هو `WLAN`. بالنسبة لـ `EAP-AKA'`، يستخدم HSS ذلك لاشتقاق `CK'`/`IK'`. انظر 3GPP TS 29.273 8.1.2.1 الفقرة.
- `RAT-Type`: 0.
- `Auth-Session-State`: 1 (NO_STATE_MAINTAINED).
- `Vendor-Specific-Application-Id` مع معرف تطبيق SWx Auth-Application-Id `16777265` ومعرف البائع `10415`.

يعيد HSS إجابة مصادقة وسائط متعددة (MAA). عندما يكون `Result-Code` هو `2001` (نجاح)، يقرأ TWAG أول `SIP-Auth-Data-Item` ويستخرج المتجه:

- `SIP-Authentication-Scheme` = نظام المتجه: `EAP-AKA'` أو `EAP-AKA`.
- `SIP-Authenticate` = RAND (16 بايت) متبوعًا بـ AUTN (16 بايت).
- `SIP-Authorization` = XRES.
- `Confidentiality-Key` = CK لـ `EAP-AKA`، أو CK' لـ `EAP-AKA'`.
- `Integrity-Key` = IK لـ `EAP-AKA`، أو IK' لـ `EAP-AKA'`.

إذا لم يكن `Result-Code` هو `2001`، أو كانت حقول المتجه مفقودة، يعامل TWAG الإجابة على أنها رفض مصادقة. يرفض TWAG المشترك مع EAP-Failure ويسجل الرفض، وليس تعطل.

إذا طلب TWAG `EAP-AKA'` وكان المتجه ليس متجه EAP-AKA'، يرفض TWAG أيضًا المشترك. AUTN هو 0 في AMF أو عندما يكون بت فصل `EAP-AKA`، ينطبق هذا عندما يكون النظام هو

انظر هرمية مفاتيح EAP-AKA'.

إشارة خطأ SWx (Experimental-Result)

تشير SWx إلى معظم الأخطاء في AVP `Experimental-Result` المجمعة (Vendor-Id `10415`)، وليس في `Result-Code` الأساسي. لذلك، يمكن أن يحمل MAA الفاشل عدم وجود `Result-Code` أيضًا TWAG أساسي على الإطلاق. يقرأ `Experimental-Result-Code`، ويسجل الاسم القابل للقراءة البشرية حتى يرى المشغل السبب الحقيقي. انظر استكشاف الأخطاء وإصلاحها للحصول على الرموز.

حالة شائعة هي `DIAMETER_ERROR_USER_UNKNOWN` (5001) أو `DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION` (5450): المشترك غير مفعل للوصول غير 3GPP على SWx، قد تفشل ال��صادقة على الرغم من أن نفس المشترك يكون معروفًا على S6a للوصول إلى EPC.

يجب على DRA توجيه تطبيق SWx إلى HSS. انظر DRA: توجيه العمارة.

Milenage المحلي

في وضع `:local`، يقوم TWAG بإنشاء المتجه باستخدام خوارزمية Milenage (3GPP TS 35.206) من مفاتيح الاختبار الموفرة (`test_keys`). المفاتيح هي `ki`، `opc`، `amf`، و`sqn`. يقوم TWAG بحساب RAND، AUTN، XRES، CK، وIK في العملية. استخدم هذا الوضع للاختبارات المعملية فقط.

المتجهات لـ EAP-SIM

تحتاج EAP-SIM إلى 2 أو 3 triplets GSM. يستخرج TWAG triplets من نفس متجهات Milenage. بالنسبة لكل متجه، يأخذ TWAG RAND، يأخذ أول 4 بايت من XRES كـ SRES، ويشتق `Kc` من CK وIK باستخدام دالة تحويل c3 (3GPP TS 33.102 الملحق C.3): `Kc = CK[0..7] XOR CK[8..15] XOR IK[0..7] XOR IK[8..15]`.

معالجة الهوية و NAI

هوية المشترك هي معرف الوصول إلى الشبكة (NAI). يتخذ NAI الشكل `{username}@{realm}`، على سبيل المثال `0{IMSI}@wlan.mnc{MNC}.mcc{MCC}.3gppnetwork.org`.

تخراج IMSI

يستخرج TWAG IMSI من NAI في خطوتين:

1. يأخذ TWAG اسم المستخدم، وهو الجزء قبل `@`.
2. يزيل TWAG `0` أو `6` (الهوية الدائمة، EAP-AKA/AKA') رقم نوع الهوية الرائد. يطابق IMSI العاري. الأرقام المتبقية هي IMSI الرائد.

يقبل TWAG IMSI من 14 أو 15 رقمًا. IMSI هو `User-Name` في SWx MAR. يستخدم TWAG هو الرقمين MNCهو أول 3 أرقام، و GTP-C: MCC لجلسة MNCو MCC لاشتقاق IMSI أيضًا التاليين.

اسم الشبكة (EAP-AKA')

يربط EAP-AKA' 3 المفاتيح باسم الشبكة. تسمي GPP هذه القيمة **معرف الشبكة الوصول (ANID)**. يرسل TWAG اسم الشبكة إلى المشترك في `AT_KDF_INPUT`. يرسل TWAG نفس السلسلة إلى HSS في AVP `ANID` من SWx MAR. يستخدم كل من HSS والمشترك ذلك لاشتقاق `CK'`/`IK'`، لذا يجب أن تكون القيمتان متطابقتين.

الافتراضي هو `WLAN`. هذا هو ANID لشبكة وصول WLAN 3 في GPP TS 24.302 الفقرة 8.1.1.2، بدون سلسلة إضافية. يقوم مفتاح التكوين `network_name` بتجاوز الافتراضي. احتفظ HSS ANID مختلف بالمفتاح غير مضبوط ما لم يتوقع.

اشتقاق المفاتيح والتسليم

تشتق كل طريقة مفتاح جلسة رئيسي (MSK) بحجم 64 بايت ومفتاح MSK موسع (EMSK) بحجم 64 بايت. يقوم TWAG بتسليم MSK إلى نقطة الوصول. يحتفظ TWAG بـ EMSK لإعادة المصادقة السريعة.

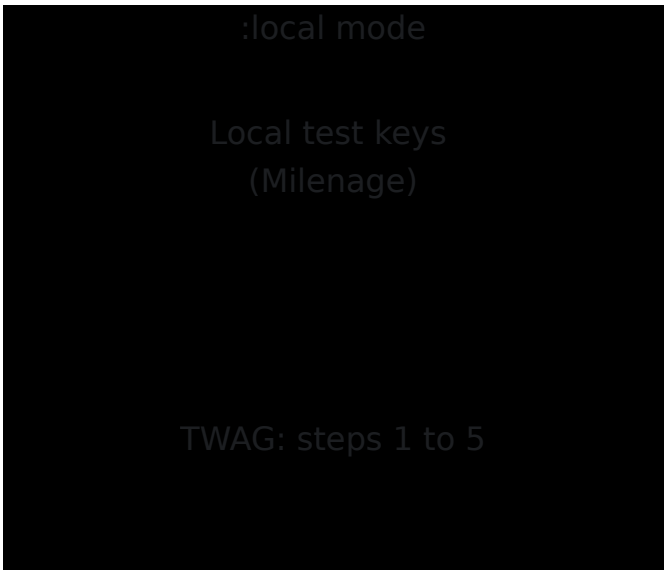
هرمية مفاتيح EAP-AKA'

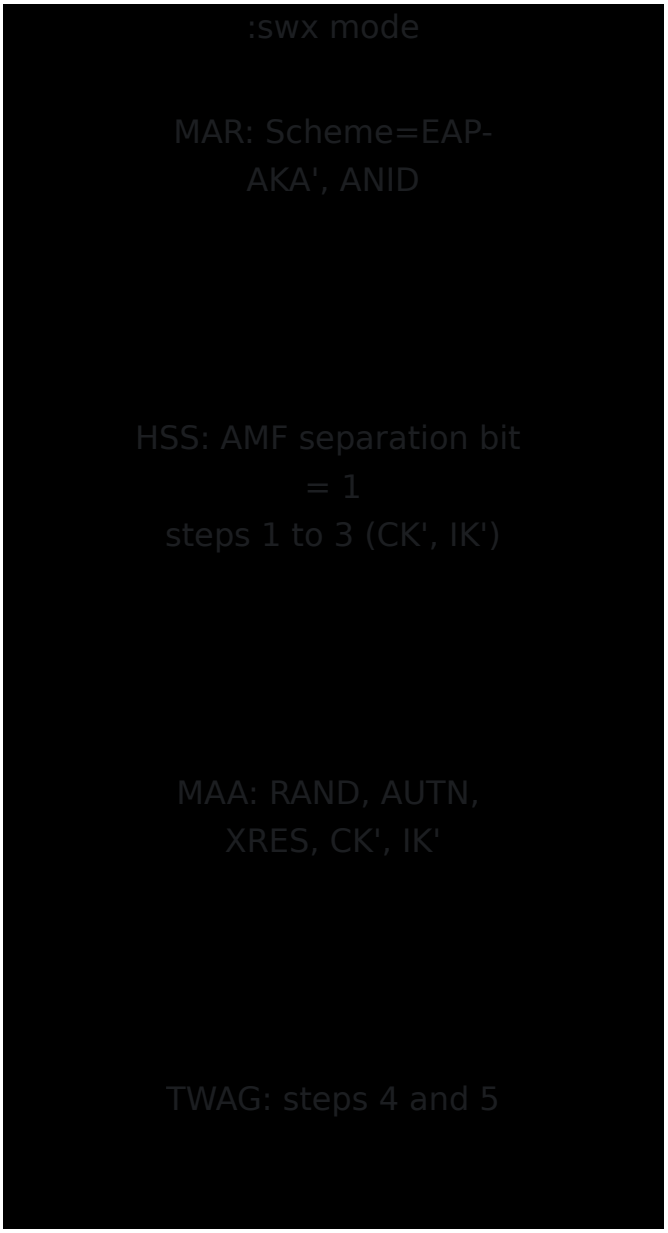
وفقًا لـ RFC 5448 3 وGPP TS 33.402 والملحق A: الفقرة 6.2

1. `Key = CK \| IK`.
2. `S = FC(0x20) \| network_name \| len(network_name) \| (SQN XOR AK) \| len(SQN XOR AK)`.

3. `CK' \| IK' = HMAC-SHA-256(Key, S)`. `CK'` هو أول 16 بايت. `IK'` هو آخر 16 بايت.
4. `MK = PRF'(IK' \| CK', "EAP-AKA'" \| Identity)`, 208 بايت. يستخدم PRF' HMAC-SHA-256.
5. يقوم TWAG بتقسيم `MK`: `K_encr` (16)، `K_aut` (32)، `K_re` (32)، `MSK` (64)، `EMSK` (64).

يحدد مصدر المتجه مكان تنفيذ الخطوات 1 إلى 3:


:local mode
Local test keys
(Milenage)
TWAG: steps 1 to 5


:swx mode
MAR: Scheme=EAP-
AKA', ANID
HSS: AMF separation bit
= 1
steps 1 to 3 (CK', IK')
MAA: RAND, AUTN,
XRES, CK', IK'
TWAG: steps 4 and 5

في وضع `:swx`، يقوم HSS بتنفيذ الخطوات 1 إلى 3. يطلب TWAG متجه EAP-AKA' في MAR. يقوم HSS بتعيين بت فصل AMF إلى 1 ويشتق `CK'`/`IK'` مع ANID. يحمل MAA `CK'` في `Confidentiality-Key` و`IK'` في `Integrity-Key`. يستخدم TWAG هذه المفاتيح كما تم استلامها وينفذ الخطوات 4 و5. لا تترك CK وIK HSS لمتجه AKA'. انظر 3GPP TS 33.402 الفقرة 6.2، الخطوة 10.

في وضع `:local`، يكون TWAG هو مصدر المتجه. يقوم TWAG بتنفيذ جميع الخطوات الخمس باستخدام مفاتيح الاختبار المكونة.

إذا أجاب HSS على طلب EAP-AKA' بنظام `EAP-AKA`، أو مع بت فصل AMF 0، يرفض TWAG المشترك مع EAP-Failure. تبدأ سطر السجل بـ `HSS vector unusable for EAP-AKA'`. الفقرة 6.2 الخطوة 15. تسمي TS 33.402 يرفض المشترك مثل هذا التحدي في أي حال، وفقًا لـ الرفض المبكر HSS كسبب بدلاً من `Client-Error` من الهاتف.

هرمية مفاتيح EAP-AKA

وفقًا لـ RFC 4187:

1. `MK = SHA1(Identity \| IK \| CK)`.
2. يقوم TWAG بتوسيع `MK` باستخدام FIPS 186-2 PRF إلى 160 بايت.
3. يقوم TWAG بتقسيم الناتج: `K_encr` (16)، `K_aut` (16)، `MSK` (64)، `EMSK` (64).

هرمية مفاتيح EAP-SIM

وفقًا لـ RFC 4186:

1. `MK = SHA1(Identity \| Kc1 \| Kc2 \| [Kc3] \| NONCE_MT \| Version_List \| Selected_Version)`.
2. يقوم TWAG بتوسيع `MK` باستخدام FIPS 186-2 PRF إلى 160 بايت.
3. يقوم TWAG بتقسيم الناتج: `K_encr` (16)، `K_aut` (16)، `MSK` (64)، `EMSK` (64).

إلى نقطة الوصول MPPE إلى MSK

يقوم TWAG بتسليم MSK في نقطة الوصول إلى 64 بايت البالغ RADIUS Access-Accept. يقوم TWAG بتقسيم MSK وترميز كل نصف كمفتاح MPPE من Microsoft (RFC 2548، RFC 3748):

- `MS-MPPE-Recv-Key` = `MSK[0..31]` (أول 32 بايت).

- `MS-MPPE-Send-Key` = `MSK[32..63]` (آخر 32 بايت).

يقوم TWAG بتشفير كل مفتاح باستخدام السر المشترك لـ RADIUS ومحقق الطلب، وفقًا لـ RFC 2548. يستخدم TWAG ملحًا جديدًا مكونًا من 2 بايت مع تعيين البت العالي لكل مفتاح. يقوم TWAG بتوقيع Access-Accept باستخدام السر المشترك. انظر RADIUS Shared Secrets للسر TWAG لمعرفة كيفية حل.

يقوم MPPE، واستعادة MSK، ويستخدم MSK كمفتاح رئيسي زوجي لـ 802.11 في مصافحة 4 طرق مع المشترك.

يتطلب Access-Accept وجود MSK صالح مكون من 64 بايت. إذا كان MSK مفقودًا أو بحجم خاطئ، يقوم TWAG بإرسال Access-Reject بدلاً من ذلك.

إعادة التزامن

غير متزامن مع الشبكة. يرسل المشترك (SQN) يمكن للمشترك الإبلاغ عن أن رقم تسلسله Synchronization-Failure (النوع الفرعي `0x04`) مع `AT_AUTS`. `AT_AUTS` هو 14 باي��: 6 بايت من SQN المخفي و8 بايت من MAC-S.

يتعامل TWAG مع إعادة التزامن على النحو التالي:

1. يقوم TWAG ببناء معلومات إعادة التزامن: RAND المخزنة متصلة مع AUTS المكون من 14 بايت.
2. يقوم TWAG بتشغيل إعادة التزامن. هذا يستعيد SQN الخاص بالمشترك باستخدام دالة Milenage f5*، يتحقق من MAC-S، ويعيد رقم تسلسل محدث.
3. عند النجاح، يقوم TWAG بإنشاء متجه جديد مع SQN المحدث، يبني تحديًا جديدًا، ويرسل Access-Challenge جديد.
4. عند الفشل، يقوم TWAG برفض المشترك مع EAP-Failure.

يتعامل TWAG مع إعادة التزامن لكل من EAP-AKA وEAP-AKA'. تستخدم إعادة التزامن مفاتيح Milenage المحلية. يجب أن تكون قيمة `AT_AUTS` بالضبط 14 بايت، وإلا فإن TWAG يرفع خطأ ويفشل الدور.

إعادة المصادقة السريعة (ERP)

يدعم TWAG بروتوكول إعادة المصادقة EAP (ERP) وفقًا لـ RFC 6696. يسمح ERP للمشترك بإعادة المصادقة دون تبادل كامل لـ EAP. تأتي المدخرات من سلسلة مفاتيح يستخر��ها TWAG

من EMSK خلال أول مصادقة كاملة.

باستخراج وتخزين مفاتيح إعادة المصادقة TWAG بعد المصادقة الكاملة، يقوم:

- `rRK` = مفتاح الجذر لإعادة المصادقة، من EMSK.
- `rIK` = مفتاح النزاهة لإعادة المصادقة، من rRK.

تستخدم جميع اشتقاقات مفاتيح ERP HMAC-SHA-256.

عندما يرسل المشترك رسالة EAP-Initiate/Re-auth (نوع EAP 41)، يقوم TWAG بما يلي:

1. إذا لم يكن لدى TWAG `rRK` أو `rIK` مخزنة، يعود TWAG إلى مصادقة كاملة. يرسل TWAG طلب AKA-Identity جديد.
2. إذا كان لدى TWAG المفاتيح، يقوم TWAG بتحليل الرسالة والتحقق من علامة المصادقة باستخدام `rIK`.
3. إذا تم التحقق من العلامة، يقوم TWAG باشتقاق MSK لإعادة المصادقة (`rMSK`) من `rRK` ورقم تسلسل الرسالة، يبني استجابة EAP-Finish/Re-auth (نوع EAP 42)، ويقبل. يصبح `rMSK` هو MSK الجديد لمفاتيح MPPE.
4. إذا لم يتم التحقق من العلامة، أو فشل التحليل، يعود TWAG إلى مصادقة كاملة.

معالجة الفشل وأكواد النتائج

نتائ EAP

الشرط	إجراء TWAG
فشل SWx MAR، أو المتجهات غير مكتملة	برفض المشترك TWAG تم رفض جلب المتجه. يقوم بشكل نظيف مع EAP-Failure، ويسجل الرفض بدلاً من حدوث عطل.
تم طلب EAP-AKA'، لكن مخطط MAA هو `EAP-AKA`	Access-Reject مع EAP-Failure. يبدأ سطر السجل بـ `HSS vector unusable for EAP-AKA'`. لا يدعم HSS متجهات EAP-AKA'.
تم طلب EAP-AKA'، لكن بت AUTN 0 هو الفصل في AMF	Access-Reject مع EAP-Failure. نفس سطر السجل. أصدر HSS رفضه متجهًا يجب على المشترك (TS 33.402 الخطوة 15 الفقرة 6.2).
فشل التحقق من `AT_MAC`	Access-Reject مع EAP-Failure.
XRES لا يتطابق مع `AT_RES`	Access-Reject مع EAP-Failure.
XRES أو حالة `K_aut` مفقود	Access-Reject مع EAP-Failure.
`AT_MAC` أو خاصية `AT_RES` مفقود	Access-Reject مع EAP-Failure.
يرسل المشترك AKA-Authentication-Reject (النوع `0` الفرعي `x02`)	Access-Reject. رفض المشترك الشبكة.
يرسل المشترك AKA-Client-Error (النوع الفرعي `0` `x0E`)	Access-Reject.
EAP-NAK بدون طريقة مدعومة	Access-Reject.

الشرط	إجراء TWAG
MSK مفقو�� أو ليس 64 بايت عند القبول	Access-Reject.
رسالة EAP غير معالجة	Access-Reject مع EAP-Failure.

أكواد نتائج Diameter لـ SWx

رمز النجاح هو `Result-Code` في أساسي. تصل أكواد الخطأ أدناه في `Experimental-Result` AVP، وليس في `Result-Code` الأساسي. انظر SWx error signalling و والملاحظات Troubleshooting.

الرمز	الاسم	المعنى
2001	DIAMETER_SUCCESS	يحمل MAA متجهًا صالحًا.
5001	DIAMETER_ERROR_USER_UNKNOWN	لا يوجد اشتراك غير 3GPP/SWx لهذا IMSI في HSS. قد يكون المشترك معروفًا على S6a/EPC.
5004	DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	بيانات المستخدم المطلوبة غير مدعومة.
5420	DIAMETER_ERROR_UNKNOWN_EPS_SUBSCRIPTION	لا يوجد اشتراك EPS لهذا المشترك.
5450	DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION	لا يوجد اشتراك غير 3GPP للمشترك.
أخرى	(خطأ Diameter)	فشل جلب المتجه. يتم رفض الدور.

المرجع: RFC 6733 Section 7.1، 3GPP TS 29.273، 3GPP TS 29.229.

الأحداث التي تبدأها الشبكة (STa)

يمكن لخادم AAA 3 في 3GPP إرسال أحداث إلى TWAG عبر واجهة STa (3GPP TS 29.273، معرف التطبيق `16777250`). يجيب TWAG على كل حدث بـ `Result-Code` `2001`.

الرسالة	الزناد	إجراء TWAG
ASR (Abort-Session-Request)	يريد خادم AAA قطع الاتصال.	يقوم TWAG بقطع جلسة المشترك، ثم يجيب ASA.
STR (Session-Termination-Request)	فصل بدأه HSS.	يقوم TWAG بقطع جلسة المشترك، ثم يجيب STA.
RAR (Re-Auth-Request)	يريد خادم AAA إعادة المصادقة.	يجيب TWAG على RAA بنجاح ويسجل الطلب. لم يتم بعد تفعيل إعادة المصادقة الكاملة للجلسة الحية من RAR.

تحمل جميع الإجابات الثلاثة Origin-Host وOrigin-Realm من هوية Diameter. انظر Configuration.

التكوين

قم بتعيين معلمات المصادقة في تكوين تطبيق `:omnitwag`. تأتي هوية Diameter (`host` و`realm`) من تكوين `:diameter_ex`، ويستخدمها TWAG كـ Origin-Host وOrigin-Realm على STa وSWx.

```
config :omnitwag,
  # مصدر المتجه: :swx (الإنتاج) أو :local (الاختبار)
  auth_mode: :swx,

  # طريقة EAP المعروضة: :eap_aka_prime (افتراضي)، :eap_aka، أو
:eap_sim
  eap_method: :eap_aka_prime,

  # اسم شبكة EAP-AKA' (ANID). يرسله TWAG في AT_KDF_INPUT وفي
  # SWx MAR. القيمة الافتراضية هي "WLAN" (TS 24.302 الفقرة
8.1.1.2). احتفظ به غير محدد في
  # النشر العادي.
  network_name: "WLAN",

  # إعادة جلسة لا تزال عالقة في مرحلة المصادقة الجارية بعد هذا
العدد من
  # (10 دقائق) 600000 الافتراضي. الحد الأدنى ثانية.
  identity_timeout_ms: 600_000,

  # حقول TWAN-Identifier، تضاف إلى STa DER/AAR عند تعيينها
  twan_ssid: "ons",
  twan_bssid: "00:11:22:33:44:55",

  # مفاتيح اختبار محلية (تستخدم فقط عند auth_mode: :local)
  test_keys: %{
    ki: "11111111111111111111111111111111",
    opc: "22222222222222222222222222222222",
    amf: "8000",
    sqn: 1200
  }
```

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`auth_mode`	Atom	لا	`:local`	مصدر المتجه . يحصل على المتجهات من H عبر SWx. `:lo` لد المتجهات من `test_keys`. م ي `:swx` بتعيين الإنتاج.
`eap_method`	Atom	لا	`:eap_aka_prime`	طريقة EAP معروضة. واحدة من `:eap_aka_pr` `:eap_aka`، `:eap_sim`. كن شترك التفاوض طريقة مدعومة مختلفة مع EAP NAK.
`network_name`	String	لا	`WLAN`	اسم شبكة EAP AKA' (ANID). يرسله TWAG ى `AT_KDF_INPU` وكـ AVP `ANID` SWx MAR. `WL` هو القيمة التي تعرفها TS 24.3 الفقرة 8.1.1.2 للوصول إلى WI
`identity_timeout_ms`	Integer	لا	`600000`	ت بالمللي ثانية ي يمكن أن تبقى لسة في مرحلة مصادقة الجارية

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				TW قبل أن يقوم بإعادة جمعها.
`twan_ssid`	String	لا	-	SSID WLAN. تعيينه، يضيف TW معرف TWAN ، رسائل STa DE وAAR.
`twan_bssid`	String	لا	-	BSSID نقطة صول. يتم دمجه مع `twan_ssid` لتشكيل معرف TWAN.
`test_keys`	Map	لا	القيم الافتراضية المدمجة	مفاتيح Milenag لمحلية. تستخدم فقط عندما يكون هو `auth_mode` `:local`. انظر key paramet

معلمات مفاتيح الاختبار

يقرأ TWAG `test_keys` فقط في وضع `:local`. لا تستخدم `test_keys` في الإنتاج.

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`ki`	String (hex)	نعم (وضع محلي)	`1111...`	مفتاح المشترك `Ki`، 16 بايت كـ 32 حرف سداسي.
`opc`	String (hex)	نعم (وضع محلي)	`2222...`	مفتاح متغير المشغل `OPc`، 16 بايت كـ 32 حرف سداسي.
`amf`	String (hex)	نعم (وضع محلي)	`8000`	حقل إدارة المصادقة، 2 بايت كـ 4 أحرف سداسية.
`sqn`	Integer	نعم (وضع محلي)	`1200`	رقم التسلسل الابتدائي.

الرؤية

يقوم TWAG بإصدار عدادات telemetry من خلال آلة حالة EAP ومعالج STa. تعرض نقطة النهاية للحصول على نقطة النهاية وأمثلة Metrics Reference العدادات. انظر Prometheus لـ الاستعلام.

مقاييس EAP

المقياس	المعنى
`eap_aka_identity_count`	تبادلات هوية EAP-AKA/AKA' (المرحلة 1).
`eap_aka_challenge_count`	تبادلات تحدي EAP-AKA/AKA' (المرحلة 2).
`eap_aka_sync_failure_count`	فشل إعادة التزامن AKA (أحداث إعادة التزامن).
`eap_aka_auth_success_count`	مصادقات EAP-AKA/AKA' الناجحة.
`eap_aka_auth_reject_count`	مصادقات EAP-AKA/AKA' المرفوضة.

يصدر TWAG أيضًا أحداث telemetry لـ EAP-SIM (`start`، `auth_success`، `auth_reject`)، لـ AKA `auth_reject` و`client_error`، و لـ ERP (`initiate`، `success`، `fallback`، `mac_failure`). انظر Metrics Reference.

مقاييس ردود RADIUS

المقياس	المعنى
`radius_access_challenge_count`	ردود Access-Challenge (دور EAP قيد التقدم).
`radius_access_accept_count`	ردود Access-Accept (مصادقة ناجحة).
`radius_access_reject_count`	ردود Access-Reject (مصادقة فاشلة).

مقاييس أحداث STa

يصدر معالج STa عداد telemetry لكل حدث يبدأ من الشبكة: `[:sta, :asr, :received, :count]`، `[:sta, :str, :received, :count]`، و `[:sta, :rar, :received, :count]`، بالإضافة إلى عدادات الجلسة `disconnect` و`reauth`.

سياق السجل

يحدد TWAG بيانات التعريف `imsi` و`identity` لكل جلسة. استخدم هذه الحقول لتتبع مشترك واحد خلال تدفق المصادقة.

استكشاف الأخطاء وإصلاحها

العرض	السبب المحتمل	
فشل المصادقة ويظهر السجل `DIAMETER_ERROR_USER_UNKNOWN (5001)`	لا يوجد اشتراك غير 3GPP/SWx في HSS. قد يكون المشترك معروفًا على S6a/EPC ولكنه غير مفعل للوصول غير 3GPP.	راك غير 3GPP HSS.
فشل المصادقة ويظهر السجل `DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION (5450)`	لا يحتوي ملف تعريف المشترك على اشتراك غير 3GPP.	راك غير 3GPP
يظهر السجل `Result-Code=nil` عند فشل MAA	أعاد SWx خطأ في `Experimental-Result` AVP، وليس في `Result-Code` الأساسي.	اقرأ `Exp` `Result` ل. يطبع TWAG البشرية
لا تكتمل المصادقة أبدًا ويتم جمع الجلسة	توقف المشترك في مرحلة المصادقة الجارية بعد انتهاء مهلة الهوية.	ن جانب م بضبط `identi` زم الأمر

	السبب المحتمل	العرض
ي الشبكة و OP/OP مع SIM :local ضع HSS :swx.	في UE فشل مصادقة الشبكة (تحقق AUTN).	يرسل المشترك AKA-Authentication-Reject
TW يقوم ا استمر، ي معالجة HSS. ر Resync	انحرف SQN الخاص بالمشترك عن SQN الشبكة.	تكرار AKA-Synchronization-Failure
ر المتجه ة. تحقق من SW المحلية	كان MSK مفقودًا أو ليس 64 بايت عند القبول.	صالح EAP-Success مع توقع Access-Reject
أو تكوين متجهات T وفقًا لـ وقت، قم e بتعيين :eap_a	أجاب HSS على MAR بمتجه EAP-AKA: مخطط EAP-AKA، أو بت الفصل AMF 0. لا يدعم HSS متجهات EAP-AKA'، أو تجاهل ANID.	HSS قبل التحدي ويظهر السجل 'EAP-AKA فشل مصادقة vector unusable for EAP-AKA'
د من أن ن ANID networ تخدم كلا الجانبين	لم يتمكن الهاتف المحمول من التحقق من التحدي. السبب المعتاد هو عدم تطابق اسم	يجيب الهاتف المحمول على تحدي EAP-AKA' مع AKA-Client-Error

	السبب المحتمل	العرض
	الشبكة: استخرج HSS `CK'`/`IK'` باستخدام ANID مختلف عن قيمة `AT_KDF_INPUT`.	

سر مشترك خاطئ، نقطة وصول) EAP التي تحدث قبل أو حول تبادل RADIUS لرفضات طبقة انظر ،(غير معروفة RADIUS Shared Secrets ومرجع حالة Sessions.

تدفقات المكالمات

نظرة عامة

توضح هذه الصفحة تدفقات الرسائل من البداية إلى النهاية لـ OmniTWAG. كل تدفق هو مخطط تسلسل بين معدات المستخدم (UE)، نقطة الوصول WiFi (AP)، TWAG، وأقران الشبكة الأساسية: HSS (SWx)، PGW (S2a)، و OCS (Gy).

اقرأ صفحات الميزات الفردية للحصول على التفاصيل وراء كل خطوة: المصادقة، S2a GTP-C، الشحن عبر الإنترنت RADIUS، و بيانات اعتماد IP، مجموعات IP، طائرة المستخدم IP، إدارة عنوان الجلسات.

جدول المحتويات

- الجهات الفاعلة والواجهات
- الاتصال الناجح - محمي، مشحون
- الاتصال - NSWO مع مجموعة IP
- الاتصال - NSWO مع توزيع DHCP
- الاتصال (طائرة بيانات AP) - كسر محلي
- فشل المصادقة - المشترك غير مزود لـ SWx
- المحاسبة وإبلاغ الاستخدام
- نفاد الحصة وإعادة المنح
- إيقاف التشغيل - فصل المشترك
- إيقاف التشغيل - طرد المشغل من واجهة برمجة التطبيقات
- إيقاف التشغيل - مهلة النشاط
- متغيرات وضع الشحن

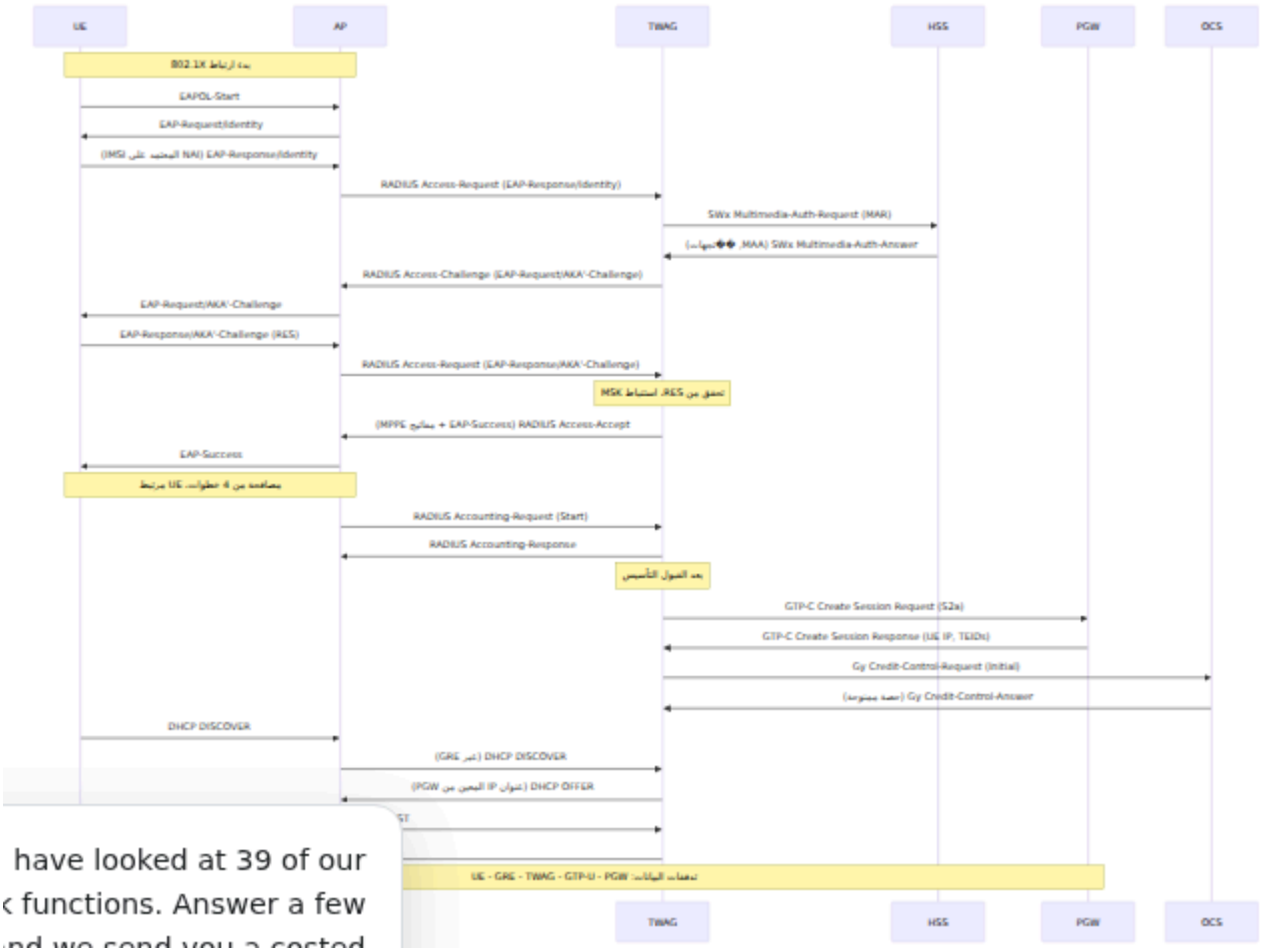
الجهات الفاعلة والواجهات

الجهة الفاعلة	الدور	الواجهة إلى TWAG
UE	جهاز مشترك مزود بشريحة SIM	802.11 / EAPOL (عبر AP)
AP	نقطة وصول WiFi وعميل RADIUS	RADIUS (UDP 1812 مصادقة، 1813 محاسبة)
TWAG	بوابة WiFi موثوقة وصول وخادم AAA 3GPP	-
HSS	خادم المشترك المنزلي	Diameter SWx (متجهات المصادقة)
PGW	بوابة الحزمة	GTP-C/GTP-U عبر S2a (محمي فقط)
OCS	نظام الشحن عبر الإنترنت	Diameter Gy (مشحون فقط)

يأتي نوع الكسر ووضع الشحن لجلسة من بيانات اعتماد AP. انظر بيانات اعتماد RADIUS.

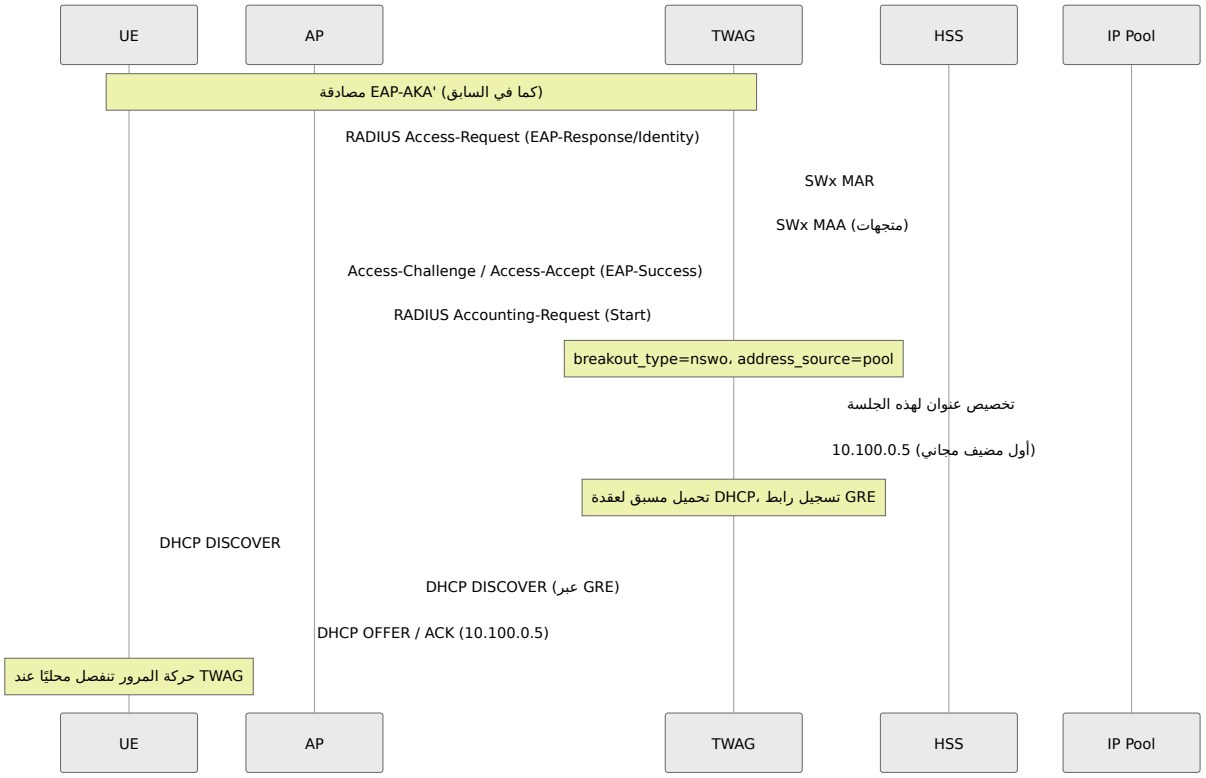
الاتصال الناجح - محمي، مشحون

هذا هو المسار الكامل السعيد لـ `breakout_type: tunneled` و `charging_mode: charged`. يقوم TWAG بمصادقة المشترك باستخدام EAP-AKA'، ويؤسس جلسة GTP إلى PGW، ويوفر عنوان IP المعين من PGW عبر DHCP، ويفتح جلسة شحن Gy.



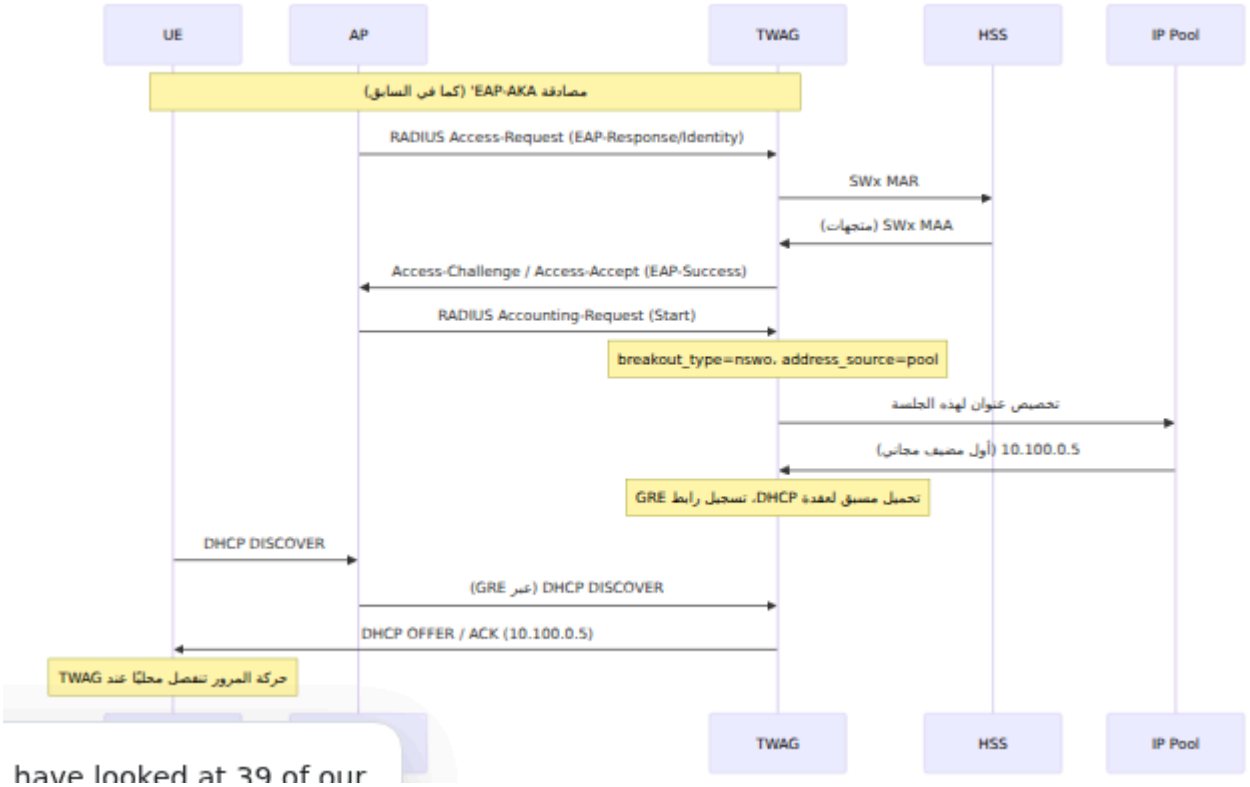
الاتصال - NSWO مع مجموعة IP

بالنسبة لـ `breakout_type: nswo` و `address_source: pool`، لا يتصل TWAG بـ PGW. تنفصل حركة DHCP. المرتبطة ويوفره عبر IP بتخصيص عنوان ثابت من مجموعة يقوم TWAG مرور المشترك محليًا.



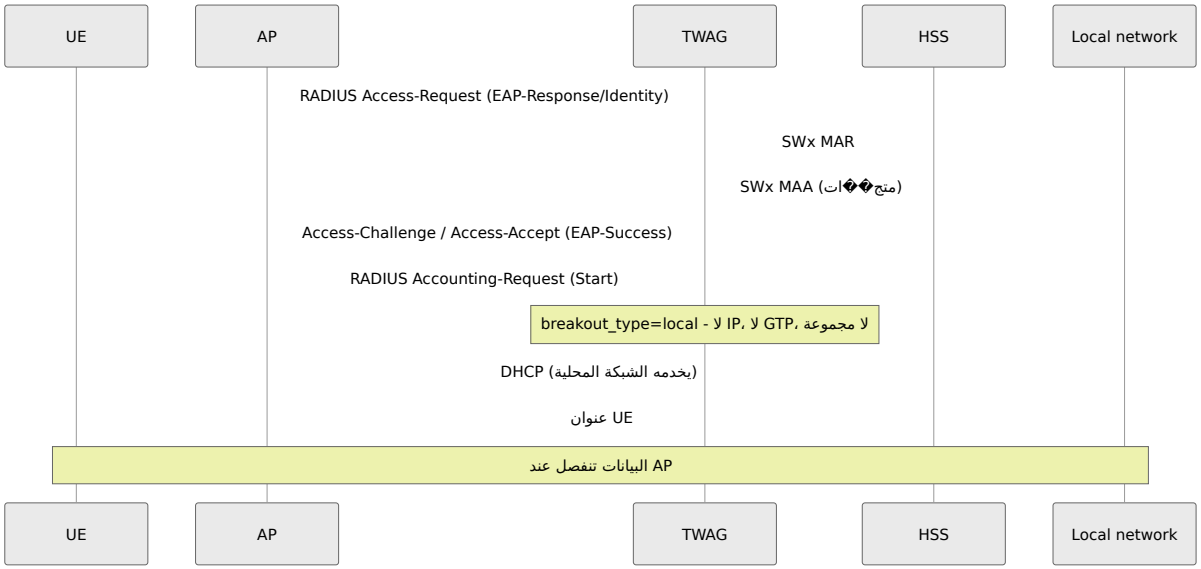
الاتصال - NSWO مع توزيع DHCP

بالنسبة لـ `breakout_type: nswo` و `address_source: dhcp`، يقوم TWAG بربط MAC بتوزيع العنوان المجاني التالي من نطاق المجموعة عندما DHCP العميل بالمجموعة. يقوم خادم يرسل UE DISCOVER. انظر مجموعة IP.



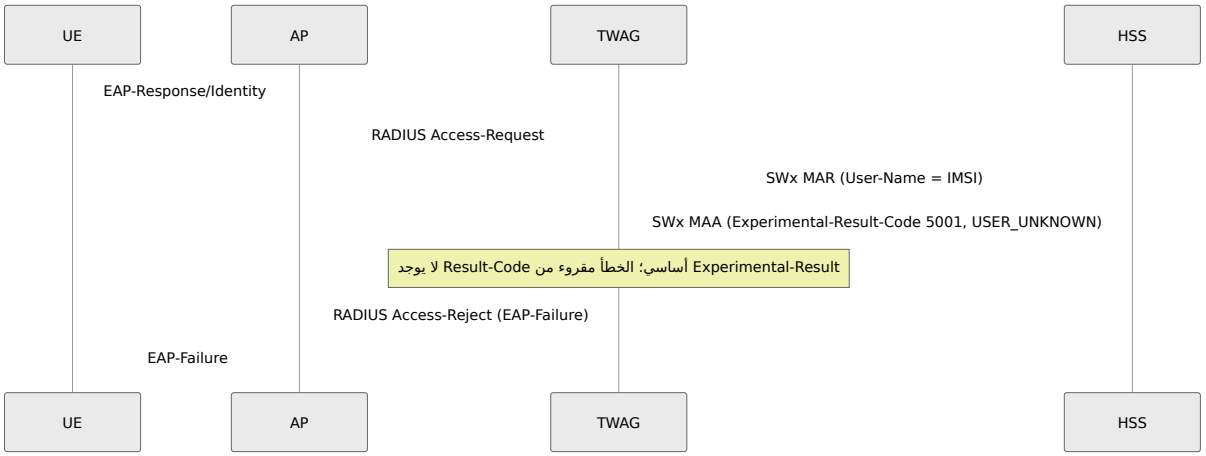
طائرة بيانات (AP) الاتصال - كسر محلي

بمصادقة TWAG طائرة البيانات. يقوم AP تمتلك ، `breakout_type: local` بالنسبة لـ أي TWAG على عنوانه من الشبكة المحلية. لا يؤسس UE يحصل IP. المشترك ولا يعين أي عنوان ولا عقدة GTP جلسة DHCP.



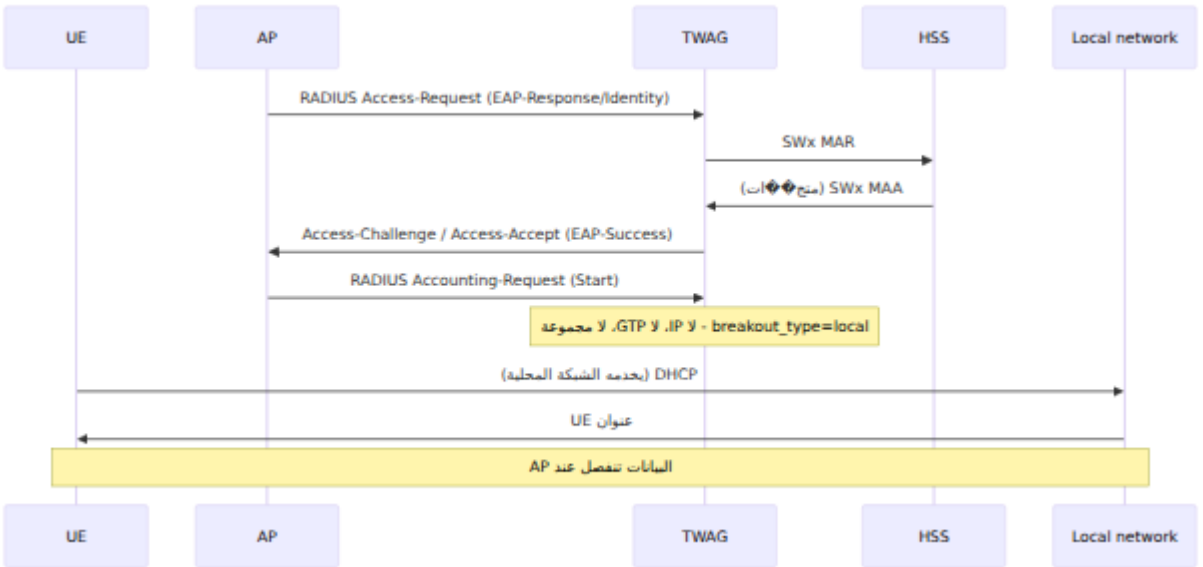
فشل المصادقة - المشترك غير مزود لـ SWx

تشير HSS إلى خطأ SWx في AVP المجمعة `Experimental-Result`، وليس في `Result-Code` إذا لم يكن لدى SWx في S6a الأساسي. يمكن أن يفشل مشترك معروف على HSS اشتراك غير 3GPP لـ IMSI. يرفض TWAG المصادقة. انظر الجلسة.



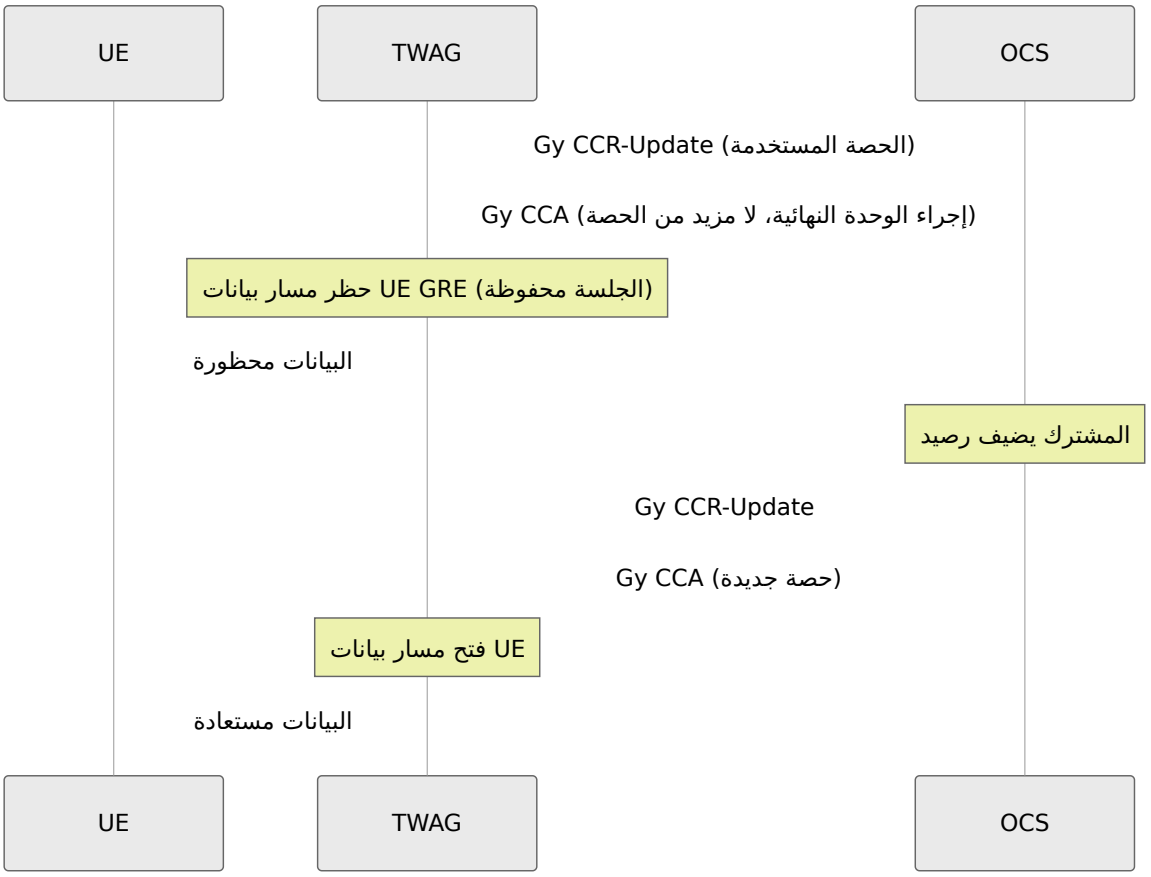
المحاسبة وإبلاغ الاستخدام

حركة المرور في الجلسة (انظر الجلسات)، وفي وضع TWAG يدمج RADIUS. ترسل AP محاسبة عند عتبة الحصة أو انتهاء مؤقت الصلاحية، وليس في كل OCS يبلغ عن الاستخدام إلى `charged`، تحديث مؤقت. انظر الشحن عبر الإنترنت.



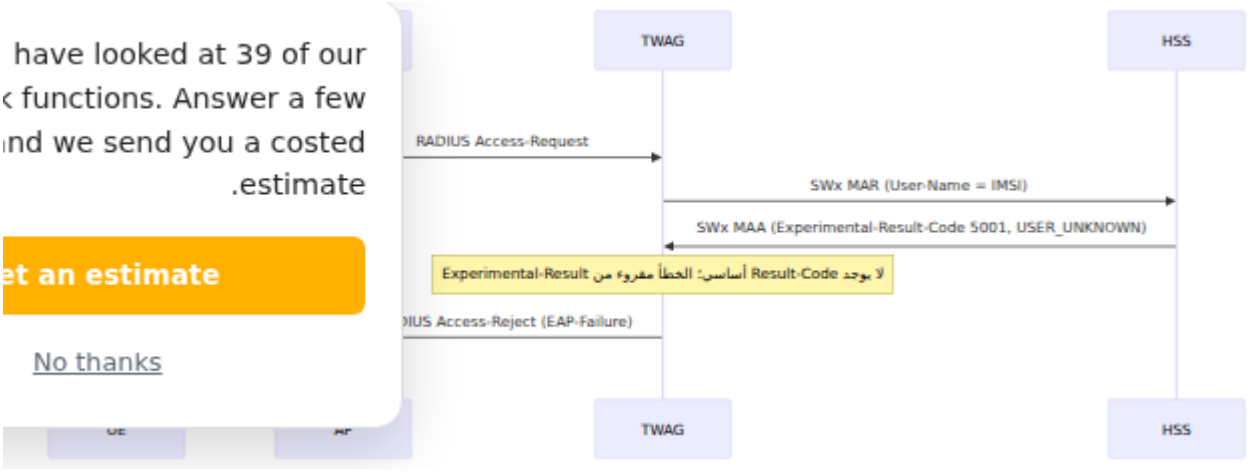
نفاد الحصة وإعادة المنح

بحظر مسار TWAG المزيد من الحصة، أو يحدد إجراء الوحدة النهائية، يقوم OCS عندما لا يمنح بيانات UE. يحتفظ TWAG حصة أعلى حتى يمكن أن يفتح بالجلسة، والعقدة، والمحاسبة UE. انظر الشحن عبر الإنترنت.



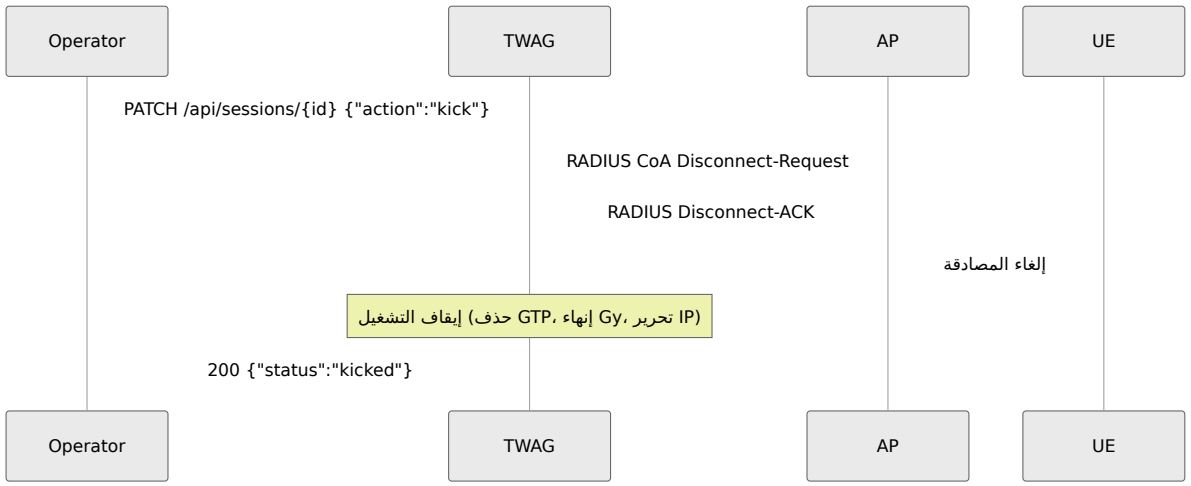
إيقاف التشغيل - فصل المشترك

بإيقاف الجلسة: يحذف جلسة TWAG طلب محاسبة توقف. يقوم AP ترسل UE، عندما ينفصل GTP (محمي)، يرسل Gy CCR-Terminate (مشحون)، ويزيل حالة الجلسة، يحرر العنوان.



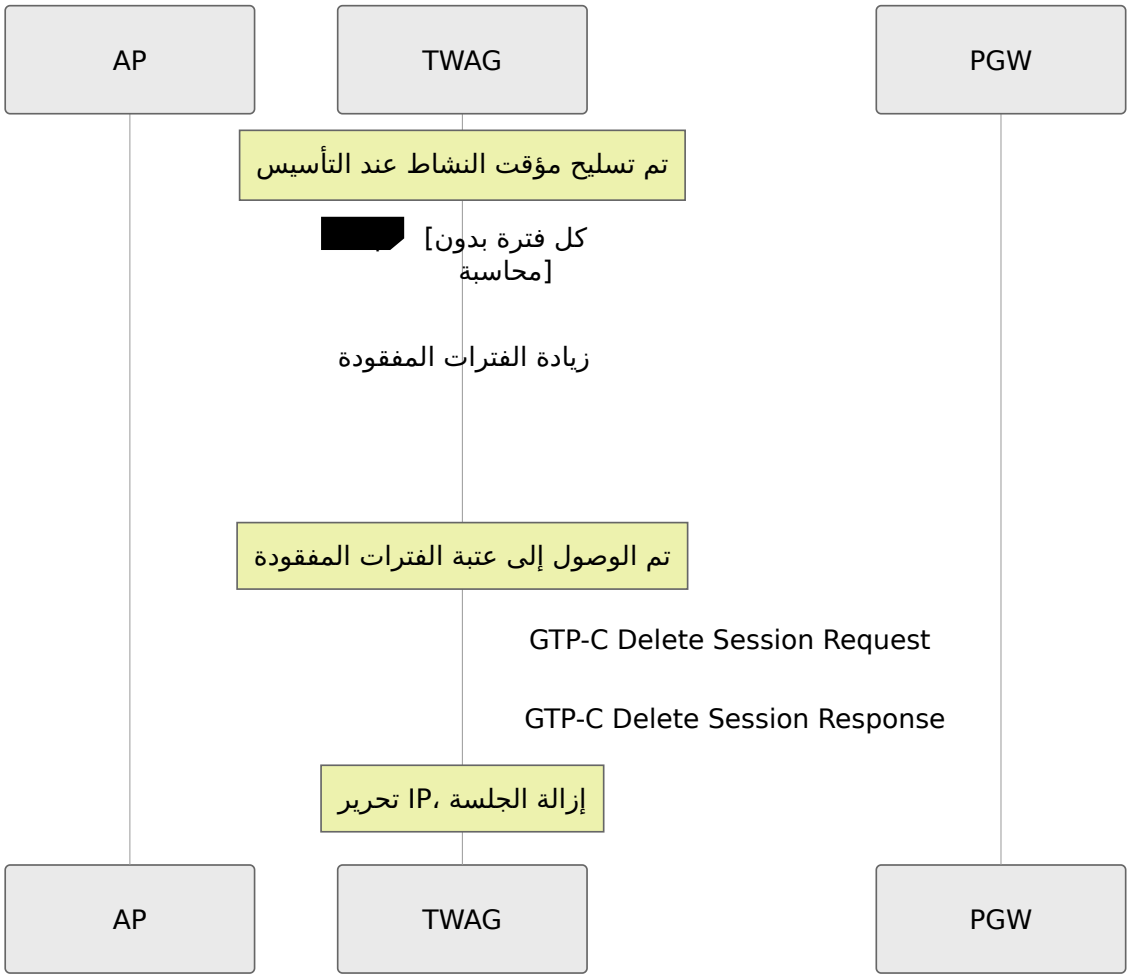
إيقاف التشغيل - طرد المشغل من واجهة برمجة التطبيقات

يمكن للمشغل إزالة جلسة عبر واجهة برمجة التطبيقات. يرسل TWAG طلب RADIUS CoA-Disconnect (Disconnect-Message) إلى AP، الذي يسقط UE، انظر ثم يوقف الجلسة. الجلسات.



إيقاف التشغيل - مهلة النشاط

يراقب TWAG جلسة قائمة مع مؤقت نشاط. تعيد تحديثات المحاسبة المؤقتة تعيين المؤقت. إذا لم أن الجلسة ميتة ويوقفها. يتم حصاد TWAG أي تحديثات لعدد الفترات المحددة، يعلن AP ترسل الجلسة التي لم تك��مل فيها المصادقة أبدًا بواسطة مهلة هوية منفصلة. انظر الجلسات.

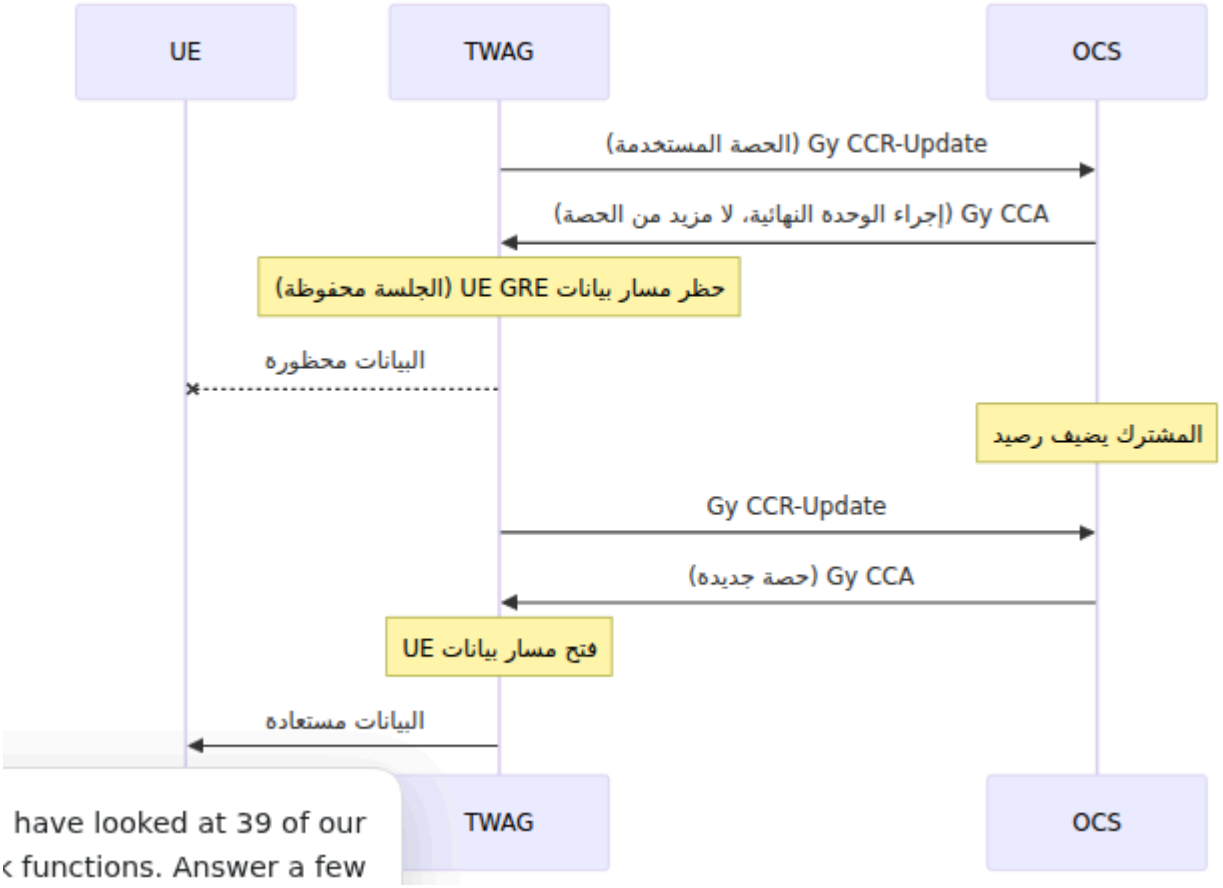


متغيرات وضع الشحن

خطوات ما بعد القبول. انظر بيانات اعتماد AP على بيانات اعتماد تغير `charging_mode` RADIUS.

charging_mode	جلسة البيانات	Gy
`charged`	تم التأسيس (حسب `breakout_type`)	CCR-Initial / Update / Terminate
`uncharged`	تم التأسيس (حسب `breakout_type`)	لا جلسة Gy
`auth_only`	لم يتم التأسيس	لا جلسة Gy

لا يرسل TWAG أعلاه، لكن NSWO يكون التدفق هو الاتصال المحمي أو `uncharged`، بالنسبة لـ `auth_only`، يتوقف التدفق بعد Access-Accept و Accounting-Start: لا يؤسس TWAG أي جلسة بيانات أي رسائل Gy. بالنسبة لـ



have looked at 39 of our
‹ functions. Answer a few

نظرة عامة

أوضاع الاتصال، WLCP، والتنقل

نظرة عامة

تشرح هذه الوثيقة أوضاع اتصال TWAG، في وبروتوكول التحكم WLAN (WLCP)، وسلوك اليوم. كما تحدد كل منطقة جزئية أو لم يتم دمجها OmniTWAG الانتقال. تصف ما يفعله برنامج بعد، حتى لا يخطط المشغلون حول سلوك لا يعمل به الكود.

يتبع TWAG نموذج WLAN 3 الموثوق في3GPP TS 23.402، القسم 16. بالنسبة للطبقة البيانات، انظر S2a والمصادقة، وإشارات التي تعتمد عليها هذه الأوضاع:

- العمارة: طبقة البيانات، دورة حياة الجلسة، والواجهات
- المصادقة: EAP-AKA / EAP-AKA' ومواد المفاتيح
- S2a GTP-C: إنشاء جلسة، حذف جلسة، وإشارات الحامل
- الجلسات: الجلسة المعتمدة ودورة حياتها
- الطبقة المستخدمة: GRE، GTP-U، وتوصيل DHCP
- المشتركة: تفريغ لكل نقطة وصول وتحصيل يتم تطبيقه بعد المصادقة أسرار RADIUS

جدول المحتويات

- نظرة عامة ومقارنة الأوضاع
- التفاوض على الوضع
- وضع الاتصال الفردي الشفاف (TSCM)
- وضع الاتصال الفردي (SCM)
- وضع الاتصال المتعدد (MCM) و WLCP
- الانتقال والتنقل
- التكوين
- الرؤية
- حالة التنفيذ

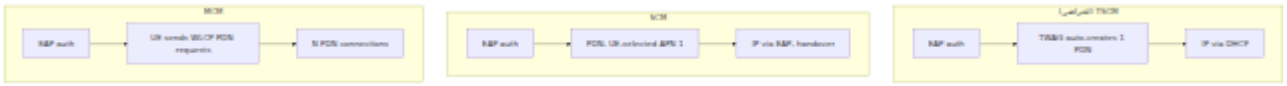
نظرة عامة ومقارنة الأوضاع

يدعم TWAG ثلاثة أوضاع اتصال لجهاز المستخدم (UE) الذي يصل إلى EPC من خلال WLAN الإشارة إلى UE الخاص به، وما إذا كان يمكن لـ IP لعنوان UE موثوق. يتحكم الوضع في كيفية تعلم APN، واحد PDN الاحتفاظ بأكثر من اتصال UE وما إذا كان يمكن لـ.

الخاصية	TSCM	SCM	MCM
رمز الوضع	`0`	`1`	`2`
الاسم الكامل	وضع الاتصال الفردي الشفاف	وضع الاتصال الفردي	وضع الاتصال المتعدد
اتصالات PDN لكل UE	واحد	واحد	عدة
تسليم عنوان IP	DHCP	EAP	EAP / WLCP
اختيار APN بالإشارة من UE	لا	نعم	نعم (لكل اتصال)
الانتقال مع الحفاظ على IP	لا	نعم	نعم
حوامل مخصصة	لا	نعم	نعم
بروتوكول التحكم في UE	لا شيء	لا شيء	WLCP (TS 24.244)
S2a على علم بـ UE	لا	نعم	نعم

إلى UE مع سلوك ما قبل الإصدار 12، حيث لا يشير TSCM هو الوضع الافتراضي. يتطابق TSCM عبر PGW المخصص من IP واحد، ويوصل عنوان PDN وينشئ اتصال، TWAG APN الشبكة. يختار DHCP.

`2` و `1` و `0` تتبع رموز الوضع AVP وضع الاتصال TWAN 3 في GPP TS 29.273.

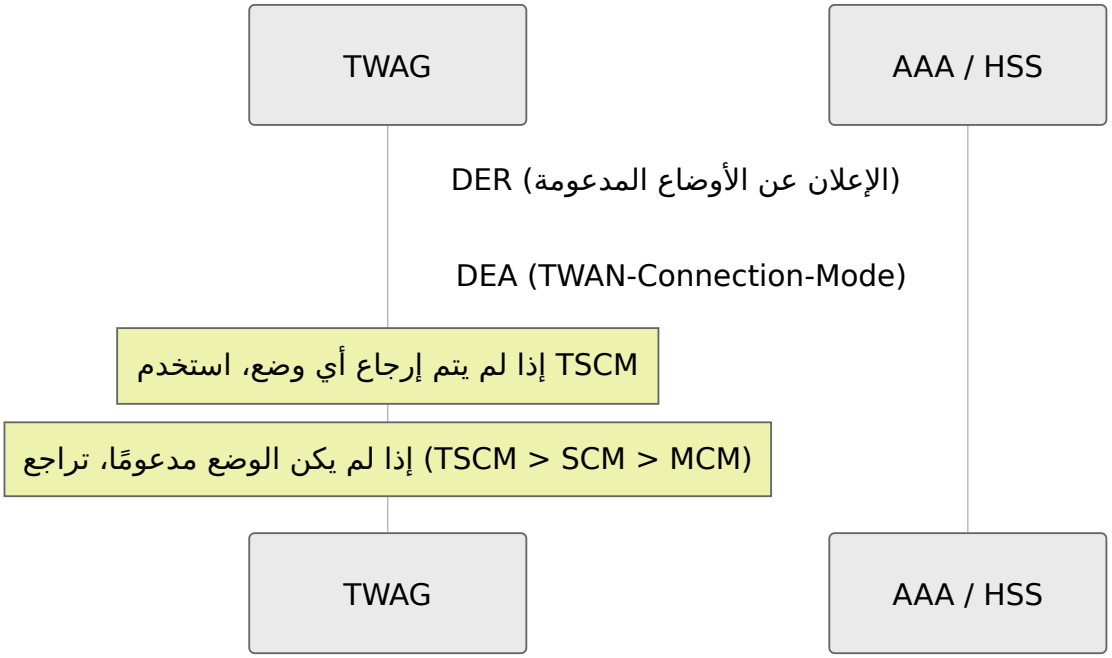


التفاوض على الوضع

انظر المصادقة. يتم التفاوض على وضع الاتصال أثناء المصادقة، في تبادل EAP الذي يحمل STa. التصميم هو EAP لتدفق نفسه:

1. يقوم TWAG بالإعلان عن الأوضاع التي يدعمها إلى خادم AAA. تأتي المجموعة المعلنة من مفتاح التكوين `connection_modes`.
2. يعيد خادم AAA الوضع المحدد في استجابة STa DEA، في AVP TWAN-Connection-Mode.
3. إذا لم يشير خادم AAA إلى وضع، يستخدم TWAG TSCM كافتراضي.

إذا اختار خادم AAA وضعًا لا يدعمه TWAG، يتراجع TWAG. تفضل ترتيب التراجع TSCM، ثم SCM، ثم MCM. يختار TWAG أول وضع مدعوم من هذا الترتيب.



يقرأ TWAG الوضع المحدد من أي من هذه المفاتيح في استجابة AAA، بالترتيب: `twan_connection_mode`، `TWAN-Connection-Mode`، `connection_mode`، أو `Connection-Mode`. يمكن أن تكون القيمة رمزًا رقميًا (`0`/`1`/`2`) أو ذرة (`:tscm`/`:scm`/`:mcm`). القيمة غير المعروفة تعود إلى TSCM.

على مسار STa، يعلن STa DER عن الوضع المدعوم المفضل لـ TWAG في AVP `TWAN-Connection-Mode`. يقوم STa DEA بقراءة الوضع المتفاوض عليه مرة أخرى ويعود إلى تحليل

TSCM عندما لا يحمل DEA أي شيء.

> **الحالة: الوضع المتفاوض عليه غير مفروض على مسار الجلسة الحية.** يقوم عميل STa (`StaClient`) ويقرأ الوضع المتفاوض عليه من DER بالإعلان عن الوضع المدعوم في ليس STa وحدة وضع الاتصال موجودة وتم اختبارها. ومع ذلك، فإن مسار المصادقة عبر DEA. مسار المصادقة RADIUS :��الحي، والعميل الحي لا يطبق أبدًا الوضع المتفاوض علي ليس لديها متصل على مسار الإرفاق، ومسار `store_connection_mode` نقطة الدخول لا انتقال بالإشارة من WLCP، لا DHCP عبر IP) TSCM الإرفاق والبيانات يتصرف دائمًا كـ UE أو APN). اليوم، تتبع كل جلسة حية مسار TSCM. انظر حالة التنفيذ.

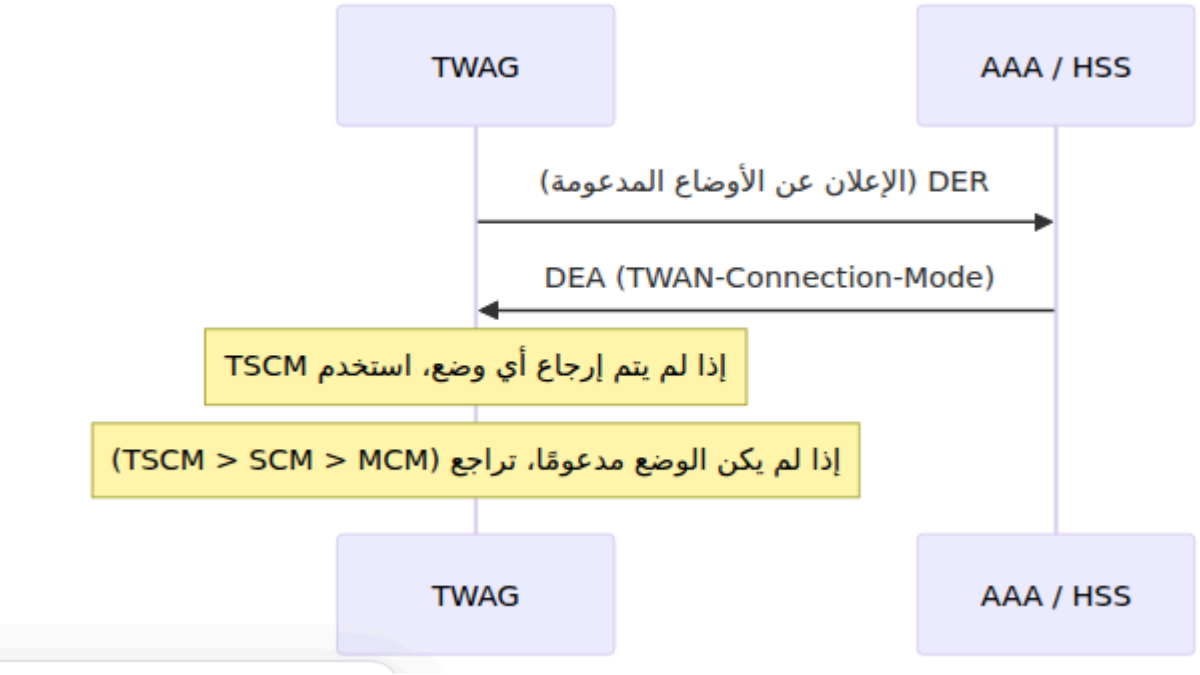
وضع الاتصال الفردي الشفاف (TSCM)

إلى UE هو الوضع الافتراضي والسلوك الذي يعمل به مسار الجلسة الحية اليوم. لا يشير TSCM الشبكة. يتم وصف TSCM هنا دورة حياة الجلسة، ويتم تلخيصه في العمارة.

في TSCM:

- يحتفظ UE باتصال PDN واحد.
- يختار TWAG APN. لا يمكن لـ UE طلب APN.
- يتلقى UE عنوان IP عبر به الخاص DHCP، يتم تقديمه بواسطة TWAG عبر نفق GRE. انظر الطبقة المستخدمة.
- لا توجد إشارات WLCP.
- غير UE بالإشارة من APN الحوامل المخصصة، واختيار IP، الانتقال مع الحفاظ على متاحة.

ينشئ TWAG جلسة S2a إلى PGW تلقائيًا بعد المصادقة. يرسل طلب إنشاء جلسة مع علم الخاص به لعنوان DHCP في خادم PGW المعين من IP الانتقال واضحًا. ثم يقوم بتخصيص عنوان MAC الخاص بـ UE. انظر S2a GTP-C للجلسة الناتجة ودورة والجلسات لتفاصيل إنشاء الجلسة و Gy. يتبع التحصيل للجلسة، عند تمكينه، عبر حياتها. انظر التحصيل عبر الإنترنت (Gy).



وضع الاتصال الفردي (SCM)

يحتفظ SCM باتصال PDN واحد لكل UE، لكن UE على علم بـ S2a. يضيف SCM هذه القدرات على TSCM:

- يتلقى UE عنوان IP عبر EAP الخاص به، وليس DHCP.
- يمكن لـ UE اختيار APN غير افتراضي.
- يحتفظ UE بعنوان IP 3 من الانتقال الخاص به عبر WLAN إلى 3GPP ومن WLAN إلى 3GPP.
- يمكن لـ PGW إنشاء حوامل مخصصة.

تبلغ وحدة وضع الاتصال عن هذه القدرات كوضع يقدم SCM عبر IP عبر EAP، ويدعم SCM. تصنف الانتقال، ويدعم اختيار APN، ويدعم الحوامل المخصصة.

> **الحالة: SCM** نموذج القدرة لـ **ليس بعد مسار تشغيل متميز.** SCM موجود، لكن كود SCM في AAA الذي يضعه خادم UE. إنشاء الجلسة لا يتفرع بعد على الوضع المتفاوض عليه. لا تعتمد على DHCP عبر IP، تم إنشاؤه تلقائيًا (PDN TSCM لا يزال يتم خدمته عبر مسار IP المقدم عبر EAP أو اختيار APN بالإشارة من UE لـ SCM في هذا الإصدار.

WLCP و وضع الاتصال المتعدد (MCM)

يتيح MCM لـ UE كل اتصال باستخدام UE في نفس الوقت. يدير PDN الاحتفاظ بعدة اتصالات بعد المصادقة، لا يقوم GPP TS 24.244المحدد في 3، بروتوكول التحكم في WLAN (WLCP). يقوم PDN WLCP. طلبات اتصال UE تلقائيًا. بدلاً من ذلك، يرسل PDN بإنشاء اتصال TWAG منفصلة نحو S2a GTP-C بجلسة PDN بربط كل اتصا TWAG PGW.

نقل WLCP

يعمل TWAG كخادم WLCP على منفذ UDP `2156`، وهو المنفذ القياسي لـ WLCP. يقوم الخادم بربط UE. يقوم الخادم بتوجيه كل حزمة إلى معالج جلسة WLCP لكل UE، معتمدًا على هوية UE ومينا IP مصدر عنوان UE بعد المصادقة بالهوية.

يتعامل القسم A.3.1. 16.1.4 TS 23.402 وفقًا لـ DTLS عبر WLCP في الإنتاج، تعمل إشارات الخادم الحالي مع طبقة UDP العادية فقط. لم يتم تطبيق DTLS بعد.

تنسيق رسالة WLCP

كل رسالة WLCP تحتوي على رأس ثابت، تليها قائمة من عناصر المعلومات (IEs).

```
(1 بايت) معرف المعاملة | (2 بايت) الطول | (1 بايت) نوع الرسالة |
IEs...
```

كل IE له هذا التنسيق:

```
نوع IE (1 بايت) | طول IE (2 بايت) | قيمة IE (متغير)
```

يحسب حقل `الطول` الرسالة الكاملة، بما في ذلك الرأس المكون من 4 بايت.

أنواع رسائل WLCP

الرمز	الرسالة	الاتجاه	الغرض
`0x01`	طلب اتصال PDN	UE إلى TWAG	طلب اتصال PDN جديد
`0x02`	قبول اتصال PDN	TWAG إلى UE	تم إنشاء الاتصال، مع IP / DNS / QoS
`0x03`	رفض اتصال PDN	TWAG إلى UE	تم رفض الاتصال، مع سبب
`0x04`	طلب فصل PDN	UE إلى TWAG	إنهاء اتصال PDN
`0x05`	قبول فصل PDN	TWAG إلى UE	تم فصل الاتصال
`0x06`	إشعار بيانات الاتجاه النزولي	TWAG إلى UE	إخطار UE ببيانات الاتجاه النزولي المعلقة

عناصر معلومات WLCP

الرمز	IE	ملاحظات
`0x01`	APN	سلسلة اسم نقطة الوصول
`0x02`	نوع PDN	`1` IPv4، `2` IPv6، `3` IPv4v6
`0x03`	PCO	خيارات تكوين البروتوكول
`0x04`	عنوان PDN	عنوان IP المخصص لـ UE (IPv4، IPv6، أو IPv4v6)
`0x05`	QoS الحامل	قيم MBR / GBR و QCI
`0x06`	TFT	نموذج تدفق البيانات
`0x07`	السبب	قيمة سبب النتيجة
`0x08`	معرف الحامل	هوية الحامل EPS (EBI)
`0x09`	عنوان DNS	عنوان DNS أو أكثر من عناوين خادم

قيم سبب WLCP

الرمز	سبب ا	المعنى
`0x10`	request_accepted	تم قبول الطلب
`0x20`	apn_not_allowed	APN غير مسموح به لهذا UE
`0x21`	no_resources	لا توجد موارد متاحة
`0x22`	unknown_apn	APN غير معروف
`0x23`	user_auth_failed	فشلت مصادقة المستخدم
`0x24`	network_failure	فشل الشبكة (فشل على سبيل المثال S2a)
`0x25`	pdn_type_not_supported	نوع PDN غير مدعوم المطلوب
`0x30`	request_rejected	تم رفض الطلب

إعداد اتصال PDN

عند وصول طلب اتصال PDN، يقوم معالج جلسة WLCP بتنفيذ هذه الخطوات:

1. يقرأ APN، نوع PDN، وPCO من الرسالة. إذا كان APN غائبًا، يستخدم `internet`. إذا كان نوع PDN غائبًا، يستخدم IPv4.
2. يتحقق من أن APN مسموح به. انظر `allowed_apns` في التكوين.
3. إذا لم يكن لدى UE IMSI معروف، يرفض الطلب بسبب `user_auth_failed`.
4. ينشئ جلسة S2a GTP-C نحو PGW لذلك APN، مع نوع RAT `3` (WLAN) وعلم الانتقال واضح.
5. يخزن اتصال GTP-U على PDN، معتمدًا EBI. عند النجاح، يسجل نفق PDN مع عنوان IP الخاص بـ UE، خوادم DNS، QoS الحامل، وعند وجوده، اتصال PDN وEBI.
6. في حالة فشل S2a، يرسل رفض اتصال PDN مع السبب `network_failure`.



إنهاء اتصال PDN

عند وصول طلب فصل PDN، يجد المعالج اتصال PDN بواسطة EBI. إذا كان EBI غير معروف، يرد S2a معروفًا، يقوم بحذف جلسة EBI إذا كان `request_rejected` بسبب رفض اتصال PDN. إزالة ا��اتصال، والرد بقبول فصل GTP-U، إلغاء تسجيل نفق GTP-C، عندما لا يتبقى لدى PDN. يتوقف معالج جلسة WLCP، اتصالات UE PDN.

إذا قام PGW المحلي. لا GTP-U المطابق ويحرر نفق PDN بحذف حامل، يزيل المعالج اتصال قد أطلق بالفعل الحامل PGW يرسل طلب حذف جلسة في هذه الحالة، لأن.

اشتقاق مفتاح WLCP

يحمي مفتاح WLCP `K_WLCP` إشارات WLCP. يتم اشتقاقه من مفتاح الجلسة الرئيسي (MSK) القسم 6.2 و الملحق A. يتبع الاشتقاق 3GPP TS 33.402 الذي تنتجه مصادقة EAP.

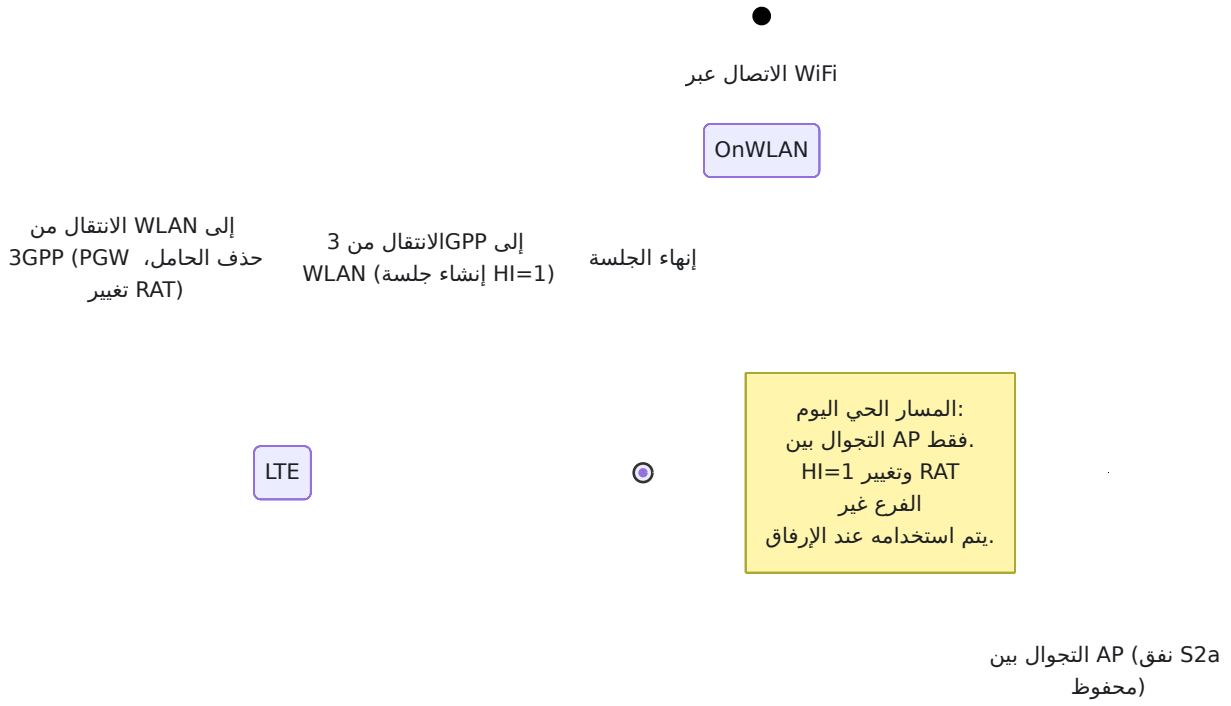
```
K_WLCP = HMAC-SHA-256(MSK, FC | P0 | L0)

FC = 0x21
P0 = عنوان IP لـ TWAG (4 بايت لـ IPv4، 16 بايت لـ IPv6)
L0 = طول P0 (2 بنظام بايت، big-endian)
```

يتم `P0` الخاص به من خلال معامل IP المفتاح بعنوان TWAG الناتج هو 32 بايت (256 بت). يربط TWAG لـ IP و علامة ثابتة عندما لا يكون عنوان MSK اشتقاق نسخة مبسطة من المفتاح من معروفًا بعد.

> **الحالة: MCM و WLCP جزئيان وغير مدمجين.** يوجد كود ترميز WLCP، وخادم WLCP واشتقاق المفتاح، وجميعها موجودة وتم اختبارها. لم يتم بدء UE، ومعالج جلسة لكل UDP، تشغيلها بواسطة التطبيق وليست مدفوعة بتدفق المصادقة. لم يتم تنفيذ ما يلي:
>
> - حماية DTLS لـ WLCP. يتم التعامل فقط مع UDP العادي.
> - إدارة الحامل المخصص داخل MCM. يحمل الترميز قيم QoS و TFT IEs، لكن المعالج لا يتصرف على إنشاء الحامل المخصص الذي بدأه PGW.
> - الانتقال داخل MCM.
> - يتم تعريف رسالة إشعار بيانات الاتجاه النزولي في الترميز ولكن لا يتم توليدها بواسطة معالج الجلسة.
>
> اعتبر MCM كمعاينة. لا تقم بتمكينه لأجهزة الإنتاج.

الانتقال والتنقل

يضع TWAG ثلاثة سيناريوهات تنقل وفقًا لـ TS 23.402. فقط التنقل بين نقاط الوصول (AP) نشط اليوم على مسار الجلسة الحية.



3 الانتقال من IGPP إلى WLAN

عندما ينتقل UE من LTE إلى WiFi، يجب على TWAG الحفاظ على جلسة IP الحالية. للقيام بذلك، يرسل TWAG طلب إنشاء جلسة مع علم الانتقال (HI) مضبوطًا. ثم يحتفظ PGW بعنوان IP الحالي وسياق الحامل، بدلاً من تخصيص عنوان جديد. انظر S2a GTP-C لتفاصيل إنشاء الجلسة وعناصر الإشارة.

يدعم S2a عملية إنشاء جلسة علم الانتقال. يمكن لمتعامل الانتقال توجيه حدث الانتقال إلى عميل UE مع تعيين علم الانتقال.

> **الحالة: المسار الرئيسي للجلسة لا يضبط علم الانتقال.** دائمًا ما يرسل إنشاء الجلسة التلقائي طلب إنشاء جلسة مع علم الانت��ال واضح. نتيجة لذلك، لا يتم استخدام بواسطة المسار العادي للإرفاق في هذا WLAN إلى GPPفي الانتقال من 3 IP الحفاظ على الإصدار.

WLAN 3 إلىGPP الانتقال من

عندما ينتقل UE من WiFi إلى LTE، يرسل PGW تغيير قيمة السبب إلى طلب حذف الحامل. تشير هذه القيم كسبب انتقال تغيير RAT: يعامل TWAG RAT.

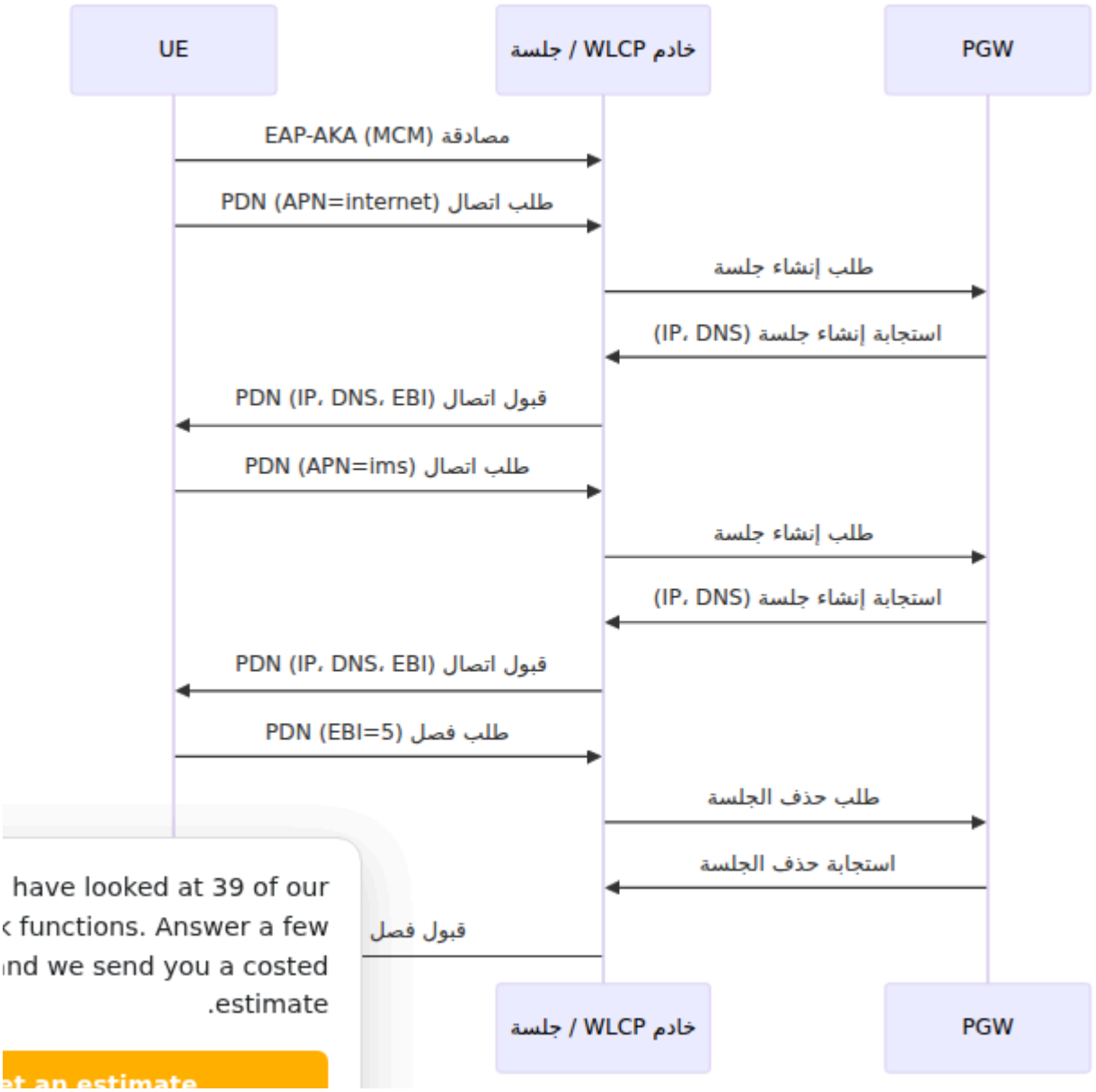
رمز السبب	الاسم
`4`	تم تغيير RAT (من 3GPP إلى غير 3GPP)
`5`	إلغاء تفعيل ISR
`10`	تم تغيير الوصول من غير 3GPP إلى 3GPP

محليًا. لا يرسل طلب حذف WiFi بتنظيف جلسة TWAG، يقوم RAT، عند حذف الحامل بسبب تغيير الخاص به على جانب IP بعنوان UE قد أطلق بالفعل الحامل. يحتفظ PGW، لأن جلسة GTP-C، LTE.

> **الحالة: معالج حذف الحامل لا يتفرع بناءً على السبب اليوم.** يتعامل عميل UE مع عن طريق إجراء تنظيف محلي ثم التوقف، لأي سبب. يوجد تصنيف PGW حذف الحامل من كمعاون، لكن لا يستخدم العميل السبب لاختيار مسا�؟ إنهاء مختلف RAT تغيير.

التنقل بين AP

نشطًا. يحتفظ S2a GTP، يبقى نفق TWAN، داخل نفس WiFi بين نقاط وصول UE عندما يتجول مختلفين. يقوم Called-Station-Id و NAS-IP-Address بنفس الهوية، لكنه يصل بعنوان UE ولا يقوم بإنهاء الجلسة. هذا يحافظ على UE في عملية عميل AP بتحديث بيانات تتبع TWAG استقرار عنوان IP الخاص بـ UE عبر تغيير AP.



هو المسار الوحيد للتنقل الذي يعمل به كود الجلسة الحية. يقوم بتحديث حقول AP التنقل بين AP. انظر AP الجديد في حالة تتبع AP ويسجل Called-Station-Id، وNAS-IP لـ UE عملية عميل المحاسبة لكل AP لبيانات تتبع AP.

التكوين

أوضاع الاتصال

القيمة هي `connection_modes`. قم بتعيين الأوضاع التي TWAG باستخدام مفتاح علن عنها��. الافتراضي هو قائمة من ذرات الوضع `[:tscm]`.

```
config :omnitwag,
  # أوضاع الاتصال التي يعلن عنها هذا TWAG إلى خادم AAA.
  connection_modes: [:tscm, :scm]
```

المعامل	النوع	مطلوب	الافتراضي	الوصف
`connection_modes`	قائمة	لا	`[:tscm]`	الأوضاع التي يعلن عنها TWAG. استخدم `:tscm`، `:scm`، و `:mcm`. الترتيب غير مهم. يتم فرز الرموز المعلنة قبل الاستخدام.

> **ملاحظة.** يتم قراءة المجموعة المعلنة بواسطة وحدة وضع الاتصال ويرسل عميل STa الوضع الحية بعد على الوضع المتفاوض RADIUS لا يتصرف مسار جلسة STa DER. المفضل في MCM. و SCM للإنتاج حتى يتم دمج `[:tscm]` عليه. انظر حالة التنفيذ. احتفظ بالافتراضي

خادم WLCP (MCM)

تعيش إعدادات خادم WLCP تحت مفتاح `:wlcp`. خادم WLCP ذو صلة فقط بـ MCM.

```
config :omnitwag,
  wlcp: %{
    enabled: true,
    port: 2156,
    allowed_apns: :all
  }
```

المعامل	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`false`	تمكين خادم WLCP. اترك `false` ما لم تختبر MCM.
`port`	عدد صحيح	لا	`2156`	منفذ UDP لـ WLCP. `2156` هو المنفذ القياسي لـ WLCP.
`allowed_apns`	ذرة أو قائمة	لا	`:all`	قائمة السماح لـ APN لطلبات PDN WLCP. استخدم `:all` للسماح بكل APN، أو قائمة APN، على سبيل المثال `["internet", "ims"]`. من سلاسل APN، يتم رفض الطلب لـ APN غير الموجود في القائمة بسبب `apn_not_allowed`.

> **ملاحظة.** لم يتم بدء تشغيل خادم WLCP بواسطة مشرف التطبيق في هذا الإصدار. تم تعريف مفتاح `enabled` للاستخدام في المستقبل.

التكوين ذي الصلة

يعيد مسار إعداد PDN لـ MCM استخدام إعدادات GTP لجلساته S2a. انظر ملخص التكوين في العمارة لكتلة `gtp`، بما في ذلك `pgw_ip`، `local_ip`، `mcc`، و `mnc`.

الرؤية

يصدر خادم WLCP أحداثًا تتعلق بالقياس. تغذي هذه الأحداث خط أنابيب ومعالجات ��لجلسة القياسatalog القياسات. انظر القياسات لك.

حدث القياس	يصدر عند
`[:wlcp, :packet, :received]`	تصل حزمة WLCP. تحمل `bytes`.
`[:wlcp, :packet, :malformed]`	فشلت حزمة في فك التشفير.
`[:wlcp, :packet, :unregistered]`	تصل حزمة من عنوان مصدر غير مسجل.
`[:wlcp, :pdn, :request]`	يتم استلام طلب اتصال PDN.
`[:wlcp, :pdn, :accept]`	تم إنشاء اتصال PDN.
`[:wlcp, :pdn, :reject]`	تم رفض اتصال PDN. تحمل السبب.
`[:wlcp, :pdn, :disconnect_request]`	يتم استلام طلب فصل PDN.
`[:wlcp, :pdn, :disconnect_accept]`	تم تحرير اتصال PDN.
`[:twag, :handover, :in]`	يتم توجيه حدث الانتقال من 3GPP إلى WLAN. تحمل `source`.
`[:twag, :handover, :out]`	يتم التعامل مع تغيير RAT من WLAN إلى 3GPP. تحمل `cause`.
`[:twag, :handover, :ap_change]`	يتم التعامل مع حدث التنقل بين AP.

يسجل خادم WLCP ومعالجات الجلسة أيضًا على مستوى المعلومات. يسجلون كل طلب اتصال قبول، رفض، وفصل، مع هوية UE، APN، وEBI. يسجل معالج الانتقال كل انتقال داخلي، مع هوية PDN، وتغيير AP، وتغيير RAT.

حالة التنفيذ

تلخص هذه الجدول ما يعمل على مسار الجلسة الحية، وما هو موجود ولكن غير مدمج، وما لم يتم تنفيذه. استخدمه للتخطيط حول السلوك الحقيقي.

الحالة	الميزة
حي	TSCM (افتراضي، PDN تم إنشاؤه تلقائيًا، IP عبر DHCP)
حي	التنقل بين AP (نفق S2a محفوظ)
لكن مسار الإرفاق دائمًا يزيله S2a، مدعوم في ترميز	إنشاء جلسة مع علم S2a الانتقال
موجود كوحدة، تم اختبارها	منطق التفاوض على وضع الاتصال والتراجع
موصول (يحمل STa DER وضع TWAN-Connection-Mode المفضل، بالإضافة إلى SSID / BSSID)	STa DER يعلن عن الأوضاع المدعومة
موصول (يحلل StaClient الوضع المتفاوض عليه، يعود إلى TSCM)	STa DEA يقرأ الوضع المحدد
غير موصول (`store_connection_mode` ليس له متصل على مسار الإرفاق)	الوضع المتفاوض عليه المطبق على الجلسة الحية
غير مدمج (يتم تقديمه كـ TSCM)	SCM كمسار تشغيل متميز (EAP IP، اختيار APN)
موجود، تم اختباره	ترميز WLCP (جميع أنواع الرسائل و IEs)
موجود، لم يتم بدء تشغيله بواسطة التطبيق	خادم WLCP UDP ومعالج جلسة لكل UE
موجود، تم اختباره	اشتقاق مفتاح WLCP (`K_WLCP`، FC=0x21)
موجود في المعالج، غير مدمج من النهاية إلى النهاية	MCM اتصالات PDN متعددة متزامنة

الميزة	الحالة
حماية DTLS لـ WLCP	لم يتم تنفيذه (العادي فقط UDP)
إدارة الحامل المخصص في MCM	لم يتم تنفيذه
توليد إشعار بيانات الاتجاه النزولي لـ WLCP	لم يتم تنفيذه (فقط الترميز)
الانتقال في MCM	لم يتم تنفيذه
الحفاظ على IP 3 منGPP إلى على مسار الإرفاق WLAN	لم يتم استخدامه (HI الإرفاق يزيل علم)
إنهاء WLAN 3 بسببGPP إلى سبب تغيير RAT	لم يتم تفرعه (تنظيف حذف الحامل مستقل عن السبب)

إدارة عنوان IP (DHCP / DHCPv6 / IPv6 RA / PCO)

نظرة عامة

تقوم OmniTWAG بتزويد كل UE بعنوان IP بعنوان هذا النظام. يغطي ومعلمات الشبكة المرتبطة به. لا P-CSCF و DNS و تسليم عناوين IPv6 (SLAAC) و إعلان موجه DHCPv6 و DHCPv4 الفرعي. يخترع النظام الفرعي عنوانًا بشكل عشوائي. إنه يقدم عنوانًا اختاره جزء آخر من النظام بالفعل. يعتمد المصدر على وضع AP لكل AP.

- يقوم **وضع النفق (الموجه المنزلي)** في PGW بتخصيص العنوان عبر S2a GTP، و تقوم OmniTWAG بتسليم نفس العنوان إلى UE. 3 يتبع هذا التصميمGPP TS 23.402 Section 16.2.
- **وضع** في **NSWO (الانفصال المحلي)** لا يوجد PGW. تقوم OmniTWAG بتخصيص **مجموعة** العنوان بنفسها من **IP** مجموعات انظر. محلية يحددها المشغل IP.

التي تتناسب مع مصدر AP يأتي الوضع ومصدر العنوان والمجموعة جمي��ها من بيانات اعتماد RADIUS. بيانات اعتماد انظر RADIUS لكيفية تطابق AP مع `breakout_type` و `address_source` و `ip_pool_id`.

انظر طائرة المستخدم المرجعية. بالنسبة لطائرة التحكم، لأوضاع التشغيل ومسار بيانات التي تدفع UE بالنسبة لآلة الحالة لكل. S2a GTP-C انظر، PCO و PAA التي تحمل GTP-C التخصيص، انظر الجلسات.

جدول المحتويات

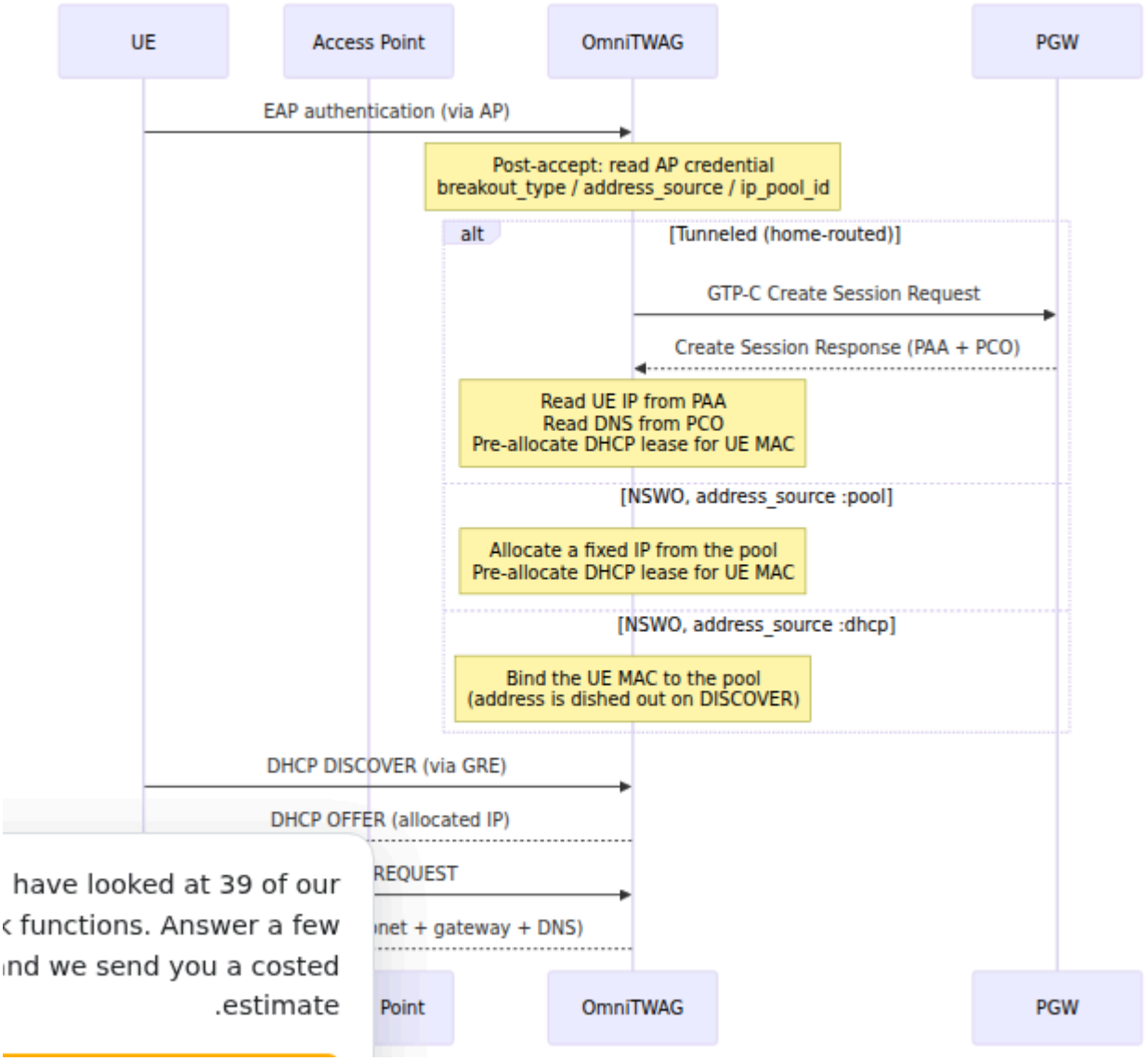
- نظرة عامة: من يخصص العنوان
- مصادر العنوان
- الجلسات النفقية: عنوان مخصص من PGW
- جلسات NSWO: و المجموعة dhcp
- DHCPv4
- DHCPv6

- إعلان موجه IPv6 (SLAAC)
- تسليم DNS و PCO
- مجموعات العناوين والاستنفاد
- التكوين
- الرؤية
- استكشاف الأخطاء وإصلاحها

نظرة عامة: من يخصص العنوان

تشغل OmniTWAG خادم DHCPv4 خفيف الوزن، وخادم DHCPv6 بدون حالة وذو حالة. لا تقوم هذه الخوادم بمسح نطاق للعثور على عنوان مجاني في الحالة النفقية. إعلان موجه IPv6. يخدم نفس خادم NSWO، DHCPv4 عنوانًا بالفعل. في وضع PGW إنها تقدم العنوان الذي خصصه أخذته OmniTWAG من مجموعة IP المحلية.

يقوم عملية جلسة per-UE، Access-Accept بالمصادقة. بعد UE تبدأ تدفق العنوان عندما يقوم لتحديد الوضع ثم AP بتشغيل خطوة إنشاء بعد القبول. تقوم هذه الخطوة بقراءة بيانات اعتماد تخصيص العنوان بالطريق الصحيح.



مصادر العنوان

مصدر العنوان من خلال حقلين AP تحدد بيانات اعتماد:

- `breakout_type`: `:tunneled`، `:nswo`، أو `:local`.
- `address_source`: `:pool` أو `:dhcp`. ينطبق هذا فقط عندما يكون `breakout_type` هو `:nswo`.

الوضع	بيانات الاعتماد	UE من يختار عنوان	كيف يصل إلى UE
نفق (موجه منزلي)	`breakout_type::tunneled`	PGW، في استجابة إنشاء جلسة GTP-C PAA.	عقد إيجار DHCPv4 مسبق، DHCPv6، أو IPv6 RA.
NSWO، ثابت	`breakout_type::nswo`، `address_source::pool`	OmniTWAG، من مجموعة `ip_pool_id`، عند الإنشاء.	عقد إيجار DHCPv4 مسبق.
NSWO، توزيع	`breakout_type::nswo`، `address_source::dhcp`	OmniTWAG، من مجموعة `ip_pool_id`، عند DISCOVER.	توزيع مجموعة عند DHCPv4 DISCOVER.
محلي AP	`breakout_type::local`	الشبكة المحلية خلف AP.	لا تقوم OmniTWAG بتخصيص أي عنوان.

مع بيانات الاعتماد، انظر بيانات RADIUS للحصول على حقول بيانات الاعتماد وكيفية تطابق مصدر اعتماد RADIUS. لمتجر المجموعة، انظر مجموعات IP.

الجلسات النفقية: عنوان مخصص من PGW

مع طلب إنشاء جلسة PGW إلى S2a بإنشاء جلسة OmniTWAG بالنسبة لجلسة نفقية، تقوم باستجابة إنشاء جلسة. تحمل الاستجابة شيئين يستخدمهما هذا النظام GTP-C. يجيب PGW الفرعي:

- **تخصيص عنوان PDN (PAA)**. هذا هو عنوان IP الخاص بـ UE.
- **خيارات تكوين البروتوكول (PCO)**. تحمل خوادم DNS، وعناوين P-CSCF، وMTU، الرابط.

مسبقًا بتخصيص عقد إيجار OmniTWAG من الاستجابة. ثم تقوم PCO و OmniTWAG PAA تقرأ بهذا العنوان OmniTWAG، ترد DHCP، طلب UE عندما يرسل UE. الخاص بـ MAC لعنوان DHCP لتبادل إنشاء S2a GTP-C. انظر PGW. أبدًا عنوانًا لم يخصصه UE المخصص مسبقًا. لا يتلقى الجلسة.

يحدد نوع PAA أي عنوان تقدمه OmniTWAG.

نوع PAA	العنوان المقدم إلى UE
`ipv4`	عنوان IPv4 من PAA.
`ipv6`	عنوان IPv6 من PAA.
`ipv4v6`	عنوان IPv4 من PAA.

مسبقًا بتخصيص عقد إيجار. OmniTWAG فلا تقوم PAA، إذا لم تحتوي استجابة إنشاء الجلسة على أي عنوان UE في تلك الحالة، لا يتلقى.

جلسات NSWO: و dhcp المجموعة

مساحة العنوان. يأتي العنوان من OmniTWAG لذا تمتلك PGW، على NSWO لا تحتوي جلسة تحتوي المجموعة على CIDR IPv4، المسماة بواسطة بيانات الاعتماد IP مجموعة `ip_pool_id`. ومدة إيجار. انظر مجموعات IP. و بوابة، وقائمة خوادم DNS،

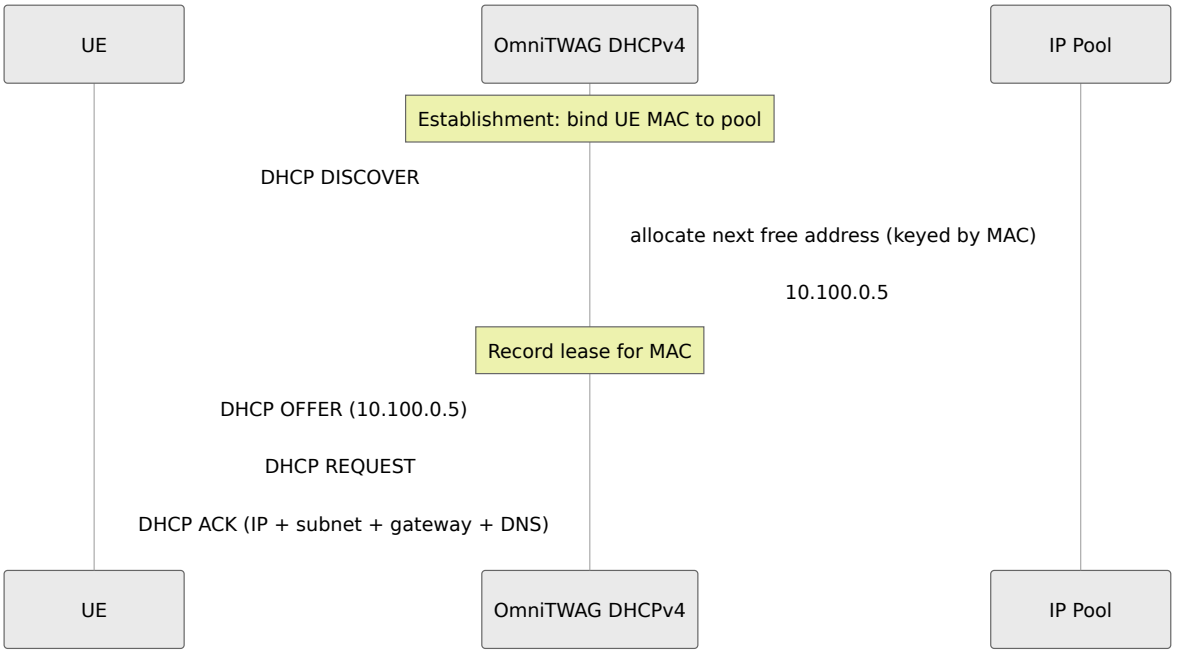
يحدد حقل `address_source` في بيانات الاعتماد كيفية وصول عنوان المجموعة إلى UE.

`address_source: :pool` (ثابت)

بتخصيص عنوان واحد من المجموعة، معتمدًا على هوية OmniTWAG عند إنشاء بعد القبول، تقوم المشترك. التخصيص هو غير متغير، لذا تحتفظ نفس الهوية بنفس العنوان عبر إعادة الإنشاء. تقوم بهذا العنوان، UE الخاص بـ MAC لعنوان DHCPv4 مسبقًا بتخصيص عقد إيجار OmniTWAG الخاص CIDR الخاصة بالمجموعة، وقناع الشبكة المشتق من DNS وبوابة المجموعة، وخوادم في هذه المرحلة. عندما يرسل GRE في مسار بيانات UE بالمجموعة. كما تسجل UE DISCOVER، يقدم الخادم العنوان المخصص مسبقًا.

`address_source: :dhcp` (توزيع عند DISCOVER)

UE الخاص بـ MAC بتخصيص عنوان بعد. إنها **ترتبط** عنوان OmniTWAG عند الإنشاء، لا تقوم بتخصيص العنوان DHCPv4 يقوم خادم DISCOVER DHCP من ذلك MAC، بالمجموعة. عند أول المجاني التالي من نطاق المجموعة، ويسجل عقد الإيجار، ويقدمه. هذا هو مسار التوزيع الديناميكي وليس عند الإنشاء، DISCOVER الجديد. يتم اختيار العنوان في وقت.



تزيل الارتباط ، `:dhcp` بإلغاء تخصيص المجموعة، ولـ OmniTWAG عند إنهاء الجلسة، تقوم AP بالمجموعة وعقد الإيجار الديناميكي. إذا كانت المجموعة مفقودة أو مستنفدة، أو لم يكن لدى `ip_pool_id`، فلا تقوم OmniTWAG بتخصيص أي عنوان ويتولى UE تخصيص عنوانه بنفسه.

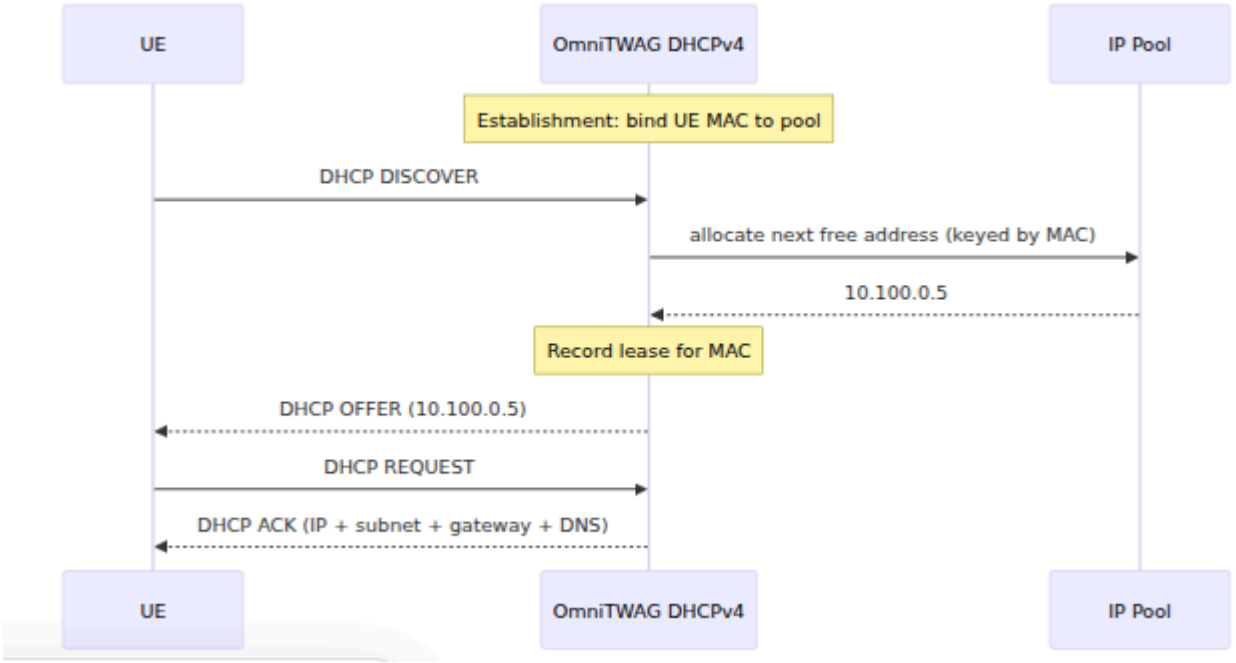
DHCPv4

في الذاكرة، ETS يخزن كل عقد إيجار في جدول. يستمع خادم DHCPv4 على منفذ UDP `67`. يصل عقد الإيجار إلى الجدول من خلال أحد مسارين. UE الخاص بـ MAC معتمدًا على عنوان.

- عنوانًا PGW **مسبق التخصيص.** تقوم عملية الجلسة بإدراج عقد إيجار عندما يخصص (نفق) أو عندما تقوم OmniTWAG بتخصيص عنوان ثابت من المجموعة (NSWO `address_source: :pool`).
- **توزيع عند DISCOVER.** بالنسبة لـ NSWO `address_source: :dhcp`، تقوم بالمجموعة. يحتفظ الخادم UE الخاص بـ MAC عملية الجلسة بدلاً من ذلك بربط عنوان مرتبط بدون عقد إيجار، MAC من DISCOVER في الذاكرة. عند أول MAC بربط لكل يقوم الخادم بتخصيص العنوان المجاني التالي من المجموعة، ويسجل عقد الإيجار، ويقدمه.

دورة حياة عقد الإيجار

بالنسبة لعقد إيجار مسبق التخصيص، يقدم الخادم العنوان الذي يوجد بالفعل في الجدول لعنوان MAC المرتبط، يقوم الخادم بإنشاء عقد الإيجار عند DISCOVER المطلوب. بالنسبة لعنوان MAC عن طريق توزيعه من المجموعة.



تتعامل OmniTWAG مع هذه الأنواع من رسائل DHCP.

الرسالة	رمز النوع	سلوك OmniTWAG
DISCOVER	1	إذا كان هناك عقد إيجار موجود لعنوان MAC، ترسل OmniTWAG OFFER. إذا لم يكن هناك عقد إيجار موجود ولكن عنوان MAC مرتبط بمجموعة، تقوم OmniTWAG بتوزيع العنوان المجاني التالي من المجموعة، وتسجيل عقد الإيجار، وإرسال OFFER. إذا لم يكن هناك عقد إيجار ولا ارتباط موجود، تسجل OmniTWAG تحذيرًا وترسل لا شيء.
REQUEST	3	إذا كان هناك عقد إيجار موجود والعنوان المطلوب (الخيار 50) يتطابق مع عقد الإيجار، أو إذا لم يكن الطلب يحتوي على عنوان IP مطلوب، ترسل OmniTWAG ACK. إذا لم يتطابق العنوان المطلوب، ترسل OmniTWAG NAK. إذا لم يكن هناك عقد إيجار موجود، ترسل OmniTWAG NAK.
RELEASE	7	تقوم OmniTWAG بوضع علامة على عقد الإيجار كـ `released`. تحتفظ OmniTWAG بسجل عقد الإيجار. تبقى اتصال PDN نشطًا، وفقًا لـ TS 23.402 §16.1.5.2 NOTE 2.
DECLINE	4	تسجل OmniTWAG بسجل عقد OmniTWAG تحذيرًا. تحتفظ الإيجار.
INFORM	8	ترسل OmniTWAG ACK مع التكوين فقط. يحمل ACK البوابة، وقناع الشبكة، وDNS (ولكن لا يحمل عنوانًا هو `yiaddr` و `0.0.0.0`).

بالنسبة لـ INFORM، تستخدم OmniTWAG `default_subnet_mask` و `default_gateway` من التكوين. تستخدم OmniTWAG `8.8.8.8` كخادم DNS في رد INFORM.

محتويات عقد الإيجار

يحمل كل عقد إيجار عنوان UE IP، وخوادم DNS، وقناع الشبكة، والبوابة، ومدة الإيجار. بالنسبة لجلسة نفقية، تقوم عملية الجلسة بتعيين عنوان UE IP وخوادم DNS من استجابة PGW، وقناع الشبكة، والبوابة، ومدة الإيجار من تكوين DHCP. بالنسبة لجلسة NSWO، تأتي هذه القيم من تكوين IP: مجموعة CIDR الخاصة بالمجموعة، وقناع الشبكة من بادئة العنوان من نطاق المجموعة، ومدة الإيجار من سجل المجموعة. انظر مجموعات، DNS، والبوابة، وخو��دم IP و التكوين.

كما يحتوي سجل عقد الإيجار على وقت `allocated_at` ووقت `expires_at`. وقت هذه القيم OmniTWAG بالإضافة إلى مدة الإيجار. تستخدم `allocated_at` هو `expires_at` للإبلاغ عن حالة الإيجار. يعمل جامع في الخلفية كل 60 ثانية ويحذف أي عقد إيجار تجاوز وقته `expires_at`. عقد الإيجار الذي لديه مدة إيجار صفر ليس لديه `expires_at` ولا ينتهي أبدًا. يتم أيضًا إزالة عقد الإيجار عند إنهاء الجلسة.

خيارات DHCP في الرد

تبني OmniTWAG كل OFFER و ACK مع هذه الخيارات DHCP.

الخيار	الرمز	المحتوى
نوع الرسالة	53	OFFER أو ACK.
معرف الخادم	54	عنوان DHCP `server_ip`.
قناع الشبكة	1	قناع الشبكة لعقد الإيجار.
الموجه	3	بوابة عقد الإيجار.
خادم اسم النطاق	6	خوادم DNS لعقد الإيجار. يتم حذفها إذا كانت القائمة فارغة.
مدة إيجار عنوان IP	51	مدة الإيجار بالثواني. يتم حذفها إذا كانت مدة الإيجار صفر.
عنوان البث	28	يتم حسابه من IP وقناع الشبكة. يتم إرساله فقط إذا كانت UE تسرد هذا الخيار في قائمة طلب المعلمات الخاصة بها (الخيار 55).

نقل DHCP عبر GRE

داخل إطار UE الخاص بـ DHCP تقوم بإعادة توجيه طلب GRE نقطة وصول تستخدم نفق GRE. يقوم خادم DHCP باستخراج الحمولة ويمررها إلى خادم Ethernet مغلف بـ GRE، الرد، OmniTWAG المصدر. عندما تبني AP بتوسيم الحزمة بعنوان OmniTWAG تقوم DHCPv4. وترسل الإطار مرة أخرى عبر نفق UDP/IP/Ethernet في إطار DHCP تقوم بلف الحمولة GRE إلى نفس AP. `68` والوجهة هي عنوان البث على منفذ العميل `10.0.0.1:67` المصدر هو.

يتم الرد على طلب DHCP يصل مباشرة إلى مقبس UDP (ليس عبر GRE) على مقبس UDP. إذا ترد على عنوان المصدر OmniTWAG لم يكن منفذ المصدر هو منفذ العميل القياسي `68`، فإن OmniTWAG RFC 2131 ومنفذ المصدر. يدعم هذا المسار أدوات الاختبار والعمليات. ��لاف ذلك، تتبع صفرًا، وتستخدم `ciaddr` تستخدم عنوان البث إذا تم تعيين علامة البث أو إذا كان :`ciaddr` إذا تم تعيين هذا العنوان.

DHCPv6

يستمع خادم DHCPv6 على منفذ UDP `547` عبر IPv6. يدعم كل من وضع بدون حالة ووضع ذو حالة.

- **وضع بدون حالة** يرد على طلب معلومات (النوع 11) مع رد معلومات (النوع 12). يحمل الرد خوادم DNS. يتبع هذا RFC 3736 و RFC 3646. يستخدم UE هذا الوضع الخاصة به RA من معالجة "التكوين الآخر (O)" عندما يقوم بتعيين علامة.
- **وضع ذو حالة** يرد على طلب (النوع 1) مع إعلان (النوع 2)، وطلب (النوع 3) مع رد مسبق التخصيص في خيار IPv6 (النوع 7). يقوم هذا الوضع بتسليم عنوان IA_NA. يتبع هذا RFC 3315.

بإدراج GTP عميل. تقوم طائرة التحكم DUID يقوم الخادم مسبقًا بتخصيص عنوان ذو حالة لكل العميل DUID التخصيص. يحتفظ الخادم بهذه التخصيصات في جدول في الذاكرة، معتمدًا على.

معالجة رسائل DHCPv6

الرسالة	النوع	سلوك OmniTWAG
طلب معلومات	11	ترسل OmniTWAG رد معلومات مع DUID الخادم، ومعرف العميل المنعكس، وخوادم DNS.
طلب	1	ترسل OmniTWAG إعلان. إذا كان لدى العميل تخصيص، DUID إذا لم يكن كذلك، يحمل الإعلان حالة. IA_NA يحمل الإعلان عنوان `NoAddrsAvail` (الرمز 2).
طلب	3	ترسل OmniTWAG رد. يؤكد الرد عنوان IA_NA لـ DUID العميل.
أنواع أخرى	-	تتجاهل OmniTWAG الرسالة.

كل رد يتضمن عنوانًا مخصصًا. RFC 3315 §15 كل رد يعكس معرف المعاملة للعميل، وفقًا لـ يضبط مؤقتات DHCPv6 الإيجار. T1 هو نصف مدة الإيجار. T2 هو أربعة أخماس مدة الإيجار.

DUID الخادم

تستخدم رقم المؤسسة (رقم المؤسسة DUID-EN) خادم من النوع OmniTWAG DUID تبني 3GPP `10415`. يتم اشتقاق المعرف من اسم العقدة، لذا فهو مستقر لعقدة معينة.

خيارات DHCPv6 في الرد

الخيار	الرمز	المحتوى
معرف العميل	1	معرف العميل المنعكس من الطلب، إذا كان موجودًا.
معرف الخادم	2	DUID الخادم.
جمعية الهوية للعناوين غير المؤقتة (IA_NA)	3	عنوان IPv6 المخصص، أو حالة `NoAddrsAvail`. وضع ذو حالة فقط.
خادم اسم النطاق المتكرر	23	خوادم DNS المكونة. يتم حذفها إذا كانت القائمة فارغة.
قائمة البحث عن النطاق	24	قائمة البحث المكونة. يتم إرسالها فقط إذا تم تعيين `dhcpv6_domain_list`.

إعلان موجه IPv6 (SLAAC)

مع تكوين عنوان بدون حالة UEs إلى PGW المخصصة من IPv6 بادئات IPv6 يقدم خادم RA (SLAAC). يقوم بتنفيذ إعلان موجه ICMPv6 وفقًا لـ RFC 4861.

بادئة لكل واجهة. يحتفظ الخادم بالبادئات في الذاكرة، مجمعة حسب GTP تضيف طائرة التحكم اسم الواجهة. يرسل الخادم إعلان موجه في حالتين:

1. على مؤقت دوري. الفاصل الزمني الافتراضي هو `30` ثانية.
2. على واجهة RA عند الطلب، عندما تطلب طائرة التحكم.

يقوم الخادم أيضًا بتحليل رسائل طلب الموجه (ICMPv6 النوع 133).

محتويات إعلان الموجه

يحمل كل إعلان موجه هذه الحقول والخيارات.

الحقل أو الخيار	القيمة
حد القفز الحالي	من `hop_limit`. `64` الافتراضي.
عمر الموجه	من `router_lifetime`. ثانية `1800` الافتراضي.
علامات O و M	إلى تكوين عنوان مُدار أو تكوين آخر RA كلاهما `0`. لا يشير
عنوان رابط المصدر (الخيار 1)	المصدر، إذا كان قيمة 6 بايت عنوان MAC.
MTU (الخيار 5)	يتم تضمينه فقط إذا تم توفير MTU.
معلومات البادئة (الخيار 3)	A و (على الرابط) L واحدة لكل بادئة. يتم تعيين علامات (مستقل).
خادم DNS المتكرر، RDNSS (الخيار 25)	من البادئات، وفقًا لـ DNS خوادم RFC 8106. يتم حذفها إذا لم تكن هناك خوادم DNS.

يحمل كل خيار معلومات البادئة البادئة، وطول البادئة، ومدة الصلاحية (الافتراضي `86400` ثانية)، تم تعيينها، يقوم UE بتشكيل A ومدة الصلاحية المفضلة (الافتراضي `14400` ثانية). نظرًا لأن علامة عنوان IPv6 هي أكبر مدة صلاحية صالحة عبر البادئات RDNSS الخاص به من البادئة. مدة.

تسليم DNS و PCO

تقوم OmniTWAG بتسليم معلومات DNS و P-CSCF هو المصدر. بعدة طرق PCO PGW حيثما كان ذلك ممكنًا، والتكوين بخلاف ذلك.

PCO من PGW

يقرأ محلل PCO 3 خيارات تكوين البروتوكول من استجابة إنشاء الجلسة، وفقًا لـ GPP TS 24.008. يعيد المحلل هذه الحقول.

الحقل	معرف بروتوكول PCO	المعنى
`dns_ipv4`	`0x000D`	عناوين خادم DNS IPv4.
`dns_ipv6`	`0x0003`	عناوين خادم DNS IPv6.
`pcscf_ipv4`	`0x000C`	عناوين P-CSCF IPv4.
`pcscf_ipv6`	`0x0001`	عناوين P-CSCF IPv6.
`mtu`	`0x0010`	رابط MTU IPv4.
`ip_alloc_nas`	`0x000A`	إلى تخصيص PGW إذا أشار `true` علامة. تكون IP من خلال إشارة NAS.

ثنائيًا معطوبًا جزئيًا، يعيد PCO إذا كان `raw`. يحتفظ المحلل أيضًا بكل خيار تم تحليله في قائمة المحلل الحقول التي قرأها حتى الآن. لا يفشل في التحليل بالكامل.

لاستجابة إنشاء الجلسة. يسرد الطلب الخيارات التي PCO بناء طلب OmniTWAG يمكن أيضًا لـ الرابط MTUو DNS IPv4 على سبيل المثال خوادم، PGW أن تعيدها OmniTWAG تريد.

تسليم DNS إلى UE

تصل خوادم DNS إلى UE من خلال النقل الذي يستخدمه UE.

النقل	مصدر DNS	الملاحظات
DHCPv4 (الخيار 6)	خوادم DNS IPv4 من PCO.	إذا لم يكن لدى PCO خادم DNS IPv4، تستخدم OmniTWAG `8.8.8.8`.
DHCPv6 (الخيار 23)	قائمة خادم DNS DHCPv6.	يتم تعيينها من PCO PGW أو من `dhcpv6_dns_servers`. الافتراضي هو Google Public DNS IPv6 إذا لم يتم تعيينها.
RA IPv6 (RDNSS، الخيار 25)	خوادم DNS IPv6 المرتبطة بالبادئة المعلنة.	يتم تسليم ا مع البادئة.

إذا كانت تلك القائمة `dns_ipv4`. من قائمة DNS IPv4 خوادم DHCPv4 تأخذ مدة إيجار `8.8.8.8` إلى. للإيجار OmniTWAG فارغة، تسقط

> **ملاحظة حول P-CSCF.** يقرأ محلل PCO عناوين P-CSCF من PGW. لا تضيف مسارات P-CSCF DHCP أو خيار RA. يتم تحليل قيم P-CSCF الحالية خيار RA و DHCPv6 و DHCP تسليم من خلال هذا النظام الفرعي في الشيفرة UE وتكون متاحة، لكنها لا تُسلم إلى المدققة.

مجموعات العناوين والاستنفاد

يعتمد سلوك الاستنفاد على الوضع.

- مساحة العنوان. PGW **نفق (موجه منزلي).** لا توجد مجموعة عنوان محلية. يمتلك لكل جلسة. لا يوجد PGW بتسليم بالضبط العنوان الذي يخصصه OmniTWAG تقوم أي عنوان، وتقوم UE فلا يتلقى، PGW PAA نطاق محلي للاستنفاد. إذا لم يعد بتسجيل الحالة OmniTWAG.
- **NSWO.** تقوم OmniTWAG بالتخصيص من مجموعة IP محلية، لذا يمكن أن تنفد لا يزيد عن `30/`. يتخطى المخصص عناوين CIDR IPv4 مجموعة. المجموعة هي الشبكة والبث ويعطي أول مضيف مجاني. عندما يكون كل مضيف قيد الاستخدام، يعود المخصص `pool_exhausted`. بالنسبة لـ `address_source: :pool`، يقوم UE بعد ذلك بتخصيص عنوانه بنفسه. بالنسبة لـ `address_source: :dhcp`، يذهب بتسجيل الاستنفاد. التخصيصات في OmniTWAG بدون إجابة وتقوم DISCOVER

انظر DHCP. الذاكرة وتعيد البناء كما تعيد الجلسات الإنشاء، تمامًا مثل عقود إيجار لتعريف المجموعة والقدرة مجموعات IP.

تقوم المساعدة `Twag.Cidr` بإجراء الرياضيات الخاصة بالشبكة للمنصة. تقوم بتحليل سلاسل هذه المساعدة RADIUS وتختبر ما إذا كان العنوان داخل شبكة. يستخدم نظام IPv6وIPv4 CIDR للاشتقاق من قناع الشبكة للمجموعة، ونطاق IP المصدر. يستخدم متجر مجموعة IP لتفويض المضيف القابل للاستخدام، والبوابة الافتراضية.

التكوين

تقرأ خوادم إدارة IP تكوينها من تكوين تطبيق `:omnitwag`. الكتل الرئيسية هي `dhcp` و `ipv6_ra`. يقرأ DHCPv6 مجموعة صغيرة من المفاتيح العليا.

```
config :omnitwag,
  # خادم DHCPv4
  dhcp: %{
    enabled: true,
    interface: "wlan0",
    server_ip: "10.0.0.1",
    default_lease_time: 3600,
    default_subnet_mask: "255.255.255.0",
    default_gateway: "10.0.0.1"
  },

  # إعلان موجه IPv6
  ipv6_ra: %{
    enabled: true,
    interface: "wlan0",
    ra_interval: 30,
    hop_limit: 64,
    router_lifetime: 1800
  },

  # DHCPv6 (مفاتيح اختيارية على المستوى الأعلى)
  dhcpv6_dns_servers: ["2001:4860:4860::8888",
"2001:4860:4860::8844"],
  dhcpv6_domain_list: ["example.com"]
```

معلمات DHCPv4 (`dhcp`)

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`true`	تمكين خادم DHCPv4. تعيينه إلى `false` لتعطيله، على سبيل المثال في بيئة اختبار.
`interface`	String	لا	`wlan0`	واجهة الشبكة لخدمة DHCP. استخدم `gre` لوضع نفق GRE.
`server_ip`	String	لا	`10.0.0.1`	معرف خادم DHCP. ترسل OmniTWAG هذه القيمة في خيار DHCP 54 وكـ مصدر للردود المغلفة بـ GRE.
`default_lease_time`	Integer	لا	`3600`	مدة الإيجار بالثواني. تطبق OmniTWAG هذه القيمة

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				على كل عقد إيجار مسبق التخصيص.
`default_subnet_mask`	String	لا	`255.255.255.0`	قناع الشبكة لعقد الإيجار ولحساب البث وفقًا لـ RFC 2131.
`default_gateway`	String	لا	`10.0.0.1`	البوابة الافتراضية لعقد الإيجار (خيار DHCP 3).

معلمات RA IPv6 (`ipv6_ra`)

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`true`	تمكين خادم RA IPv6. تعيينه إلى `false` لتعطيله.
`interface`	String	لا	`wlan0`	واجهة الشبكة لإعلانات الموجه.
`ra_interval`	Integer	لا	`30`	الفاصل الزمني بالثواني بين إعلانات الموجه الدورية.
`hop_limit`	Integer	لا	`64`	حقل حد القفز الحالي في إعلان الموجه.
`router_lifetime`	Integer	لا	`1800`	عمر الموجه بالثواني في إعلان الموجه.

معلمات DHCPv6 (المستوى الأعلى)

المعلمة	النوع	مطلوب	الافتراضي	وصف
`dhcpv6_dns_servers`	قائمة من String	لا	Google Public DNS IPv6 (`2001:4860:4860::8888`, `2001:4860:4860::8844`)	D خوادم رد IPv6 DHCPv أيضًا أن حدد هذه ائمة من PCO PC في وقت التشغيل.
`dhcpv6_domain_list`	قائمة من String	لا	(غير محدد)	ة البحث عن DNS DHCPv خيار 24) ذا لم يتم تحديدها، تتجاهل OmniT الخيار.

الرؤية

واجهة الويب

تحتوي لوحة التحكم على صفحة **مجموعة DHCP** في `/dhcp`. تعرض الصفحة كل عقد إيجار ووقت بدء الإيجار، ووقت انتهاء الإيجار، وعنوان IP، وعنوان UE الخاص بـ MAC مع عنوان DHCPv4 والحالة. الحالة هي `نشطة` أو `منـتـهـيـة`. تعرض الصفحة عدًا تنازليًا مباشرًا لكل عقد إيجار نشط. حدد صف عقد إيجار لرؤية تفاصيل العقد بالكامل: قناع الشبكة، والبوابة، وخوادم DNS، ومدة قيد التشغيل، DHCPv4 الإيجار، والطوابع الزمنية. يتم تحديث الصفحة كل ثانية. إذا لم يكن خادم `الخادم غير قيد ال`شغيل تعرض الصفحة.

واجهة برمجة التطبيقات REST

تقدم واجهة برمجة التطبيقات REST بيانات عقد إيجار DHCPv4 تحت علامة `DHCP`.

الطريقة	المسار	الوصف
GET	`/dhcp` (فهرس)	قائمة بجميع عقود إيجار DHCPv4 مع عدد ملخص.
GET	`/dhcp/{id}` (عرض)	الحصول على عقد إيجار واحد بواسطة عنوان MAC. `id` هو عنوان MAC مفصول بعلامة النقطتين.

تحتوي استجابة الفهرس على علامة `enabled`، وقائمة `leases`، وإجمالي `count`، وعدد `active`، وعدد `expired`. إذا لم يكن خادم DHCPv4 قيد التشغيل، تعيد الفهرس `enabled: false` مع قائمة فارغة. تعيد نقطة النهاية العرض `404` إذا لم يتطابق أي عقد إيجار مع MAC، و `503` إذا لم يكن الخادم قيد التشغيل.

يحتوي كل كائن عقد إيجار على هذه الحقول.

الحقل	الوصف
`mac`	عنوان MAC الخاص بـ UE، مفصول بعلامة النقطتين.
`ip`	عنوان IPv4 المعين.
`subnet_mask`	قناع الشبكة لعقد الإيجار.
`gateway`	بوابة عقد الإيجار.
`dns_servers`	قائمة بخوادم DNS.
`lease_time`	مدة الإيجار بالثواني.
`allocated_at`	وقت بدء الإيجار، بالثواني منذ بداية Unix.
`expires_at`	وقت انتهاء الإيجار، بالثواني منذ بداية Unix.
`status`	`نشطة` أو `منـتـهـيـة`.
`time_remaining`	ثوانٍ حتى انتهاء الصلاحية، أو `0` إذا انتهت.

أحداث القياس

تقوم خوادم إدارة IP بإصدار أحداث القياس. يمكن للمشغل ربط هذه الأحداث بمصدر قياس. انظر مرجع القياس لنقطة نهاية Prometheus.

الحدث	المصدر	المعنى
`[:dhcp, :lease, :allocate]`	DHCPv4	تم تخصيص عقد إيجار مسبق لعنوان MAC.
`[:dhcp, :lease, :deallocate]`	DHCPv4	تمت إزالة عقد إيجار عند الإنهاء.
`[:dhcp, :lease, :reap]`	DHCPv4	تمت إزالة عقد إيجار منتهي الصلاحية بواسطة جامع الخلفية.
`[:dhcp, :discover]`	DHCPv4	تم الرد على DISCOVER بـ OFFER من عقد إيجار موجود.
`[:dhcp, :discover, :pool_allocated]`	DHCPv4	تم الرد على DISCOVER من عنوان MAC مرتبط بالمجموعة بتوزيع عنوان مجموعة جديد (NSWO `:dhcp`).
`[:dhcp, :discover, :no_allocation]`	DHCPv4	وصل DISCOVER إلى عنوان MAC بدون عقد إيجار وبدون ارتباط بالمجموعة.
`[:dhcp, :ack]`	DHCPv4	تم الرد على REQUEST بـ ACK.
`[:dhcp, :nak]`	DHCPv4	تم الرد على REQUEST بـ NAK.
`[:dhcp, :release]`	DHCPv4	أطلق عميل عقد إيجاره.
`[:dhcp, :decline]`	DHCPv4	رفض عميل عقد إيجاره.
`[:dhcp, :inform]`	DHCPv4	تم الرد على INFORM.
`[:dhcp, :packet, :malformed]`	DHCPv4	تم استلام حزمة DHCP معطوبة.
`[:dhcpv6, :info_request, :received]`	DHCPv6	تم استلام طلب معلومات.

الحدث	المصدر	المعنى
`[:dhcpv6, :solicit, :received]`	DHCPv6	تم استلام طلب.
`[:dhcpv6, :request, :received]`	DHCPv6	تم استلام طلب.
`[:dhcpv6, :info_reply, :sent]`	DHCPv6	تم إرسال رد معلومات.
`[:dhcpv6, :advertise, :sent]`	DHCPv6	تم إرسال إعلان.
`[:dhcpv6, :reply, :sent]`	DHCPv6	تم إرسال رد.
`[:ipv6_ra, :prefix, :add]`	IPv6 RA	تمت إضافة بادئة إلى واجهة.
`[:ipv6_ra, :prefix, :remove]`	IPv6 RA	تمت إزالة بادئة من واجهة.
`[:ipv6_ra, :advertisement, :sent]`	IPv6 RA	تم إرسال إعلان موجه.

استكشاف الأخطاء وإصلاحها

لا يحصل UE على عنوان IP

الأعراض: يقوم UE بالمصادقة ولكنه لا يحصل على عنوان IPv4. تظهر صفحة مجموعة DHCP الخاص بـ UE. يتم إطلاق حدث `[:dhcp, :discover, :no_allocation]` عدم وجود إيجار لعنوان MAC.

الأسباب المحتملة (النفق):

- لم تحتوي استجابة إنشاء جلسة GTP على PAA، لذا لم تقم OmniTWAG مسبقًا بتخصيص عقد إيجار.
- لم يتم إنشاء جلسة GTP-C، لذا لم يتم إنشاء أي عقد إيجار.

الأسباب المحتملة (NSWO):

- لا تحتوي بيانات اعتماد AP على `ip_pool_id`، لذا لا تقوم OmniTWAG بتخصيص أي عنوان.
- المجموعة مستنفدة، لذا لم يكن هناك عنوان مجاني يمكن توزيعه.
- بالنسبة لـ `address_source: :dhcp`، وصل DISCOVER قبل أن يتم ربط MAC بالمجموعة، أو لم يتم تشغيل الارتباط لأن الجلسة لم يكن لديها MAC بعد.

السبب الشائع:

- خادم DHCPv4 غير قيد التشغيل.

الحل:

1. تحقق من سجلات OmniTWAG لمسار الإنشاء (النفق مقابل NSWO) وعنوان IP الخاص بـ UE.
2. بالنسبة للجلسات النفقية، تأكد من أن PGW يعيد PAA لـ APN.
3. بالنسبة للجلسات NSWO، تأكد من أن بيانات اعتماد AP تسمي `ip_pool_id` صالح و بيانات اعتماد IP RADIUS. وأن المجموعة لديها سعة مجانية. انظر مجموعات.
4. تأكد من أن صفحة مجموعة DHCP تعرض خادم DHCPv4 كقيد التشغيل.

يحصل UE على عنوان ولكن لا يوجد DNS

الأعراض: لدى UE عنوان IPv4 ولكن لا يمكنه حل الأسماء.

الأسباب المحتملة:

- لم يعد PCO PGW أي خادم DNS IPv4. في هذه الحالة، تستخدم OmniTWAG `8.8.8.8`.
- لا يمكن لـ UE الوصول إلى خادم DNS الذي قدمه PGW.

الحل:

1. أو من خلال واجهة برمجة DHCP لعقد الإيجار على صفحة مجموعة اقرأ خوادم DNS التطبيقات REST.

2. تأكد من أن PCO PGW يعيد خادم DNS المتوقع.
3. تأكد من أن خادم DNS يمكن الوصول إليه من مسار بيانات UE.

يتلقى UE NAK

الأعراض: يرسل UE REQUEST ويتلقى NAK. يتم إطلاق حدث `[:dhcp, :nak]`.

الأسباب المحتملة:

- طلب UE عنوان IP (الخيار 50) لا يتطابق مع عقد الإيجار المخصص مسبقًا.
- تمت إزالة عقد الإيجار، على سبيل المثال بعد إنهاء الجلسة.

الحل:

1. تأكد من وجود عقد إيجار لعنوان MAC الخاص بـ UE.
2. تأكد من أن UE يطلب نفس IP الذي خصصه PGW أو المجموعة.
3. بعد أن يعيد المصادقة DHCP يعيد بدء تبادل UE إذا تم إنهاء الجلسة، دع.

الصفحات ذات الصلة

- نظرة عامة
- مجموعات IP
- بيانات اعتماد RADIUS
- الجلسات
- S2a GTP-C
- طائرة المستخدم
- التحصيل عبر الإنترنت (Gy)

نظرة عامة

مجموعات IP

نظرة عامة

تقوم OmniTWAG بتعيين عناوين IPv4 لجلسات NSWO (عدم انقطاع WLAN Offload) من **مجموعة IP**. NSWO هو انقطاع محلي مدعوم من TWAG: تقوم OmniTWAG بإنهاء حركة مرور المستخدم وتفكيكها محليًا. تعرف مجموعة IP كتلة CIDR IPv4، وخوادم DNS، وبوابة، ومدة الإيجار. يقوم المشغل بإضافة وتغيير وإزالة المجموعات عند الطلب من خلال واجهة برمجة التطبيقات REST أو واجهة الويب الخاصة بلوحة التحكم.

لذا تبقى المجموعات، DETS بتخزينها في ملف OmniTWAG تعريفات المجموعات دائمة. تقوم OmniTWAG بإعادة بناء موجودة بعد إعادة التشغيل. يتم تخصيص العناوين في الذاكرة. تقوم التخصيصات عندما تعيد الجلسات الاتصال بعد إعادة التشغيل.

جدول المحت��يات

- المفاهيم
- كيفية حصول الجلسة على عنوان
- تخصيص العنوان
- نموذج المجموعة
- واجهة برمجة التطبيقات REST
- واجهة الويب
- استكشاف الأخطاء وإصلاحها

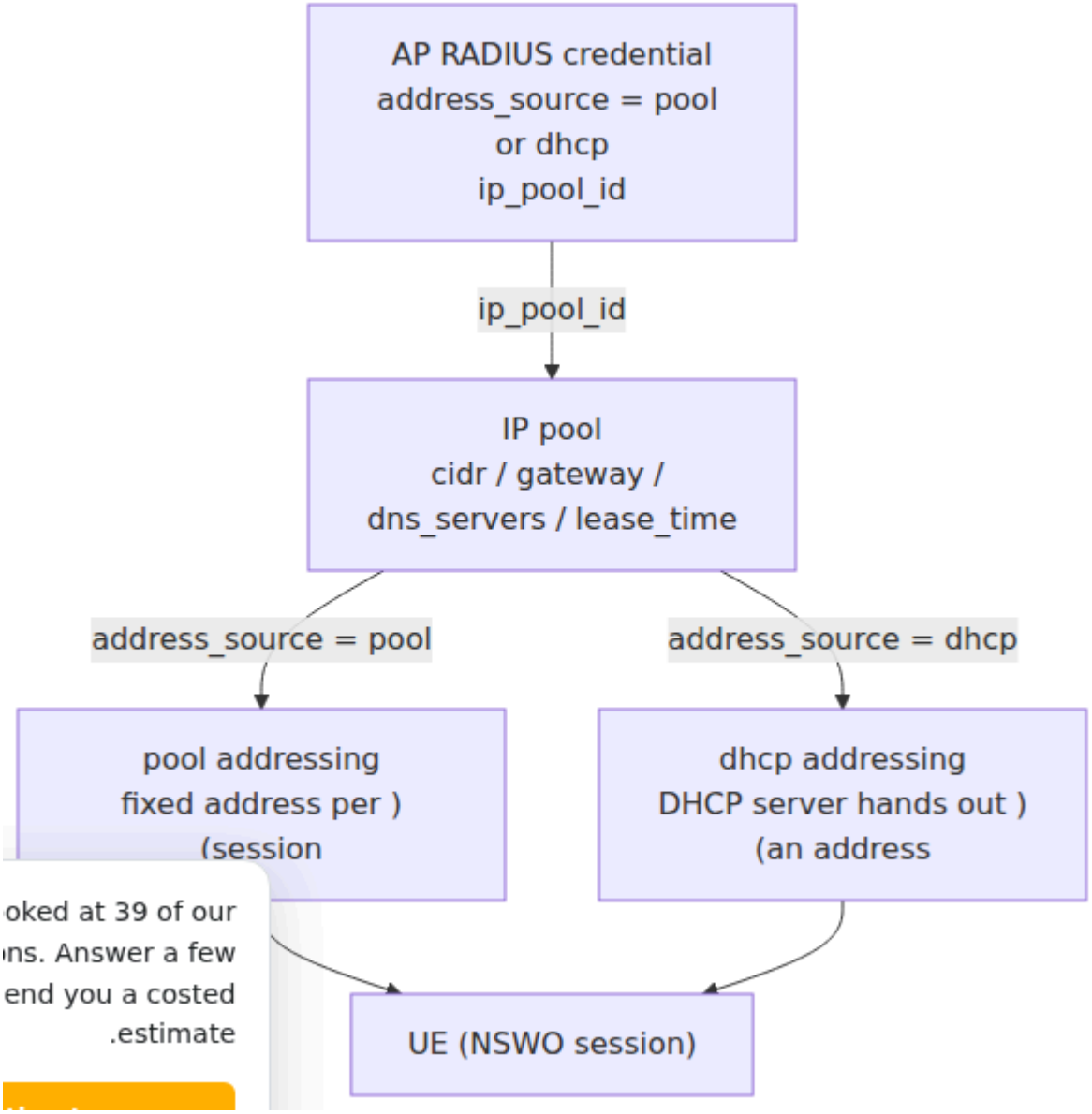
المفاهيم

مجموعة **IP** هي مجموعة من العناوين من كتلة CIDR IPv4، بوابة، واحدة. تحتوي كل مجموعة على وقائمة بخوادم DNS، ومدة إيجار.

ترتبط مجموعة IP بنقطة وصول من خلال بيانات اعتماد RADIUS. تحتوي الخاصة بنقطة الوصول RADIUS المجموعة. انظر أسرار `id` يحمل هذا الحقل. `ip_pool_id` بيانات الاعتماد على حقل من تلك نقطة الوصول من المجموعة NSWO لنموذج بيانات الاعتماد المشتركة. يتم تعيين جلسات المرتبطة.

يحدد هذا الحقل كيفية منح OmniTWAG العنوان لجهاز المستخدم (UE). تحتوي كل بيانات اعتماد أيضًا على حقل `address_source`. هناك مصدران للعناوين:

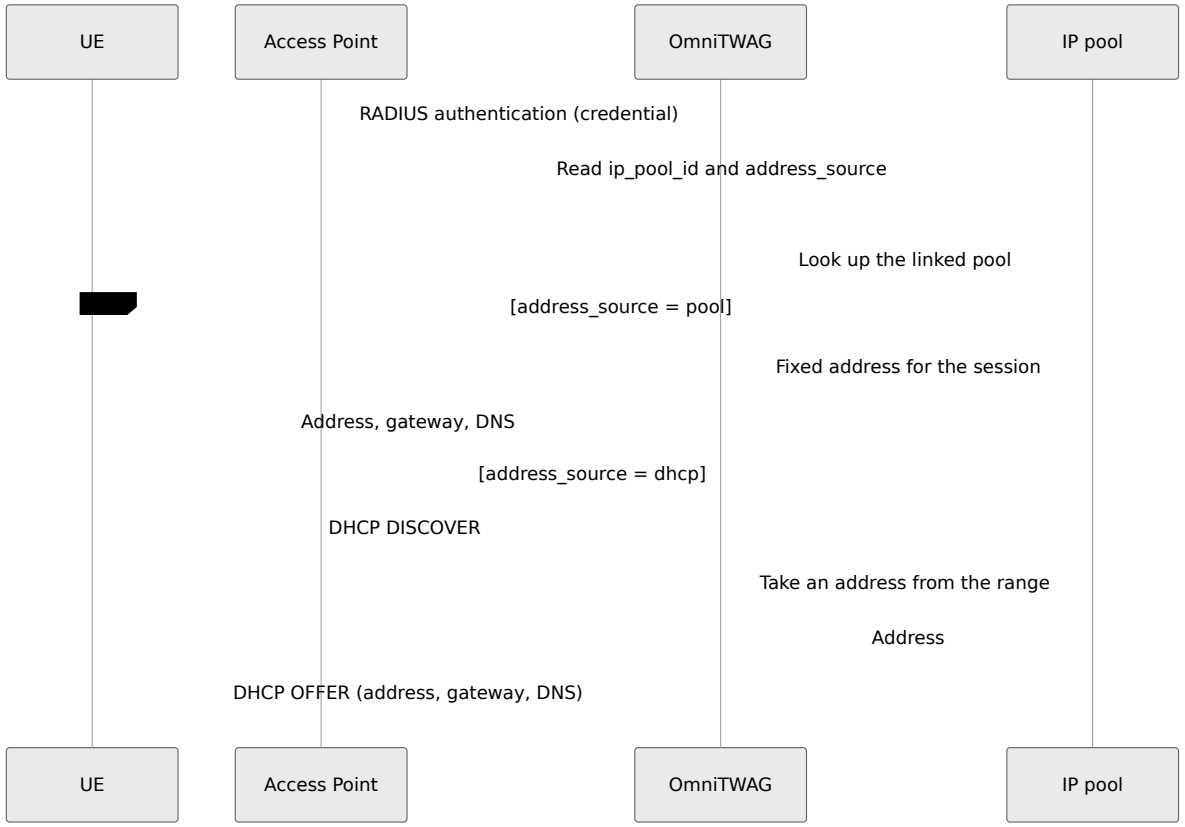
مصدر العنوان	السلوك
`pool`	يتم OmniTWAG تقوم بتخصيص عنوان ثابت لكل جلسة من المجموعة. اختيار العنوان عند إعداد الجلسة.
`dhcp`	يقوم خادم DHCP الخاص بـ OmniTWAG بتوزيع عنوان من نطاق المجموعة ردًا على DHCP DISCOVER من جهاز المستخدم.



كيفية حصول الجلسة على عنوان

تقوم OmniTWAG بتعيين كل جلسة NSWO من المجموعة المرتبطة ببيانات اعتماد نقطة الوصول. الخطوات هي:

1. تقوم نقطة الوصول بالمصادقة من خلال بيانات اعتماد RADIUS الخاصة بها.
2. تقوم OmniTWAG بقراءة حقل `ip_pool_id` في بيانات الاعتماد للعثور على المجموعة.
3. تقوم OmniTWAG بقراءة حقل `address_source` في بيانات الاعتماد.
4. إذا كان `address_source` هو `pool`، تقوم OmniTWAG بتخصيص عنوان ثابت للجلسة من المجموعة.
5. إذا كان `address_source` هو `dhcp`، تنتظر OmniTWAG DHCP DISCOVER من جهاز المستخدم. يقوم خادم DHCP بعد ذلك بتوزيع عنوان من نطاق المجموعة.
6. تقوم OmniTWAG بتزويد جهاز المستخدم بالعنوان، والبوابة، وخوادم DNS من المجموعة.



تخصيص العنوان

تقوم OmniTWAG بتخصيص المضيفين من CIDR عنوان الشبكة المجموعة. يتخطى التخصيص وعنوان البث. أول مضيف قابل للاستخدام هو عنوان الشبكة زائد واحد.

يجب أن يكون بادئة CIDR للمجموعة `30/` أو أكبر لوجود مضيفين قابلين للاستخدام. تحتوي كتلة `30/` على 2 مضيفين قابلين للاستخدام. تحتوي بادئة أصغر على مضيفين قابلين للاستخدام أقل، لذا ترفضها OmniTWAG.

عندما يتم تخصيص كل مضيف قابل للاستخدام، تعيد OmniTWAG `pool_exhausted`. لا يمكن لجلسة أخرى من نقطة الوصول المرتبطة الحصول على عنوان حتى يتم تحرير تخصيص.

يحتوي حقل `allocated` في المجموعة على العدد الحالي للتخصيصات. تقوم OmniTWAG بحساب هذا العدد من التخصيصات في الذاكرة.

نموذج المجموعة

تحتوي كل مجموعة على هذه الحقول.

الحقل	النوع	الوصف
`id`	سلسلة	معرف فريد (UUID). يقوم الخادم بتعيين هذه القيمة.
`name`	سلسلة	تسمية قابلة للقراءة البشرية، على سبيل المثال `WiFi ضيوف ملبورن`.
`cidr`	سلسلة	كتلة CIDR IPv4 للمجموعة، على سبيل المثال `10.60.0.0/24`. يجب أن تكون البادئة `/30` أو أكبر لوجود مضيفين قابلين للاستخدام.
`gateway`	سلسلة	عنوان بوابة IPv4 المقدم لجهاز المستخدم. الافتراضي هو أول مضيف قابل للاستخدام من CIDR إذا تم تجاهله.
`dns_servers`	قائمة من السلاسل	عناوين خوادم DNS IPv4 المقدمة لجهاز المستخدم.
`lease_time`	عدد صحيح	مدة الإيجار بالثواني. الافتراضي هو `3600`.
`default`	منطقي	تكون هذه المجموعة هي النطاق، عندما يكون `true` بالتوزيع منها لأي DHCP. يقوم خادم DHCP الافتراضي لـ عميل ليس لديه إيجار مسبق التخصيص ولا ربط مجموعة. يمكن أن تكون مجموعة واحدة فقط هي الافتراضية في وقت واحد. الافتراضي هو `false`.
`allocated`	عدد صحيح	عدد التخصيصات الحالية. يقوم الخادم بحساب هذه القيمة.
`inserted_at`	عدد صحيح	الوقت الذي تم فيه إنشاء المجمو��ة، بالمللي ثانية منذ بداية Unix. يقوم الخادم بتعيين هذه القيمة.
`updated_at`	عدد صحيح	الوقت الذي تم فيه تغيير المجموعة آخر مرة، بالمللي ثانية منذ بداية Unix. يقوم الخادم بتعيين هذه القيمة.

يقوم المشغل بتعيين `name` و `cidr` و `gateway` و `dns_servers` و `lease_time`. يقوم الخادم بتعيين `id` و `allocated` و `inserted_at` و `updated_at`.

REST واجهة برمجة التطبيقات

تقدم واجهة برمجة التطبيقات REST الخاصة بـ OmniTWAG هذه النقاط النهائية عبر HTTPS على المنفذ المخصص لواجهة برمجة التطبيقات (`8444` بشكل افتراضي). المسار الأساسي هو `/ip_pools`.

الطريقة	المسار	الإجراء	الوصف
GET	`/ip_pools`	index	قائمة بجميع المجموعات. تكون النتيجة مقسمة وقابلة للبحث بواسطة `name` أو `cidr`.
GET	`/ip_pools/{id}`	show	الحصول على مجموعة واحدة بواسطة `id`.
POST	`/ip_pools`	create	إنشاء مجموعة.
PUT	`/ip_pools/{id}`	update	تغيير مجموعة.
DELETE	`/ip_pools/{id}`	delete	إزالة مجموعة.

جسم الطلب

تقبل `POST` و `PUT` جسم JSON مع هذه الحقول.

الحقل	النوع	مطلوب	الوصف
`name`	سلسلة	لا	تسمية قابلة للقراءة البشرية.
`cidr`	سلسلة	نعم	كتلة CIDR IPv4. يجب أن تكون البادئة `/30` أو أكبر.
`gateway`	سلسلة	لا	عنوان بوابة IPv4. الافتراضي هو أول مضيف إذا تم تجاهله. CIDR قابل للاستخدام من
`dns_servers`	قائمة من السلاسل	لا	عناوين خوادم DNS IPv4.
`lease_time`	عدد صحيح	لا	مدة الإيجار بالثواني. الافتراضي هو `3600`.
`default`	منطقي	لا	وضع علامة على هذه المجموعة كنطاق الافتراضي. يؤدي تعيينها إلى مسح DHCP العلامة على أي مجموعة أخرى.

بتغيير الحقول الموجودة فقط في الجسم. تبقى الحقول التي ليست في الجسم على `PUT` تقوم قيمتها الحالية.

الاستجابات

الحالة	المعنى
`200 OK`	كانت الطلب ناجحًا (index، show، update، delete).
`201 Created`	تم إنشاء المجموعة.
`404 Not Found`	لا توجد مجموعة بالـ `id` المعطى.
`422 Unprocessable Entity`	الـ `cidr` ليس كتلة CIDR IPv4 صالحة، أو أن البادئة صغيرة جدًا لوجود مضيفين قابلين للاستخدام.

مثال: قائمة المجموعات

الطلب:

```
GET /ip_pools
```

الاستجابة:


```
{
  "count": 1,
  "ip_pools": [
    {
      "id": "0d1e2f3a-4b5c-6d7e-8f90-1a2b3c4d5e6f",
      "name": "WiFi ضيوف ملبورن",
      "cidr": "10.60.0.0/24",
      "gateway": "10.60.0.1",
      "dns_servers": ["8.8.8.8", "8.8.4.4"],
      "lease_time": 3600,
      "allocated": 12,
      "inserted_at": 1734512400000,
      "updated_at": 1734512400000
    }
  ]
}
```


مثال: إنشاء مجموعة

الطلب:

```
POST /ip_pools
```

```
{
  "name": "WiFi ضيوف ملبورن",
  "cidr": "10.60.0.0/24",
  "gateway": "10.60.0.1",
  "dns_servers": ["8.8.8.8", "8.8.4.4"],
  "lease_time": 3600
}
```

`201` تعود الطلب الناجح بـ `Created` مع المجموعة الجديدة، بما في ذلك `id` الخاص بها. إذا تم تستخدم المج��وعة أول مضيف قابل للاستخدام من CIDR (`10.60.0.1`، `gateway` تجاهل في هذا المثال).

مثال: CIDR صغير جدًا

الطلب:

```
{
  "name": "مجموعة معطلة",
  "cidr": "10.60.0.0/31"
}
```

الاستجابة (`422 Unprocessable Entity`):

```
{
  "error": "cidr too small: 10.60.0.0/31 has no usable hosts"
}
```

المجموعة الافتراضية

يمكن أن تكون مجموعة واحدة هي النطاق الافتراضي لـ DHCP. يقوم خادم DHCP بتوزيع عنوان من المجموعة الافتراضية لأي عميل ليس لديه إيجار مسبق التخصيص ولا ربط مجموعة صريح. استخدم المجموعة الافتراضية لتقديم نطاق محدد عبر واجهة برمجة التطبيقات لخدمة DHCP الأساسية، وليس فقط لجلسات NSWO.

أو خانة الاختيار على صفحة الويب. يمكن أن تكون `default`، قم بتعيين الافتراضي باستخدام حقل مجموعة واحدة فقط هي الافتراضية في وقت واحد. عند وضع علامة على مجموعة كافتراضية،

تقوم OmniTWAG بمسح العلامة على المجموعة الافتراضية السابقة.

إيجارات IP: تسجل كل إيجار نشط مصدره. انظر عرض الإيجار يظهر `PGW (tunneled)`، أو `NSWO` مجموعة `المجموعة الافتراضية` مسماة، أو.

واجهة الويب

تسرد الصفحة كل مجموعة مع اسمها. تحتوي لوحة التحكم على صفحة إدارة **مجموعات IP**. تحتوي الصفحة على عناصر تحكم لإضافة وتحرير وحذف CIDR والبوابة وعدد التخصيصات. مجموعة.

تعرض صفحة إيجارات IP. السابقة تحمل الآن تسمية **إيجارات DHCP** كانت صفحة **مجموعة IP**. الإيجارات النشطة.

استكشاف الأخطاء وإصلاحها

استنفاد مجموعة

الأعراض: لا يمكن لجلسات NSWO الجديدة من نقطة الوصول الحصول على عنوان. تعيد OmniTWAG `pool_exhausted`.

الأسباب المحتملة:

- تم تخصيص كل مضيف قابل للاستخدام في CIDR المجموعة.
- CIDR المجموعة صغير جدًا لعدد الجلسات النشطة.

الحل:

1. تحقق من عدد `allocated` مقابل عدد المضيفين القابلين للاستخدام في CIDR.
2. قم بتوسيع CIDR أو المجموعة لإضافة ا��مزيد من المضيفين القابلين للاستخدام، حرر التخصيصات القديمة عن طريق إنهاء الجلسات الخاملة.
3. تأكد من أن مدة الإيجار ليست طويلة جدًا بحيث تبقى العناوين المحررة مخصصة.

نقطة الوصول لا تستخدم مجموعة

الأعراض: لا يتم تعيين الجلسات من نقطة الوصول من أي مجموعة IP.

الأسباب المحتملة:

- المدعوم NSWO تستخدم نقطة الوصول انقطاعًا محليًا مملوكًا لنقطة الوصول، وليس من TWAG. تقوم نقطة وصول انقطاع محلي مملوكة لنقطة الوصول بتعيين عملائها ولا تستخدم مجموعة OmniTWAG.
- لا تحتوي بيانات اعتماد نقطة الوصول على `ip_pool_id`، لذا لا توجد مجموعة مرتبطة.

الحل:

1. تأكد من أن نقطة الوصول تستخدم NSWO المدعوم من TWAG. فقط جلسات NSWO تستخدم مجموعة.
2. إذا كان يجب أن تستخدم نقطة الوصول مجموعة، قم بتعيين `ip_pool_id` على بيانات اعتماد RADIUS الخاصة بها إلى `id` المجموعة. انظر أسرار RADIUS المشتركة.

جهاز المستخدم لا يحصل على عنوان

الأعراض: يتصل جهاز المستخدم ولكن لا يتلقى عنوان IPv4.

الأسباب المحتملة:

- لا يتطابق `address_source` في بيانات الاعتماد مع كيفية طلب جهاز المستخدم عنوانًا. مع `dhcp`، يجب على جهاز المستخدم إرسال DHCP DISCOVER. مع `pool`، تقوم OmniTWAG مسبقًا بتخصيص العنوان.
- المجموعة المرتبطة مستنفدة.
- يشير `ip_pool_id` في بيانات الاعتماد إلى مجموعة غير موجودة.

الحل:

1. تأكد من أن `address_source` في بيانات الاعتماد يتطابق مع سلوك جهاز المستخدم.
2. تأكد من أن المجموعة المرتبطة تحتوي على عناوين مجانية. تحقق من عدد `allocated`.
3. تأكد من أن `ip_pool_id` في بيانات الاعتماد يشير إلى مجموعة صالحة.

نظرة عامة

TWAG مرجع مقاييس

نظرة عامة

يقدم TWAG مقاييس Prometheus على المنفذ **9568** (المحدد بواسطة `prometheus.port`). يتم تحديث مقاييس القياس بواسطة جهاز استشعار كل 5 ثوانٍ. يتم إصدار مقاييس العد من مسار الشيفرة الذي يحفزها.

جدول المحتويات

- نقطة نهاية المقاييس
- مقاييس مصادقة RADIUS
- مقاييس تفويض RADIUS ومعدل الحد
- مقاييس محاسبة RADIUS
- مقاييس EAP
- مقاييس العميل ونقطة الوصول والجلسة
- مقاييس تدفق البيانات
- مقاييس جلسة TWAG ومسار البيانات
- مقاييس شحن Gy عبر الإنترنت
- مقاييس STa Diameter
- مقياس رسالة Diameter
- مقاييس NSWO
- مقاييس DHCP
- مقاييس DHCPv6 و IPv6 RA
- مقاييس WLCP
- مقاييس Erlang VM
- مثال Grafana استعلامات
- قواعد التنبيه
- صفحات ذات صلة

نقطة نهاية المقاييس

```
http://<twag-host>:9568/metrics
```

يقوم Prometheus بتسطيح كل اسم حدث إلى اسم مقياس عن طريق استبدال النقاط بشرطات سفلية. على سبيل المثال، يتم عرض الحدث `[:radius, :access, :request, :count]` كـ `radius_access_request_count`.

مقاييس مصادقة RADIUS

تتبع هذه العدادات تدفقات طلب/استجابة الوصول لكل من RADIUS RFC 2865.

المقياس	النوع	التسميات	الوصف
`radius_access_request_count`	عداد	لا شيء	حزم طلب الوصول RADIUS المستلمة.
`radius_access_accept_count`	عداد	لا ش��ء	حزم قبول الوصول RADIUS المرسلة (مصادقة ناجحة).
`radius_access_reject_count`	عداد	لا شيء	حزم رفض الوصول RADIUS المرسلة (فشل المصادقة).
`radius_access_challenge_count`	عداد	لا شيء	حزم تحدي الوصول RADIUS المرسلة (جارٍ تبادل EAP).

استعلامات مثال:

```
# معدل الطلبات في الثانية
rate(radius_access_request_count[5m])

# معدل التحديات (المفاوضات النشطة EAP)
rate(radius_access_challenge_count[5m])

# نسبة نجاح المصادقة
sum(rate(radius_access_accept_count[5m])) /
  (sum(rate(radius_access_accept_count[5m])) +
sum(rate(radius_access_reject_count[5m])))
```

مقاييس تفويض RADIUS ومعدل الحد

تتبع هذه العدادات الحزم التي تم إسقاطها أو وضع علامة عليها قبل أو أثناء المصادقة. انظر رفض RADIUS المشتركة و أسرار RADIUS.

المقياس	النوع	التسميات	
`radius_auth_unauthorized_source_count`	عداد	`source`	ن عنوان ر��ية ول غير الحزمة
`radius_auth_bad_secret_count`	عداد	`source`, `credential_id`	ع بيانات ي فحص Messa خاطئ)
`radius_access_rate_limited_count`	عداد	`nas_ip`	سقاطها لأن NA `rate_` النافذة

استعلامات مثال:

```
# نقاط الوصول غير المعروفة التي تظهر (أضف بيانات اعتماد لهذه)
increase(radius_auth_unauthorized_source_count[1h])

# نقاط الوصول التي تحتوي على سر مشترك خاطئ
sum by (source) (increase(radius_auth_bad_secret_count[1h]))

# أجهزة NAS المحدودة بمعدل
sum by (nas_ip) (increase(radius_access_rate_limited_count[15m]))
```

مقاييس محاسبة RADIUS

تتبع رسائل محاسبة RADIUS لكل من RFC 2866.

radius_accounting_request_count

النوع: عداد

الوصف	التسميات
نوع حالة المحاسبة (انظر أدناه).	`status_type`

قيم نوع الحالة: `start`، `stop`، `interim_update`، `accounting_on`، `accounting_off`.

استعلامات مثال:

```
# بدء الجلسات في الدقيقة
rate(radius_accounting_request_count{status_type="start"}[5m]) *
60

# إيقاف الجلسات في الدقيقة
rate(radius_accounting_request_count{status_type="stop"}[5m]) * 60
```

مقاييس EAP

تتبع هذه العدادات مراحل EAP-AKA لكل من RFC 4187، بالإضافة إلى EAP-SIM، إعادة المصادقة EAP (ERP)، وأخطاء EAP العامة.

المقياس	النوع	الوصف
`eap_aka_identity_count`	عداد	تبادلات هوية EAP-AKA (المرحلة 1).
`eap_aka_challenge_count`	عداد	تبادلات تحدي EAP-AKA (المرحلة 2).
`eap_aka_sync_failure_count`	عداد	فشل مزامنة EAP-AKA (SQN خارج المزامنة، يحفز إعادة المزامنة).
`eap_aka_auth_success_count`	عداد	مصادقات EAP-AKA الناجحة.
`eap_aka_auth_reject_count`	عداد	مصادقات EAP-AKA المرفوضة (فشل UE في مصادقة الشبكة / فشل AUTN).
`eap_aka_client_error_count`	عداد	إشعارات أخطاء عميل EAP-AKA المستلمة من UE.
`eap_auth_rejected_count`	عداد	رفضات المصادقة المتوقعة (على سبيل المثال HSS USER_UNKNOWN) التي ترفض UE بشكل نظيف.
`eap_process_crash_count`	عداد	أخطاء غير متوقعة أثناء معالجة رسالة EAP (تم الحفاظ على الجلسة، تم رفض UE).
`eap_sim_start_count`	عداد	تبادلات بدء EAP-SIM.
`eap_sim_auth_success_count`	عداد	مصادقات EAP-SIM الناجحة.
`eap_sim_auth_reject_count`	عداد	مصادقات EAP-SIM المرفوضة.
`eap_erp_initiate_count`	عداد	بدء إعادة المصادقة EAP ERP.
`eap_erp_success_count`	عداد	إعادة مصادقات EAP ERP الناجحة.
`eap_erp_mac_failure_count`	عداد	فشل التحقق من MAC في EAP ERP.

المقياس	النوع	الوصف
`eap_erp_fallback_count`	عداد	تراجع EAP ERP إلى المصادقة الكاملة. التسمية `reason`.

استعلامات مثال:

```
# فشل المزامنة (يجب أن تكون نادرة - تنبه إذا كانت > 0)
increase(eap_aka_sync_failure_count[1h])

# مصادقات AKA الناجحة في الدقيقة
rate(eap_aka_auth_success_count[5m]) * 60

# أعطال معالجة EAP (يجب أن تبقى ثابتة)
increase(eap_process_crash_count[1h])
```

مقاييس العميل ونقطة الوصول والجلسة

يتم أخذ عينات من هذه المقاييس كل 5 ثوانٍ بواسطة جهاز الاستشعار.

المقياس	النوع	التسميات	الوصف
`radius_active_clients_count`	مقياس	لا شيء	العملاء الذين تم مصادقتهم حاليًا (عمليات `Twag.Session.Client` الحية).
`radius_access_points_count`	مقياس	لا شيء	نقاط الوصول المسجلة (مدخلات `APState`).
`radius_clients_per_ap_count`	مقياس	`nas_ip`, `ssid`	لعملاء المتصلين بكل نقطة وصول.
`radius_active_sessions_count`	مقياس	`status`	الجلسات مجمعة حسب حالة المحاسبة (`start`, `stop`, `interim_update`).
`radius_active_sessions_total`	مقياس	لا شيء	الجلسات في حالة `start` أو `interim_update`.

استعلامات مثال:

```
# أعلى 5 نقاط وصول مشغولة
topk(5, radius_clients_per_ap_count)

# العملاء حسب SSID
sum by (ssid) (radius_clients_per_ap_count)

# تنبيه على انخفاض مفاجئ في الجلسات النشطة
delta(radius_active_sessions_total[5m]) < -10
```

مقاييس تدفق البيانات

تجمع هذه المقاييس عبر جميع الجلسات المتعقبة من عدادات محاسبة RADIUS.

المقياس	النوع	الوحدة	الوصف
`radius_data_bytes_in`	مقياس	بايت	إجمالي البايتات المستلمة عبر الجلسات (Acct-Input-Octets).
`radius_data_bytes_out`	مقياس	بايت	إجمالي البايتات المرسلة عبر الجلسات (Acct-Output-Octets).
`radius_session_total_time`	مقياس	ثواني	إجمالي وقت الجلسة عبر الجلسات (Acct-Session-Time).

استعلامات مثال:

```
# إجمالي التدفق بالميغابايت
(radius_data_bytes_in + radius_data_bytes_out) / 1024 / 1024

# متوسط مدة الجلسة
radius_session_total_time / radius_active_sessions_total
```

مقاييس جلسة TWAG ومسار البيانات

تتبع هذه العدادات أحداث دورة حياة كل جلسة يتم إصدارها بواسطة `Twag.Session.Client`.

المقياس	النوع	التسميات	وصف
`twag_session_teardown_count`	عداد	`reason`	ت إنهاء الجلسة. الأسباب: `accounting_` `admin_disco` `network_dis` `identity_ti` `liveness_ti`
`twag_bearer_modify_command_count`	عداد	لا شيء	أحداث PGW M Bearer-Comm بقة على جلسة
`twag_bearer_update_count`	عداد	لا شيء	أحداث PGW U ة على Bearer جلسة.
`twag_detach_cleanup_start_count`	عداد	لا شيء	تنظيف الفصل
`twag_detach_cleanup_complete_count`	عداد	لا شيء	تنظيف الفصل
`twag_detach_pgw_delete_count`	عداد	لا شيء	طلبات PGW D فصل Session
`twag_detach_liveness_timeout_count`	عداد	لا شيء	لتي تم تحفيزها طة مهلة الحياة
`twag_liveness_arp_probe_success_count`	عداد	لا شيء	اح استقصاءات للحياة.
`twag_liveness_arp_probe_failure_count`	عداد	لا شيء	شل استقصاءات للحياة.
`twag_handover_in_count`	عداد	`source`	ات الانتقال إلى الداخل.

المقياس	النوع	التسميات	وصف
`twag_handover_out_count`	عداد	`cause`	ات الانتقال إلى الخارج.
`twag_handover_ap_change_count`	عداد	ل شيء	ر نقطة الوصول داخل الجلسة.

استعلامات مثال:

```
# أسباب إنهاء الجلسات خلال الساعة الماضية
sum by (reason) (increase(twag_session_teardown_count[1h]))

# الجلسات التي تم إنهاؤها بسبب عدم إكمال المصادقة
increase(twag_session_teardown_count{reason="identity_timeout"}
[1h])

# الجلسات التي تم إسقاطها لأن UE صمت
increase(twag_detach_liveness_timeout_count[1h])
```

> ملاحظة: يتم إصدار أحداث حصة Gy `twag_gy_quota_blocked` و `twag_gy_quota_unblocked` بواسطة `Twag.Session.Client` ولكنها غير معلنة كمقاييس Prometheus اليوم، لذلك لا تظهر على نقطة نهاية `/metrics`. إنها مرئية في السجلات المنسقة.

مقاييس شحن Gy عبر الإنترنت

تتبع هذه العدادات التحكم في الائتمان Diameter Ro/Gy، المستخدمة فقط للاختراق المحلي NSWO. انظر الشحن عبر الإنترنت.

المقياس	النوع	التسميات	الوصف
`twag_gy_ccr_sent_count`	عداد	`type`	طلبات التحكم في الائتمان المرسلة إلى OCS. `type` هو `initial`، `update`، أو `terminate`.
`twag_gy_ccr_error_count`	عداد	`type`	فشل إرسال أو بناء CCR.
`twag_gy_cca_received_count`	عداد	`type`، `result`	إجابات التحكم في الائتمان المستلمة من OCS.

استعلامات مثال:

```
# معدل إرسال CCR حسب النوع
sum by (type) (rate(twag_gy_ccr_sent_count[5m]))

# فشل CCR
sum by (type) (increase(twag_gy_ccr_error_count[1h]))

# نتائج CCA
sum by (result) (rate(twag_gy_cca_received_count[5m]))
```

مقاييس STa Diameter

تتبع هذه العدادات الطلبات الواردة STa التي يتم التعامل معها بواسطة TWAG.

المقياس	النوع	التسميات	الوصف
`sta_asr_received_count`	عداد	لا شيء	طلبات إنهاء الجلسة المستلمة.
`sta_rar_received_count`	عداد	لا شيء	طلبات إعادة المصادقة المستلمة.
`sta_str_received_count`	عداد	لا شيء	طلبات إنهاء الجلسة المستلمة.
`sta_session_disconnect_count`	عداد	`reason`	فصل الجلسات STa.
`sta_session_reauth_count`	عداد	`re_auth_type`	إعادة مصادقات الجلسة STa.

مقياس رسالة Diameter

diameter_message_count

النوع: عداد

التسميات	الوصف
`application`	تطبيق Diameter (على سبيل المثال `swx`, `sta`).
`command`	اسم الأمر (على سبيل المثال `MAR`, `MAA`).
`direction`	`inbound` أو `outbound`.

استعلامات مثال:

```
# معدل رسائل Diameter حسب التطبيق
sum by (application) (rate(diameter_message_count[5m]))
```

مقاييس NSWO

الوصف	النوع	المقياس
تخصيصات IP المحلية NSWO.	عداد	`nswo_allocate_count`
إصدارات IP المحلية NSWO.	عداد	`nswo_release_count`

مقاييس DHCP

مسار توزيع `discover.pool_allocated` يغطي حدث DHCPv4. تتبع هذه العدادات خادم NSWO، حيث يقوم الخادم بتخصيص عنوان جديد من مجموعة مرتبطة عند DISCOVER.

المقياس	النوع	الوصف
`dhcp_lease_allocate_count`	عداد	تخصيصات الإيجار.
`dhcp_lease_deallocate_count`	عداد	إلغاء تخصيصات الإيجار.
`dhcp_discover_count`	عداد	حزم DISCOVER المقدمة من إيجار مسبق التخصيص.
`dhcp_discover_no_allocation_count`	عداد	DISCOVER بدون إيجار وبدون مجموعة مرتبطة (لا يوجد عنوان لتقديمه).
`dhcp_discover_pool_allocated_count`	عداد	DISCOVER المقدمة من خلال توزيع عنوان جديد من مجموعة مرتبطة (NSWO).
`dhcp_ack_count`	عداد	حزم ACK المرسلة.
`dhcp_nak_count`	عداد	حزم NAK المرسلة.
`dhcp_release_count`	عداد	حزم RELEASE المستلمة.
`dhcp_decline_count`	عداد	حزم DECLINE المستلمة.
`dhcp_inform_count`	عداد	حزم INFORM المستلمة.
`dhcp_packet_malformed_count`	عداد	حزم DHCP غير صحيحة.

استعلامات مثال:

```
# معدل توزيع المجموعة (توجيه NSWO)
rate(dhcp_discover_pool_allocated_count[5m])

# DISCOVER التي لم يكن بالإمكان تقديمها
increase(dhcp_discover_no_allocation_count[15m])
```

> ملاحظة: يقوم خادم DHCP أيضًا بإصدار `dhcp_lease_reap` عند حصاد إيجار منتهي الصلاحية. لم يتم الإعلان عن هذا الحدث كمقياس Prometheus يظهر على اليوم ول⁉⁉ نقطة نهاية `/metrics`.

مقاييس DHCPv6 و IPv6 RA

المقياس	النوع	الوصف
`dhcpv6_info_request_received_count`	عداد	حزم DHCPv6 Information-Request المستلمة.
`dhcpv6_solicit_received_count`	عداد	حزم DHCPv6 Solicit المستلمة.
`dhcpv6_request_received_count`	عداد	حزم DHCPv6 Request المستلمة.
`dhcpv6_info_reply_sent_count`	عداد	حزم DHCPv6 Information-Reply المرسلة.
`dhcpv6_advertise_sent_count`	عداد	حزم DHCPv6 Advertise المرسلة.
`dhcpv6_reply_sent_count`	عداد	حزم DHCPv6 Reply المرسلة.
`ipv6_ra_prefix_add_count`	عداد	إضافات بادئة IPv6 RA.
`ipv6_ra_prefix_remove_count`	عداد	إزالات بادئة IPv6 RA.
`ipv6_ra_advertisement_sent_count`	عداد	إعلانات موجهة IPv6 المرسلة.

مقاييس WLCP

تتبع هذه العدادات بروتوكول التحكم في WLAN المستخدم لوضع الاتصال المتعدد.

المقياس	النوع	الوحدة	الوصف
`wlcp_packet_received_count`	عداد	لا شيء	حزم WLCP المستلمة.
`wlcp_packet_received_bytes`	مجموع	بايت	إجمالي بايتات حزم WLCP المستلمة.
`wlcp_packet_malformed_count`	عداد	لا شيء	حزم WLCP غير صحيحة.
`wlcp_packet_unregistered_count`	عداد	لا شيء	حزم WLCP من عملاء غير مسجلين.
`wlcp_pdn_request_count`	عداد	لا شيء	طلبات اتصال PDN.
`wlcp_pdn_accept_count`	عداد	لا شيء	قبول اتصال PDN.
`wlcp_pdn_reject_count`	عداد	لا شيء	رفض اتصال PDN.
`wlcp_pdn_disconnect_request_count`	عداد	لا شيء	طلبات فصل PDN.
`wlcp_pdn_disconnect_accept_count`	عداد	لا شيء	قبول فصل PDN.

مقاييس Erlang VM

تقدم هذه المقاييس رؤية إلى وقت تشغيل BEAM.

الذاكرة

المقياس	الوصف
`vm_memory_total`	إجمالي الذاكرة المخصصة (بايت).
`vm_memory_processes`	الذاكرة المستخدمة بواسطة عمليات Erlang.
`vm_memory_processes_used`	الذاكرة المستخدمة فعليًا بواسطة العمليات.
`vm_memory_system`	الذاكرة المستخدمة بواسطة وقت التشغيل.
`vm_memory_atom`	الذاكرة المستخدمة بواسطة الذرات.
`vm_memory_atom_used`	الذاكرة المستخدمة فعليًا بواسطة الذرات.
`vm_memory_binary`	الذاكرة المستخدمة بواسطة الثنائيات.
`vm_memory_code`	الذاكرة المستخدمة بواسطة الشيفرة المحملة.
`vm_memory_ets`	الذاكرة المستخدمة بواسطة جداول ETS (حالة الجلسة ونقطة الوصول).

النظام

المقياس	الوصف
`vm_system_info_process_count`	العدد الحالي لعمليات Erlang.
`vm_system_info_port_count`	العدد الحالي للمنافذ.
`vm_system_info_atom_count`	العدد الحالي للذرات.
`vm_system_info_schedulers`	إجمالي خيوط الجدولة.
`vm_system_info_schedulers_online`	خيوط الجدولة المتصلة.

المجدولين

المقياس	الوصف
`vm_statistics_run_queue`	إجمالي طول قائمة التشغيل.
`vm_total_run_queue_lengths_total`	إجمالي قائمة تشغيل المجدول.
`vm_total_run_queue_lengths_cpu`	قائمة تشغيل المجدول CPU.
`vm_total_run_queue_lengths_io`	قائمة تشغيل المجدول IO.

استعلامات مثال:

```
# إجمالي الذاكرة بالميغابايت
vm_memory_total / 1024 / 1024

# تشبع قائمة التشغيل (يجب أن يكون منخفضًا)
avg_over_time(vm_statistics_run_queue[5m])
```

مثال Grafana استعلامات

نظرة عامة على المصادقة

```
# المقبولات في الثانية
sum(rate(radius_access_accept_count[5m]))

# المرفوضات في الثانية
sum(rate(radius_access_reject_count[5m]))

# نسبة النجاح المئوية
100 * sum(rate(radius_access_accept_count[5m])) /
  (sum(rate(radius_access_accept_count[5m])) +
sum(rate(radius_access_reject_count[5m])))
```

إحصائيات لكل نقطة وصول

```
# الطلبات حسب نقطة الوصول (طلب الوصول ليس لديه تسمية nas_ip؛
استخدم المحاسبة بدلاً من ذلك)
sum by (nas_ip) (rate(radius_accounting_request_count[5m]))

# العملاء حسب نقطة الوصول
radius_clients_per_ap_count
```

تحليل الرفض ومعدل الحد

```
# رفضات المصادقة حسب فئة السبب
sum(increase(radius_access_reject_count[1h]))
sum(increase(radius_auth_unauthorized_source_count[1h]))
sum(increase(radius_auth_bad_secret_count[1h]))

# أسباب إنهاء الجلسات
sum by (reason) (increase(twag_session_teardown_count[1h]))
```

استخدام البيانات

```
# إجمالي التدفق بالميغابايت
(radius_data_bytes_in + radius_data_bytes_out) / 1024 / 1024
```

قواعد التنبيه

التنبيهات الحرجة

```
groups:
  - name: twag_critical
    rules:
      - alert: HighAuthenticationFailureRate
        expr: >
          sum(rate(radius_access_reject_count[5m])) /
          (sum(rate(radius_access_accept_count[5m])) +
sum(rate(radius_access_reject_count[5m]))) > 0.1
        for: 5m
        labels:
          severity: critical
        annotations:
          summary: "معدل فشل المصادقة مرتفع (> 10%)"

      - alert: EAPSyncFailures
        expr: increase(eap_aka_sync_failure_count[5m]) > 0
        for: 1m
        labels:
          severity: warning
        annotations:
          summary: "تم الكشف عن فشل مزامنة EAP-AKA"

      - alert: UnknownRadiusSources
        expr: increase(radius_auth_unauthorized_source_count[15m])
> 0
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "حزم RADIUS من مصادر بدون بيانات اعتماد مطابقة"

      - alert: BadRadiusSecret
        expr: increase(radius_auth_bad_secret_count[15m]) > 0
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "حزم RADIUS المرفوضة بسبب سر مشترك خاطئ"
```

```
      - alert: NoActiveClients
        expr: radius_active_clients_count == 0
        for: 15m
        labels:
          severity: warning
        annotations:
          summary: "لا يوجد عملاء نشطون لمدة 15 دقيقة"
```

تنبيهات الموارد

```
groups:
  - name: twag_resources
    rules:
      - alert: HighMemoryUsage
        expr: vm_memory_total > 1073741824
        for: 10m
        labels:
          severity: warning
        annotations:
          summary: "استخدام الذاكرة في TWAG يتجاوز 1GB"

      - alert: HighRunQueue
        expr: avg_over_time(vm_statistics_run_queue[5m]) > 10
        for: 5m
        labels:
          severity: warning
        annotations:
          summary: "ارتفاع قائمة تشغيل المجدول يشير إلى تشبع CPU"
```

صفحات ذات صلة

- العمارة
- رفض RADIUS
- أسرار RADIUS المشتركة
- الجلسات
- الشحن عبر الإنترنت

- محاسبة لكل نقطة وصول

نظرة عامة

الشحن عبر الإنترنت (Gy)

نظرة عامة

يمكن لـ OmniTWAG شحن جلسات البيانات في الوقت الحقيقي ضد نظام الشحن عبر الإنترنت (OCS). يستخدم OmniTWAG واجهة Diameter Ro (Gy) لإرسال طلبات التحكم في الائتمان (CCR) واستقبال إجابات التحكم في الائتمان (CCA). يتيح ذلك لمشغل الشبكة تطبيق التحكم في الائتمان المدفوع مسبقًا على حركة مرور WLAN التي يخدمها TWAG.

ينطبق الشحن عبر الإنترنت على الجلسات التي يمتلك فيها TWAG مسار البيانات، أي **NSWO** هو TWAG في هذه الحالة، يكون TWAG. وحركة المرور المرتكزة على **(الانفصال المحلي)** كنقطة تنفيذ الشحن. في TWAG النقطة التي تخرج منها حركة المرور إلى الإنترنت، لذا يعمل بأداء الشحن، لذا عادةً ما يترك المشغل وضع PGW يقوم **وضع التوجيه المنزلي (GTP)**، الشحن العالمي `:disabled`. لوضعيات بيانات الطائرة راجع مرجع خطة المستخدم.

تحدد تحكمان ما إذا كانت Gy تعمل لجهاز UE معين:

- **وضع الشحن العالمي** (`online_charging.mode`). يحدد أي طلبات تحكم في الائتمان يمكن لـ OmniTWAG إرسالها على الإطلاق.
- **وضع الشحن لكل نقطة وصول** على بيانات اعتماد AP (`charging_mode`). يحدد، لذلك UE. راجع بيانات اعتماد RADIUS. يفتح جلسة Gy لكل نقطة وصول، ما إذا كان

راجع وضع الشحن لكل نقطة وصول. يجب أن تسمح كلا التحكمين بالشحن لكي يتم إرسال CCR-Initial.

جدول المحتويات

- المفاهيم
- أوضاع الشحن
- وضع الشحن لكل نقطة وصول
- تدفق التحكم في الائتمان
- الحصة، الاستخدام، وإعادة التفويض
- تنفيذ الحصة
- مجموعة التصنيف ووحدات الخدمة

- التكوين
- السل��ك التشغيلي ومعالجة الأخطاء
- قابلية المراقبة
- الجداول المرجعية

المفاهيم

واجهة Gy هي تطبيق Diameter و يحمل رسائل التحكم في الائتمان بين عنصر الشبكة و OCS. يستخدم OmniTWAG 3 قاموسGPP Ro مع Auth-Application-Id `4`، كما هو محدد في RFC 4006 3 وGPP TS 32.299. يستخدم OmniTWAG Service-Context-Id `32251@3gpp.org`، وهو سياق الشحن PS 3 لـGPP.

يرسل OmniTWAG خلال الجلسة ثلاثة أنواع من طلبات التحكم في الائتمان:

- **CCR-Initial (CCR-I)**: يطلب OmniTWAG من OCS بدء التحكم عند بدء الجلسة. في الائتمان للمشترك.
- **CCR-Update (CCR-U)**: يبلغ OmniTWAG خلال الجلسة عن البيانات المستخدمة ويطلب المزيد من الحصة.
- **CCR-Termination (CCR-T)**: يبلغ OmniTWAG عند انتهاء الجلسة عن البيانات المستخدمة النهائية ويغلق جلسة التحكم في الائتمان.

ترد OCS في الائتمان على كل طلب بإجابة التحكم (CCA). تحمل CCA `Result-Code`، ومنح اختياري للحصة (`Granted-Service-Unit`)، و `Validity-Time` اختياري.

يحافظ OmniTWAG على حالة Gy على جلسة مشترك. تحتوي حالة Gy منفصلة لكل `Session-Id` الحالي، وعدد الاستخدام التراكمي، وآخر حصة منحتها Diameter، و `CC-Request-Number` ويتخلص من الحالة عند انتهاء الجلسة، CCR-I هذه الحالة عند إرسال OmniTWAG ينشئ OCS.

أوضاع الشحن

معامل `online_charging.mode` يختار واحدًا من ثلاثة أوضاع هو وضع الشحن **العالمي**. إرسالها. ثم يحدد وضع OmniTWAG ويتحكم في أي طلبات تحكم في الائتمان يمكن لـ لكل نقطة وصول (انظر وضع الشحن لكل نقطة وصول) ما إذا كان `charging_mode` على الإطلاق لكل UE. يفتح جلسة Gy OmniTWAG

الوضع	عند CCR-I البدء	خلال CCR-U الجلسة	عند CCR-T النهاية
`:disabled`	لا	لا	لا
`:authorize_only`	نعم	لا	نعم
`:online_charging`	نعم	نعم	نعم

`:disabled`

لا يتصل OmniTWAG بـ OCS. هذه هي الوضع الافتراضي. استخدم هذا الوضع لعملية التوجيه المنزلي (GTP)، حيث يقوم PGW بأداء الشحن.

`:authorize_only`

يرسل OmniTWAG CCR-I عند بدء الجلسة و CCR-T عند انتهاء الجلسة. لا يرسل OmniTWAG رسائل CCR-U المؤقتة. استخدم هذا الوضع للتحقق من رصيد المشترك عند البدء ولإبلاغ الاستخدام الكلي في النهاية، دون إدارة حصة حية.

`:online_charging`

يرسل OmniTWAG CCR-I عند البدء، و CCR-U في كل تحديث مؤقت للمحاسبة، و CCR-T عند النهاية. استخدم هذا الوضع لإدارة الحصة بالكامل، حيث تمنح OCS الجلسة خلال وتحديث الحصة.

وضع الشحن لكل نقطة وصول

تحمل كل بيانات اعتماد AP حقل `charging_mode`. هذا منفصل عن `online_charging.mode` الذي يقوم بحل بيانات الاعتماد من مصدر OmniTWAG العالمي للجلسة، لذا يمكن أن يكون لكل نقطة وصول سلوكها الخاص. انظر بيانات اعتماد RADIUS.

وضع `charging_mode` لكل نقطة وصول	المعنى	التأثير على Gy
`:charged`	شحن حركة مرور هذه النقطة. هذا هو الوضع الافتراضي.	يفتح OmniTWAG جلسة Gy (CCR-Initial) عندما يسمح UE لـ الوضع العالمي بذلك أيضًا.
`:uncharged`	خدمة هذه النقطة ولكن لا تشحنها.	يقوم OmniTWAG بإنشاء جلسة Gy. البيانات ولكن لا يفتح أي جلسة CCR. لا يتم إرسال أي
`:auth_only`	المصادقة فقط، لا جلسة بيانات.	يقوم OmniTWAG بمصادقة المشترك ويتوقف. لا ينشئ جلسة Gy. بيانات ولا يفتح أي جلسة

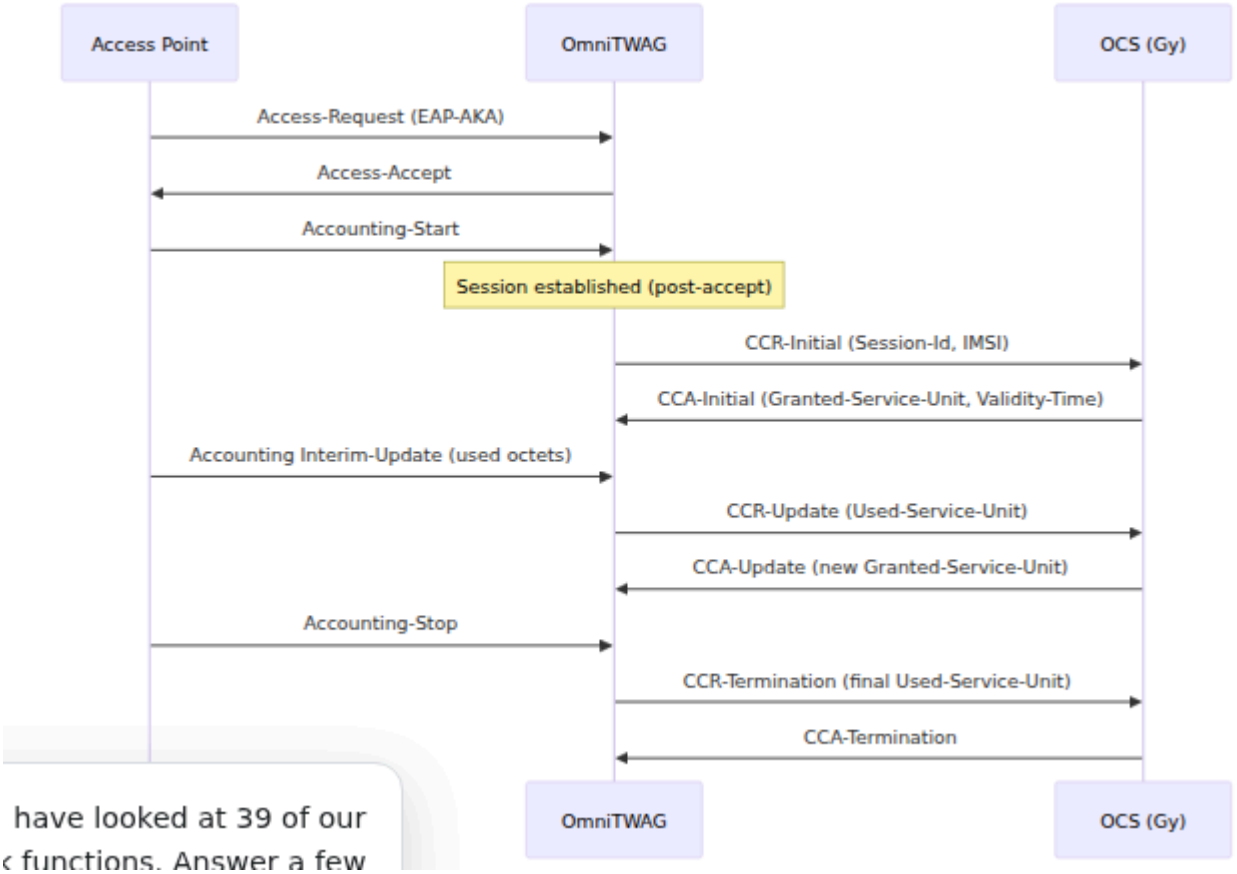
يرسل OmniTWAG CCR-Initial فقط عندما **تتحقق** جميع هذه الشروط:

- وضع `online_charging.mode` العالمي ليس `:disabled` (مفعل Gy عميل).
- تحتوي الجلسة على IMSI.
- وضع بيانات اعتماد AP `charging_mode` هو `:charged`.

إذا فشلت أي شرط، لا يفتح OmniTWAG أي جلسة Gy لـ UE، ولا يتم إرسال CCR-T أو CCR-U بشكل مستقل عن الوضع ا��عالمي: Gy لاحقًا. وبالتالي، فإن وضع كل نقطة وصول يتحكم في `:uncharged` المعلمة بـ AP فإن، `:online_charging` حتى مع تعيين الوضع العالمي إلى تنتج أي حركة Gy.

تدفق التحكم في الائتمان

تتبع جلسة التحكم في الائتمان جلسة المشترك. يقوم OmniTWAG بتحفيز كل طلب تحكم في الائتمان من نقطة معينة في دورة حياة جلسة RADIUS.



بدء الجلسة (CCR-Initial)

يرسل OmniTWAG CCR-I بعد أن ينشئ الجلسة. يتم تنفيذ إنشاء الجلسة في خطوة ما بعد القبول، التي يقوم خادم RADIUS بتحفيزها بعد Access-Accept و Accounting-Start. يرسل OmniTWAG CCR-I فقط عندما يكون وضع الشحن العالمي مفعلًا، وتحتوي الجلسة على IMSI، وبيانات اعتماد AP `charging_mode` هي `:charged`. انظر وضع الشحن لكل نقطة وصول.

تحمل CCR-I IMSI المشترك في AVP `Subscription-ID` مع النوع `1` (END_USER_IMSI). تعين CCR-I `Multiple-Services-Indicator` إلى `1` وتضم مجموعة واحدة من `Multiple-Services-Credit-Control` (MSCC) مع `Requested-Service-Unit` فارغ و `Rating-Group` المكونة.

التحديثات المؤقتة (CCR-Update)

يدمج كل تحديث مؤقت للمحاسبة من RADIUS حجم البيانات في وضع `:online_charging`، في كل OmniTWAG CCR-U لا يرسل Gy. المبلغ عنها ووقت الجلسة في عدادات استخدام فقط عندما يتم تفعيل أحد هذه المحفزات CCR-U تحديث مؤقت. يرسل:

- تجاوز الحجم المستخدم الكسر المحدد من الحجم الممنوح (الـ `quota.update_threshold`، `0.8` الافتراضي).
- انتهاء صلاحية `Validity-Time` للحصة الممنوحة.

في OCS التحديث المؤقت الذي لا يتجاوز المحفز يسجل الاستخدام محليًا فقط، لذا لا يتم استشارة حجم البيانات المستخدمة ووقت OmniTWAG، يقرأ CCR-U كل تحديث مؤقت. عندما يتم إرسال CCR-U أيضًا تتضمن `Used-Service-Unit` AVP الجلسة من سمات المحاسبة ويبلغ عنها في `Requested-Service-Unit` فارغ، حتى تتمكن OCS من منح المزيد من الحصة.

خارج مسار المحاسبة عندما يتم تفعيل مؤقت صلاحية الحصة. انظر تنفيذ CCR-U يتم أيضًا إرسال الحصة.

يقرأ OmniTWAG هذه السمات المحاسبية من RADIUS لـ CCR-U:

سمة RADIUS	حقل Gy
`Acct-Input-Octets`	`CC-Input-Octets`
`Acct-Output-Octets`	`CC-Output-Octets`
`Acct-Session-Time`	`CC-Time`

يحسب OmniTWAG `CC-Total-Octets` كمجموع المدخلات والمخرجات.

انتهاء الجلسة (CCR-Termination)

عندما يتم إنهاء الجلسة، على سبيل المثال عند RADIUS Accounting-Stop. يبلغ OmniTWAG عن الاستخدام التراكمي النهائي في AVP `Used-Service-Unit` ويعين `Termination-Cause` `1` إلى (DIAMETER_LOGOUT). يرسل OmniTWAG CCR-T ضع�ضع في كل من `:authorize_only` ووضع `:online_charging`. يرسل OmniTWAG CCR-T

الحصة، الاستخدام، وإعادة التفويض

الحصة الممنوحة

يمكن أن تحمل كل CCA `Granted-Service-Unit` داخل المجموعة الأولى من MSCC. يخزن OmniTWAG القيم الممنوحة في حالة Gy:

- `CC-Total-Octets`، `CC-Input-Octets`، `CC-Output-Octets`: حجم البيانات الممنوح.
- `CC-Time`: الوقت الممنوح.
- `Validity-Time`: يحول OmniTWAG الوقت بالثواني الذي تبقى فيه المنحة صالحة. هذا إلى موعد نهائي مطلق ويشغل مؤقتًا ضده.

يقرأ OmniTWAG أيضًا `Final-Unit-Indication` من MSCC و `Result-Code` على مستوى MSCC من كل CCA. يتم تخزين `Final-Unit-Action` من TERMINATE، REDIRECT، أو RESTRICT_ACCESS، أو `Result-Code` من MSCC `4010` (END_USER_SERVICE_DENIED) أو `4012` (CREDIT_LIMIT_REACHED) كإشارة لنفاد الائتمان. انظر تنفيذ الحصة.

يقوم OmniTWAG بتحديث المنحة المخزنة في كل CCA-U و CCA-I ناجحة.

الإبلاغ عن الاستخدام

يحتفظ OmniTWAG بعدادات الاستخدام التراكمية في حالة Gy. تعد عدادات المحاسبة من تراكمي�? للجلسة، لذا يبلغ كل تحديث مؤقت عن الإجمالي حتى الآن. يسجل RADIUS العدادات المبلغ عنها ويرسلها كـ OmniTWAG `Used-Service-Unit`. تعين CCR-U `Reporting-Reason` `4` إلى (VALIDITY_TIME). تعين CCR-T `Reporting-Reason` `2` إلى (FINAL).

إعادة التفويض

يعيد OmniTWAG التفويض على مسارين:

- يتجاوز عتبة الحصة أو يجد RADIUS **على الحركة.** يؤدي تحديث مؤقت للمحاسبة من فترة التحديث المؤقت هي خاصية نقطة. CCR-U أن الصلاحية قد انتهت إلى تحفيز الوصول، لذا فإن فترة تحديث مؤقت أقصر تعطي قياسًا أدق.

- يشغل OmniTWAG مؤقت صلاحية الحصة من `Validity-Time` **على الوقت.** OmniTWAG الممنوحة. إذا تم تفعيل المؤقت مع القليل من الحركة أو بدونها، لا يزال يمكن لـ `Validity-Time` OCS لإعادة التفويض. إذا لم ترسل CCR-U المكونة. مع عدم وجود أي منهما، `quota.validity_time` العودة إلى OmniTWAG لا يتم تشغيل مؤقت صلاحية.

يزداد `CC-Request-Number` بمقدار واحد بعد كل CCA ناجحة. تعطي هذه القيمة كل طلب في جلسة التحكم في الائتمان رقم تسلسل فريد، كما هو مطلوب في RFC 4006.

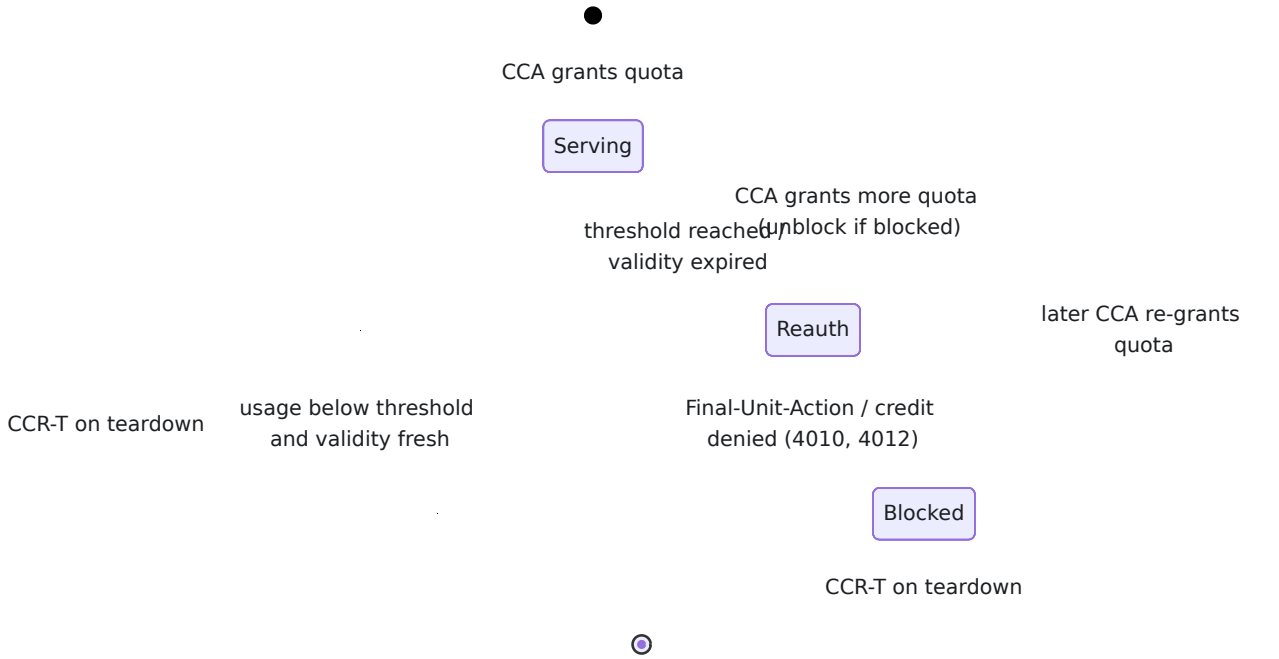
تنفيذ الحصة

يفرض OmniTWAG نفاد الائتمان في وضع `:online_charging`. لا يحتوي TWAG على وظيفة يقوم بإلغاء GRE: طائرة مستخدم منفصلة، لذا فإن رافعة التنفيذ الخاصة به هي مسار بيانات تسجيل UE من مسار البيانات، مما يسقط الرفع والهبوط لذلك UE.

يؤدي رد CCR-U إلى تحفيز التنفيذ عندما تظهر حالة Gy نفاد الائتمان، أي عندما:

- تشير إلى أي `Final-Unit-Action` (TERMINATE، REDIRECT، أو RESTRICT_ACCESS)، أو
- تعيد `Result-Code` من MSCC `4010` `4012` أو.

نظرًا لأن TWAG لا يمكنه الوفاء بـ REDIRECT أو RESTRICT_ACCESS على مسار البيانات كإيقاف. عندما يتم تفعيل التنفيذ، يقوم `Final-Unit-Action` الخاص به، يتم التعامل مع أي IP، ولكنه يحتفظ بالجلسة، وإيجار UE بحظر مسار بيانات OmniTWAG والمحاسبة على قيد الحياة. تعيد إعادة التفويض اللاحقة التي تمنح حصة قابلة للاستخدام مسا�ة البيانات.



التنفيذ هو جهد أفضل ويفشل في حالة الأخطاء في النقل: CCR-U الذي يفشل في طبقة أو إشارة OCS أبدًا. يحدث الحظر فقط عند رفض الائتمان بشكل صريح من UE لا يمنع Diameter نفاد الائتمان. انظر السلوك التشغيلي ومعالجة الأخطاء.

مجموعة التصنيف ووحدات الخدمة

يستخدم OmniTWAG `rating_group` مجموعة تصنيف واحدة للجلسة بأكملها. يحدد معامل قيمة `Rating-Group` في MSCC من CCR-I. لا يقوم OmniTWAG القيمة الافتراضية هي `1`. منحة حجم OmniTWAG بتقسيم الحركة إلى مجموعات تصنيف متعددة أو معرفات خدمة. يطلب مجمعة مع `Requested-Service-Unit` فارغ، لذا تقرر OCS المنحة.

التكوين

قم بتعيين معلمات الشحن عبر الإنترنت تحت تطبيق `:omnitwag`، في كتلة `online_charging` من `config/runtime.exs`.

```
config :omnitwag,
  online_charging: %{
    # وضع الشحن العالمي: :disabled، :authorize_only، أو
:online_charging
    mode: :disabled,

    # مجال Diameter لـ OCS (Destination-Realm لـ CCR)
    ocs_realm: "epc.mnc001.mcc001.3gppnetwork.org",

    # مجموعة التصنيف لمجموعة التحكم في الائتمان المتعددة الخدمات
    rating_group: 1,

    # إدارة الحصة (تستخدم في وضع :online_charging)
    quota: %{
      # الكسر من الحجم الممنوح الذي يتم عنده تحفيز CCR-Update
      update_threshold: 0.8,

      # وقت صلاحية النسخة الاحتياطية (بالثواني) عندما لا ترسل OCS
Validity-Time
      validity_time: 3600
    }
  }
```

المعلمات

المعامل	النوع	مطلوب	الافتراضي	الوصف
`mode`	Atom	لا	`:disabled`	ع الشحن العالمي. `:disab` واحد من `:authorize_on` أو `:online_charg` نظر أوضاع الشحن
`ocs_realm`	String	لا	مجال Diameter	مجال Diameter ل OCS. يستخدم OmniTWAG ذا كـ `Destination-Realm` في كل CC إذا لم يتم تعيينه، يستخدم OmniTW المجال المحلي لـ Diameter.
`rating_group`	Integer	لا	`1`	قيمة `Rating-Gr` التي يضعها OmniTWAG في MSCC من CCR-Initial.
`quota.update_threshold`	Float	لا	`0.8`	سر (0.0 إلى 1.0) من الحجم الممنوح ذي يتم عنده تحفيز CCR-Update.
`quota.validity_time`	Integer	لا	(غير محدد)	صلاحية الحصة لاحتياطية بالثواني، لمستخدمة لتشغيل ت الصلاحية عندما OCS لا ترسل

الوصف	الافتراضي	مطلوب	النوع	المعامل
`Validity-Time` م يتم تعيينها، لا يتم يل مؤقت احتياطي				

لكل نقطة وصول ليس جزءًا من هذه الكتلة. إنه موجود على كل بيانات `charging_mode` وضع اعتماد AP. انظر بيانات اعتماد RADIUS.

تأتي `Origin-Host` و `Origin-Realm` لـ Gy من هوية Diameter في تكوين `:diameter_ex` (`host` و `realm`). لم يتم تكوين `Destination-Host`. يتعلم OmniTWAG `Destination-Host` من `Origin-Host` من أول CCA، ويضيف هذا AVP إلى رسائل CCR-U و CCR-T لاحقًا.

نقل Diameter وتطبيق Ro

يرسل عميل Gy عبر كومة Diameter المشتركة. قم بتكوين OCS كند Diameter، وقم بتمكين تطبيق `:ro`، في تكوين `:diameter_ex`.

```
config :diameter_ex,
  diameter: %{
    service_name: :omnitouch_twag,
    host: "amanaki",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    request_timeout: 5000,
    applications: [
      %{
        application_name: :ro,
        application_dictionary: :diameter_gen_3gpp_ro,
        vendor_specific_application_ids: [
          %{vendor_id: 0, auth_application_id: 4,
acct_application_id: nil}
        ]
      }
    ],
    peers: [
      %{
        host: "ocs.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.179.2.233",
        port: 3868,
        transport: :diameter_tcp,
        initiate_connection: true
      }
    ]
  }
```

المعامل	النوع	مطلوب	الافتراضي	
`service_name`	Atom	نعم	-	م خدمة يرسل طلبات
`host`	String	نعم	-	D هوية (host) `Origi` `host`
`realm`	String	نعم	-	D مجال ستخدم `Origi` `Desti` م تعيين `ocs_r`
`request_timeout`	Integer	لا	5000	لانتظار ل على الطلب
`application_name`	Atom	نعم	-	تطبيق ينه إلى
`application_dictionary`	Atom	نعم	-	قاموس ينه إلى `:diam` لـ Gy.
`vendor_specific_application_ids`	List	نعم	-	دد من بائع. لـ `vendo` `auth_` `4`.

المعامل	النوع	مطلوب	الافتراضي	
`peers`	List	نعم	-	أقران أضف ت الند

معلمات الند

المعامل	النوع	مطلوب	الافتراضي	الوصف
`host`	String	نعم	-	هوية الند Diameter (FQDN). ب أن تتطابق مع هوية OCS.
`realm`	String	نعم	-	مجا�ة الند Diameter. يتم تعيينه إلى مجال OCS.
`ip`	String	نعم	-	عنوان IP لـ OCS للاتصال TCP.
`port`	Integer	لا	3868	منفذ Diameter لـ OCS. المنفذ القياسي هو 3868.
`transport`	Atom	لا	`:diameter_tcp`	بروتوكول النقل. استخدم `:diameter_t` لـ TCP.
`initiate_connection`	Boolean	لا	false	عندما يكون `true`، يبدأ OmniTWAG الاتصال بالند.

ملاحظة: تُظهر كتلة `online_charging` في `config/runtime.exs` المرسلة أيضًا على المستوى الأعلى، `request_timeout`، و `service_identifier`، و `ocs_host`. لا تقرأ الشفرة الحالية `subsequent_request` و `initial_request` و `quota` ومفاتيح `mode`، و `ocs_realm`، و `rating_group`، و للشحن هذه المفاتيح. تقرأ Diameter يأتي مهلة طلب `quota.validity_time`، و `quota.update_threshold`. يطلب OmniTWAG الحصة مع `Requested-` من `:diameter_ex` `request_timeout`.

> لا تشكل `subsequent_request` و `initial_request` فارغ، لذا فإن `Service-Unit` اليوم. لا تعتمد على المفاتيح غير المقروءة حتى تدعمها الشفرة CCR.

السلوك التشغيلي ومعالجة الأخطاء

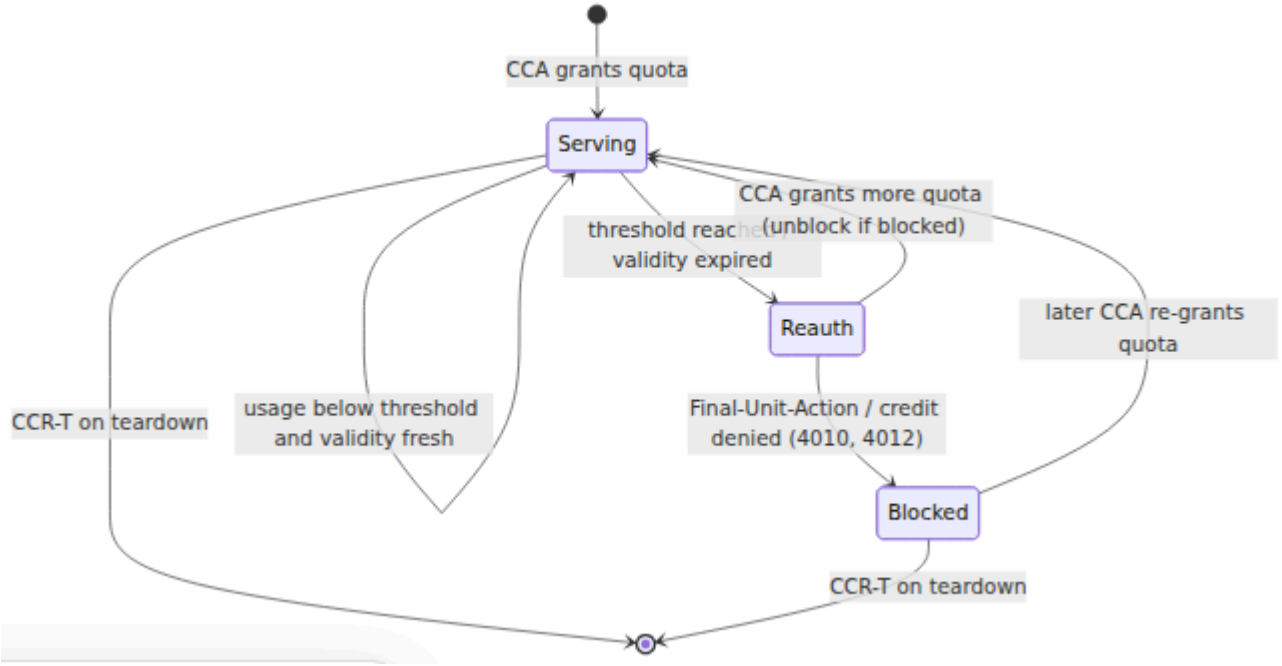
سلوك الفشل المفتوح

يعامل OmniTWAG فشل نقل Gy في الائتمان على أنه غير قاتل. إذا فشل طلب التحكم في الائتمان، تستمر جلسة المشترك ولا يقوم OmniTWAG بحظر الحركة.

- **OCS غير متاح أو مهلة**: يفشل CCR في نقل Diameter. يسجل OmniTWAG تحذيرًا. بالنسبة لـ CCR-I، يحتفظ OmniTWAG بحالة Gy، لذا يمكنه إرسال CCR-T لاحقًا. بالنسبة لـ CCR-U، يحتفظ OmniTWAG بحالة Gy ولا يمنع السابقة UE. بالنسبة لـ CCR-T، يسجل OmniTWAG التحذير ويكمل الإنهاء.
- **رمز نتيجة CCA خطأ**: تعيد OCS `2001` رمز نتيجة على مستوى الأمر ليس (DIAMETER_SUCCESS). يسجل OmniTWAG الخطأ ويعتبر الطلب فاشلاً. يحتفظ OmniTWAG بالجلسة حية.

بحظر مسار OmniTWAG، يقوم `:online_charging` التنفيذ منفصل عن فشل النقل. في وضع `Final-Unit-Action` الائتمان بشكل صريح أو تشير إلى OCS عندما ترفض UE بيانات MSCC لـ CCA. انظر تنفيذ الحصة. لا يمنع أبدًا في حالة فشل النقل، ولا يرفض الوصول في وضع `:authorize_only`. خطط لتكامل OCS هذا الانقسام في الاعتبار م��.

ملخص دورة حياة جلسة التحكم في الائتمان



معالجة رمز النتيجة

يقرأ OmniTWAG رمز النتيجة على مستويين.

- يعامل OmniTWAG `2001` على أنه نجاح. كما **رمز النتيجة على مستوى الأمر.** يعامل رمز النتيجة المفقود على أنه نجاح، لأن بعض ردود الأقران تصل كسجل خام بدون رمز نتيجة مفكك. أي قيمة أخرى على مستوى الأمر هي خطأ: يسجل OmniTWAG ذلك، ولا يعيد المحاولة، ويحتفظ بالجلسة حية.
- **رمز النتيجة على مستوى MSCC.** يتم قراءة MSCC، داخل المجموعة الأولى من `4012` أو (END_USER_SERVICE_DENIED) `4010` رمز النتيجة (CREDIT_LIMIT_REACHED) كإشارة لرفض الائتمان. في وضع `:online_charging`، يقود هذا التنفيذ ويمنع مسار بيانات UE. انظر تنفيذ الحصة.

قابلية المراقبة

يصدر OmniTWAG أحداث Telemetry لكل طلب وإجابة تحكم في الائتمان. تحمل الأحداث قيمة بيانات وصفية `type` من `:initial`، `:update`، أو `:terminate`.

حدث Telemetry	متى	بيانات وصفية
`[:twag, :gy, :ccr, :sent]`	يرسل OmniTWAG CCR	`type`
`[:twag, :gy, :cca, :received]`	يستقبل OmniTWAG CCA	`type`، `result` (`:success` أو `:error`)
`[:twag, :gy, :ccr, :error]`	يفشل CCR في النقل	`type`
`[:twag, :gy, :quota, :blocked]`	تم حظر مسار بيانات UE بسبب نفاد الائتمان	`identity`
`[:twag, :gy, :quota, :unblocked]`	تم استعادة مسار بيانات UE بعد إعادة المنح	`identity`

> **ملاحظة:** لم يتم تسجيل هذه الأحداث Telemetry لـ Gy كقياسات Prometheus في البناء اليوم، استخدم سجلات Gy الحالي. ا تصدر مرجع القياسات عنها بعد. لمراقبة سلوك التطبيق. يسجل عميل Gy كل من CCR-I و CCR-U و CCR-T على مستوى INFO، وكل فشل على مستوى WARN أو ERROR. تحمل خطوط السجل `Session-Id` من Diameter، وبالنسبة لـ CCR-I، تحمل IMSI.

الجداول المرجعية

قيم CC-Request-Type

القيمة	الاسم	الرسالة
1	INITIAL_REQUEST	CCR-Initial
2	UPDATE_REQUEST	CCR-Update
3	TERMINATION_REQUEST	CCR-Termination

تم تعريف القيم في RFC 4006 §8.3.

قيم Reporting-Reason المستخدمة

القيمة	الاسم	OmniTWAG حيث يستخدم
2	FINAL	CCR-Termination
4	VALIDITY_TIME	CCR-Update

رمز النتيجة

الرمز	المستوى	الاسم	سلوك OmniTWAG	جع
2001	أمر	DIAMETER_SUCCESS	يعتبر نجاحًا. تتقدم حالة Gy.	RF 67 §7.
(مفقود)	أمر	-	يعتبر نجاحًا، لردود السجلات الخام.	-
أي أخرى	أمر	(خطأ)	يسجل كخطأ. تستمر الجلسة.	RF 40 §9
4010	MSCC	END_USER_SERVICE_DENIED	يقرأ كرفض ائتمان. ينفذ في وضع (UE يمنع) `:online_charging`.	RF 40 §9
4012	MSCC	CREDIT_LIMIT_REACHED	يقرأ كرفض ائتمان. ينفذ في وضع (UE يمنع) `:online_charging`.	RF 40 §9

قيم Final-Unit-Action

تحمل MSCC `Final-Unit-Indication` `Final-Unit-Action`. لا يمتلك OmniTWAG وظيفة طائرة مستخدم، لذا لا يمكنه الوفاء بـ REDIRECT أو RESTRICT_ACCESS على مسار البيانات. يتعامل مع أي Final-Unit-Action كإيقاف ويمنع UE.

القيمة	الاسم	سلوك OmniTWAG
0	TERMINATE	يمنع مسار بيانات UE (تظل الجلسة محفوظة).
1	REDIRECT	يمنع مسار بيانات UE (إعادة التوجيه غير مدعومة).
2	RESTRICT_ACCESS	يمنع مسار بيانات UE (التقييد غير مدعوم).

تم تعريف Final-Unit-Indication في 3GPP TS 32.299 و RFC 4006 §5.6.

تطبيق Diameter

ID	الواجهة	القاموس	الاتجاه	المرجع
4	Ro / Gy	`diameter_gen_3gpp_ro`	TWAG إلى OCS	RFC 4006، 3GPP TS 32.299

مراجع المواصفات

الموضوع	المواصفة
تطبيق التحكم في الائتمان Diameter	RFC 4006
تطبيقات الشحن Diameter (Ro)	3GPP TS 32.299
بنية الشحن	3GPP TS 32.240
TWAG / 3 الوصول غيرIGPP (S2a، NSWO)	3GPP TS 23.402
بروتوكول Diameter الأساسي	RFC 6733

الصفحات ذات الصلة

- نظرة عامة
- بيانات اعتماد RADIUS
- مجموعات IP
- إدارة عنوان IP
- الجلسات
- S2a GTP-C
- خطة المستخدم

نظرة عامة

محاسبة لكل نقطة وصول

نظرة عامة

يجمع OmniTWAG بيانات محاسبة RADIUS وعدد الحركة إجمالي المشغل يرى. لكل نقطة وصول الجلسات لكل نقطة وصول. هذه البيانات منفصلة عن سجلات المحاسبة لكل جلسة. يقوم OmniTWAG بتجميع إجماليات كل نقطة وصول بواسطة `NAS-IP-Address` لنقطة الوصول. يعود، UBNT على سبيل المثال بعض طرازات) `NAS-IP-Address` عندما تتجاهل نقطة الوصول بحيث ترتبط المحاسبة بنفس إدخال، RADIUS لحزمة UDP المصدر IP إلى عنوان OmniTWAG نقطة الوصول الذي أنشأته المصادقة.

جدول المحتويات

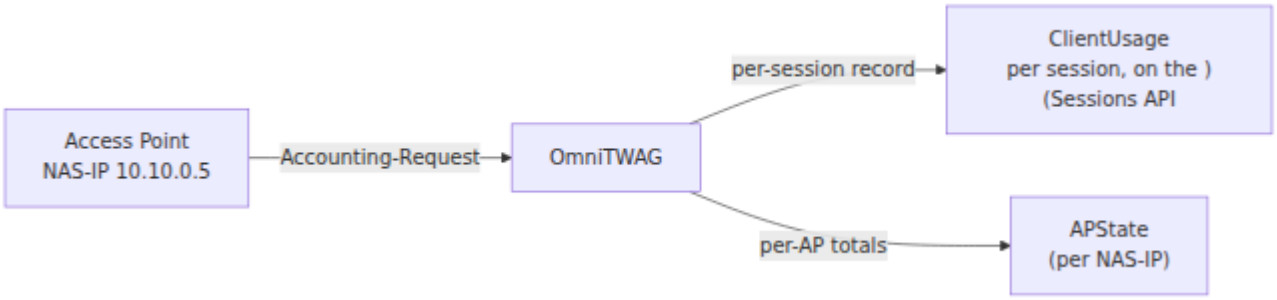
- المفاهيم
- كيفية حساب الإجماليات
- الحقول المسجلة
- عدد العملاء النشطين
- أي�� يمكن رؤية البيانات
- العلاقة بالبيانات لكل جلسة
- استكشاف الأخطاء وإصلاحها
- صفحات ذات صلة

المفاهيم

لكل جلسة عميل. تحتوي الحزمة RADIUS Accounting-Request ترسل نقطة الوصول حزم على `Acct-Status-Type` الذي يوضح الحدث:

- بدأت جلسة: (`1`) **بدء**.
- الجلسة نشطة، مع العدادات حتى الآن: (`3`) **تحديث مؤقت**.
- توقفت الجلسة، مع العدادات النهائية: (`2`) **توقف**.

من كل حزمة. يضيف `NAS-IP-Address` العدادات من الأوكتات والحزم و OmniTWAG يقرأ هذه القيم إلى الإجماليات الجارية لتلك النقطة. هذا يوفر للمشغل عرضًا لكل نقطة OmniTWAG وصول للحركة والجلسات.



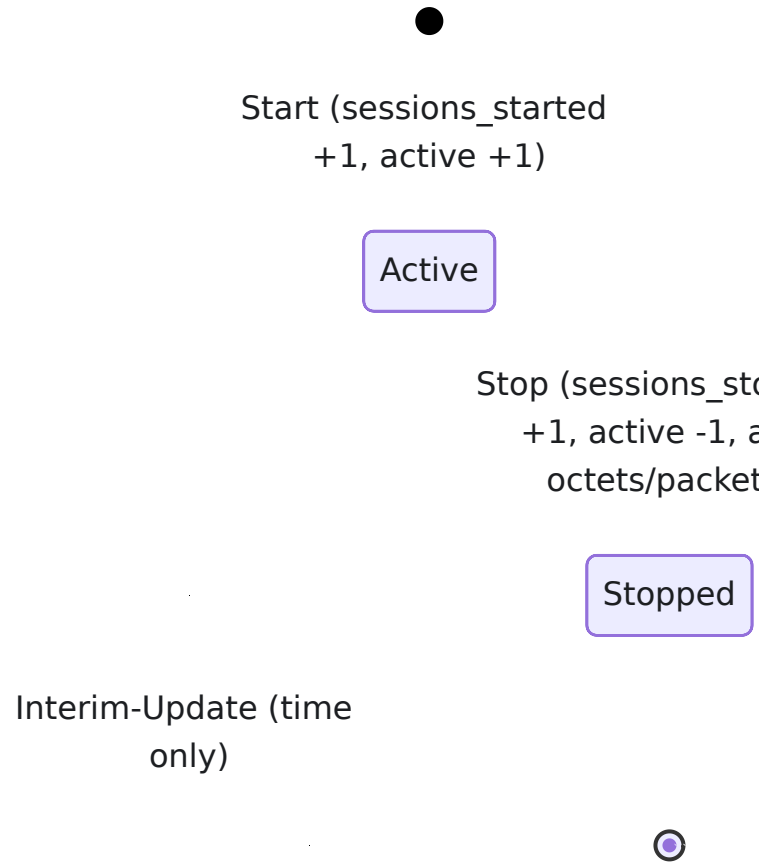
كيفية حساب الإجماليات

تراكمية لكل جلسة. يقوم تحديث مؤقت RADIUS تكون عدادات الأو��ات والحزم في وتوقف كلاهما بالإبلاغ عن الإجمالي للجلسة حتى الآن، وليس التغيير منذ آخر حزمة. إذا أضاف العدادات من كل حزمة، فإنه سيحسب نفس الحركة أكثر من مرة OmniTWAG.

عدادات الأوكتات والحزم إلى الإجماليات لكل نقطة OmniTWAG لتجنب العد المزدوج، يضيف وصول **فقط عند التوقف**. يقوم التوقف بالإبلاغ عن الإجمالي النهائي لجلسة مكتملة. القواعد هي:

- **البدء**: زيادة `acct_sessions_started` بمقدار واحد. زيادة `acct_active_sessions` بمقدار واحد.
- **التوقف**: زيادة `acct_sessions_stopped` بمقدار واحد. تقليل `acct_active_sessions` بمقدار واحد، ولكن ليس أقل من صفر. إضافة العدادات النهائية للأوكتات والحزم إلى الإجماليات لكل نقطة وصول.
- **التحديث المؤقت**: تحديث وقت المحاسبة الأخير فقط. لا تغير الإجماليات عند.

توقفًا لجلسة لم يرها تبدأ، فإن عدد الجلسات النشطة لا ينخفض إلى أقل OmniTWAG إذا تلقى يضيف الأوكتات والحزم النهائية. إذا تلقى OmniTWAG من صفر. لا يزال OmniTWAG بإنشاء إدخال لكل OmniTWAG لنقطة وصول لم يرها من قبل، يقوم Accounting-Request نقطة وصول. هذا يعني أن نقطة الوصول التي تتعامل مع المحاسبة فقط لا تزال تتبع.



الحقول المسجلة

يسجل OmniTWAG هذه الحقول لكل نقطة وصول، بالإضافة إلى بيانات التعريف الخاصة بنقطة الوصول مثل SSID و`Called-Station-Id`.

الحقل	النوع	الوصف
`acct_input_octets`	عدد صحيح	إجمالي الأوكتات المدخلة، المجمعة عبر الجلسات المتوقفة.
`acct_output_octets`	عدد صحيح	إجمالي الأوكتات الخارجة، المجمعة عبر الجلسات المتوقفة.
`acct_input_packets`	عدد صحيح	إجمالي الحزم المدخلة، المجمعة عبر الج��سات المتوقفة.
`acct_output_packets`	عدد صحيح	إجمالي الحزم الخارجة، المجمعة عبر الجلسات المتوقفة.
`acct_sessions_started`	عدد صحيح	عدد الجلسات التي بدأت على هذه النقطة.
`acct_sessions_stopped`	عدد صحيح	عدد الجلسات التي توقفت على هذه النقطة.
`acct_active_sessions`	عدد صحيح	مقياس الجلسات المفتوحة المستمدة من المحاسبة: `started` ناقص `stopped`، لا تقل أبدًا عن صفر. تعكس فقط ما تقارير المحاسبة RADIUS، لذلك يمكن أن تزيد عند فقدان نقطة الوصول لحزم التوقف (على سبيل المثال بعد إعادة التشغيل) وتبقى قديمة حتى تصل حزم التوقف أو تنتهي صلاحية الإدخال. هذا ليس رقم "العملاء النشطين" المعروض في صفحة نقاط الوصول — انظر عدد العملاء النشطين.
`last_accounting_at`	عدد صحيح	وقت آخر حزمة محاسبة، بالمللي ثانية منذ بداية Unix.

المدخلات هي حركة المرور. RFC 2866 في RADIUS تتبع اتجاه عدادات الأوكتات والحزم تعريف من العميل إلى الشبكة. المخرجات هي حركة المرور من الشبكة إلى العميل.

عدد العملاء النشطين

في واجهة برمجة `client_count` رقم **العملاء النشطين** في صفحة نقاط الوصول، وحقول التطبيقات لنقطة الوصول، يبلغان عن عدد العملاء **المتصلين الآن**. هذه القيمة ليست عداد المحاسبة `acct_active_sessions`. يتم اشتقاقها من عمليات الجلسات الحية في الذاكرة التي يديرها OmniTWAG لكل عميل مصادق عليه، مجمعة حسب `NAS-IP-Address` لنقطة الوصول.

تراقب كل عملية جلسة الحية من تحديثات المحاسبة المؤقتة. عندما يتوقف عميل عن إرسال تحديثات RADIUS لفترة محددة من الفترات، تقوم العملية بتفكيك نفسها، سواء وصلت حزمة Accounting-Stop أم لا. نظرًا لأن عدد العملاء النشطين هو عد لعمليات الجلسة الحية هذه، فإنه ينخفض إلى الصفر من تلقاء نفسه عندما تنقطع نقطة الوصول — ل�ن يعتمد على نقطة الوصول لإرسال توقف، ولا يرتفع بعد إعادة تشغيل نقطة الوصول.

استخدم `client_count` (الرقم الحي) كعدد العملاء المتصلين حاليًا. استخدم `acct_active_sessions` عندما تريد تحديدًا مقياس الجلسات المفتوحة المبلغ عنها من قبل المحاسبة، مع مراعاة التحذيرات المذكورة أعلاه.

أين يمكن رؤية البيانات

تكون الحقول لكل نقطة وصول جزءًا من سجل نقطة الوصول. يقرأها المشغل في مكانين:

- **واجهة برمجة التطبيقات REST**: تعيد نقطة النهاية `GET /access_points` كل نقطة وصول مع حقول المحاسبة لكل نقطة وصول. تعيد نقطة النهاية `GET /access_points/{id}` نقطة وصول واحدة بواسطة `NAS-IP-Address` الخاص بها.
- **واجهة الويب**: تعرض صفحة **نقاط الوصول** كل نقطة وصول. قم بتوسيع نقطة وصول لرؤية بياناتها الكاملة، بما في ذلك حقول المحاسبة لكل نقطة وصول.

العلاقة بالبيانات لكل جلسة

يقوم RADIUS، تكون الإجماليات لكل نقطة وصو�ن عبارة عن تجميع. لكل طلب محاسبة بكتابة سجلين OmniTWAG:

- `APState` ومفاتيحها **الإجماليات لكل نقطة وصول** الموصوفة هنا، المحتفظ بها في بواسطة NAS-IP.

- **سجل لكل جلسة**، المحتفظ به في `ClientUsage` ومفاتيحها بواسطة `Acct-Session-Id`. هذا هو عرض حركة المرور والمحاسبة الحية لكل مشترك، وهو مكشوف على واجهة برمجة التطبيقات للجلسات، وليس على سجل نقطة الوصول. انظر الجلسات.

تقوم الإجماليات لكل نقطة وصول بحساب الأوكتات والحزم فقط عند التوقف، لذا فإنها تتأخر عن العرض الحي لكل جلسة خلال جلسة نشطة. استخدم واجهة برمجة التطبيقات للجلسات عندما تحتاج إلى الاستخدام الحالي لمشترك واحد، والإجماليات لكل نقطة وصول عندما تحتاج إلى حركة المرور وعدد الجلسات على مدى الحياة لنقطة وصول.

من طلب الوصول، انظر AP تم تسجيل) يتم إنشاء إدخال نقطة الوصول إما بواسطة المصادقة أو، لنقاط الوصول التي تتعامل مع المحاسبة فقط، بواسطة أول (أسرار RADIUS المشتركة Accounting-Request. المصدر لم IP لا تظهر نقطة وصول أبدًا إذا تم إسقاط حزمها لأن عنوان يتطابق مع أي شبكة بيانات اعتماد.

استكشاف الأخطاء وإصلاحها

لا تتغير الإجماليات

الأعراض: تبقى إجماليات الأوكتات والحزم لنقطة الوصول عند الصفر، حتى على الرغم من استخدام العملاء للشبكة.

الأسباب المحتملة:

- لا ترسل نقطة الوصول حزم توقف. يضيف OmniTWAG الأوكتات والحزم فقط عند التوقف.
- لا ترسل نقطة الوصول المحاسبة على الإطلاق.

الحل:

1. تأكد من أن نقطة الوصول ترسل حزم Accounting-Request إلى OmniTWAG.
2. تأكد من أن نقطة الوصول ترسل توقفًا في نهاية الجلسة.
3. تأكد من أن السر المشترك للمحاسبة على نقطة الوصول يتطابق مع البيانات المعتمدة المسجلة. انظر أسرار RADIUS المشتركة.

يبدو أن عدد الجل��ات النشطة مرتفع جدًا

الأعراض: تكون قيمة `acct_active_sessions` أعلى من العدد الحقيقي للعملاء النشطين.

الأسباب المحتملة:

- أرسلت نقطة الوصول حزم بدء ولكن لم ترسل حزم التوقف المطابقة، على سبيل المثال بعد إعادة تشغيل نقطة الوصول.

الحل:

1. تأكد من أن نقطة الوصول ترسل توقفًا لكل جلسة.
2. قم بتعيين فترة تحديث مؤقت على نقطة الوصول، بحيث يرى OmniTWAG الجلسات النشطة.
3. يصحح العدد النشط نفسه مع وصول حزم التوقف الجديدة. لا ينخفض العدد إلى أقل من صفر.

هذا يؤثر فقط على `acct_active_sessions`. في صفحة نقاط رقم **العملاء النشطين** غير متأثر، لأنه عدد لعمليات الجلسة الحية بدلاً من عداد (`client_count` وحقول API) الوصول المحاسبة. انظر عدد العملاء النشطين.

لا تظهر نقطة الوصول

الأعراض: لا تظهر نقطة وصول ترسل المحاسبة في القائمة.

الأسباب المحتملة:

- أسقط OmniTWAG الحزم لأن عنوان IP المصدر لم يتطابق مع أي شبكة بيانات اعتماد.

الحل:

1. تحقق من مقياس `radius_auth_unauthorized_source_count`. انظر مرجع المقاييس RADIUS و رفض.
2. أضف بيانات اعتماد لشبكة نقطة الوصول. انظر أسرار RADIUS المشتركة.

صفحات ذات صلة

- نظرة عامة
- الجلسات
- أسرار RADIUS المشتركة
- رفض RADIUS
- مرجع المقاييس
- العمارة

نظرة عامة

معايير أداء OmniTWAG

من خلال التحكم في المصادقة وسرعة الإشارة في بوابة الوصول Trusted WLAN.

بيئة الاختبار

المعالج	Intel(R) Core(TM) i5-5250U CPU @ 1.60GHz (2 cores)
وقت التشغيل	Elixir 1.17.0 / Erlang OTP 27 (JIT) (erts 15.0.1)
القياس	ثانية تسخين + 3 ثواني قياس + 1 ثانية ذاكرة لكل عملية 1
الالتزام	`main` @ `01ec4e8`

يتم الإبلاغ عن السرعة بوصفها **ips** (تكرارات في الثانية: كلما كانت أعلى كانت أسرع). **المتوسط** و **الوسيط** هما زمن الاستجابة لكل مكالمة بالميكروثانية؛ الوسيط هو تقدير أفضل لزمن الاستجابة الثابت النموذجي. **Mem/op** هو الذاكرة المخصصة لكل مكالمة.

المصادقة الكاملة (من النهاية إلى النهاية)

الشكل الرئيسي: كل سيناريو يربط تسلسل الاتصال الكامل (فك ت��فير هوية، معالجة EAP، فك تشفير الاستجابة، والتحقق من MAC، بناء التحدي EAP-AKA'، متجه المصادقة، تسلسل مفاتيح MAC)، هي **الاتصالات الكاملة، أي الجلسات، في الثانية لكل نواة** (**ips**). لذا فإن سرعته عبر HSS يستقبله من *STa* ؛ *وضع الوضع المحلي* (Milenage) يحسب متجه المصادقة على الجهاز SWx/STa.

السيناريو	السرعة (ips)	المتوسط (µs)	الوسيط (µs)	Mem/op
الاتصال الكامل EAP-AKA'، وضع STa (متجه من HSS)	17,311	57.77	52.90	7,048 B
الاتصال الكامل EAP-AKA'، الوضع المحلي (متجه محسوب على الجهاز)	12,493	80.05	73.31	10,560 B

التشفير

عمليات التشفير لكل مصادقة: توليد متجه المصادقة SIM (Milenage)، تسلسل مفاتيح EAP-AKA' (CK'/IK'، مفاتيح الجلسة، MAC)، مفاتيح إعادة المصادقة السريعة ERP، ودالة اشتقاق المفاتيح العامة 3GPP.

العملية	السرعة (ips)	المتوسط (µs)	الوسيط (µs)	Mem/op
اشتقاق مفتاح WLCP (EMSK -> مفتاح WLCP)	262,975	3.80	3.54	72 B
بناء حزمة التحدي EAP-AKA' (ترميز)	257,991	3.88	0.87	456 B
اشتقاق CK'/IK' لـ EAP-AKA'	225,191	4.44	3.93	328 B
حساب MAC لـ EAP-AKA' (HMAC-SHA-256/16)	223,503	4.47	4.11	72 B
دالة اشتقاق المفاتيح العامة 3GPP (HMAC-SHA-256)	198,596	5.04	4.32	248 B
اشتقاق rMSK لـ ERP (لكل إعادة مصادقة)	113,269	8.83	8.01	376 B
إعادة المصادقة السريعة الكاملة ERP (rRK -> rIK -> rMSK)	61,496	16.26	14.97	520 B
حساب Milenage_all (RES، CK، IK، AK، MAC-A)	52,451	19.07	16.11	3,560 B
اشتقاق المفاتيح لـ EAP-AKA' (MK -> جميع مفاتيح الجلسة)	31,696	31.55	28.93	1,552 B
التشفير الكامل للمصادقة لـ EAP-AKA' (CK'/IK' + جميع المفاتيح)	28,380	35.24	32.59	1,808 B

العملية	ما تفعله
بناء حزمة التحدي لـ EAP-AKA'	ترميز طلب EAP/AKA'-Challenge (AT_RAND، AT_AUTN، AT_KDF، AT_MAC).
اشتقاق مفتاح WLCP	يشتق مفتاح حماية WLCP من EMSK (وضع الاتصال المتعدد).
دالة اشتقاق المفاتيح العامة 3GPP	دالة اشتقاق المفاتيح HMAC-SHA-256 المستخدمة عبر تسلسل المفاتيح.
حساب MAC لـ EAP-AKA'	HMAC-SHA-256 AT_MAC على حزمة EAP، مقطوعة إلى 16 بايت.
اشتقاق CK'/IK' لـ EAP-AKA'	يحول CK/IK إلى CK'/IK' مرتبط باسم شبكة الوصول.
اشتقاق rMSK لـ ERP	مفتاح جلسة لكل إعادة مصادقة لـ EAP (RFC 6696).
إعادة المصادقة السريعة الكاملة	سلسلة اشتقاق كاملة rRK → rIK → rMSK لإعادة مصادقة سريعة.
حساب Milenage_all	متجه مصادقة AKA واحد: RES، CK، IK، AK، MAC-A.
اشتقاق المفاتيح لـ EAP-AKA'	يوسع المفتاح الرئيسي إلى K_encr، K_aut، K_re، MSK، EMSK.
التشفير الكامل للمصادقة لـ EAP-AKA'	اشتقاق CK'/IK' بالإضافة إلى التوسع الكامل لمفاتيح الجلسة.

ترميز الحزم

لوضع WLCP (TS 24.244) معالجة رسالة EAP، عمليات ترميز/فك ترميز إشارة: تحليل حزمة RADIUS Access-Accept المبنية على كل MPPE الاتصال المتعدد، وسمات مفتاح

العم��ية	السرعة (ips)	المتوسط (µs)	الوسيط (µs)	Mem/op
فك ترميز WLCP (طلب اتصال PDN)	4,229,558	0.24	0.20	448 B
ترميز WLCP (طلب اتصال PDN)	2,492,441	0.40	0.24	160 B
ترميز WLCP + فك ترميز ذهابًا وإيابًا	1,989,407	0.50	0.40	608 B
فك ترميز حزمة هوية EAP	336,816	2.97	2.66	1,136 B
بناء VSA لـ MPPE (Send-Key، RC4 + MD5)	135,026	7.41	5.32	1,296 B

العملية	ما تفعله
فك ترميز WLCP	يحلل طلب اتصال PDN WLCP من الشبكة.
ترميز WLCP	يسلسل طلب اتصال PDN WLCP إلى الشبكة.
ترميز WLCP + فك ترميز ذهابًا وإيابًا	ترميز رسالة WLCP واحدة ثم فك ترميز.
فك ترميز حزمة هوية EAP	يحلل استجابة هوية EAP (استخراج NAI).
بناء VSA لـ MPPE	يبني MS-MPPE-Send-Key RADIUS VSA (RC4 + MD5) الذي يحمل MSK.

أسرار RADIUS المشتركة (حسب مجموعة عنوان IP المصدر)

نظرة عامة

تقوم OmniTWAG بمصادقة كل عميل RADIUS (أو نقطة وصول، NAS) باستخدام سر مشترك. تتيح هذه الميزة للمشغل إدارة **العديد** من الأسرار المشتركة، كل منها مرتبط بشبكات فرعية المصدر. تشارك مجموعة من نقاط الوصول التي تشترك في شبكة IP واحدة أو أكثر من عنوان فرعية أيضًا سرًا واحدًا. يقوم المشغل بإضافة وتغيير وإزالة هذه البيانات حسب الطلب من خلال أو واجهة الويب الخاصة بلوحة التحكم. المتجر دائم، لذا فإن بيانات REST واجهة برمجة التطبيقات الاعتماد تبقى بعد إعادة التشغيل.

جدول المحتويات

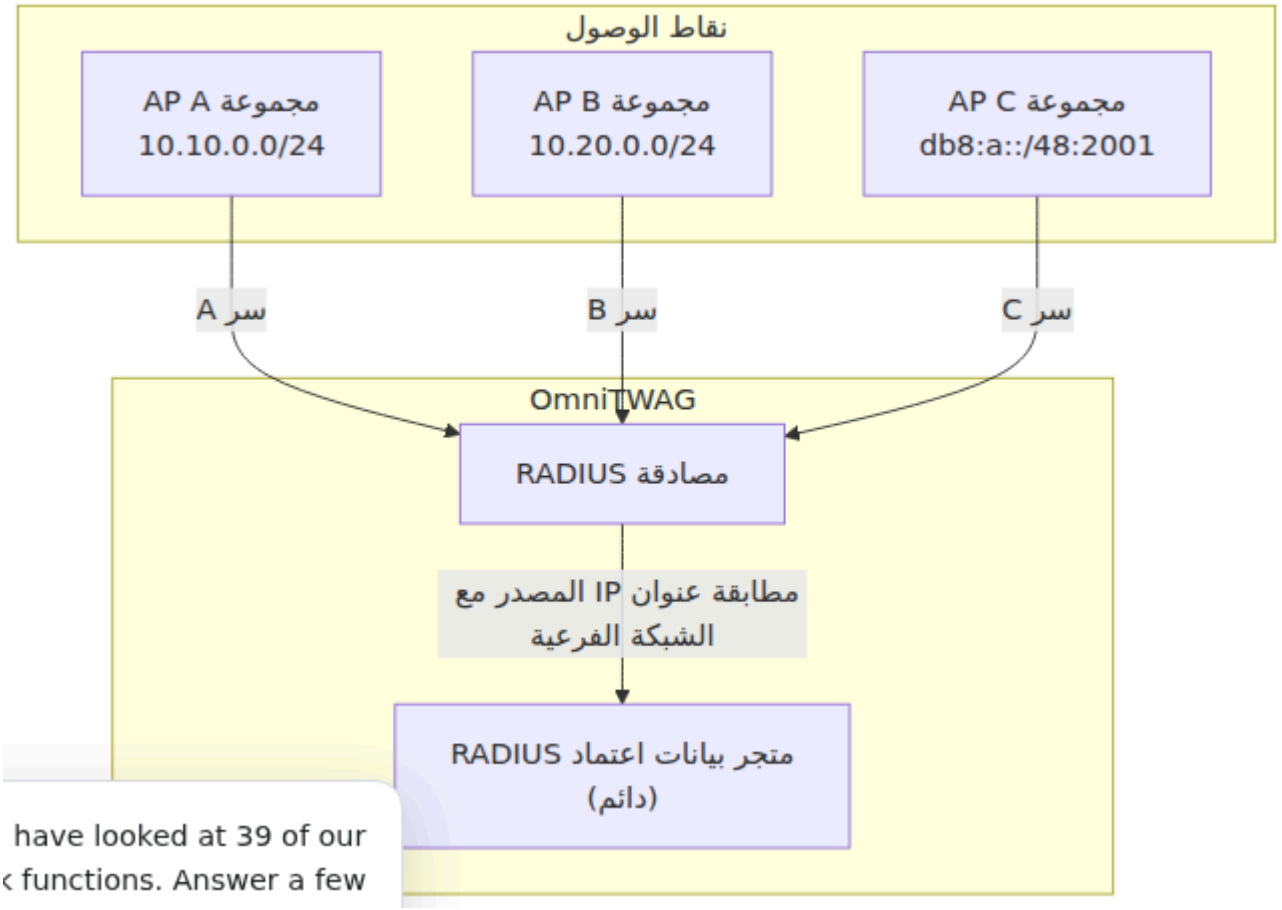
- المفاهيم
- كيف تستخدم المصادقة بيانات الاعتماد
- نموذج بيانات الاعتماد
- التفريغ والشحن لكل نقطة وصول
- واجهة برمجة التطبيقات REST
- واجهة الويب
- التكوين
- الهجرة من سر ثابت واحد
- المقاييس
- استكشاف الأخطاء وإصلاحها

المفاهيم

تربط **بيانات الاعتماد** سرًا مشتركًا واحدًا بشبكات فرعية واحدة أو أكثر من **المصدر**. شبكة المصدر هي كتلة CIDR. يمكن أن تكون الشبكة الفرعية IPv4 أو IPv6 أو مزيجًا من الاثنين.

عنوان IP المصدر هو عنوان IP لنقطة الوصول التي ترسل حزمة RADIUS. تقرأ OmniTWAG خاصية `NAS-IP-Address` المستلمة. لا تستخدم OmniTWAG عنوان IP المصدر من حزمة UDP لاختيار السر، لأن المهاجم يمكنه تعيين تلك الخاصية إلى أي قيمة.

تقوم شبكة بيانات الاعتماد أيضًا **بتفويض** نقطة الوصول. إذا تطابق عنوان IP المصدر مع شبكة بيانات الاعتماد، يتم تفويض نقطة الوصول. إذا لم يتطابق عنوان IP المصدر مع أي شبكة بيانات الاعتماد، تقوم OmniTWAG بإسقاط الحزمة. هذا يعني أنه عندما يضيف المشغل بيانات اعتماد جديدة، يتم تفويض نقطة الوصول في نفس الوقت لنقطة وصول جديدة.



كيف تستخدم المصادقة بيانات الاعتماد

تقوم OmniTWAG بحل السر المشترك لكل حزمة RADIUS واردة. الخطوات هي:

1. تقرأ OmniTWAG عنوان IP المصدر للحزمة.
2. تجد OmniTWAG بيانات الاعتماد التي تتطابق شبكتها الفرعية مع عنوان IP المصدر. إذا تطابقت أكثر من شبكة فرعية واحدة، تستخدم OmniTWAG الشبكة الفرعية ذات **أطول بادئة** (أكثر تطابقًا).

3. بإسقاط الحزمة. المصدر غير OmniTWAG إذا لم تتطابق أي شبكة فرعية، تقوم مفوض.
4. سر تلك البيانات الاعتمادية لفك تشفير OmniTWAG إذا تطابقت شبكة فرعية، تستخدم MPPE، ولتوقيع `Message-Authenticator` الحزمة، للتحقق من الرد.

فإن نقطة، `Message-Authenticator` إذا تطابقت شبكة فرعية ولكن لم يتم التحقق من بتسجيل هذا الحدث OmniTWAG الوصول تحمل سرًا مختلفًا عن الموجود في السجل. تقوم تعالج الحزمة. يتم توقيع الرد بالسر الموجود في السجل، لذا OmniTWAG وزيادة مقياس. لا تزال ترفض نقطة الوصول الرد وتفشل المصادقة. هذه السلوك يجعل من السهل العثور على سر مُهيأ بشكل خاطئ. لا تقوم بإسقاط الحزمة، لذا لا يتم إسقاط حالة صالحة عن طريق الخطأ.



نموذج بيانات الاعتماد

تحتوي كل بيانات اعتماد على هذه الحقول.

الحقل	النوع	الوصف
`id`	سلسلة	معرف فريد (UUID). يقوم الخادم بتعيين هذه القيمة.
`name`	سل��لة	تسمية قابلة للقراءة البشرية، على سبيل المثال `في ملبورن CBD نقاط وصول`.
`secret`	سلسلة	سر RADIUS مشترك.
`subnets`	قائمة من السلاسل	شبكة فرعية واحدة أو أكثر من كتل CIDR (IPv4، IPv6، أو مزيج)، على سبيل المثال `["2001" ,"10.10.0.0/24:db8:a::/48"]`.
`breakout_type`	سلسلة	معالجة بيانات الطائرة للجلسات من هذه نقطة الوصول: `tunneled`، `nswo`، أو `local`. القيمة الافتراضية `tunneled`. انظر التفريغ والشحن لكل نقطة وصول.
`address_source`	سلسلة	كيفية تعيين عنوان UE IP: `pool` أو `dhcp`. القيمة الافتراضية `pool`. انظر التفريغ والشحن لكل نقطة وصول.
`charging_mode`	سلسلة	سلوك الشحن عبر الإنترنت Gy: `charged`، `uncharged`، أو `auth_only`. القيمة الافتراضية `charged`. انظر التفريغ والشحن لكل نقطة وصول.
`ip_pool_id`	سلسلة	`id` اختياري لـ مجموعة IP التي تعالج جلسات `nswo` من هذه نقطة الوصول. `null` تعني عدم وجود مجموعة.
`inserted_at`	عدد صحيح	الوقت الذي تم فيه إنشاء بيانات الاعتماد، بالمللي ثانية منذ بداية Unix. يقوم الخادم بتعيين هذه القيمة.
`updated_at`	عدد صحيح	الوقت الذي تم فيه تغيير بيانات الاعتماد آخر مرة، بالمللي ثانية منذ بداية Unix. يقوم الخادم بتعيين هذه القيمة.

يقوم المشغل بتعيين `name`، `secret`، `subnets`، `breakout_type`، `address_source`، `charging_mode`، و `ip_pool_id`. يقوم الخادم بتعيين `id`، `inserted_at`، و `updated_at`.

التفريغ والشحن لكل نقطة وصول

تتحكم كل بيانات اعتماد أيضًا في بيانات الطائرة والشحن لنقاط الوصول في المجموعة. تحافظ مع الشحن عبر الإنترنت PGW إلى GTP القيم الافتراضية على السلوك القياسي: نفق.

breakout_type

تحدد `breakout_type` كيفية مغادرة حركة مرور المشتركين لـ TWAG.

القيمة	الوصف
`tunneled`	تقوم OmniTWAG بإنشاء جلسة GTP-C/GTP-U إلى PGW وتحويل حركة مرور المشتركين عبر النفق. هذه هي القيمة الافتراضية. انظر واجهة GTP-C S2a.
`nswo`	تقوم OmniTWAG بتثبيت الجلسة محليًا ولا تقوم بتحميل WLAN غير سلس. تقوم OmniTWAG بتعيين عنوان UE من مجموعة IP. تمر بالتنقل إلى PGW. وتخرج إلى الشبكة المحلية TWAG حركة مرور المشتركين عبر.
`local`	تمتلك نقطة الوصول بيانات الطائرة. تقوم OmniTWAG بمصادقة المشترك ولا تعين أي IP. يحصل UE على عنوانه من الشبكة المحلية.

address_source

تنطبق `address_source` فقط عندما تكون `breakout_type` هي `nswo`. تحدد كيفية تعيين عنوان UE IP. انظر مجموعة IP.

القيمة	الوصف
`pool`	تقوم OmniTWAG بتخصيص عنوان ثابت مسبقًا من مجموعة IP المرتبطة لكل جلسة. هذه هي القيمة الافتراضية.
`dhcp`	يقوم خادم DHCP الخاص بـ OmniTWAG عندما يرسل UE طلب DHCP DISCOVER بتوزيع عنوان من نطاق المجموعة.

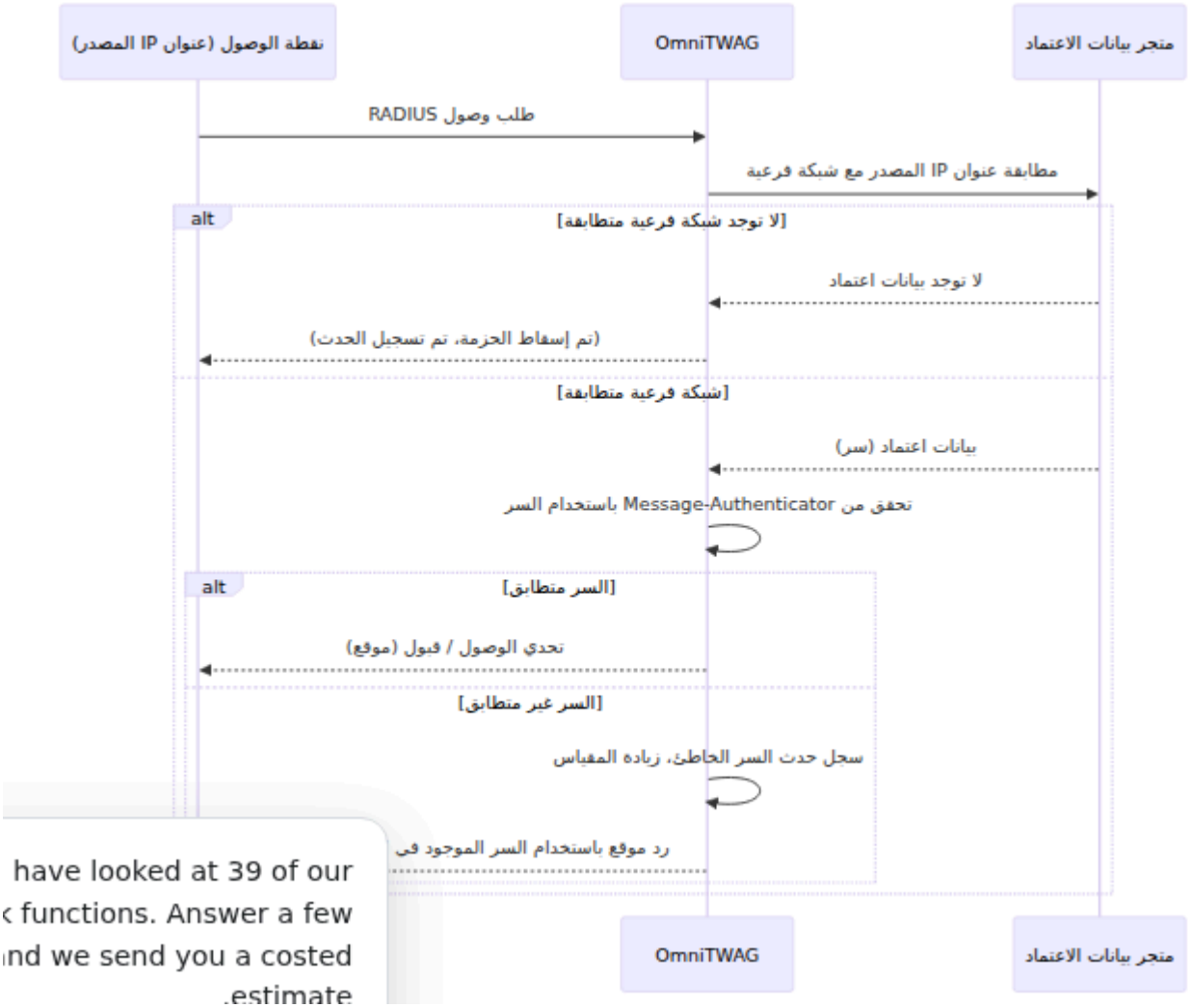
charging_mode

تحدد `charging_mode` سلوك الشحن عبر الإنترنت Gy. انظر الشحن عبر الإنترنت.

القيمة	الوصف
`charged`	تقوم OmniTWAG بفتح جلسة شحن عبر الإنترنت Gy وتبلغ عن الاستخدام إلى OCS. هذه هي القيمة الافتراضية.
`uncharged`	تقوم OmniTWAG بإنشاء جلسة بيانات ولكن لا تفتح جلسة Gy. استخدم هذه القيمة للوصول ذي السعر الثابت أو غير المشحون.
`auth_only`	تقوم OmniTWAG بمصادقة المشترك ولكن لا تنشئ جلسة بيانات. استخدم هذه القيمة عندما يوفر نظام آخر الاتصال.

كيفية تفاعل الحقول

تأخذ `charging_mode: auth_only` الأولوية. عندما تستخدم بيانات الاعتماد `auth_only`، لا تقوم OmniTWAG بإنشاء جلسة بيانات، لذا فإن `breakout_type` و `address_source` ليس لهما تأثير.



REST واجهة برمجة التطبيقات

تقدم واجهة برمجة التطبيقات REST الخاصة بـ OmniTWAG هذه النقاط النهائية عبر HTTPS على المكون (`8444` بشكل افتراضي). المسار الأساسي هو `api_ex` منفذ `/radius_credentials`.

الطريقة	المسار	الإجراء	الوصف
GET	`/radius_credentials`	index	قائمة بجميع بيانات الاعتماد.
GET	`/radius_credentials/{id}`	show	الحصول على بيانات اعتماد واحدة بواسطة `id`.
POST	`/radius_credentials`	create	إنشاء بيانات اعتماد.
PUT	`/radius_credentials/{id}`	update	تغيير بيانات اعتماد.
DELETE	`/radius_credentials/{id}`	delete	إزالة بيانات اعتماد.

جسم الطلب

تقبل `POST` و `PUT` جسم JSON مع هذه الحقول.

الحقل	النوع	مطلوب	الوصف
`name`	سلسلة	لا	تسمية قابلة للقراءة البشرية.
`secret`	سلسلة	نعم	سر RADIUS مشترك. يجب ألا يكون فارغًا.
`subnets`	قائمة من السلاسل	نعم	شبكة فرعية واحدة أو أكثر من كتل CIDR صالحة. يجب ألا تكون فارغة.
`breakout_type`	سلسلة	لا	`tunneled`، `nswo`، أو `local`. القيمة الافتراضية `tunneled`. انظر التفريغ والشحن لكل نقطة وصول.
`address_source`	سلسلة	لا	`pool` أو `dhcp` (لـ `nswo`). القيمة الافتراضية `pool`.
`charging_mode`	سلسلة	لا	`charged`، `uncharged`، أو `auth_only`. القيمة الافتراضية `charged`.
`ip_pool_id`	سلسلة	لا	`id` لمجموعة IP لتوجيه `nswo`. تعني لسلة فارغة عدم وجود مجموعة..

تقوم `PUT` بتغيير الحقول فقط في الجسم. تبقى الحقول التي ليست في الجسم على قيمتها الحالية.

الردود

الحالة	المعنى
`200 OK`	كانت الطلب ناجحة (index، show، update، delete).
`201 Created`	تم إنشاء بيانات الاعتماد.
`404 Not Found`	لا توجد بيانات اعتماد بالـ `id` المعطى.
`422 Unprocessable Entity`	`secret` فارغ، أو شبكة فرعية ليست كتلة CIDR صالحة، أو `breakout_type` / `address_source` / `charging_mode` ليست قيمة صالحة.

مثال: قائمة بيانات الاعتماد

الطلب:

```
GET /radius_credentials
```

الرد:

```
{
  "count": 1,
  "radius_credentials": [
    {
      "id": "0d1e2f3a-4b5c-6d7e-8f90-1a2b3c4d5e6f",
      "name": "في ملبورن CBD نقاط وصول",
      "secret": "s3cr3t",
      "subnets": ["10.10.0.0/24", "2001:db8:a::/48"],
      "inserted_at": 1734512400000,
      "updated_at": 1734512400000
    }
  ]
}
```

مثال: إنشاء بيانات اعتماد

الطلب:

```
POST /radius_credentials
```

```
{
  "name": "في ملبورن CBD نقاط وصول",
  "secret": "s3cr3t",
  "subnets": ["10.10.0.0/24", "2001:db8:a::/48"]
}
```

تعود الطلب الناجح بـ `201` `Created` مع بيانات الاعتماد الجديدة، بما في ذلك `id` الخاص بها.

مثال: شبكة فرعية غير صالحة

الطلب:

```
{
  "secret": "s3cr3t",
  "subnets": ["10.10.0.0/24", "not-a-subnet"]
}
```

الرد (`422 Unprocessable Entity`):

```
{
  "error": "شبكة CIDR غير صالحة: not-a-subnet"
}
```

واجهة الويب

تحتوي لوحة التحكم على صفحة **أسرار RADIUS** في `/radius_credentials`. تسرد الصفحة كل بيانات الاعتماد مع اسمها، والشبكات الفرعية، وسر مقنع، وآخر وقت تم تغييره. تحتوي الصفحة على نموذج لإضافة بيانات اعتماد وأدوات لتحرير أو حذف بيانات اعتماد. أدخل شبكة فرعية واحدة أو أكثر في حقل الشبكات الفرعية. افصل الشبكات الفرعية بفاصلة أو سطر جديد.

التكوين

يحتفظ متجر بيانات اعتماد RADIUS ببياناته في ملف DETS. قم بتعيين مسار الملف في كتلة `radius_config`.

```
config :omnitwag,
  radius_config: %{
    # المسار إلى متجر بيانات اعتماد RADIUS الدائم.
    credentials_dets_path: "priv/radius_credentials.dets",
    # (انظر "الهجرة" أدناه) حقول السر الثابتة القديمة.
    allowed_source_subnets: [],
    secret: "123456"
  }
```

المعامل	النوع	مطلوب	القيمة الافتراضية
`credentials_dets_path`	سلسلة	لا	`priv/radius_credentials.d`
`secret`	سلسلة	لا	`123456`

المعامل	النوع	مطلوب	القيمة الافتراضية
`allowed_source_subnets`	قائمة من السلاسل	لا	`[]`

الهجرة من سر ثابت واحد

استخدمت الإصدارات السابقة سرًا ثابتًا واحدًا و قائمة السماح الاختيارية `allowed_source_subnets`. عند بدء التشغيل الأول، إذا كان متجر بيانات الاعتماد فارغًا، تقوم OmniTWAG بتهيئة بيانات اعتماد واحدة من هذه الحقول القديمة. يتم تشغيل التهيئة فقط عندما يكون كلا الأمرين صحيحين:

- المتجر لا يحتوي على بيانات اعتماد.
- `allowed_source_subnets` ليست فارغة و `secret` تم تعيين.

تستخدم بيانات الاعتماد المهيأة السر القديم والشبكات الفرعية القديمة. هذا يحافظ على عمل نشر موجود بعد الترقية. تقوم OmniTWAG بتسجيل رسالة عند تهيئة بيانات اعتماد.

إذا كانت `allowed_source_subnets` فارغة، فإن OmniTWAG لا تقوم بتهيئة بيانات اعتماد. RADIUS حتى يضيف المشغل بيانات اعتماد. في هذه الحالة، ترفض OmniTWAG جميع طلبات

أضف بيانات الاعتماد من خلال واجهة برمجة التطبيقات REST أو واجهة الويب.

هذه الحقول تعمل فقط. `allowed_source_subnets` أو `secret` لا تقرأ المصادقة لكل حزمة كتهيئة عند بدء التشغيل الأول. إدارة بيانات الاعتماد الحية من خلال واجهة برمجة التطبيقات أو واجهة الويب.

المقاييس

انظر مرجع المقاييس. Prometheus تكشف OmniTWAG عن هذه العدادات على نقطة نهاية للحصول على نقطة النهاية وأمثلة الاستعلام.

radius_auth_unauthorized_source_count

النوع: عداد
الوصف: عدد حزم RADIUS المصدر لم يتطابق مع أي شبكة IP التي تم إسقاطها لأن عنوان بيانات اعتماد.

التسمية	الوصف
`source`	عنوان IP المصدر للحزمة التي تم إسقاطها.

radius_auth_bad_secret_count

النوع: عداد
الوصف: عدد حزم RADIUS المصدر مع بيانات اعتماد، ولكن لم يتم التحقق IP التي تطابق عنوان من `Message-Authenticator`. تحمل نقطة الوصول سرًا مختلفًا عن الموجود في السجل.

التسمية	الوصف
`source`	عنوان IP لنقطة الوصول.
`credential_id`	`id` لبيانات الاعتماد المتطابقة.

استكشاف الأخطاء وإصلاحها

نقطة الوصول لا تتلقى ردًا

الأعراض: ترسل نقطة الوصول طلبات RADIUS ولكن لا تتلقى أي رد. تزداد مقياس `radius_auth_unauthorized_source_count`.

الأسباب المحتملة:

- المصدر لنقطة الوصول IP لا تحتوي أي شبكة بيانات اعتماد على عنوان.
- مختلف عن المتوقع، على سبيل المثال عنوان IP ترسل نقطة الوصول من عنوان NAT.

الحل:

1. ابحث عن عنوان IP المصدر لنقطة الوصول في سجلات OmniTWAG.
2. تأكد من أن شبكة بيانات الاعتماد تحتوي على ذلك IP.
3. أضف بيانات اعتماد للشبكة الفرعية الصحيحة، إذا لم تغطي أي بيانات اعتماد IP.

نقطة الوصول مفوضة ولكن المصادقة تفشل

الأعراض: تزداد مقياس `radius_auth_bad_secret_count` لنقطة الوصول. لا يمكن للعملاء المصادقة.

الأسباب المحتملة:

- تحمل نقطة الوصول سرً مشتركًا مختلفًا عن بيانات الاعتماد الموجودة في السجل.

الحل:

1. اقرأ تسمية `credential_id` على المقياس، أو ابحث عن رسالة السر الخاطئ في السجلات.
2. قارن السر على نقطة الوصول مع السر في بيانات الاعتماد.
3. صحح السر على نقطة الوصول، أو قم بتحديث بيانات الاعتماد لتتطابق.

فقدان بيانات الاعتماد بعد إعادة التشغيل

الأعراض: تكون قائمة بيانات الاعتماد فارغة بعد إعادة التشغيل. ترفض OmniTWAG جميع الطلبات.

الأسباب المحتملة:

- يشير `credentials_dets_path` إلى دليل غير قابل للكتابة، أو إلى مسار يتم مسحه عند إعادة التشغيل.

الحل:

1. قم بتعيين `credentials_dets_path` إلى دليل بيانات دائم وقابل للكتابة.
2. تأكد من أن عملية OmniTWAG يمكنها الكتابة إلى ذلك المسار.
3. أضف بيانات الاعتماد مرة أخرى من خلال واجهة برمجة التطبيقات أو واجهة الويب.

رفضات RADIUS

نظرة عامة

يتيح ذلك للمشغل اكتشاف نقطة وصول RADIUS مصادر OmniTWAG تتبع التي تم رفض حزمها. RADIUS غير معروفة أو تم تكوينها بشكل خاطئ بسرعة. هذه الميزة هي صورة مرآة لـ أسرار المشتركة OmniTWAG، ويسجل متتبع: تخزن بيانات الاعتماد سجلات المصادر التي **تقبلها** OmniTWAG. الرفض المصادر التي **ترفضها**.

يحتفظ المتتبع ببياناته في الذاكرة. البيانات ليست دائمة. يتم إعادة تعيين المتتبع عند إعادة التشغيل. هذا عن قصد. انظر استكشاف الأخطاء وإصلاحها.

جدول المحتويات

- المفاهيم
- كيف تصل الحزمة إلى المتتبع
- أسباب الرفض
- نموذج الإدخال
- سلوك التخزين
- واجهة برمجة التطبيقات REST
- المقاييس
- استكشاف الأخطاء وإصلاحها

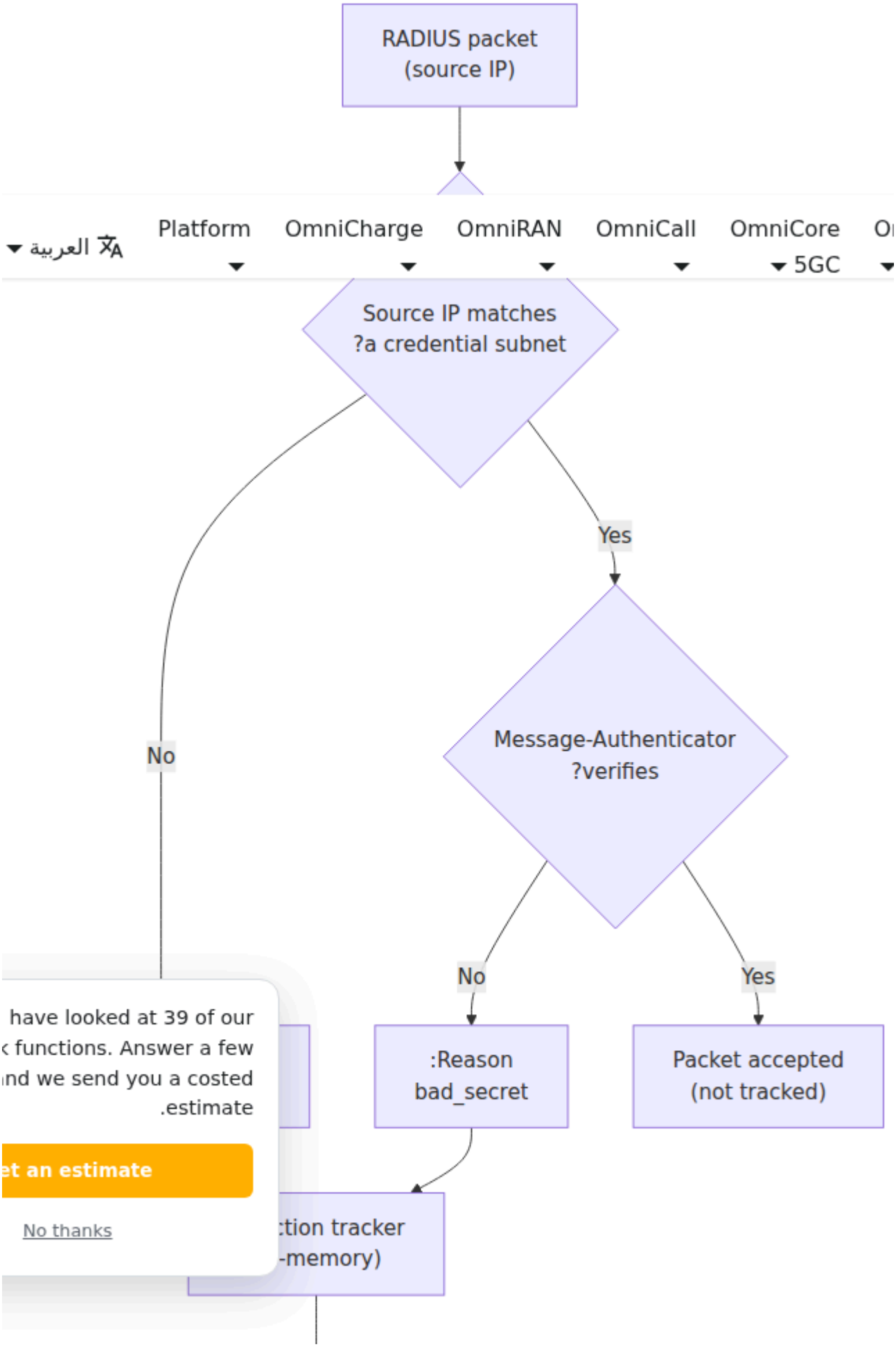
المفاهيم

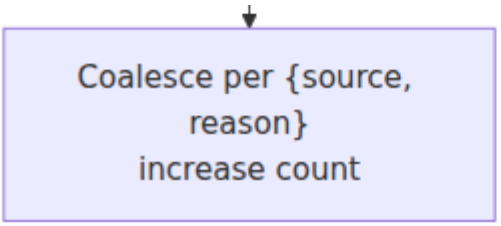
يسجل المتتبع. OmniTWAG لم تقبلها RADIUS أرسل حزمة IP هو عنوان **المصدر المرفوض** إدخالًا واحدًا لكل زوج فريد من **المصدر** و **السبب**. إذا تم رفض نفس المصدر عدة مرات لنفس السبب، تزيد OmniTWAG عدادًا على الإدخال الموجود. لا تضيف OmniTWAG صفًا جديدًا.

تقرأ OmniTWAG عنوان IP **المصدر** هو عنوان IP الذي أرسل حزمة RADIUS. **عنوان IP** المستلمة. لا تستخدم OmniTWAG خاصية `NAS-IP-Address`، لأن المصدر من حزمة UDP المهاجم يمكنه تعيين تلك الخاصية إلى أي قيمة.

كيف تصل الحزمة إلى المتتبع

تطابق OmniTWAG كل حزمة RADIUS واردة مع الشبكات الفرعية للبيانات الاعتماد. يتم رفض الحزمة عندما تفشل في أحد الفحصين. يسجل المتتبع المصدر والسبب لكل حزمة مرفوضة.


RADIUS packet
(source IP)
العربية
Platform
OmniCharge
OmniRAN
OmniCall
OmniCore
5GC
Source IP matches
?a credential subnet
Yes
No
Message-Authenticator
?verifies
No
Yes
:Reason
bad_secret
Packet accepted
(not tracked)
have looked at 39 of our
functions. Answer a few
nd we send you a costed
.estimate
et an estimate
No thanks
tion tracker
-memory)



أسباب الرفض

يتم رفض المصدر لأحد سببين.

السبب	المعنى
`unauthorized_source`	المصدر مع أي شبكة فرعية للبيانات IP لم يتطابق عنوان الاعتماد. هذه هي حالة OmniTWAG بإسقاط الحزمة. قامت نقطة الوصول غير المعروفة.
`bad_secret`	تطابقت شبكة فرعية للبيانات الاعتماد، لكن `Message-Authenticator` للحزمة لم يتحقق. تحتوي نقطة الوصول على سر مشترك مختلف عن الموجود في السجلات.

يسجل المتتبع أيضًا البيانات الاعتماد التي تطابقت. هذا يخبر `bad_secret`، بالنسبة لإدخال المشغل بأي بيانات اعتماد يجب التحقق منها.

نموذج الإدخال

كل إدخال يحتوي على هذه الحقول.

الحقل	النوع	الوصف
`source`	سلسلة	عنوان IP المصدر للحزمة المرفوضة. هذه القيمة هي معرف الإدخال.
`reason`	سلسلة	سبب الرفض: `unauthorized_source` أو `bad_secret`.
`count`	عدد صحيح	عدد المرات التي رفضت فيها OmniTWAG هذا المصدر لهذا السبب.
`first_seen`	عدد صحيح	الوقت الذي تم فيه رفض المصدر لأول مرة، بالمللي ثانية منذ بداية Unix.
`last_seen`	عدد صحيح	الوقت الذي تم فيه رفض المصدر آخر مرة، بالمللي ثانية منذ بداية Unix.
`credential_id`	سلسلة	للبيانات الاعتماد المطابقة. يتم تعيينه فقط عندما `id` يكون `reason` هو `bad_secret`.
`credential_name`	سلسلة	للبيانات الاعتماد المطابقة. يتم تعيينه فقط عندما `name` يكون `reason` هو `bad_secret`.

تكون حقول `credential_id` و `credential_name` فارغة لإدخال `unauthorized_source`، لأنه لم تتطابق أي بيانات اعتماد.

سلوك ��لتخزين

المتتبع هو تخزين في الذاكرة. له هذه الخصائص.

- **غير دائم.** يتم إعادة تعيين التخزين عند إعادة التشغيل. لا يبقى بعد إعادة تشغيل العملية.
- **مجمعة.** تسجل OmniTWAG إدخالًا واحدًا لكل زوج من `source` و `reason`. يزيد `count` ويحدث `last_seen`. لا تضيف صفًا.
- **محدودة.** يحتفظ التخزين بعدد أقصى من المصادر. الحد الأقصى الافتراضي هو 256.

- الإدخال الذي لديه OmniTWAG **إخلاء الأقل رؤية.** عندما يكون التخزين ممتلئًا، تزيل IP لتوفير مساحة لمصدر جديد. التخزين محدود لأن عنوان `last_seen` أقدم قيمة المصدر المزيّفة التخزين بلا IP المصدر يمكن تزييفه. لا يمكن أن تنمو فيضانات عناوين حدود.

REST واجهة برمجة التطبيقات

تقدم واجهة برمجة التطبيقات REST الخاصة بـ OmniTWAG هذه النقاط النهائية على منفذ API المكون (`8444` بشكل افتراضي). المسار الأساسي هو `/radius_rejections`.

الطريقة	المسار	الإجراء	الوصف
GET	`/radius_rejections`	index	قائمة بالمصادر المرفوضة. القائمة مقسمة إلى صفحات. البحث عن طريق `source` أو `reason`.
DELETE	`/radius_rejections/{id}`	delete	نسيان مصدر. `{id}` هو عنوان المصدر IP.

لنسيان مصدر بعد حل المشكلة، على سبيل المثال بعد إضافة بيانات اعتماد `DELETE` استخدم تغطي عنوان المصدر IP.

الاستجابات

الحالة	المعنى
`200 OK`	كانت الطلب ناجحة.
`404 Not Found`	لا يوجد إدخال له عنوان المصدر المعطى IP.

مثال: قائمة بالمصادر المرفوضة

الطلب:

```
GET /radius_rejections
```

الاستجابة:

```
{
  "count": 2,
  "radius_rejections": [
    {
      "source": "203.0.113.7",
      "reason": "unauthorized_source",
      "count": 42,
      "first_seen": 1734512400000,
      "last_seen": 1734512999000,
      "credential_id": null,
      "credential_name": null
    },
    {
      "source": "10.10.0.15",
      "reason": "bad_secret",
      "count": 3,
      "first_seen": 1734512500000,
      "last_seen": 1734512890000,
      "credential_id": "0d1e2f3a-4b5c-6d7e-8f90-1a2b3c4d5e6f",
      "credential_name": "Melbourne CBD APs"
    }
  ]
}
```

مثال: نسيان مصدر

الطلب:

```
DELETE /radius_rejections/203.0.113.7
```

الاستجابة:

```
{
  "deleted": "203.0.113.7"
}
```

المقاييس

توثق ميزة البيانات الاعتماد. يزيد كل عداد في نفس Prometheus يكمل متتبع الرفض عدادين من الوقت الذي تسجل فيه OmniTWAG رفضًا.

العداد	سبب الرفض
`radius_auth_unauthorized_source_count`	`unauthorized_source`
`radius_auth_bad_secret_count`	`bad_secret`

تقدم العدادات إجماليات على مر الزمن. يوفر المتتبع عرضًا مباشرًا لكل مصدر. انظر أسرار Prometheus وأمثلة المشتركة لتعريفات العدادات، و مرجع المقاييس لنقطة نهاية RADIUS الاستعلام.

استكشاف الأخطاء وإصلاحها

تظهر نقطة وصول غير معروفة في القائمة

الأعراض: يظهر مصدر مع تعيين `reason` إلى `unauthorized_source`. تزيد مقياس `radius_auth_unauthorized_source_count` لذلك المصدر.

الأسباب المحتملة:

- المصدر IP لا تحتوي أي شبكة فرعية للبيانات الاعتماد على عنوان.
- نقطة الوصول خلف NAT. يختلف عنوان IP المصدر الذي تراه OmniTWAG عن عنوان نقطة الوصول نفسها.

الحل:

1. اقرأ حقل `source` من الإدخال.

2. تأكد من أن هذه نقطة وصول معروفة.
3. أضف شبكة فرعية للبيانات الاعتماد تغطي عنوان IP المصدر الذي تراه OmniTWAG. استخدم العنوان المترجم، وليس عنوان نقطة الوصول. انظر NAT، فعليًا. في حالة أسرار RADIUS المشتركة.
4. احذف الإدخال باستخدام `DELETE /radius_rejections/{id}` لنسيان المصدر.

تظهر نقطة وصول معروفة كـ bad_secret

الأعراض: يظهر مصدر معروف مع تعيين `reason` إلى `bad_secret`. تزيد مقياس `radius_auth_bad_secret_count` لذلك المصدر.

الأسباب المحتملة:

- تحتوي نقطة الوصول على سر مشترك مختلف عن البيانات الاعتماد الموجودة في السجلات.

الحل:

1. اقرأ حقلي `credential_id` و `credential_name` من الإدخال. هذه تسمي البيانات الاعتماد المطابقة.
2. قارن السر في نقطة الوصول مع السر في تلك البيانات الاعتماد.
3. قم بتصحيح السر في نقطة الوصول، أو تحديث البيانات الاعتماد لتتناسب. انظر أسرار RADIUS المشتركة.
4. احذف الإدخال باستخدام `DELETE /radius_rejections/{id}` لنسيان المصدر.

القائمة فارغة بعد إعادة التشغيل

الأعراض: تكون قائمة الرفض فارغة بعد إعادة التشغيل، على الرغم من أنه تم إدراج مصادر قبل إعادة التشغيل.

السبب:

- هذا سلوك متوقع. يحتفظ المتتبع ببياناته في الذاكرة. البيانات ليست دائمة. يتم إعادة تعيين التخزين عند إعادة التشغيل.

الحل:

- لا حاجة لأي إجراء. تعيد الرفض الجديدة ملء القائمة. استخدم مقاييس `radius_auth_unauthorized_source_count` و `radius_auth_bad_secret_count` للحصول على تاريخ يبقى بعد ��عادة التشغيل.

نظرة عامة

واجهة S2a / GTP-C إلى PGW

نظرة عامة

تربط واجهة S2a بين OmniTWAG وبوابة بيانات الحزمة (PGW). تحمل اتصال PDN المعتمد على GTP لشبكة WLAN موثوقة (TWAN). تعمل OmniTWAG كنقطة نهاية GTP-C لـ TWAN. هذا الدور مشابه لـ ePDG على واجهة S2b، ولكنه يستخدم أنواع واجهة S2a ومعرف TWAN.

تحتوي واجهة S2a على مستويين:

- **GTP-C (مستوى التحكم)**: ينشئ ويعدل ويحذف جلسات PDN. كما يدير أيضًا إدارة المسار. تغطي هذه الوثيقة GTP-C.
- **GTP-U (مستوى المستخدم)**: يحمل بيانات UE في أنفاق GTP. راجع دليل مستوى المستخدم.

يتبع GTP-C على S2a 3GPP TS 29.274 (GTPv2-C). تستخدم TWAG أنواع رسائل GTPv2-C وعناصر المعلومات (IEs) مع أنواع واجهة محددة لـ S2a.

جدول المحتويات

- أوضاع الانفصال الثلاثة S2a: أين تتناسب
- الدور في دورة حياة الجلسة
- أنواع واجهة S2a
- إنشاء الجلسة
  - التحفيز
  - طلب إنشاء الجلسة
  - الناقل الافتراضي
  - استجابة إنشاء الجلسة
  - الجلسات الطارئة
- إدارة الناقل
- تدمير الجلسة
- إدارة المسار

- التكوين
- جداول المراجع
- الرصد
- استكشاف الأخطاء وإصلاحها
- 3 مراجعGPP

أوضاع الانفصال الثلاثة S2a: أين تتناسب

تحل OmniTWAG وضع مستوى البيانات لكل نقطة وصول (AP)، التي RADIUS من بيانات اعتماد على بيانات الاعتماد أحد الأوضاع الثلاثة. راجع بيانات `breakout_type` يحدد قيمة AP. تتطابق مع اعتماد RADIUS لإعدادات `breakout_type` و `address_source` و `ip_pool_id`.

الوضع (`breakout_type`)	IP من يعين للـ UE	مستوى البيانات	S2a / GTP المستخدم
`tunneled`	PGW (في عنصر تخصيص عنوان PDN)	GRE من AP إلى TWAG، ثم GTP-U على S2a إلى PGW، ثم إلى الإنترنت بواسطة PGW	نعم. هذه الوثيقة.
`nswo`	TWAG، من مجموعة IP	GRE من AP إلى TWAG، ثم انفصال محلي إلى الإنترنت (NAT) في TWAG	لا. لا توجد جلسة PGW.
`local`	الشبكة المحلية في AP	مستوى البيانات. AP يمتلك أي حركة TWAG لا يحمل مرور.	لا. لا توجد جلسة PGW، لا IP.

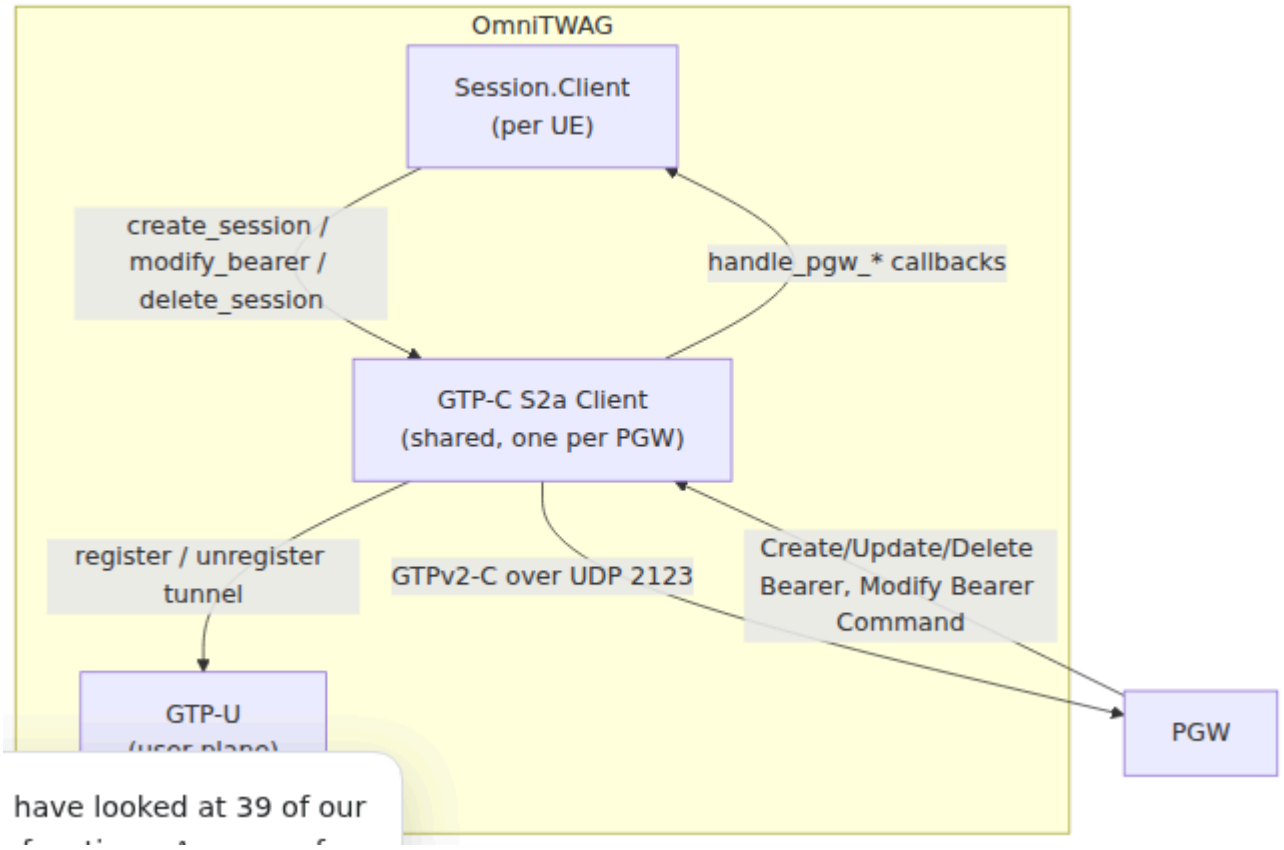
بتخصيص PGW يقوم، `tunneled` في وضع . `tunneled` فقط في وضع S2a على GTP-C ينطبق بإنشاء TWAG لا يقوم، `local` و `nswo` ويطبق السياسة والرسوم. في أوضاع UE للـ IP عنوان جلسة PDN، لذا لا يتم إرسال أي رسالة S2a.

تنطبق الشحنات عبر Gy. وليس TWAG، بواسطة PGW `tunneled` تتم عملية الشحن في وضع على جانب TWAG على الأوضاع المنفصلة محليًا في الشحن عبر الإن��رنت.

> ملاحظة: يوفر معالج عالمي منفصل لـ Non-Seamless WLAN Offload (NSWO) (`Twag.NSWO.Handler`، مفعل بـ `nswo.enabled: true`) انفصالًا محليًا لكل جلسة. راجع قسم الانفصال المحلي في دليل مستوى المستخدم. نوع GTP. عندما لا يتم استخدام الانفصال `nswo` لكل AP ويفضل بيانات الاعتماد مدفوع بنموذج الموصوف أعلاه هو نموذج.

الدور في دورة حياة الجلسة

يتعامل مع جميع الجلسات ضد (`Twag.Gtp.GtpcS2a`) هو عملية واحدة مشتركة GTP-C عميل مصدقة تدفع تبادل إنشاء جلسة واحد. تستدعي `tunneled` واحد UE مُكون. كل جلسة PGW عملية `Session.Client` لكل جلسة عميل GTP-C. لا ترسل رسائل GTPv2-C بنفسها.



أنواع واجهة S2a

يستخدم TWAG أنواع واجهة S2a F-TEID. هذه تختلف عن S2b (ePDG)، التي تستخدم الأنواع 30 و 31. القيم تتبع الجدول 8.22-1 TS 29.274.

نوع الواجهة	القيمة	الاتجاه	الاستخدام
`s2a_twan_gtp_c`	35	تحكم TWAG	في طلب إنشاء TWAG F-TEID الجلسة
`s2a_twan_gtp_u`	34	مستخدم TWAG	TWAG bearer F-TEID (GTP-U)
`s2a_pgw_gtp_c`	36	تحكم PGW	في استجابة إنشاء PGW F-TEID الجلسة
`s2a_pgw_gtp_u`	37	مستخدم PGW	PGW bearer F-TEID (GTP-U)

نوع RAT هو دائمًا WLAN (القيمة 3).

إنشاء الجلسة

التحفيز

بدء المحاسبة، مما يحفز معالجة ما بعد القبول. AP الجلسة. ترسل EAP تبدأ المصادقة الناجحة عبر يقوم `Session.Client` بحل وضع انفصال AP. لوضع `tunneled`، يستدعي عميل GTP-C لإنشاء جلسة PDN. إذا كانت قيمة المعلمة `gtp.enabled` هي `false`، يتخط TWAG S2a.. في أوضاع TWAG لا يقوم بإنشاء الجلسة. إذا كانت الجلسة لا تحتوي على IMSI، `local` و `nswo`، لا يرسل TWAG أي رسالة S2a. لدورة حياة الجلسة الكاملة راجع الجلسات.

طلب إنشاء الجلسة

يرسل TWAG طلب إنشاء جلسة (حسب نوع الرسالة TS 29.274 §7.2.1) إلى PGW. يقوم بإنشاء TWAG لمستوى التحكم و TEID جديد غير قابل للتنبؤ TEID لمستوى المستخدم للطلب. يبني الطلب مع هذه IEs:

عنصر المعلومات	المصدر / القيمة	الملاحظات
IMSI	اشتراك UE	يتم حذفه إذا لم يكن موجودًا.
الشبكة الخادمة (MCC/MNC)	`gtp.mcc` / `gtp.mnc`، أو الأرقام الأولى من IMSI	يتم حذفه إذا كانت أي من القيم مفقودة.
نوع RAT	WLAN (3)	ثابت لـ S2a.
F-TEID (التحكم)	35 نوع الواجهة، TEID تحكم TWAG، IP محلي لـ TWAG	يحدد نقطة نهاية GTP-C لـ TWAG.
اسم نقطة الوصول (APN)	`gtp.apn`، الافتراضي `internet`. APN الطارئ إذا تم الطلب.	راجع الجلسات لطارئة��.
وضع الاختيار	2 (مقدم من الشبكة، الاشتراك غير مؤكد)	APN دائمًا مقدم من الشبكة في TWAN.
تخصيص عنوان PDN (PAA)	النوع المطلوب مع عنوان صفر	TWAG يطلب عنوانًا. يقوم PGW بتخصيصه.
الحد الأقصى لمعدل البت الإجمالي (APN-AMBR)	256000 الافتراضي uplink / 256000 downlink	يتم تجاوزها إذا تم تقديم معدل.
سياق الناقل لإنشائه	EBI 5 الافتراضي، F-TEID الناقل (34 النوع)، QoS	راجع الناقل الافتراضي.
قيود APN	2 (عادي)، أو 0 للطوارئ	
هوية ME (IMEISV)	هوية معدات UE	يتم حذفه إذا لم يكن موجودًا.
الاسترداد	عداد استرداد TWAG	يستخدم لاكتشاف إعادة التشغيل.

عنصر المعلومات	المصدر / القيمة	الملاحظات
خصائص الشحن	`0x0800`	قيمة ثابتة.
معرف TWAN	SSID من `twan_ssid`، BSSID اختياري من `twan_bssid`	يحدد WLAN.
المنطقة الزمنية للـ UE	مستمدة من تعويض الوقت المحلي للمضيف	
الإشارة	علامة النقل	يتم تعيين علامة النقل للنقل الداخل.

من خلال معلمة `:ipv4v6` أو `:ipv6`، `:ipv4` يمكن تعيينه إلى IPv4. يكون نوع PDN افتراضيًا IPv4. يكون عنوان PAA المطلوب دائمًا صفرًا، لذا يقوم PGW بتخصيص العنوان `gtp.pdn_type`. الحقيقي.

> ملاحظة: لا يتم تضمين IE خيارات تكوين البروتوكول الإضافية (APCO). لا يطلب TWAG أو PCO من DNS في الوقت الحالي. يقوم بقراءة APCO من خلال P-CSCF أو DNS عناوين PGW الإضافية في الاستجابة إذا قدم IE PCO واحدًا.

الناقل الافتراضي

ينشئ TWAG ناقلًا افتراضيًا واحدًا لكل جلسة EBI. لا يحتوي الناقل على 5. الافتراضي هو QoS لذا يحمل كل الحركة. تستخدم TFT، مرشحات الثابتة:

معلمة QoS	القيمة
QCI	9
مستوى الأولوية	10
قدرة الاستبقاء	معطلة
قابلية الاستبقاء	مفعلة
GBR / MBR (uplink و downlink)	0

لا يدعم TWAG إدارة الناقل راجع الناقلات المخصصة.

استجابة إنشاء الجلسة

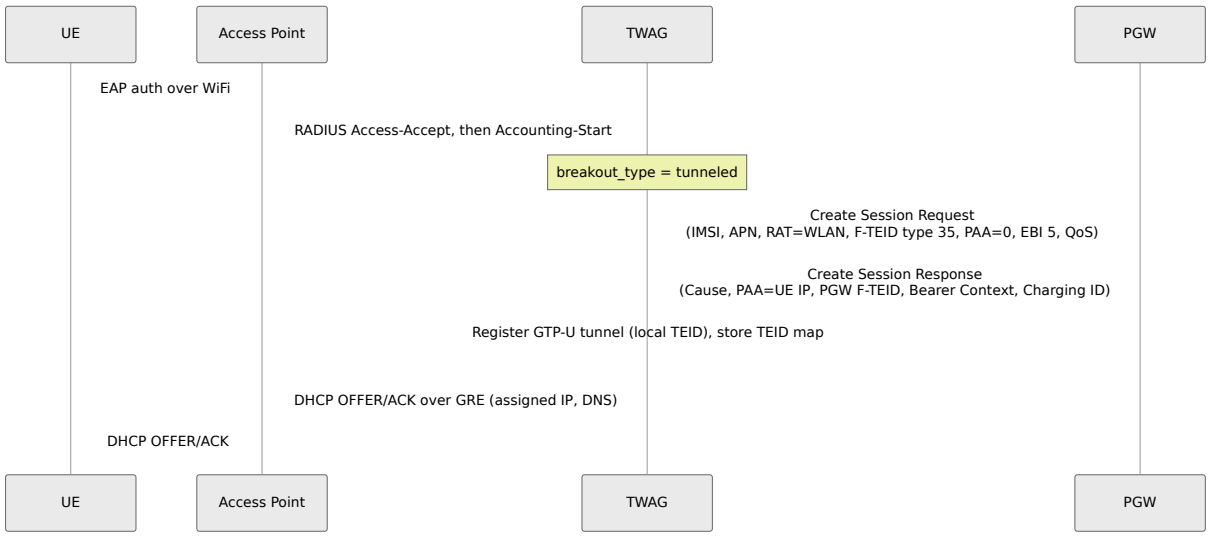
يتم مطابقة الاستجابة مع الطلب المعلق حسب رقم التسلسل. يتحقق TWAG من عنصر السبب. الطلب يكون ناجحًا إذا كان السبب هو `request_accepted`، `new_pdp_type_due_to_network_preference`، أو `new_pdp_type_due_to_single_address_bearer_only`. أي سبب آخر يعيد `gtpc_error` مع قيمة السبب تلك.

عند النجاح، يقرأ TWAG هذه القيم من الاستجابة:

عنصر الاستجابة	القيمة المستخرجة	الاستخدام
تخصيص عنوان PDN (PAA)	عنوان IP المخصص للـ UE	يتم تسليمه إلى الـ UE عبر DHCP عبر GRE. راجع إدارة عنوان IP.
F-TEID (تحكم PGW)	TEID تحكم PGW وIP PGW	يستخدم كوجهة للرسائل التحكم اللاحقة.
سياق الناقل	F-TEID الناقل (TEID وIP GTP-U PGW)، EBI، معرف الشحن	يستخدم لتسجيل نفق GTP-U.
APN-AMBR	حدود معدلات الجلسة	مخزنة على الجلسة.
PCO / PCO الإضافية	عناوين خادم DNS	يتم تسليمها إلى الـ UE عبر DHCP.

يخزن TWAG خريطة من TEID التحكم المحلي الخاص به إلى TEID التحكم PGW وهويات UE. لاحقًا إلى الجلسة الصحيحة. إذا لم يكن هناك PGW تقوم هذه الخريطة بتوجيه الرسائل التي يبدأها للناقل، يعود F-TEID PGW المستخدم إلى TWAG لنفق مستوى المستخدم.

بعد النجاح، يقوم `Session.Client` بتسجيل نفق GTP-U (مستوى المستخدم TEID الذي يولد المخصصين، ويسجل الـ DNSو IP مع DHCP ويخصص عقدة، (TWAG المحلي على جانب UE لتوجيه الـ GRE للنفق ومسار الاتجاه الهابط. راجع مستوى المستخدم في الاتجاه الهابط.



الجلسات ��لطارئة

إذا طلبت الجلسة خدمة طارئة، يستخدم TWAG APN الطوارئ. تحدد معلمة `emergency_apn` هذا APN. القيمة الافتراضية هي `sos`. لجلسة طارئة، يتم تعيين قيود APN (لا قيود) إلى 0.

إدارة الناقل

الناقل الافتراضي فقط

يدعم OmniTWAG وضع الناقل الافتراضي فقط. لا يدعم الناقلات المخصصة. يتبع هذا ملف تعريف الاتصال الفردي الشفاف لـ TWAN (TSCM). يمكن لمدير الناقل تتبع جدول الناقلات المعتمد على EBI، ولكن S2a ينشئ فقط الناقل الافتراضي.

تعديل الناقل (من TWAG initiated)

إرسال طلب تعديل الناقل TWAG (TS 29.274 §7.2.7). يحمل هذا الطلب سياق ناقل TWAG مستوى المستخدم لـ F-TEID الافتراضي، و EBI (النوع 34)، وIP لـ TWAG المحلي. يقوم TWAG بمطابقة استجابة تعديل الناقل حسب رقم TEID التحكم PGW الوجهة هو TEID التسلسل ويتحقق من عنصر السبب للنجاح. يعيد النقل الداخل استخدام مسار إنشاء الجلسة مع تعيين علامة النقل، وليس تعديل ��اقل منفصل.

الإجراءات المinitiated من PGW

إجراءات الناقل TWAG على مقبس GTP-C الخاص به. TEID يمكن أن يبدأ PGW هذه. يستخدم TWAG خريطة TEID المخزنة في الرسالة هو TEID الوجهة لـ TWAG المحلي. ثم يقوم بإخطار عملية UE وهويات PGW التحكم TEID للعثور على `Session.Client` المطابقة.

رسالة PGW	استجابة TWAG	السلوك
طلب إنشاء الناقل	استجابة إنشاء الناقل، السبب `request_rejected`	جميع الناقلات المخصصة TWAG يرفض (TSCM). لا يتم إنشاء ناقل.
أمر تعديل الناقل	طلب تعديل الناقل مرة أخرى إلى PGW	TWAG يعترف بالمعلمات الجديدة (APN-AMBR، F-TEID). إذا فشل الإرسال، يرسل إشارة فشل تعديل الناقل مع السبب `system_failure`.
طلب تحديث الناقل	استجابة تحديث الناقل، السبب `request_accepted` لكل ناقل	يقبل TWAG تحديث QoS ويخطر الجلسة.
طلب حذف الناقل	استجابة حذف الناقل، السبب `request_accepted`	راجع تدمير الجلسة.

بالنسبة لأمر تعديل الناقل، يقرأ TWAG APN-AMBR وسياق الناقل (EBI، F-TEID الجديد، QoS). للاعتراف. إذا كان سياق الناقل يحمل PGW يخطر عملية الجلسة، ثم يرسل طلب تعديل ناقل إلى F-TEID GTP-U بالقيم البعيدة الجديدة. بالنسبة لطلب GTP-U جديد، تعيد الجلسة تسجيل نفق ويخطر الجلسة، ثم يقبل (EBI، QoS)، وكل سياق ناقل TWAG APN-AMBR تحديث الناقل، يقرأ كل ناقل في الاستجابة.

تدمير الجلسة

حذف الجلسة (initiated من TWAG)

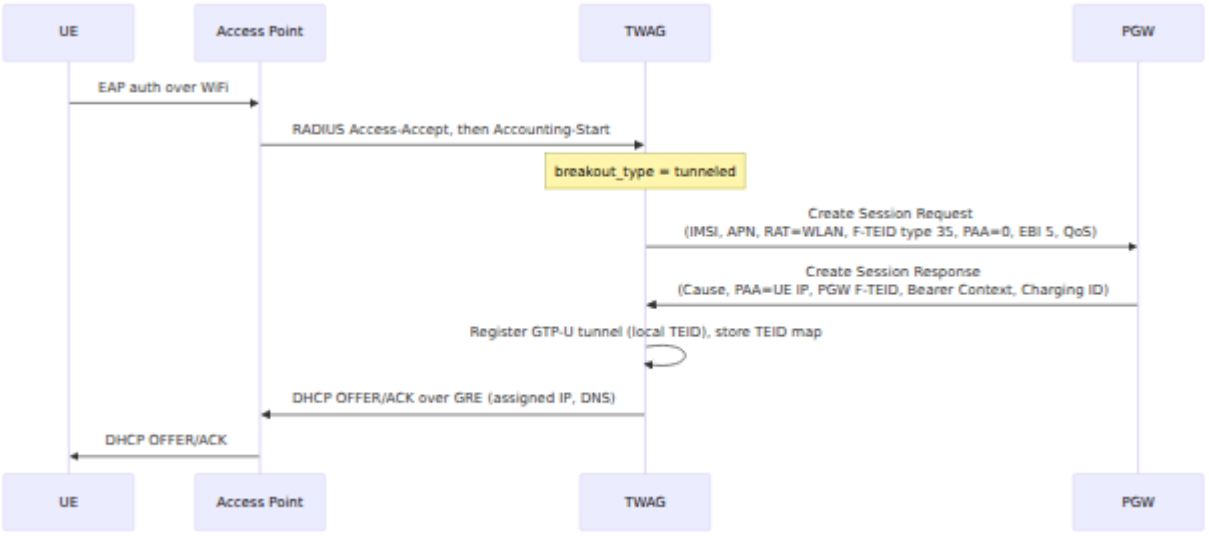
يحذف TWAG جلسة PDN عندما ينفصل UE. تستدعي عملية `Session.Client` تدمير GTP-C. يرسل TWAG طلب حذف الجلسة (TS 29.274 §7.2.9) إلى TEID التحكم PGW. يحمل الطلب:

- معرف الناقل EPS (EBI 5 الافتراضي، الافتراضي)
- السبب (الافتراضي `local_detach`)

بمطابقة استجابة حذف الجلسة حسب رقم التسلسل ويتحقق من عنصر السبب. ثم TWAG يقوم بإلغاء تسجيل نفق GTP-U، وإفراج عقدة DHCP وأي عنوان من IP، وإلغاء تسجيل UE من GRE، وتنظيف الجلسة. إذا كانت الجلسة لا تحتوي على TEID التحكم PGW. TEID لذلك TEID يزيل إدخالات خريطة TEID التحكم PGW (على سبيل المثال، جلسة `local` أو `nswo`)، يتخطى TWAG حذف GTP-C. بعد الحذف، يقوم `Session.Client`

حذف الناقل (initiated من PGW)

يمكن أن يبدأ PGW التدمير مع طلب حذف الناقل. يقرأ TWAG EBI المرتبط، وقائمة EBI المطابقة، التي تقوم بتنظيف محلي فقط. لا يرسل `Session.Client` والسبب. يخطر عملية TWAG قد حذف الناقل بالفعل. ثم يرسل PGW طلب حذف الجلسة في هذه الحالة، لأن TWAG المرتبط هو الناقل EBI إذا كان `request_accepted` استجابة حذف الناقل مع السبب الافتراضي، يتم تدمير الاتصال الكامل لـ PDN.



إدارة المسار

صدى

يدير TWAG إدارة مسار GTPv2-C مع طلب صدى واستجابة صدى (TS 29.274 §6). تقوم معلمة PGW طلب صدى إلى TWAG بتفعيل ذلك. تكون مفعلة بشكل افتراضي. يرسل `echo_enabled` كل 60 ثانية. يحمل كل طلب صدى رقم تسلسل. تحمل كل استجابة صدى عداد استرداد TWAG.

عندما يرسل PGW طلب صدى، يرد TWAG باستجابة صدى تحمل عداد استرداد TWAG.

حالة المسار

يتتبع TWAG حالة المسار إلى PGW. تشير استجابة صدى الناجحة إلى أن المسار UP وتعيد تعيين عدد الفشل. تزيد حالات الفشل المتتالية في الصدى عدادًا. بعد 3 حالات فشل متتالية، يشير TWAG إلى أن المسار DOWN.

اكتشاف إعادة تشغيل PGW

يخزن TWAG عداد استرداد PGW من كل استجابة صدى. إذا تغير العداد، يكتشف TWAG إعادة تشغيل PGW. يخطر كل عم��ية جلسة بسبب ثم يقوم بتنظيف جميع الجلسات المتأثرة. `pgw_restart` Clears خريطة TEID.

مهلة الطلب وإعادة الإرسال

يستخدم TWAG مؤقت T3-RESPONSE وN3-REQUESTS لإعادة المحاولات لطلبات التحكم.

المؤقت / العداد	القيمة	المعنى
T3-RESPONSE	3000 مللي ثانية	الوقت للانتظار لاستجابة قبل إعادة الإرسال.
N3-REQUESTS	3	الحد الأقصى لإعادة الإرسال قبل فشل الطلب.

إذا انتهت مهلة الطلب، يعيد TWAG إرسال نفس الرسالة بنفس رقم التسلسل. يعيد بدء المؤقت. بعد 3 محاولات بدون استجابة، يفشل TWAG إنشاء الجلسة. تعيد فشل `timeout` إلى الطلب. يفشل المتصل. تتبع إعادة إرسال الصدى نفس حدود المؤقت وإعادة المحاولة. يعد فشل الصدى جزءًا من عتبة المسار DOWN.

عند بدء التشغيل، يفتح TWAG مقبس GTP-C UDP. إذا لم يتمكن المقبس من الفتح، يعيد المحاولة كل 5 ثوانٍ.

التكوين

في `omnitwag` هذه الخريطة هي جزء من تكوين تطبيق `gtp`. تحت خريطة S2a يتم تكوين `runtime.exs`.

```
config :omnitwag,
  gtp: %{
    # تمكين واجهة S2a (مطلوبة للانفصال الم tunneled)
    enabled: true,

    # نقطة نهاية GTP-C لـ PGW
    pgw_ip: "10.5.198.1",
    pgw_port: 2123,

    # IP المحلي لـ TWAG لـ GTP-C و GTP-U F-TEIDs
    local_ip: "10.5.198.200",

    # منفذ مستوى المستخدم GTP-U
    gtpu_port: 2152,

    # إدارة المسار (صدى)
    echo_enabled: true,

    # الافتراضات لطلب إنشاء الجلسة
    apn: "internet",
    pdn_type: :ipv4
  }
```

معلمات GTP

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`false`	تمكين واجهة S2a. تعيين `true` إلى للانفصال الم tunneled. عندما تكون `false`، لا يبدأ TWAG ويتخطى عميل GTP-C لكل جلسة S2a.
`pgw_ip`	String	نعم (إذا تم تمكينه)	`127.0.0.1`	عنوان IP لـ GTP-C PGW. يرسل TWAG جميع رسائل GTPv2-C إلى هذا العنوان.
`pgw_port`	Integer	لا	`2123`	منفذ GTP-C UDP لـ PGW. المنفذ القياسي لـ GTP-C هو 2123.
`local_ip`	String	لا	يتم اكتشافه تلقائيًا	IP المحلي لـ TWAG. يستخدم في F-TEIDs وكعنوان مصدر لـ GTP-C و GTP-U. إذا لم يتم تعيينه، يكتشف TWAG IP الصادر تلقائيًا.
`gtpu_port`	Integer	لا	`2152`	منفذ GTP-U UDP لمستوى المستخدم. راجع مستوى المستخدم.
`echo_enabled`	Boolean	لا	`true`	تمكين إدارة مسار GTPv2-C Echo إلى PGW.
`apn`	String	لا	`internet`	اسم نقطة الوصول لجلسة PDN.

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`pdn_type`	Atom	لا	`:ipv4`	نوع PDN: `:ipv4`، `:ipv6`، أو `:ipv4v6`.
`mcc`	String	لا	أول 3 أرقام IMSI	رمز الدولة المحمول لعنصر الشبكة الخادمة.
`mnc`	String	لا	أرقام IMSI 4-5	رمز الشبكة المحمول لعنصر الشبكة الخادمة.

معلمات الطوارئ و TWAN

تُقرأ المعلمات التالية من بيئة تطبيق `omnitwag`، وليس من خريطة `gtp`.

المعلمة	النوع	الافتراضي	الوصف
`emergency_apn`	String	`sos`	APN المستخدم لجلسة طارئة. يتم تعيين قيود APN الجلسات إلى 0 له��ه.
`twan_ssid`	String	`TWAG`	SSID الموضوع في عنصر معرف TWAN.
`twan_bssid`	Binary	(غير محدد)	BSSID اختياري مكون من 6 بايت لعنصر معرف TWAN. يتم حذفه إذا لم يكن قيمة صحيحة مكونة من 6 بايت.

> ملاحظة: يتصل عميل GTP-C بـ PGW واحد. لا يوجد اختيار لكل APN أو متعدد في PGW. لتغيير PGW، قم بتحديث `pgw_ip` الوقت الحالي.

جداول المراجع

أنواع رسائل GTPv2-C (S2a)

الرسالة	الاتجاه	الغرض
طلب صدى / استجابة	كلاهما	إدارة المسار.
طلب إنشاء الجلسة / استجابة	TWAG إلى PGW	إنشاء جلسة PDN.
طلب تعديل الناقل / استجابة	TWAG إلى PGW	تحديث F-TEID للناقل أو QoS.
طلب حذف الجلسة / استجابة	TWAG إلى PGW	تدمير جلسة PDN.
طلب إنشاء الناقل / استجابة	PGW إلى TWAG	ناقل مخصص. مرفوض من قبل TWAG.
طلب تحديث الناقل / استجابة	PGW إلى TWAG	تحديث QoS. مقبول من قبل TWAG.
أمر تعديل الناقل	PGW إلى TWAG	يطلب PGW من TWAG تحديث معلمات الناقل.
إشارة فشل تعديل الناقل	TWAG إلى PGW	ترسل عندما لا يمكن تلبية أمر تعديل الناقل.
طلب حذف الناقل / استجابة	PGW إلى TWAG	تدمير مinitiated من PGW.

رموز سبب GTPv2-C

يستخدم TWAG هذه القيم السبب. تتبع الرموز TS 29.274 §8.4.

الرمز	الاسم	المعنى
2	فصل محلي	السبب الافتراضي لحذف جلسة م من initiated TWAG.
13	فشل الشبكة	فشل الشبكة المبلغ عنه من قبل النظير.
16	الطلب مقبول	نجاح.
64	السياق غير موجود	لا يوجد لدى النظير سياق مطابق.
72	فشل النظام	يستخدم في إشارة فشل تعديل الناقل.
92	فشل مصادقة المستخدم	تم رفض المصادقة.
93	الوصول إلى APN مرفوض	APN غير مسموح به.
94	الطلب مرفوض	طلب إنشاء الناقل TWAG يستخدم عندما يرفض.
96	IMSI/IMEI غير معروف	المشترك غير معروف.

الرصد

أحداث القياس للنشاط ��لناقل وتدمير الجلسة. تدفع هذه الأحداث المقاييس في TWAG ينشر مرجع المقاييس.

الحدث	متى
`[:twag, :bearer, :modify_command]`	يتلقى TWAG أمر تعديل الناقل من PGW.
`[:twag, :bearer, :update]`	يتلقى TWAG طلب تحديث الناقل من PGW.
`[:twag, :detach, :pgw_delete]`	يتلقى TWAG طلب حذف الناقل من PGW.
`[:twag, :session, :teardown]`	يتم تدمير الجلسة.
`[:twag, :detach, :cleanup_start]`	يبدأ تدمير الجلسة.
`[:twag, :detach, :cleanup_complete]`	يكتمل تدمير الجلسة.

حالة العميل

يقدم عميل GTP-C لقطة حالة. تظهر هذه الحالة صحة مسار S2a.

الحقل	المعنى
`connected`	مقبس GTP-C UDP مفتوح.
`pgw_ip` / `pgw_port`	نقطة نهاية PGW المكونة.
`pending_requests`	عدد طلبات GTP-C قيد الطيران.
`path_up`	حالة مسار الصدى إلى PGW.
`echo_failures`	عدد حالات فشل الصدى المتتالية.
`recovery_counter`	عداد استرداد TWAG.

السجل

يسجل عميل GTP-C كل إجراء. تشمل خطوط السجل الرئيسية:

- إنشاء الجلسة، حذف الجلسة، وإرسال تعديل الناقل والاستجابات.
- تغييرات حالة المسار: `Path to PGW ... is UP` و `Path to PGW ... is DOWN`.
- اكتشاف إعادة تشغيل PGW مع العدادات القديمة والجديدة.
- رسائل إنشاء وتحديث وتعديل وحذف الناقل الم initiated من PGW.

استكشاف الأخطاء وإصلاحها

فشل إنشاء الجلسة

الأعراض: لا يتم إنشاء الجلسات. يظهر السجل `GTP Create Session failed`.

الأسباب المحتملة:

- يرفض PGW الطلب بسبب سبب غير نجاح.
- المسار إلى PGW معطل.
- APN غير مُعد على PGW.
- IMSI غير معروف للنواة.

الحل:

1. تحقق من رمز السبب المعاد مقابل جدول رموز السبب.
2. تحقق من حالة المسار مع حالة العميل (`path_up`).
3. تأكد من أن APN مُعد على PGW.
4. تأكد من أن المشترك مُعد في HSS.

معطل PGW المسار إلى

الأعراض: يظهر السجل `Path to PGW ... is DOWN`. تفشل الجلسات الجديدة.

الأسباب المحتملة:

- PGW غير قابل للوصول عل UDP 2123.
- جدار ناري يحظر GTP-C.
- PGW غير قيد التشغيل.

الحل:

1. تأكد من أن قيم `pgw_ip` و `pgw_port` صحيحة.
2. تأكد من أن مسار الشبكة يسمح بـ UDP 2123 في كلا الاتجاهين.
3. تأكد من أن خدمة GTP-C لـ PGW قيد التشغيل.
4. انتظر حتى يتم إرسال الصدى التالي. تشير استجابة صدى ناجحة إلى أن المسار UP.

الجلسات تتقطع بعد إعادة تشغيل PGW

الأعراض: يتم تدمير جميع الجلسات معًا. يظهر السجل `PGW restart detected`.

الأسباب المحتملة:

- أعاد PGW التشغيل وغير عداد الاسترداد الخاص به.

الحل:

1. هذا سلوك متوقع. يقوم TWAG بتنظيف الجلسات القديمة بعد إعادة تشغيل PGW.
2. تأكد من أن PGW مستقر. يعيد UE المصادقة وإعادة إنشاء الجلسات.

الجلسات تتأسس ولكن لا توجد تدفقات بيانات

الأعراض: يحصل UE على عنوان IP، لكن الحركة لا تمر.

الأسباب المحتملة:

- نفق GTP-U أو مسار GRE غير متاح.

الحل:

1. تأكد من أن `gtp.enabled` و `gre.enabled` كلاهما `true` للانفصال الم tunneled.
2. تحقق من إحصائيات GTP-U وGRE في دليل مستوى المستخدم.

مراجع 3GPP

العنوان	المواصفة
بروتوكول نفق GPRS المتطور لمستوى التحكم (GTPv2-C).	TS 29.274
تحسينات المعمارية للوصولات غير 3GPP (TWAN، S2a).	TS 23.402
الوصول إلى EPC 3 عبر الشبكات غير 3GPP.	TS 24.302

نظرة عامة

الجلسات

نظرة عامة

تمثل OmniTWAG. يقوم OmniTWAG بتحديد الجلسة **الجلسة** مشتركًا مصادقًا واحدًا على حسب هوية المشترك (IMSI أو اسم المستخدم). يحتفظ OmniTWAG بالجلسات في الذاكرة. يوفر واجهة برمجة التطبيقات للجلسات حالة الجلسة الحية.

تحمل واجهة الجلسات أيضًا حركة مرور المشترك. يدمج OmniTWAG سجل محاسبة RADIUS في الجلسة بواسطة `Acct-Session-Id`. وبالتالي، تعتبر الجلسة المصدر الوحيد لكل من حالة المشترك وحركة مرور المشترك. لا يوجد نقطة محاسبة منفصلة. المحاسبة جزء من الجلسة.

جدول المحتويات

- المفاهيم
- دورة حياة حالة المصادقة
- نموذج الجلسة
- مرجع حالة المصادقة
- واجهة برمجة التطبيقات REST
- إجراءات لكل جلسة
- أمثلة JSON
- واجهة الويب
- استكشاف الأخطاء وإصلاحها

المفاهيم

يمتلك كل مشترك مصادق جلسة واحدة. يقوم OmniTWAG بإنشاء الجلسة عندما يبدأ طلب وصول RADIUS مصادقة EAP. يقوم OmniTWAG بتحديث الجلسة مع تقدم المصادقة وعندما يتم إنشاء مسار البيانات.

تتبع الجلسة هوية المشترك، وعنوان MAC للعميل، وعنوان IP المخصص لـ UE، ونقطة الوصول، وعنوان DNS. عندما تصل محاسبة RADIUS للمشترك، يدمج GTP والمرحلة، وحالة EAP وطريقة عدادات الحركة في الجلسة OmniTWAG.

شكل الجلسة مفتوح النهاية. المفاتيح الموجودة تعتمد على طريقة المصادقة ومدى تقدم الجلسة. تحتوي الجلسة التي بدأت فقط على مفاتيح أقل من الجلسة التي وصلت إلى قبول EAP RADIUS وأنشأت مسار بيانات GTP وDHCP.

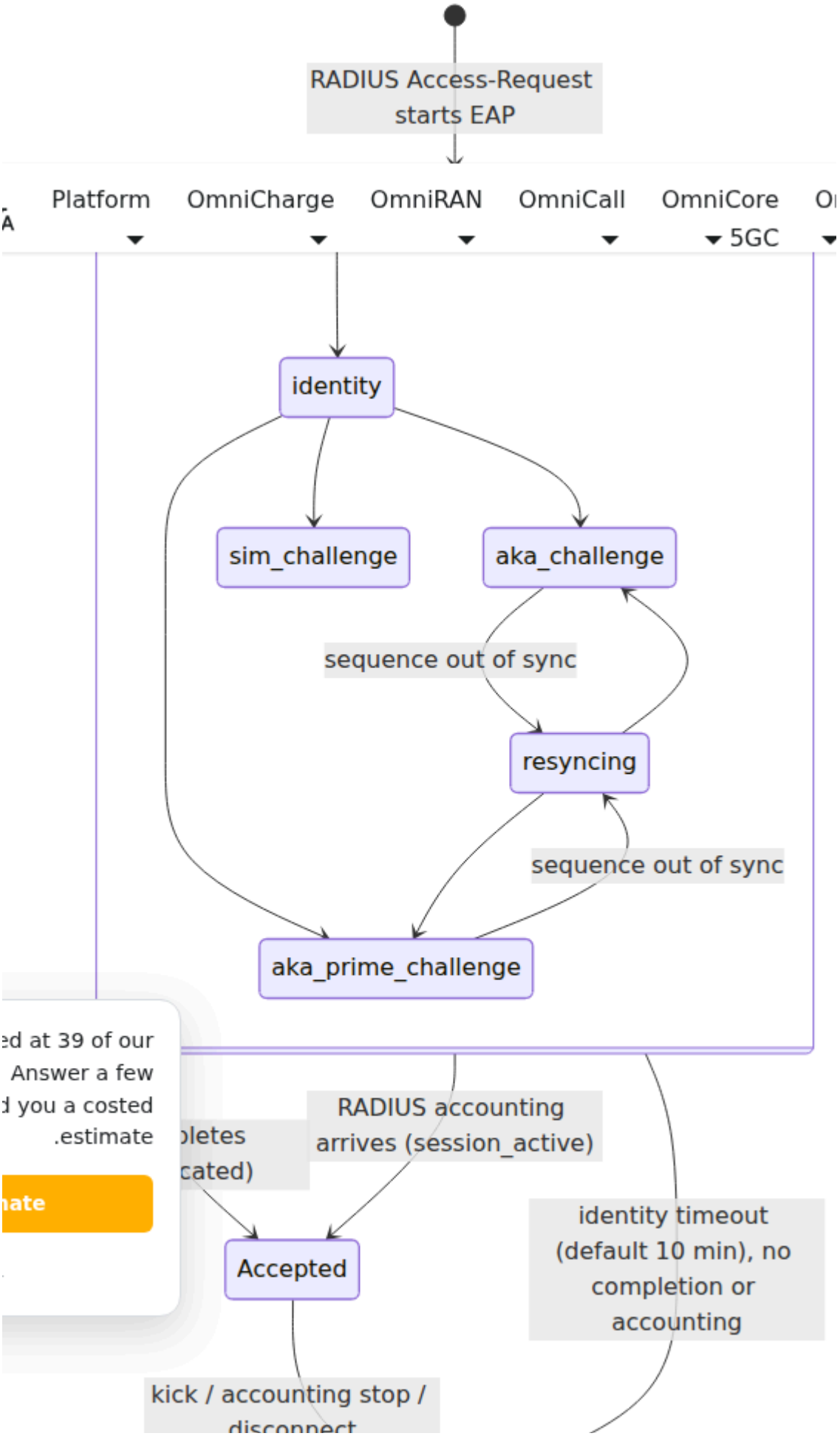
دورة حياة حالة المصادقة

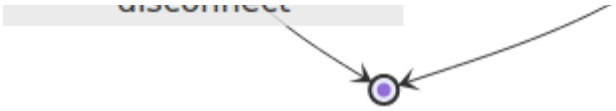
تمتلك الجلسة حالة مصادقة. يتم اشتقاق الحالة من مرحلة EAP للجلسة (`eap_phase`).

- بينما تكون الجلسة **تحت المصادقة** `eap_phase` هي مرحلة مصادقة قيد التقدم. المراحل قيد التقدم هي `identity`، `aka_challenge`، `aka_prime_challenge`، `sim_challenge`، و`resyncing`.
- تكون الجلسة **مقبولة** بمجرد أن يتم المصادقة عليها، أو بمجرد أن تكون نشطة (`session_active`).

تتم ترقية الجلسة التي تتلقى محاسبة RADIUS إلى حالة نشطة. تتدفق المحاسبة فقط لمشترك تم المصادقة عليه بالفعل. وبالتالي، فإن وصول المحاسبة هو دليل على أن المشترك نشط، لذا يقوم OmniTWAG بوضع علامة على الجلسة كمقبولة.

تتم إزالة الجلسة التي تبقى في مرحلة مصادقة قيد التقدم. إذا بدأت الجلسة المصادقة، ولم تكتمل أبدًا، ولم تتلقَ محاسبة، يقوم OmniTWAG بإزالة الجلسة بعد انتهاء المهلة. هذا يمنع محاولة المصادقة غير المكتملة من الاستمرار كـ تحت المصادقة إلى الأبد. المهلة الافتراضية هي 10 دقائق.


RADIUS Access-Request starts EAP
Platform
OmniCharge
OmniRAN
OmniCall
OmniCore 5GC
identity
sim_challenge
aka_challenge
sequence out of sync
resyncing
sequence out of sync
aka_prime_challenge
RADIUS accounting arrives (session_active)
Accepted
identity timeout (default 10 min), no completion or accounting
kick / accounting stop / disconnect



نموذج الجلسة

تمتلك الجلسة الحقول أدناه. الشكل مفتوح النهاية، لذا قد تحمل الجلسة أيضًا مفاتيح GTP أو محاسبة أخرى. يتم عرض كل حقل أدناه كسلسلة قابلة للطباعة، أو عدد صحيح، أو قائمة. يتم عرض القيم الثنائية كسلاسل قابلة للطباعة أو كقيم سداسية. يتم عرض مجموعات IP كسلاسل نقطية.

الحقل	النوع	الوصف
`identity`	سلسلة	هوية الجلسة. هذه هي IMSI أو اسم المستخدم. يقوم OmniTWAG بتحديد الجلسة بواسطة هذه القيمة.
`imsi`	سلسلة	IMSI المشترك.
`mac_address`	سلسلة	عنوان MAC للـ UE.
`ue_ip`	سلسلة	عنوان IP المخصص للـ UE، كسلسلة نقطية.
`nas_ip`	سلسلة	عنوان IP المصدر لنقطة الوصول (RADIUS `NAS-IP-Address`).
`called_station_id`	سلسلة	معرف نقطة الوصول (RADIUS `Called-Station-Id`).
`calling_station_id`	سلسلة	عنوان MAC للعميل (RADIUS `Calling-Station-Id`).
`acct_session_id`	سلسلة	معرف جلسة محاسبة RADIUS. يدمج OmniTWAG سجل المحاسبة بواسطة هذه المفتاح.
`eap_phase`	سلسلة	المرحلة الحالية لـ EAP. هذه القيمة تحدد حالة المصادقة. انظر مرجع حالة المصادقة.
`eap_type`	سلسلة	طريقة EAP المستخدمة، على سبيل المثال `aka` أو `aka_prime`.
`pgw_ip`	سلسلة	عنوان IP ـ PGW، كسلسلة نقطية.
`bearer_id`	عدد صحيح	معرف حاملة EPS.
`dns_servers`	قائمة من السلاسل	خوادم DNS المخصصة للـ UE.

الحقل	النوع	الوصف
`created_at`	عدد صحيح	وقت إنشاء الجلسة، بالمللي ثانية منذ بداية نظام Unix.
`last_activity`	عدد صحيح	وقت آخر نشاط، بالمللي ثانية منذ بداية نظام Unix.
`established_at`	عدد صحيح	وقت إنشاء الجلسة، بالمللي ثانية منذ بداية نظام Unix.
`acct_input_octets`	عدد صحيح	بايتات مستلمة من الـ UE. مدمجة من محاسبة RADIUS.
`acct_output_octets`	عدد صحيح	بايتات مرسلة إلى الـ UE. مدمجة من محاسبة RADIUS.
`acct_input_packets`	عدد صحيح	حزم مستلمة من الـ UE. مدمجة من محاسبة RADIUS.
`acct_output_packets`	عدد صحيح	حزم مرسلة إلى الـ UE. مدمجة من محاسبة RADIUS.
`acct_session_time`	عدد صحيح	مدة جلسة المحاسبة، بالثواني. مدمجة من محاسبة RADIUS.
`acct_status_type`	عدد صحيح	أحدث حالة محاسبة. `1` هو البداية، `2` هو الإيقاف، `3` هو مؤقت.
`acct_last_update`	عدد صحيح	وقت آخر تحديث للمحاسبة، بالمللي ثانية منذ بداية نظام Unix.

تكون حقول `acct_*` موجودة فقط بعد دمج سجل محاسبة المشترك في الجلسة.

مرجع حالة المصادقة

يقوم OmniTWAG بربط قيمة `eap_phase` بحالة معروضة. الجدول أدناه يسرد الربط.

`eap_phase`	الحالة المعروضة	حالة المصادقة
`identity`	الهوية	تحت المصادقة
`aka_challenge`	تحدي AKA	تحت المصادقة
`aka_prime_challenge`	تحدي AKA'	تحت المصادقة
`sim_challenge`	تحدي SIM	تحت المصادقة
`resyncing`	إعادة المزامنة	تحت المصادقة
`authenticated`	مقبول	مقبول
`session_active`	مقبول	مقبول
`accepted`	مقبول	مقبول
`rejected`	مرفوض	مرفوض

تُعتبر أي قيمة أخرى لـ `eap_phase` تحت المصادقة.

واجهة برمجة التطبيقات REST

تقدم واجهة برمجة التطبيقات REST الخاصة بـ OmniTWAG هذه النقاط النهائية عبر HTTPS على المنفذ المخصص لواجهة برمجة التطبيقات (`8444` بشكل افتراضي). المسار الأساسي هو `/sessions`.

الطريقة	المسار	الإجراء	الوصف
GET	`/sessions`	index	قائمة الجلسات المصادق عليها. الاستجابة مقسمة وقابلة للبحث.
GET	`/sessions/{id}`	show	الحصول على جلسة واحدة بواسطة `identity`.
DELETE	`/sessions/{id}`	delete	إزالة الجلسة وفصل المشترك.
PATCH	`/sessions/{id}`	action	تنفيذ إجراء على الجلسة. الإجراء في جسم JSON.
PUT	`/sessions/{id}`	action	تنفيذ إجراء على الجلسة. الإجراء في جسم JSON.

معامل المسار `{id}` هو `identity` للجلسة (أو اسم المستخدم IMSI).

البحث والترقيم

معلمات الترقيم والبحث index تقبل نقطة النهاية.

المعامل	النوع	الوصف
`offset`	عدد صحيح	عدد الجلسات التي يجب تخطيها قبل الصفحة.
`limit`	عدد صحيح	الحد الأقصى لعدد الجلسات في الصفحة.
`q`	سلسلة	مصطلح البحث. يي��وم OmniTWAG بمطابقة المصطلح مع حقول البحث أدناه.

يتم مطابقة مصطلح `q` للجلسة مع هذه الحقول.

حقل البحث	المطابقات
`identity`	هوية الجلسة (IMSI أو اسم المستخدم).
`imsi`	IMSI المشترك.
`nas_ip`	عنوان IP المصدر لنقطة الوصول (`NAS-IP-Address`).
`called_station_id`	معرف نقطة الوصول.
`calling_station_id`	عنوان MAC للعميل.
`mac_address`	عنوان MAC لـ UE.
`ue_ip`	عنوان IP المخصص لـ UE.

جسم طلب الإجراء

تقبل `PATCH` و `PUT` جسم JSON يحتوي على حقل واحد.

الحقل	النوع	مطلوب	الوصف
`action`	سلسلة	نعم	الإجراء الذي يجب تنفيذه. يجب أن يكون `kick`، `start_accounting`، أو `stop_accounting`.

انظر إجراءات لكل جلسة لمعرفة ما يفعله كل إجراء.

الاستجابات

الحالة	المعنى
`200 OK`	كانت الطلب ناجحة (index، show، delete، action).
`404 Not Found`	لا توجد جلسة بالـ `identity` المعطى.
`422 Unprocessable Entity`	الإجراء ليس واحدًا من `kick`، `start_accounting`، أو `stop_accounting`.

تعود استجابة الإجراء الناجحة بجسم يحتوي على حقل `status` و`identity`. تعود استجابة الحذف بـ `{"status": "deleted", "identity": ...}`.

إجراءات لكل جلسة

`PATCH` لطلب JSON يعمل الإجراء على تنفيذ عملية إدارية ضد جلسة حية. أرسل الإجراء في جسم أو `PUT` إلى `/sessions/{id}`.

الإجراء	التأثير	`status` نتيجة
`kick`	إرسال RADIUS CoA-Disconnect إلى نقطة الوصول وإزالة الجلسة.	`kicked`
`start_accounting`	وضع علامة على الجلسة كنشطة وبدء المحاسبة. هذا يرقى بالجلسة إلى مقبول.	`accounting_started`
`stop_accounting`	إنهاء المحاسبة، كما لو أن نقطة الوصول أرسلت Accounting-Stop. هذا يزيل الجلسة.	`accounting_stopped`

لفصل المشترك بشكل `kick` يزيلان الجلسة. استخدم `stop_accounting` و `kick` كل من لإنهاء الجلسة كما ستن��يها الشبكة `stop_accounting` نشط عند نقطة الوصول. استخدم

أمثلة JSON

جلسة مع حركة مرور

الطلب:

```
GET /sessions/001010000000001
```

الاستجابة:

```
{
  "identity": "001010000000001",
  "imsi": "001010000000001",
  "mac_address": "AA:BB:CC:DD:EE:FF",
  "ue_ip": "10.45.0.2",
  "nas_ip": "192.0.2.10",
  "called_station_id": "AA-BB-CC-DD-EE-FF:WiFi-Calling",
  "calling_station_id": "11-22-33-44-55-66",
  "acct_session_id": "5A2E1F0C",
  "eap_phase": "session_active",
  "eap_type": "aka_prime",
  "pgw_ip": "192.0.2.20",
  "bearer_id": 5,
  "dns_servers": ["8.8.8.8", "8.8.4.4"],
  "created_at": 1712000000000,
  "last_activity": 1712000600000,
  "established_at": 1712000004000,
  "acct_input_octets": 1048576,
  "acct_output_octets": 5242880,
  "acct_input_packets": 1200,
  "acct_output_packets": 3400,
  "acct_session_time": 600,
  "acct_status_type": 3,
  "acct_last_update": 1712000600000
}
```

إجراء kick

الطلب:

```
PATCH /sessions/001010000000001
```

```
{
  "action": "kick"
}
```

الاستجابة (`200 OK`):

```
{
  "status": "kicked",
  "identity": "001010000000001"
}
```

إجراء غير معروف

الطلب:

```
{
  "action": "reboot"
}
```

الاستجابة (`422 Unprocessable Entity`):

```
{
  "error": "Unknown action \"reboot\" (expected
kick|start_accounting|stop_accounting)",
  "identity": "001010000000001"
}
```

واجهة الويب

تسرد الصفحة كل جلسة مع حالة المصادقة. **RADIUS** تحتوي لوحة التحكم على صفحة **عملاء** الخاصة بها. تظهر الصفحة عدد الجلسات المقبولة، وتحت المصادقة، والمرفوضة. استخدم الصفحة لمراجعة الجلسات الحية بسرعة.

استكشاف الأخطاء وإصلاحها

جلسة عالقة "تحت المصادقة"

الأعراض: تظهر الجلسة حالة تحت المصادقة. لا تتغير الحالة إلى مقبول. تبقى الجلسة في مرحلة EAP مثل `identity`، `aka_challenge`، `aka_prime_challenge`، `sim_challenge`، أو `resyncing`.

الأسباب المحتملة:

- بدأ المشترك مصادقة EAP لكنه لم يكملها أبدًا.
- توقفت نقطة الوصول عن إرسال استجابات EAP.
- فشل المشترك في المصادقة ولم يعاود المحاولة.

كيف يتم حلها:

1. يقوم OmniTWAG بتفعيل مهلة عندما تدخل الجلسة في مرحلة مصادقة قيد التقدم.
2. إذا لم تكمل الجلسة المصادقة أبدًا ولم تتلقَ محاسبة، يقوم OmniTWAG بإزالة الجلسة عندما تنتهي المهلة. المهلة الافتراضية هي 10 دقائق.
3. تنتقل الجلسة التي تكمل المصادقة إلى حالة مقبول. تتم ترقية الجلسة التي تتلقى محاسبة RADIUS وتنتقل أيضًا إلى مقبول إلى حالة نشطة.

لإزالة جلسة عالقة على الفور، أرسل إجراء `kick` أو طلب `DELETE` إلى `/sessions/{id}`.

جلسة لا تظهر حركة مرور

الأعراض: الجلسة مقبولة، لكن حقول `acct_*` غائبة أو صفرية.

الأسباب المحتملة:

- لم يتم استلام سجل محاسبة RADIUS بعد للمشترك.
- يحتوي سجل المحاسبة على `Acct-Session-Id` مختلف عن الجلسة.

الحل:

1. تأكد من أن نقطة الوصول ترسل محاسبة RADIUS إلى OmniTWAG.
2. تأكد من أن `Acct-Session-Id` للمحاسبة يتطابق مع `acct_session_id` للجلسة. يقوم OmniTWAG بدمج الحركة بواسطة هذه المفتاح.

3. انتظر حتى التحديث المؤقت التا��ي للمحاسبة، ثم اقرأ الجلسة مرة أخرى.

نظرة عامة

مسار المستخدم ومسار البيانات

نظرة عامة

يفصل OmniTWAG بين مستوى التحكم ومستوى المستخدم. يعمل مستوى التحكم على التحقق الحقيقية. تصف هذه UE من الهوية وإشارات الجلسة. يحمل مستوى المستخدم حركة مرور وكيف يبني ويفكك نفق UE، حزم OmniTWAG الصفحة مستوى المستخدم. تشرح كيف ينقل GTP-U، وكيف يعيد توجيه الحزم الهابطة إلى UE.

لإشارات جلسة GTP-C التي تنشئ مسار البيانات المن tunneled، انظر S2a / GTP-C. لرؤية النظام الكامل، انظر الهندسة المعمارية.

جدول المحتويات

- مستوى التحكم ومستوى المستخدم
- أنماط مسار البيانات
- مسار البيانات GRE
- نفق GTP-U
- إعادة توجيه الحزم الهابطة
- حاملات وقوالب تدفق الحركة
- معالجة الأخطاء
- MTU والتجزئة
- التكوين
- قابلية المراقبة

مستوى التحكم ومستوى المستخدم

يعمل مستوى التحكم ومستوى المستخدم كعمليات منفصلة.

يقوم **مستوى التحكم** بالأعمال التالية:

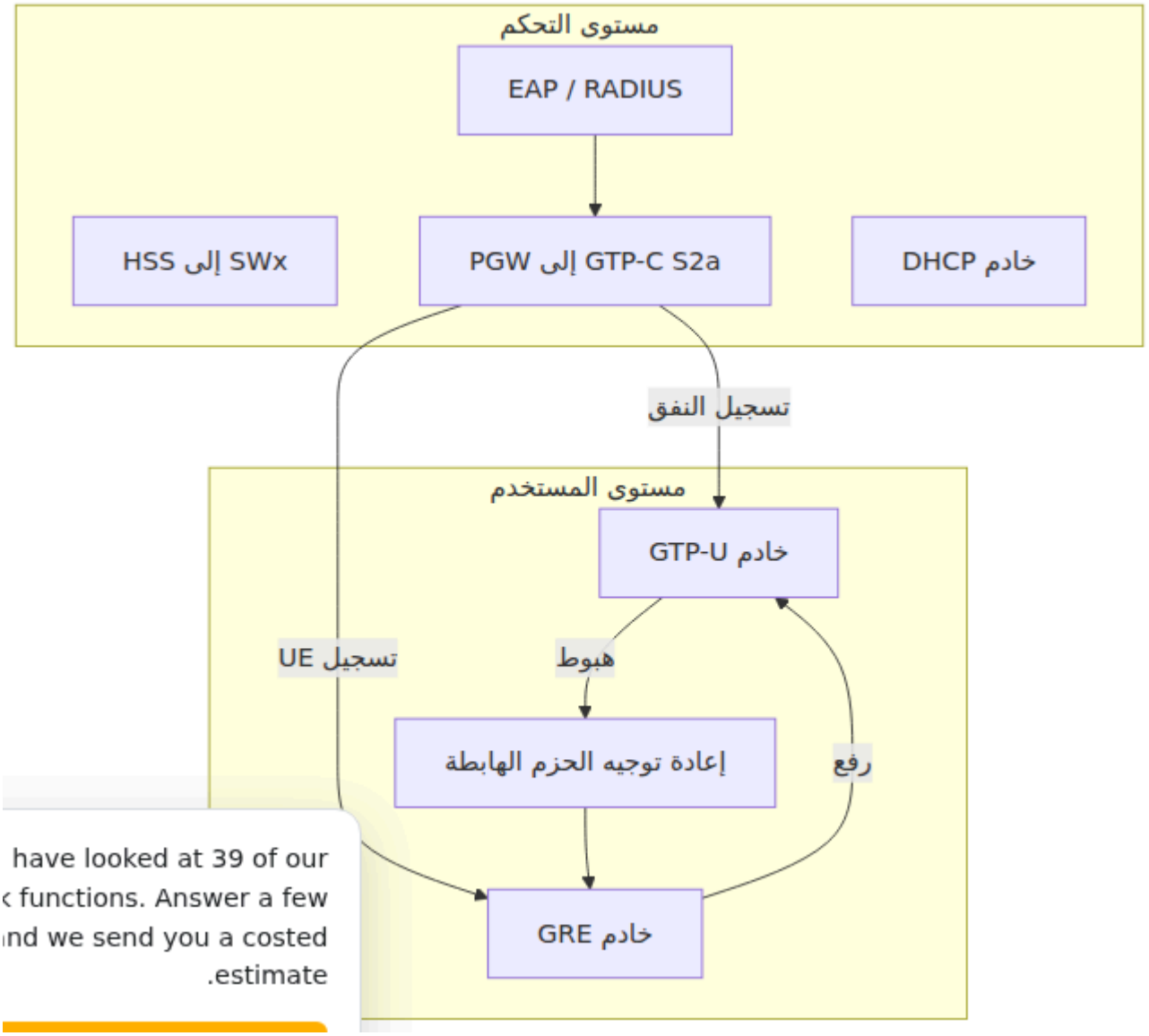
- التحقق من الهوية عبر EAP باستخدام RADIUS مع نقطة الوصول.

- جلب متجه المصادقة من HSS عبر Diameter SWx.
- إشارات جلسة GTP-C إلى PGW على واجهة S2a. هذا ينشئ ويحذف اتصال PDN والحاملات. انظر S2a / GTP-C.
- تسليم عنوان DHCP إلى UE. انظر إدارة عنوان IP.

يقوم **مستوى المستخدم** بالأعمال التالية:

- نفق GRE إلى نقطة الوصول.
- نفق GTP-U إلى PGW على واجهة S2a-U، وفقًا لـ 3GPP TS 29.281 (وضع tunneled فقط).
- إعادة توجيه الحزم الهابطة نحو UE.
- تصنيف حزم الرفع إلى الحاملات.

يقوم مستوى التحكم بإعداد حالة مستوى المستخدم. بعد التحقق من الهوية، تقوم عملية الجلسة بإنشاء جلسة GTP-C (في وضع tunneled)، وتسجيل نفق GTP-U، وتسجيل UE مع خادم GRE. ثم يحمل مستوى المستخدم الحركة.



أنماط مسار البيانات

يحدد OmniTWAG وضع مستوى البيانات لكل نقطة وصول (AP) من بيانات اعتماد RADIUS التي تتطابق مع AP. قيمة `breakout_type` في بيانات الاعتماد تحدد أحد الأنماط الثلاثة. انظر بيانات اعتماد RADIUS لإعدادات `breakout_type` و `address_source` و `ip_pool_id`.

الوضع (`breakout_type`)	عنوان IP المخصص لـ UE بواسطة	يحمل TWAG الحركة	المسار
`tunneled`	PGW	نعم	GRE من AP إلى TWAG، ثم GTP-U على S2a إلى PGW.
`nswo`	TWAG، من مجموعة IP	نعم	GRE من AP إلى TWAG، ثم خروج محلي إلى الإنترنت (NAT) عند TWAG.
`local`	الشبكة المحلية عند AP	لا	مستوى البيانات. AP تمتلك أي حزم TWAG لا يحمل ولا يخصص أي IP.

في كلا الوضعين، ترسل breakout. `nswo` و `tunneled` على كل من GRE ينطبق مسار البيانات في AP الحزم الهابطة مرة أخرى إلى TWAG في GRE، ويرسل TWAG إطارات AP إلى UE في GRE. الفرق هو في الرفع بعد GRE:

- **`tunneled`**: يقوم TWAG بتغليف حزمة الرفع في GTP-U ويرسلها إلى PGW. يقوم PGW بتخصيص عنوان IP لـ UE ويطبق السياسة والرسوم.
- **`nswo`**: يقوم TWAG بكسر الرفع محليًا إلى الإنترنت مع قاعدة تمويه NAT. يقوم TWAG بتخصيص عنوان IP لـ UE من مجموعة IP. لا يوجد PGW أو جلسة GTP-C. يتم تطبيق Gy على جانب التحصيل عبر الإنترنت TWAG.

في وضع `local`، لا يقوم TWAG بتخصيص IP ولا يحمل الحركة، لذا لا يتم استخدام لا مسار GRE ولا GTP-U لتلك AP.

وضع tunneled (GTP-U إلى PGW)

في وضع tunneled، يقوم OmniTWAG بنفق حركة مرور UE إلى PGW. يقوم PGW بتخصيص عنوان IP لـ UE، ويطبق السياسة والرسوم، ويقدم الوصول إلى الإنترنت. هذه هي واجهة S2a وفقًا لـ3GPP TS 23.402 القسم 16.

مسار الرفع هو:

```
UE --WiFi--> AP --GRE--> TWAG --GTP-U S2a--> PGW --> الإنترنت
```

مسار الهبوط هو العكس:

```
الإنترنت --> PGW --GTP-U S2a--> TWAG --GRE--> AP --WiFi--> UE
```

و قم، `true` إلى `gre.enabled` و `true` إلى `gtp.enabled` لاستخدام هذا الوضع، قم بتعيين `breakout_type` إلى `tunneled` بتعيين بيانات اعتماد AP. انظر التكوين.

خروج محلي (NSWO)

تعتبر Non-Seamless WLAN Offload (NSWO) خروجًا محليًا. تخرج حركة مرور UE مباشرة إلى PGW. يقوم TWAG بتخصيص عنوان IP لـ UE من TWAG إلى الإنترنت. لا تذهب الحركة إلى TWAG من NAT. ويطبق تمويه 3 هذا وفقًا لـ GPP TS 23.402 16.2 القسم.

يمتلك OmniTWAG طريقتين للوصول إلى NSWO:

1. **خروج لكل AP (مفضل)**: قم بتعيين بيانات اعتماد AP `breakout_type` إلى `nswo`. يأتي عنوان UE من مجموعة IP المسماة بـ `ip_pool_id`. يحدد `address_source` في بيانات الاعتماد كيفية ذلك:
   - `pool` يخصص عنوان ثابت من المجموعة ويسجل GRE مرة واحدة.
   - `dhcp` يربط MAC UE بالمجموعة ويسمح لخادم DHCP في TWAG بتوزيع عنوان في DISCOVER DHCP. يتم تسجيل الهبوط GRE عندما يكون العنوان معروفًا.
2. **معالج NSWO العالمي**: يوفر `Twag.NSWO.Handler` خروجًا محليًا لكل جلسة (ويطبق `nswo.enabled: true` عندما لا يتم استخدام GTP. يتم تحديده باستخدام `gtp.enabled: false`). يدير المعالج مجموعة IP محلية واحدة ويقوم عندما يكون TWAG عن إنشاء الجلسة، يقوم `iptables` باستخدام NAT بتكوين قاعدة تمويه لـ UE، ويسجل DHCP عبر UE بتخصيص عنوان من المجموعة المحلية، ويوصله إلى الهبوط GRE، دون PGW / جلسة GTP-C. يتم الإفراج عن التخصيص عند إنهاء الجلسة.

بالنسبة لكلا المسارين، يتم تمويه الرفع إلى الإنترنت وتعود الحزمة الهابطة عبر مسار GRE. انظر إدارة عنوان IP ومجموعة IP للحصول على العناوين.

يقرأ معالج NSWO العالمي هذه المعلمات من خريطة `nswo`:

المعلمة	النوع	الافتراضي	الوصف
`enabled`	Boolean	`false`	بدء معالج NSWO العالمي وتوجيه الجلسات عبر الخروج المحلي.
`local_pool`	String (CIDR)	`10.100.0.0/16`	المجموعة التي يتم تخصيص عنوان UE منها.
`nat_interface`	String	`eth0`	واجهة الخروج لقاعدة تمويه NAT.
`dns_servers`	List	`["8.8.8.8", "8.8.4.4"]`	خوادم DNS المعلنة لـ UE. لا يحتوي الخروج المحلي على PGW PCO لنقلها.

مسار البيانات GRE

هو نقطة النهاية لمستوى المستخدم نحو نقطة الوصول. (`Twag.Gre.Server`) يعتبر خادم GRE ترسل نقطة الوصول إطارات UE إلى TWAG في GRE، وفقًا لـ RFC 2784 و RFC 2890. يقوم خادم GRE أيضًا بإرسال الحزم الهابطة واستجابات DHCP مرة أخرى إلى نقطة الوصول. GRE هو المسار المواجه لـ AP لكل من `tunneled` و `nswo` breakout.

يستخدم خادم GRE مقبسًا خامًا لبروتوكول IP 47 (GRE)، تم فتحه باستخدام `:socket.open/3`. يجب على المضيف منح القدرة `CAP_NET_RAW`. إذا لم يفتح المقبس، يسجل الخادم خطأ ويحاول مرة أخرى كل 10 ثوانٍ. GRE مغلق بشكل افتراضي. لتشغيله، قم بتعيين `gre.enabled` إلى `true`.

تصنيف GRE الوارد

يقرأ خادم GRE رأس IP الخارجي، ويزيله، ويفكك رأس GRE. يدعم الخادم نوعين من حمولات GRE:

بروتوكول GRE	المعنى	المعالجة
`0x6558`	جسر Ethernet الشفاف	استخراج إطار Ethernet الداخلي، ثم تصنيفه حسب نو�� الإيثير.
`0x0800`	IPv4	اعتبره حزمة IPv4 للرفع.

بالنسبة لإطار جسر Ethernet الداخلي الشفاف، يقرأ الخادم نوع الإيثير:

نوع الإيثير	المعنى	المعالجة
`0x0800`	IPv4	إذا كانت الحزمة DHCP، تمرر إلى خادم DHCP. إذا لم يكن كذلك، يتم توجيهها إلى مسار الرفع.
`0x0806`	ARP	يتم التعامل معها محليًا. لا يتم توجيهها.
`0x86DD`	IPv6	يتم توجيهها إلى مسار الرفع.

يحتفظ الخادم بخريطة عنوان MAC لـ UE إلى عنوان IP هذه الخريطة لنقطة الوصول. يتعلم الخادم من MAC المصدر لكل إطار وارد. تتيح هذه الخريطة للخادم توجيه الإطارات الهابطة مرة أخرى إلى نقطة الوصول الصحيحة.

معالجة الرفع

بالنسبة لحزمة IP للرفع، يقرأ خادم GRE عنوان IP هذا هو عنوان IP المصدر لـ UE. يبحث الخادم عن عنوان IP لـ UE في جدول UE في عملية الجلسة. يجد الخادم هوية الجلسة المسجل للعثور على TEID السجل ويقرأ GTP-U المحلي للجلسة. ثم يرسل الحزمة بشكل غير متزامن إلى خادم ذلك TEID المحلي (في وضع tunneled). يتيح الإرسال غير المتزامن تجنب حالة الجمود بين عمليات GRE و GTP-U.

بعد، فإن الخادم يسقط GTP-U أو إذا لم يكن للجلسة نفق، إذا لم يكن هناك جلسة لعنوان IP لـ UE، صغيرة (أقل من 20 بايت) IP الحزمة. كما يتم إسقاط حزمة.

> ملاحظة: بالنسبة لخروج `nswo`، تحمل مجموعة IP المحلية وقاعدة تمويه NAT إلى الرفع tunneled. لتوجيه الهبوط بنفس الطريقة كما في وضع GRE UE الإنترنت. يسجل خادم

تسجيل UE للهبوط

يحتفظ التسجيل GRE. مع خادم UE عندما تصبح الجلسة نشطة، تقوم عملية الجلسة بتسجيل لنقطة الوصول، وهوية الجلسة. يستخدم خادم IP وعنوان MAC لـ UE، وعنوان IP لـ UE، بعنوان هذه البيانات لتوجيه الحزم الهابطة. عند إنهاء الجلسة، تقوم عملية الجلسة بإلغاء تسجيل GRE UE.

نفق GTP-U

يعتبر خادم GTP-U (`Twag.Gtp.GtpU`) هو نقطة النهاية لمستوى المستخدم نحو PGW ي�ي واحد على المنفذ `2152` ويحتفظ بجدول من الأنفاق. UDP يقوم بتشغيل مقبس tunneled. وضع يقوم الخادم بتنفيذ GTPv1-U 3 وفقًا لـGPP TS 29.281.

معالجة TEID

يمتلك كل نفق TEID محلي وTEID بعيد. TEID البعيد هو TEID لـ PGW. يستخدم TWAG TEID المحلي في رأس الحزم التي يرسلها إلى PGW. يستخدم PGW TEID البعيد في رأس الحزم التي يرسلها إلى TWAG. يبحث TWAG عن TEID المحلي في جدول النفق للعثور على النفق.

تقوم بتسجيل النفق. يقوم، PGW عندما تحصل عملية الجلسة على استجابة إنشاء الجلسة من خادم GTP-U بإنشاء TEID. يستخدم TEID قيمة عشوائية مشفرة من 32 بت لـ TWAG المحلي. غير القابلة للتنبؤ في TEID 3 المحلي، ولا يستخدم أبدًا الصفر. يتبع هذا متطلباتGPP TS 29.274.

يحتفظ النفق المسجل بهذه الحقول:

الحقل	الوصف
`local_teid`	الحزم الهابطة باستخدام هذه TEID على جانب TWAG. يرسل PGW القيمة.
`remote_teid`	الحزم الرافعة باستخدام هذه TEID على جانب PGW. يرسل TWAG القيمة.
`remote_ip`	عنوان IP GTP-U لـ PGW.
`remote_port`	منفذ UDP GTP-U لـ PGW. `2152` الافتراضي.
`session_id`	هوية الجلسة للنفق.

تغليف الرفع

ويضع الرأس أمام حزمة GTPv1-U G-PDU بإنشاء رأس GTP-U للرفع، يقوم خادم UE لكل حزمة IP الداخلية. يحمل الرأس إصدار GTP (1)، ونوع البروتوكول (GTP)، ونوع الرسالة (G-PDU، وطول الحمولة، و TEIDعنوان إلى الخادم الحزمة يرسل .البعيد IP ومنفذ PGW عبر مقبس 255)، على مسار الإرسال غير المتزامن، مما يتجنب حالة الجمود GTP-U خادم GRE يستدعي خادم .UDP بين العمليتين.

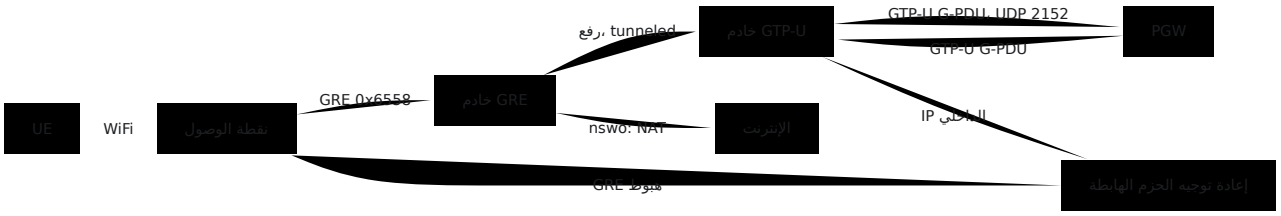
فك تغليف الهبوط

يتصرف الخادم بناءً على نوع GTP-U. يقرأ الخادم رأس GTP-U، لكل حزمة تصل إلى مقبس الرسالة:

الرسالة	النوع	الإجراء
G-PDU	255	ابحث عن النفق بواسطة TEID حزمة توجيه IP المحلي، ثم أعد الداخلية إلى إعادة توجيه الحزم الهابطة.
طلب صدى	1	الرد مع استجابة صدى.
استجابة صدى	2	قبول وتجاهل.
إشارة خطأ	26	قبول وتجاهل.
علامة نهاية	254	قبول وتجاهل.

رقم التسلسل، رقم) وأي حقول رأس اختيارية GTP-U يقوم الخادم بإزالة رأس، G-PDU بالنسبة لـ N-PDU، ونوع رأس الامتداد التالي). ثم يمرر الخادم حزمة IP الداخلية إلى `Twag.Downlink`. انظر إعادة توجيه الحزم الهابطة.

مرة GTP-U ليس له نفق، يسقط الخادم الحزمة ويرسل إشارة خطأ TEID إلى G-PDU إذا وصلت أخرى إلى المصدر. انظر معالجة الأخطاء.



إعادة توجيه الحزم الهابطة

تستقبل إعادة توجيه الحزم الهابطة (`Twag.Downlink`) حزم IP الداخلية من فك تغليف GTP-U. تحتوي إعادة التوجيه على مسارين وتفضل GRE. ترسل إعادة التوجيه كل حزمة نحو UE.

مسار GRE (مفضل)

تقرأ إعادة التوجيه عنوان IP. يعمل GRE، ترسل إعادة التوجيه الحزمة عبر GRE إذا كان خادم GRE. يبحث خادم GRE. تستدعي إعادة التوجيه خادم UE لـ IP الوجهة للحزمة الداخلية. هذا هو عنوان GRE لجسر Ethernet المسجل، ويغلف الحزمة في إطار UE في جدول UE لـ IP عن عنوان GRE

عبر UE لنقطة الوصول. تقوم نقطة الوصول بتسليم الإطار إلى IP الشفاف، ويرسلها إلى عنوان WiFi.

بالنسبة لإطار Ethernet الهابط، يستخدم خادم GRE عنوان MAC لـ UE كعنوان MAC الوجهة. المصدر MAC ثابت محلي الإدارة (`02:00:00:00:00:01`) كعنوان MAC يستخدم الخادم عنوان.

مسار المقبس الخام (خيار احتياطي)

تستخدم إعادة التوجيه مقبسًا خامًا. تقوم إعادة، GRE أو فشل إرسال GRE، إذا لم يعمل خادم من جدول التوجيه UE الخام. ثم ي��وم النواة بتوجيه الحزمة إلى IP التوجيه بحقن حزمة المحلي.

تقوم إعادة التوجيه بتعيين خيار IPv6. تفتح إعادة التوجيه مقاسين خامين: واحد لـ IPv4 وآخر لـ IPv6). يعني هذا الخيار أن إعادة التوجيه تزود الرأس (`IPV6_HDRINCL` لـ IPv6 و`IP_HDRINCL`) الكامل لـ IP. على بعض النوى، لا يزال المقبس يعمل بدون هذا الخيار، لذا فإن الفشل في تعيين الخيار ليس قاتلاً.

يجب على المضيف منح القدرة `CAP_NET_RAW` للمقابس الخام. إذا لم يفتح المقبس، تسجل إعادة التوجيه تحذيرًا وتعطل تلك العائلة من العناوين. إذا لم يكن متاحًا لا GRE ولا مقبس خام، تحسب إعادة التوجيه وتقوم بإسقاط الحزم، وتسجل تحذيرًا مرة واحدة.

اختيار المسار

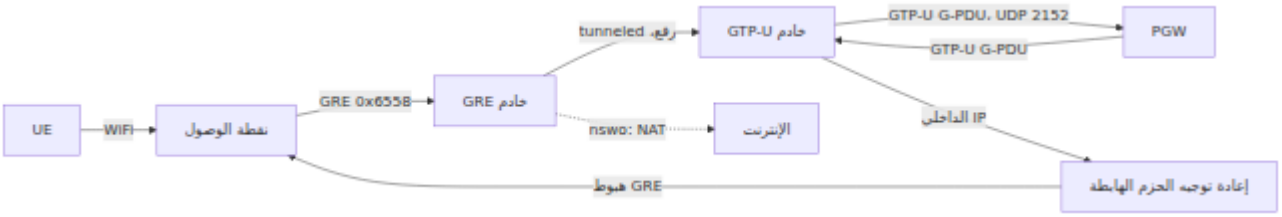
تحدد معلمة `prefer_gre` ترتيب اختيار المسار.

- `prefer_gre: true` (افتراضي): تحاول إعادة التوجيه نفق GRE أولاً وتعود إلى المقبس الخام إذا كان GRE غير متاح أو فشل إرسال GRE.
- `prefer_gre: false`: تحاول إعادة التوجيه المقبس الخام أولاً لعائلة عنوان الحزمة وتستخدم GRE فقط عندما يكون ذلك المقبس الخام غير متاح.

فحوصات الحزمة

تسقط إعادة التوجيه حزمة في هذه الحالات:

- تم تعطيل إعادة التوجيه بواسطة التكوين.
- لا يوجد مقبس متاح، و GRE غير متاح.
- الحزمة صغيرة (أقل من 20 بايت).
- لا تستطيع إعادة التوجيه قراءة عنوان IP الوجهة.



الحاملات وقوالب تدفق الحركة

يدير مدير الحاملات (`Twag.Bearer.Manager`) الحاملات لجلسة. تتوافق كل حاملة مع هوية حامل EPS (EBI). تحتوي الحاملة على TEIDs لـ GTP-U، ومرشحات حزمة قالب تدفق الحركة (TFT)، وفئة QoS (QCI). 3GPP TS 23.402 واحدة من الحاملات هي ��لحاملة الافتراضية. يتبع هذا القسم 16.1.6.1.

الحاملات الافتراضية والمخصصة

نوع الحاملة	مرشحات TFT	الغرض
افتراضي	لا شيء	يحمل كل الحركة التي لا تتطابق مع حاملة مخصصة.
مخصص	واحد أو أكثر	يحمل الحركة التي تتطابق مع مرشحات حزمة TFT الخاصة به.

إذا تمت إزالة الحاملة الافتراضية، يقوم مدير الحاملات بإشارة إنهاء الجلسة بالكامل. تؤدي إزالة حاملة مخصصة إلى إزالة تلك الحاملة فقط.

مرشحات حزمة TFT

تعتبر TFT 3GPP TS 24.008 قالب تدفق حركة وفقًا لـ 3GPP TS 24.008. تحتوي على TFT القسم 10.5.6.12. عملية وقائمة من مرشحات الحزمة. يحتوي كل مرشح حزمة على اتجاه، وأولوية، وقائمة من المكونات. يدعم محلل TFT هذه أنواع المكونات:

المطابقة	المكون
عنوان وجهة الحزمة.	عنوان IP البعيد و القناع IPv4
عنوان مصدر الحزمة.	عنوان IP المحلي و القناع IPv4
عنوان IPv6.	عنوان IPv6 البعيد/المحلي و البادئة
رقم بروتوكول IP.	معرف البروتوكول
منفذ مصدر UE.	منفذ محلي واحد / نطاق منفذ محلي
منفذ الوجهة.	منفذ بعيد واحد / نطاق منفذ بعيد
بايت TOS، مع قناع.	نوع الخدمة / فئة الحركة
لا يتم مطابقته في الرفع TWAN.	فهرس معلمة الأمان
لا يتم مطابقته (فقط IPv6).	علامة التدفق

يدعم المحلل عمليات TFT: إنشاء، حذف، إضافة مرشحات، استبدال مرشحات، حذف مرشحات، وعدم القيام بأي عملية. يقوم مدير الحاملات بتطبيق هذه العمليات عندما يرسل PGW طلب تحديث الحاملة.

تصنيف الرفع

يربط مصنف الرفع كل حزمة رفع بحاملة. القواعد هي:

1. اقرأ عنوان IP المصدر، وعنوان IP الوجهة، والبروتوكول، والمنافذ، و TOS من الحزمة.
2. اختبر الحزمة مقابل مرشحات TFT للحاملات المخصصة.
3. يتطابق مرشح فقط إذا تطا��قت جميع مكوناته. هذه هي منطق AND.
4. إذا تطابق أكثر من مرشح، اختر المرشح الذي يحمل أقل رقم أولوية. رقم أولوية أقل يعني أولوية أعلى.
5. إذا لم تتطابق أي حاملة مخصصة، اختر الحاملة الافتراضية.

يتطابق مرشح فارغ (مرشح بدون مكونات) مع جميع الحزم. هذه هي wildcard.

> **ملاحظة:** يتواجد مدير الحاملات ومصنف TFT لدعم الحاملات المخصصة. يقوم مسار GRE المحلي للجلسة. يعتمد تقسيم الرفع متعدد الحاملات TEID للرفع بإعادة توجيه الحركة على TSCM بموجب TWAG لإنشاء حاملات مخصصة للجلسة، والتي يرفضها PGW بالكامل على (انظر S2a / GTP-C).

معالجة الأخطاء

صدى GTP-U

يستخدم PGW و TWAG طلب صدى GTP-U عندما يتلقى. واستجابة الصدى لاختبار مسار النفق على تنفيذ صدى خاص بها GTP-C S2a طلب صدى، يرد باستجابة صدى. تعمل عملية خادم GTP-U عندما يكون `gtp.echo_enabled` هو `true`. انظر S2a / GTP-C.

إشارة خطأ GTP-U

مرة أخرى GTP-U إشارة خطأ GTP-U ليس له نفق، يرسل خادم TEID إلى G-PDU إذا وصلت إلى المصدر. تحمل إشارة الخطأ TEID غير المعروف وعنوان نظير GTP-U لـ TWAG. هذا يخبر بالتوقف عن إرسال الحركة على النفق الميت. كما يسقط الخادم الحزمة ويزيد عدد الأخطاء PGW.

علامة نهاية GTP-U

إرسال علامة نهاية على نفق قبل أن يقوم بتفكيك النفق. هذا من أجل الانتقال. GTP-U يمكن لخادم تخبر علامة النهاية النظير أنه لن تتبعها المزيد من الحزم على المسار القديم.

أخطاء فك التشفير

من فك تشفير حزمة، فإنه يسجل تحذيرًا ويزيد عدد الأخطاء. إذا لم GTP-U إذا لم يتمكن خادم من فك تشفير حزمة، أو حصل على بروتوكول أو نوع إيثير غير معروف، فإنه يعد GRE يتمكن خادم الحدث ويسقط الحزمة.

والتجزئة MTU

يبني خادم GRE رأس IPv4 الخارجي لكل حزمة GRE هابطة. رقم بروتوكول GRE هو 47.

لتجنب التجزئة، يجب على نقطة UE. بايتات رأس إلى حزمة GRE و GTP-U تضيف كل من تغليف الوصول تقليل MSS TCP و MTU الوصول المرجعي للنفق. يقوم تكوين نقطة الوصول بتعيين Cisco `mss 1410` و `mtu 1500` على نفق GRE. لتكوين نقطة الوصول انظر الهندسة المعمارية.

التكوين

و `gre` و `gtp` الكتل ذات الصلة هي `:omnitwag`. تقرأ عمليات مستوى المستخدم تكوين تطبيق `downlink`. من بيانات اعتماد RADIUS، يأتي وضع خروج AP وليس من هذه الكتل. انظر بيانات اعتماد RADIUS.

```
config :omnitwag,
  # GTP-U و GTP-C نحو PGW (S2a) - وضع tunneled
  gtp: %{
    enabled: false,
    pgw_ip: "10.5.198.1",
    pgw_port: 2123,
    local_ip: "10.5.198.200",
    gtpu_port: 2152,
    echo_enabled: true
  },

  # GRE نحو نقطة الوصول
  gre: %{
    enabled: false,
    local_ip: "10.5.198.200"
  },

  # إعادة توجيه الهبوط
  downlink: %{
    enabled: true,
    ip_hdr_incl: true,
    prefer_gre: true
  }
```

معلمات GTP

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	ل��	`false`	بدء خوادم GTP-C و GTP-U. تعيين `true` لوضع tunneled.
`pgw_ip`	String	لا	`"10.5.198.1"`	عنوان IP لـ PGW لـ GTP-C و GTP-U.
`pgw_port`	Integer	لا	`2123`	منفذ UDP GTP-C لـ PGW.
`local_ip`	String	لا	تلقائي الكشف	عنوان IP المحلي لـ GTP. يستخدم TWAG لـ GTP-U كمصدر لحزم وعنوان نظير إشارة الخطأ.
`gtpu_port`	Integer	لا	`2152`	المنفذ UDP المحلي لخادم GTP-U. هذا هو المنفذ القياسي لـ GTP-U.
`echo_enabled`	Boolean	لا	`true`	تشغيل صدى GTP-C نحو PGW. انظر S2a / GTP-C.

معلمات GRE

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`false`	تعيين `true` بدء خادم GRE. من نقطة UE لاستقبال إطارات الوصول عبر GRE. مطلوب لكل من `tunneled` و `nswo` breakout.
`local_ip`	String	لا	`"0.0.0.0"`	عنوان IP المحلي لربط المقبس الخام لـ GRE. هذا هو عنوان IP الوجهة الذي ترسل إليه نقطة الوصول حركة GRE.

معلمات الهبوط

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`true`	بدء إعادة توجيه الحزم الهابطة. تسقط `false`، عندما تكون إعادة التوجيه جميع الحزم الهابطة.
`ip_hdr_incl`	Boolean	لا	`true`	تعيين خيارات `IP_HDRINCL` و `IPV6_HDRINCL` على المقابس الخام بحيث تزود إعادة التوجيه الرأس الكامل لـ IP. عندما تكون `false`، لا يتم ما لم تعيين الخيار `true`. اترك يرفض النواة `IP_HDRINCL`.
`prefer_gre`	Boolean	لا	`true`	ترتيب اختيار المسار. عندما تكون `true`، تحاول إعادة التوجيه أولاً وتعود إلى GRE المقبس الخام. عندما تكون `false`، تحاول المقبس الخام فقط عندما GRE أولاً وتستخدم يكون المقبس الخام غير متاح.

قدرة المضيف

يستخدم كل من خادم GRE ومسار المقبس الخام للهبوط المقابس الخام. يجب على المضيف منح القدرة `CAP_NET_RAW`. يحاول خاد GRE المقبس بدون هذه القدرة، لا تفتح المقابس الخام.

إعادة توجيه الحزم الهابطة في موضح هو كما تتراجع، أو الحزم توجيه إعادة تسقط ثوانٍ. 10 كل.

قابلية المراقبة

تحافظ عمليات مستوى المستخدم على إحصائيات داخلية. كل عملية تبلغ عن حالتها الخاصة، تغطي وإعادة توجيه الحزم الهابطة. بالنسبة لمقاييس GRE، وخادم GTP-U، نقطة نهاية نفق OmniTWAG، التي يصدرها Prometheus انظر مرجع المقاييس.

حالة GTP-U

تبلغ حالة GTP-U عن `socket_open` و `local_ip` و `tunnel_count` وخريطة `stats` متداخلة:

الإحصائية	الوصف
`packets_in`	عدد الحزم المستلمة على مقبس GTP-U.
`packets_out`	عدد الحزم المرسلة على مقبس GTP-U.
`bytes_in`	إجمالي البايتات المستلمة.
`bytes_out`	إجمالي البايتات المرسلة.
`errors`	عدد أخطاء فك التشفير وأحداث النفق غير المعروفة.
`tunnel_count`	عدد الأنفاق المسجلة (حقل من المستوى الأعلى).

حالة GRE

تبلغ حالة GRE عن `running` و `socket_open` و `local_ip` و `ap_tunnels` و `registered_ues` وخريطة `stats` متداخلة:

الإحصائية	الوصف
`packets_in`	عدد حزم GRE المستلمة.
`packets_out`	عدد حزم GRE المرسلة.
`bytes_in` / `bytes_out`	إجمالي البايتات الداخلة والخارجة.
`dhcp_in`	عدد حزم DHCP المستلمة من نقطة الوصول.
`uplink_forwarded`	عدد حزم الرفع التي تم توجيهها إلى GTP-U.
`downlink_forwarded`	عدد حزم الهبوط المرسلة إلى نقطة الوصول.
`unknown_protocol`	عدد الحزم التي تحتوي على بروتوكول أو نوع إيثير غير معروف.
`errors`	عدد الأخطاء في فك التشفير والإرسال.
`registered_ues`	عدد UE (حقل من المستوى الأعلى) المسجلين.

إحصائيات الهبوط

الإحصائية	الوصف
`forwarded`	عدد حزم IPv4 الموجهة (GRE ومقبس IPv4 الخام).
`forwarded_v6`	عدد حزم IPv6 الموجهة.
`dropped`	عدد الحزم المسقطة.
`errors`	عدد أخطاء الإرسال.
`bytes`	إجمالي البايتات الموجهة.
`enabled`	حالة تمكين إعادة التوجيه.
`socket_open`	حالة مقبس IPv4 الخام.

نظرة عامة