

بنية OmniTWAG

نظرة عامة

القسم GPP TS 23.402 وفقًا لمعيار 3 (TWAG) موثوقة WLAN هو بوابة وصول OmniTWAG مقدمة المصادقة، (EPC) الموثوقة في النواة المتطورة للحزم WLAN 16. تربط نقاط الوصول. إدارة الجلسات، ونفق بيانات الطائرة.

جدول المحتويات

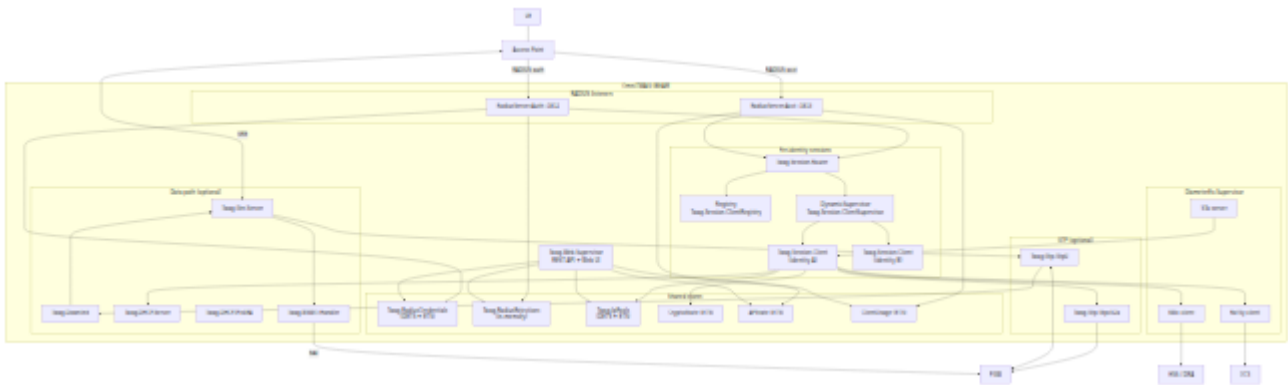
- بنية المكونات والعمليات
- شجرة الإشراف
- مرجع المكونات
- أنماط التشغيل
- GRE نفق AP تكامل
- DHCP سلوك
- المصادقة
- دورة حياة الجلسة (الموجهة إلى المنزل)
- Diameter واجهات
- ملخص التكوين
- اش◆◆ قاق المفاتيح
- صفحات ذات صلة

بنية المكونات والعمليات

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

:المجموعات الرئيسية هي

- واجهة الويب REST **ويب وإدارة العمليات**: واجهة برمجة التطبيقات (`Twag.Web.Supervisor`).
- لكل مشترك، يتم `Twag.Session.Client` واحد `GenServer`: **جلسات لكل هوية** يقوم `DynamicSupervisor` ويبدأ بواسطة `Registry` العثور عليه من خلال `Twag.Session.Router` بعملية البحث أو الإنشاء.
- **المخازن المشتركة**: `Twag.RadiusCredentials` (أسرار مشتركة دائمة)، `Twag.RadiusRejections` (مصادر مرفوضة في الذاكرة)، `Twag.IpPools` و `ClientUsage` و `APState` و `CryptoState` ومخازن، (مجموعات العناوين) ETS. المدعومة بواسطة.
- **RADIUS**: `RadiusServer.Auth` (المنفذ 1812) و `RadiusServer.Acct` (المنفذ 1813) **مستمعو**.
- **Diameter**: `DiameterEx.Supervisor` يحمل أقران SWx (متجهات المصادقة)، `STa` (الشحن عبر الإنترنت) و `Ro/Gy`، (إعادة المصادقة والإلغاء).
- **GTP**: `Twag.Gtp.GtpU` (طائرة المستخدم) و `Twag.Gtp.GtpS2a` (التحكم) `gtp.enabled` بدء تشغيلها فقط عندما يكون صحيحًا.
- **مسار البيانات**: `Twag.Gre.Server`، `Twag.Downlink`، `Twag.DHCP.Server`، `Twag.DHCP.IPv6RA`، و `Twag.NSW0.Handler`، يتم بدء تشغيل كل منها فقط، عندما يكون كتلة تكوينها مفعلة.



شجرة الإشراف

حد أقصى 10 عمليات إعادة تشغيل في `one_for_one`: يستخدم المشرف الجذر استراتيجية مصدر قبل وصول أول حزمة IP تبدأ الأطفال بهذا الترتيب، بحيث يتم حل الأسرار لكل (60 ثانية RADIUS:



الأطفال المعلمين بـ (*) يتم بدء تشغيلهم فقط عندما يكون كتلة تكوينهم مفعلة (انظر ملخص التكوين).

مرجع المكونات

المكون	النوع	يبدأ عند
<code>Twag.Web.Supervisor</code>	مشرف	دائمًا
<code>DiameterEx.Supervisor</code>	مشرف	دائمًا
<code>Twag.Session.ClientRegistry</code>	سجل	دائمًا
<code>Twag.Session.ClientSupervisor</code>	DynamicSupervisor	دائمًا
<code>Twag.Session.Router</code>	وحدة	عند الطلب
<code>Twag.Session.Client</code>	GenServer	لكل هوية
<code>Twag.RadiusCredentials</code>	GenServer	دائمًا
<code>Twag.RadiusRejections</code>	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

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

(GTP نفق) نمط التوجيه المنزلي

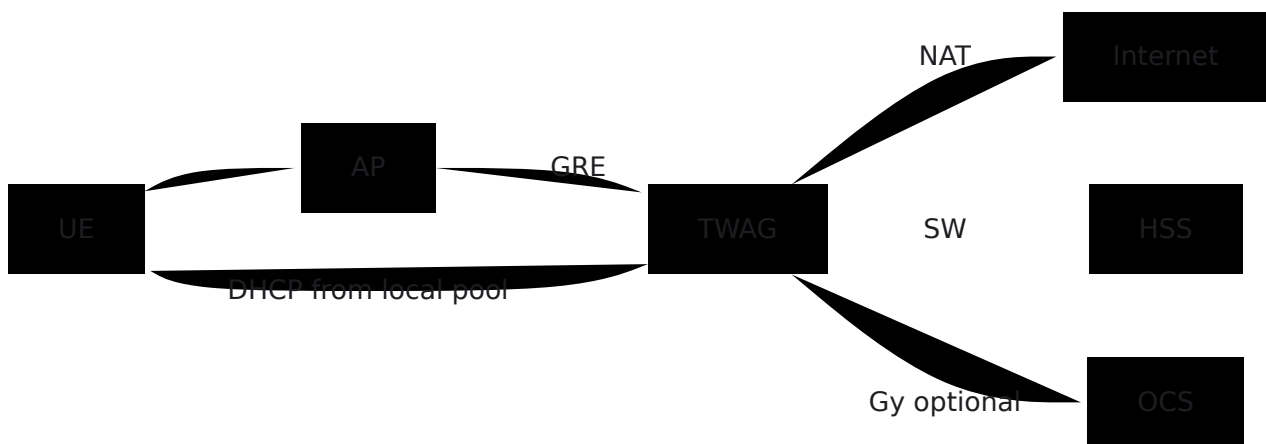
ل IP بتخصيص عنوان PGW. يقوم PGW إلى (S2a واجهة) GTP-C/GTP-U يتم نفق الحركة عبر وتطبيق السياسة/الشحن، وتوفير الوصول إلى الإنترنت، UE.



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

(NSWO) نمط الانفصال المحلي

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



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

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

GRE نفق AP تكامل

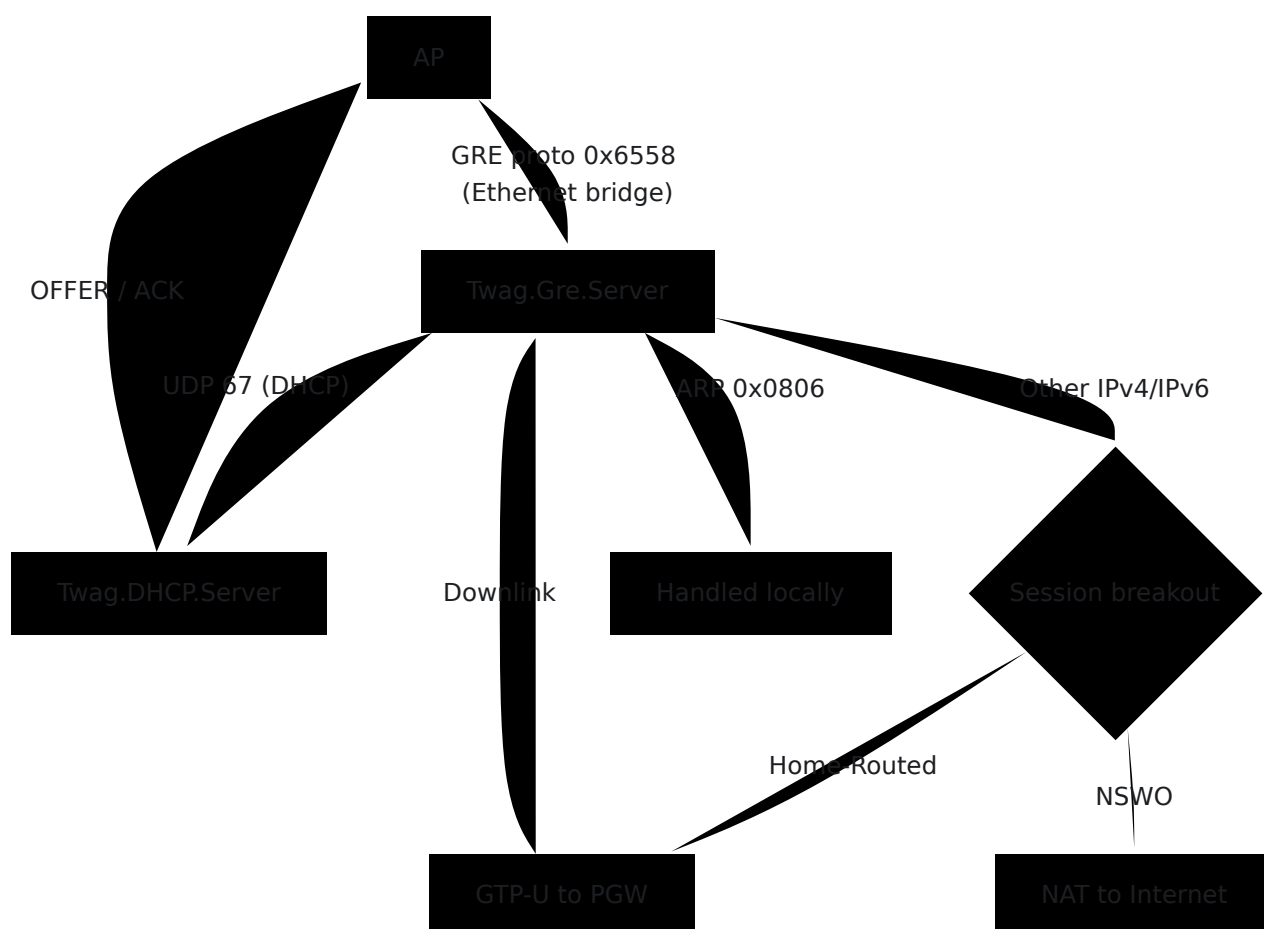
يوفر ذلك (IP 47 بروتوكول) GRE عبر TWAG إلى UE الخاصة بـ L2 بنفق إطارات AP يقوم القسم 16.1.2 TS 23.402 وفقًا لمعيار TWAG و UE الرابط المطلوب بين.

Cisco من AP تكوين

```
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
```

GRE تدفق بيانات



DHCP سلوك

النمط	IP مصدر	DHCP خادم	ملاحظات
وجه إلى المنزل	PGW (في استجابة PAA لإنشاء الجلسة)	مسبقًا بتخصيص TWAG يقوم ويقدمه عبر PGW، عنوان DHCP عبر GRE	DNS من PGW PCO
انفصال محلي	مجموعة محلية لـ TWAG (Twag.IpPools)	بالتخصيص من TWAG يقوم المجموعة المرتبطة عند (توزيع المجموعة) DISCOVER	DNS من تكوين المجموعة

على TWAG الخاص بـ DHCP يعمل خادم:

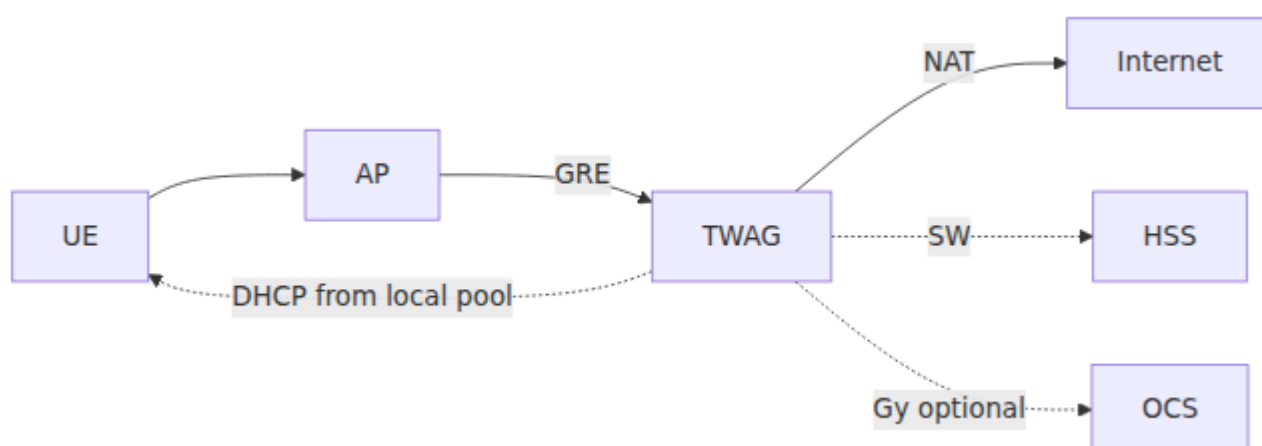
1. GRE عبر نفق UE من DHCP DISCOVER استلام.

2. PGW المخصص من IP في نمط التوجيه المنزلي، يكون هذا هو عنوان OFFER تقديم.
- مرتبطاً MAC الذي تم تخصيصه مسبقاً للجلسة. في نمط الانفصال المحلي، عندما يكون مجموعة، يقوم الخادم بتوزيع عنوان جديد من المجموعة.
3. لإكمال التبادل REQUEST/ACK التعامل مع.
4. AP إلى ومن GRE عبر نفق DHCP تمرير جميع حركة مرور.

المصادقة

EAP-مجتمعة، تقوم بإجراء مصادقة GPP من 3 AAA و خادم TWAG كخادم OmniTWAG تعمل لكل EAP تعمل آلة حالة Diameter SWx عبر HSS محلياً واسترجاع متجهات المصادقة من AKA الخاصة به Twag.Session.Client مشترك داخل

تدفق المصادقة



المصدر ضد IP بتفويض RADIUS قبل معالجة أي حزمة، يقوم مستمع يتم إسقاط المصدر الذي لا يحتوي على شبكة بيانات اعتماد Twag.RadiusCredentials. يتم تسجيل المصدر الذي يتطابق ولكنه يفشل في unauthorized_source مطابقة وتسجيله ك RADIUS. انظر رفض bad_secret ك Message-Authenticator التحقق من

أوضاع المصادقة

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

EAP طريقة

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

دورة حياة الجلسة (الموجهة إلى المنزل)

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 ->

OFFER WITH PGW IP

Data flows: UE -> GRE -
> GTP-U -> PGW ->
Internet

Teardown: GTP-C Delete
Session, GTP-U + DHCP
cleanup

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)
انظر مرجع المقاييس و الجلسات. liveness_timeout. و،(أبدًا

Diameter واجهات

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

DRA توجيه

HSS إلى SWx توجيه DRA يجب على

```
%{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	يسترجع :swx HSS المتجهات من يستخدم :local Milenage مفاتيح اختبار المحلية.
eap_method	:eap_aka	المعروضة EAP طريقة (:eap_aka أو :eap_aka_prime).
identity_timeout_ms	600000	الوقت الذي يمكن أن تبقى فيه الجلسة في مرحلة الهوية قبل أن يتم سبب الإنهاء) إنهاؤها (identity_timeout).
gtp.enabled	true	بدء تشغيل الأطفال GTP-C/GTP-U (نمط) (التوجيه المنزلي).
gtp.pgw_ip	127.0.0.1	GTP- ل PGW عنوان C/GTP-U.
gtp.local_ip	لا شيء	المحلي ل TWAG عنوان GTP.
gtp.pgw_port	2123	GTP-C ل PGW. منفذ
gtp.gtpu_port	2152	GTP- المنفذ المحلي ل U.
gtp.echo_enabled	true	GTP إرسال نبضات إبقاء إلى PGW.

المعلمة	الافتراضي	الوصف
<code>gre.enabled</code>	<code>false</code>	بدء تشغيل خادم GRE لنفق AP.
<code>gre.local_ip</code>	<code>0.0.0.0</code>	العنوان المحلي الذي GRE يرتبط به خادم.
<code>downlink.enabled</code>	<code>true</code>	بدء تشغيل ناقل الانخفاض.
<code>dhcp.enabled</code>	<code>false</code>	بدء تشغيل خادم DHCPv4.
<code>dhcp.interface</code>	لا شيء	لوضع النفق، أو "gre" للتسليم اسم NIC المباشر.
<code>ipv6_ra.enabled</code>	<code>false</code>	بدء إعلانات جهاز التوجيه IPv6 و DHCPv6.
<code>nsw.enabled</code>	<code>false</code>	بدء تشغيل معالج الانفصال المحلي NSWO.
<code>nsw.local_pool</code>	لا شيء	احتياطي لتخصيص CIDR الانفصال المحلي.
<code>nsw.nat_interface</code>	لا شيء	NAT/ للخروج لـ NIC تخفي.
<code>online_charging.mode</code>	<code>:disabled</code>	Gy وضع: <code>:disabled</code> ، <code>:authorize_only</code> ، أو <code>:online_charging</code> .

المعلمة	الافتراضي	الوصف
<code>rate_limit.max_failures</code>	10	فشل المصادقة لكل NAS في النافذة قبل إسقاط طلبات الوصول.
<code>rate_limit.window_ms</code>	60000	نافذة تحديد المعدل بالميلي ثانية.
<code>prometheus.port</code>	9568	منفذ مقاييس Prometheus.
<code>radius_config.acct_interim_interval</code>	300	فترة المحاسبة المؤقتة AP (بالثواني) المعلن لـ Access-Accept في.

اشتقاق المفاتيح

لـ EAP-AKA' (RFC 5448 و A.2 الملحق TS 33.402 وفقًا لمعيار):

```
HSS provides: RAND, AUTN, XRES, CK, IK
TWAG derives: CK' = KDF(CK||IK, FC=0x20, network_name, SQN(+)AK)
               IK' = (second half of KDF output)
               MK  = PRF'(IK'||CK', "EAP-AKA'" || Identity)
               MSK, EMSK, K_aut from MK
```

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)
```

TS 24.302 تنسيق اسم الشبكة وفقًا لمعيار:

```
WLAN:mnc{MNC}.mcc{MCC}.3gppnetwork.org
```

صفحات ذات صلة

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

نظرة عامة

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

نظرة عامة

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

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

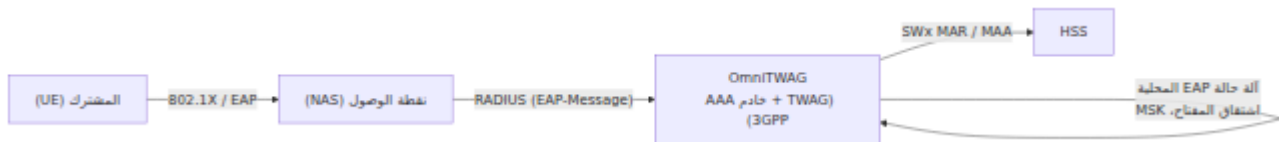
جدول المحتويات

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

نظرة عامة

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

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



ومفتاح المصادقة، (XRES) بحالة التشفير لكل هوية. تحتفظ بالاستجابة المتوقعة TWAG تحتفظ TWAG بعد أن تسلم EAP بين جولات (الممتد MSK مفتاح) EMSK، و MSK، و RAND، و (K_{aut}) بتشفير المواد الحساسات للمفتاح TWAG تقوم MPPE مفاتيح.

المدعومة EAP طرق

EAP ولكن قيمة نوع، TLV تستخدم كل طريقة نفس تنسيق خاصية EAP ثلاث طرق TWAG تدعم مختلفة وهيكل مفتاح مختلف.

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

اختيار الطريقة والتفاوض

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

NAK تسرد (3 EAP نوع) EAP-NAK يمكن ❖❖ لمشارك رفض الطريقة المعروضة باستخدام هذه القائمة وتختار أول نوع تدعمه. تدعم TWAG التي يفضلها المشترك. تقرأ EAP أنواع (EAP-SIM) و 18، (EAP-AKA) 23، (EAP-AKA') 50: NAK الأنواع في

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

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

والمراحل EAP آلة حالة

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

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

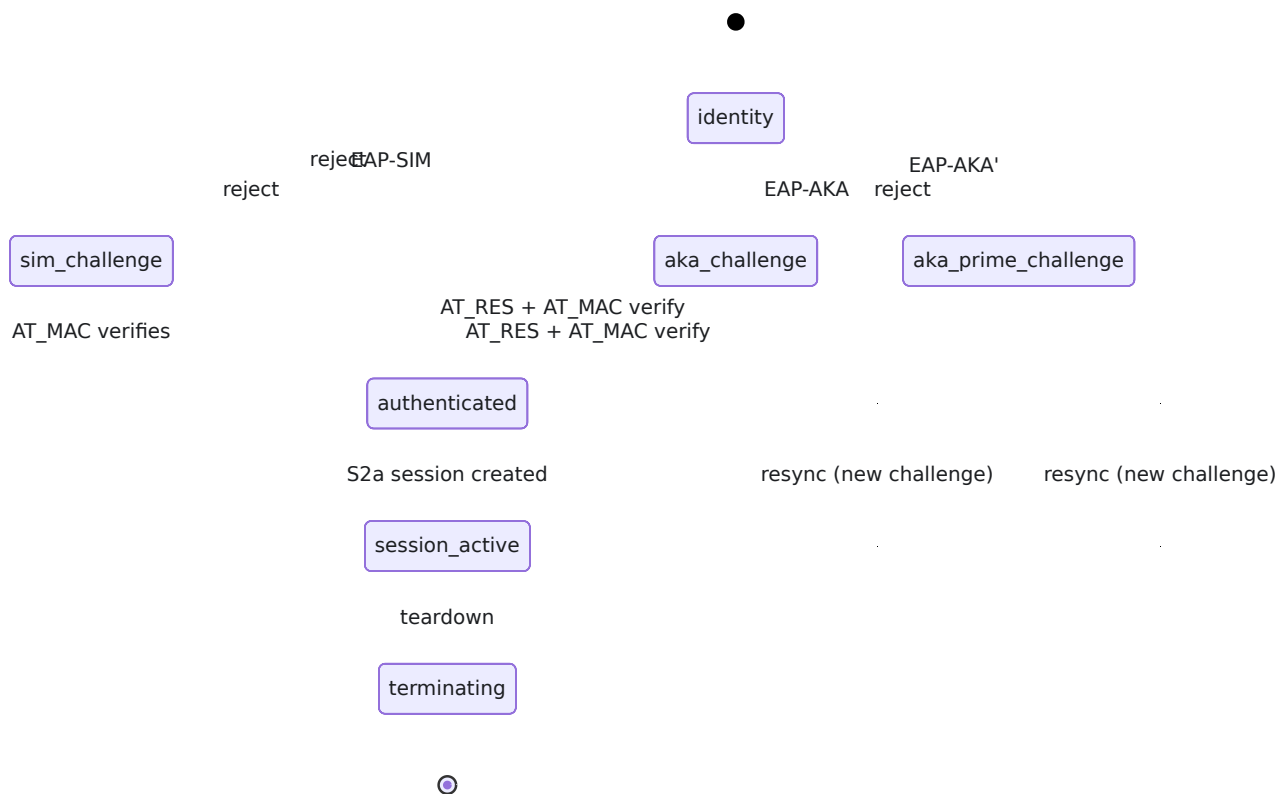
:توجد قيمتان إضافيتان للمرحلة في الكود

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

، (identity، aka_challenge) تتم حصاد جلسة تبقى في مرحلة مصادقة قيد التقدم بعد انتهاء مهلة الهوية. قم (resyncing، أو sim_challenge، aka_prime_challenge،

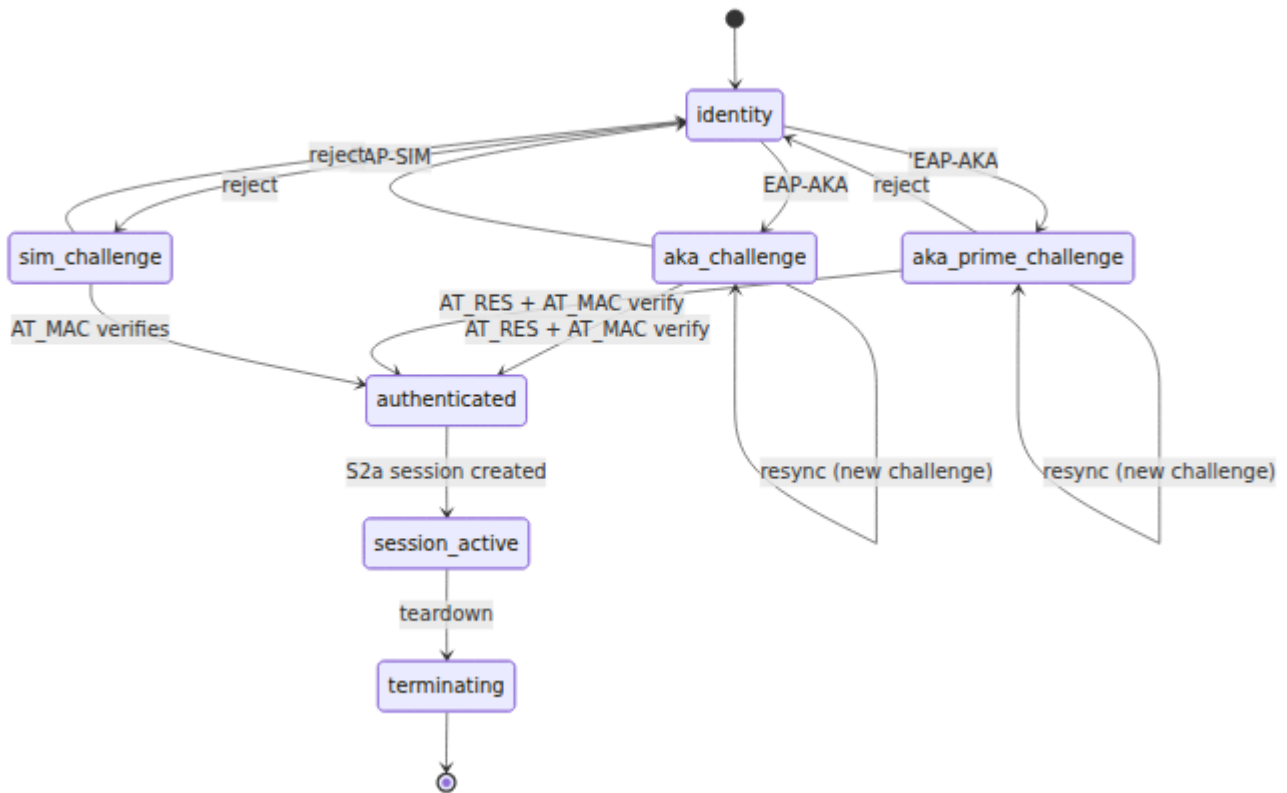
راجع ال  كوين. `identity_timeout_ms`. بتعيين المهلة باستخدام

API. تربط صفحة **الجلسات** هذه المراحل بحالة مصادقة الجلسة المعروضة في واجهة المستخدم و



تسلسل المصادقة

EAP-AKA'. EAP-AKA تتضمن السلسلة الكاملة مرحلة الهوية ومرحلة التحدي. المثال أدناه يظهر `AT_RES`. ولا يرسل AKA-Identity، جولة بدء بدلاً من جولة EAP-SIM له نفس الشكل. يستخدم



مرحلة الهوية

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

مرحلة التحدي

1. من الهوية وتحصل على متجهات المصادقة. راجع **مصادر متجهات** TWAG IMSI تستخرج المصادقة.
2. راجع **اشتقاق المفاتيح** MSK. باشتقاق مفاتيح الجلسة، بما في ذلك TWAG تقوم التسليم.
3. يحمل التحدي EAP-AKA' التحدي. بالنسبة لـ TWAG تبني `AT_RANDOM`، `AT_AUTN`، `AT_KDF_INPUT` (اسم الشبكة)، `AT_KDF`، `AT_BIDDING`، `AT_RESULT_IND`، و `AT_MAC`، يحمل التحدي EAP-AKA بالنسبة لـ `AT_RANDOM`، `AT_AUTN`، و `AT_MAC`. يحمل التحدي EAP-SIM بالنسبة لـ `AT_RANDOM` (2 أو 3 RANDs) و `AT_MAC`.

- ثم يعيد الاستجابة ،MAC و (AUTN) يتحقق المشترك من الشبكة.
- من الاستجابة. راجع **تحقق الاستجابة** TWAG تتحقق.
- TWAG EAP- Success عند النج❖❖ح، تعيد Failure.

تحقق الاستجابة

EAP-AKA و EAP- من استجابة التحدي بترتيب ثابت. الترتيب هو نفسه بالنسبة ل TWAG تتحقق AKA'.

- TWAG مفقودة، ترفض XRES المخزنة أو K_aut **تحقق الحالة**. إذا كانت
- TWAG مفقودة، ترفض AT_MAC أو AT_RES **تحقق الخاصية**. إذا كانت
- عبر الحزمة MAC وإعادة حساب ،AT_MAC بتصغير حقل TWAG تقوم **MAC تحقق**. EAP-AKA' تستخدم HMAC-SHA1 EAP-AKA وتقارن. تستخدم ،K_aut باستخدام HMAC-SHA-256. كلاهما مقطوع إلى 16 بايت.
- المخزنة. المقارنة هي زمن XRES مع AT_RES TWAG **تحقق الاستجابة**. تقارن.
- تحقق الطول ومقارنة بايت زمن ثابت TWAG **ثابت** لمنع هجمات الزمن. تستخدم TWAG خلاف ذلك، ترفض TWAG والاستجابة، تقبل MAC **النتيجة**. إذا تطابق كل من

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

مصاد❖❖ متجهات المصادقة

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

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

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

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

HSS إلى SWx

عبر واجهة HSS إلى Multimedia-Auth-Request (MAR) طلب TWAG ترسل، `swx`: في وضع MAR: يحمل. (معرف التطبيق 16777265، 3GPP TS 29.273) SWx

- `User-Name`: IMSI.
- `EAP-` مضبوطة على `SIP-Authentication-Scheme` مع `SIP-Auth-Data-Item` `SIP-Authorization` (معلومات) بالنسبة لإعادة التزامن، يحمل العنصر أيضًا. AKA. (AUTS متصل بـ RAND: إعادة التزامن).
- `SIP-Number-Auth-Items`: 1.
- `ANID`: WLAN.
- `RAT-Type`: 0.
- `Auth-Session-State`: 1 (NO_STATE_MAINTAINED).
- `Vendor-Specific-Application-Id` مع معرف تطبيق SWx Auth 16777265 وVendor-Id 10415.

هو 2001 `Result-Code` عندما يكون. Multimedia-Auth-Answer (MAA) برد HSS تعود وتستخرج المتجه `SIP-Auth-Data-Item` أول TWAG (نجاح)، تقرأ:

- `SIP-Authenticate` = RAND (16 بايت) متصل بـ AUTN (16 بايت).
- `SIP-Authorization` = XRES.
- `Confidentiality-Key` = CK.
- `Integrity-Key` = IK.

في جلبها TWAG هو 2001، أو كانت حقول المتجه مفقودة، تفشل `Result-Code` إذا لم يكن وتعاملها كرفض للمصادقة (ليس خطأ داخليًا). ترفض مرحلة التحدي المشترك بشكل نظيف مع EAP-Failure.

SWx (Experimental-Result) إشارات خطأ

(Vendor-Id) المجموعة AVP Experimental-Result إلى معظم الأخطاء في SWx تشير الفاشل لذلك لا يحمل أي MAA الأساسي. يمكن أن يحمل Result-Code وليس في (10415) Experimental-Result-Code أيضًا TWAG أساسي على الإطلاق. تقرأ Result-Code وتسجل الاسم القابل للقراءة البشرية حتى يرى المشغل السبب الحقيقي. راجع **استكشاف الأخطاء وإصلاحها** للحصول على الرموز.

أو (5001) DIAMETER_ERROR_USER_UNKNOWN حالة شائعة هي المشترك غير مفعل: (5450) DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION لذا تفشل المصادقة على الرغم من أن نفس المشترك قد يكون SWx على GPP للوصول غير 3 EPC للوصول إلى S6a معروفاً على.

DRA راجع **العمارة: توجيه**. HSS إلى SWx توجيه تطبيق DRA يجب على.

المحلي Milenage

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

EAP-SIM المتجهات لـ

المجموعات من نفس متجهات TWAG تستخرج GSM. إلى 2 أو 3 مجموعات EAP-SIM تحتاج وتنشئ SRES كـ XRES وتأخذ أول 4 بايت من RAND TWAG لكل متجه، تأخذ Milenage . (C.3 الملحق 33.102 3GPP TS): Kc = CK[0..7] XOR CK[8..15] XOR IK[0..7] XOR IK[8..15].

NAI معالجة الهوية و

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

IMSI استخراج

في خطوتين NAI من TWAG IMSI تستخرج

1. @ اسم المستخدم، وهو الجزء قبل TWAG تأخذ.
2. أو (EAP-AKA/AKA، الهوية الدائمة) رقم نوع الهوية الرائد. رقم 0 الرائد TWAG تنزيل IMSI العاري. الأرقام المتبقية هي IMSI رقم 6 الرائد يتوافق مع

تستخدم SWx MAR. في User-Name هو IMSI. مكونة من 14 أو 15 رقمًا TWAG IMSI تقبل هو MNC هو أول 3 أرقام، و MCC و MNC لجلسة GTP-C: اشتقاق IMSI أيضًا TWAG الرقمين التاليين.

(EAP-AKA') اسم الشبكة

وهو مدخل AT_KDF_INPUT المفاتيح باسم الشبكة. يذهب اسم الشبكة في EAP-AKA' يربط إذا لم يتم network_name قم بتعيين اسم الشبكة باستخدام مفتاح التكوين CK' / IK' لاشتقاق GPP TS 24.302 وفقًا لـ 3 Diameter اسم الشبكة من مجال TWAG تعيين المفتاح، تشتق

- الرائدة من المجال epc. TWAG تنزيل.
- TWAG تصنيف WLAN:.

يعطي اسم epc.mnc{MNC}.mcc{MCC}.3gppnetwork.org على سبيل المثال، المجال إذا لم يكن المجال يحتوي على WLAN:mnc{MNC}.mcc{MCC}.3gppnetwork.org الشبكة بادئة epc. TWAG تستخدم ، بادئة

اشتقاق المفاتيح والتسليم

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

EAP-AKA' هيكل مفتاح

A: الملحق GPP TS 33.402 و RFC 5448 وفقًا لـ

1. Key = CK \ | IK.

2. $S = FC(0x20 \parallel network_name \parallel len(network_name) \parallel (SQN \oplus AK) \parallel len(SQN \oplus AK))$.
3. $CK' \parallel IK' = HMAC\text{-}SHA\text{-}256(Key, S)$. CK' هو أول 16 بايت IK' هو آخر 16 بايت.
4. $MK = PRF'(IK' \parallel CK', "EAP\text{-}AKA" \parallel Identity)$, يستخدم 208 بايت. PRF' HMAC-SHA-256.
5. بتقسيم TWAG تقوم MK : K_{encr} (16), K_{aut} (32), K_{re} (32), MSK (64), $EMSK$ (64).

EAP-AKA هيكل مفتاح

RFC 4187 وفقًا لـ

1. $MK = SHA1(Identity \parallel IK \parallel CK)$.
2. PRF FIPS 186-2 إلى 160 بايت باستخدام MK بتوسيع TWAG تقوم.
3. بتقسيم الناتج TWAG تقوم: K_{encr} (16), K_{aut} (16), MSK (64), $EMSK$ (64).

EAP-SIM هيكل مفتاح

RFC 4186 وفقًا لـ

1. $MK = SHA1(Identity \parallel Kc1 \parallel Kc2 \parallel [Kc3] \parallel NONCE_MT \parallel Version_List \parallel Selected_Version)$.
2. PRF FIPS 186-2 إلى 160 بايت باستخدام MK بتوسيع TWAG تقوم.
3. بتقسيم الناتج TWAG تقوم: K_{encr} (16), K_{aut} (16), MSK (64), $EMSK$ (64).

إلى نقطة الوصول MPPE إلى MSK

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

- $MS\text{-}MPPE\text{-}Recv\text{-}Key = MSK[0..31]$ (أول 32 بايت).
- $MS\text{-}MPPE\text{-}Send\text{-}Key = MSK[32..63]$ (آخر 32 بايت).

Request و RADIUS بتشفير كل مفتاح باستخدام السر المشترك لـ TWAG تقوم ملحقًا جديدًا مكونًا من 2 بايت مع تعيين TWAG تستخدم RFC 2548 وفقًا لـ Authenticator.

باستخدام السر المشترك. راجع Access-Accept بتوقيع TWAG البت العالي لكل مفتاح. تقوم للسر TWAG لمعرفة كيفية حل RADIUS الأسرار المشتركة لـ

كمفتاح رئيسي MSK وتستخدم MSK واستعادة MPPE، تقوم نقطة الوصول بفك تشفير مفاتيح زوجي لعملية المصافحة الرباعية 802.11 مع المشترك

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

إعادة التزامن

خارج التزامن مع الشبكة. يرسل المشترك (SQN) يمكن للمشارك الإبلاغ ع❖❖ أن رقم تسلسله هو 14 بايت: AT_AUTS. AT_AUTS مع (x04النوع الفرعي 0) AKA-Synchronization-Failure (MAC-S المخفي و8 بايت من SQN 6 بايت من

مع إعادة التزامن كما يلي TWAG تتعامل:

1. البالغ AUTS المخزنة متصلة بـ RAND :بناء معلومات إعادة التزامن TWAG تقوم 14 بايت.
2. المشترك باستخدام دالة SQN بتشغيل إعادة التزامن. يستعيد هذا TWAG تقوم 14 بايت. ويعيد رقم تسلسل محدث، MAC-S، يتحقق من ،Milenage f5*
3. المحدث، تبني تحديثًا جديدًا، وترسل SQN متجهًا جديدًا مع TWAG عند النجاح، تولد جديدة Access-Challenge.
4. EAP-Failure المشترك مع TWAG عند الفشل، ترفض.

تستخدم إعادة التزامن مفاتيح EAP-AKA' و EAP-AKA مع إعادة التزامن لكل من TWAG تتعامل خطأ TWAG بالضبط 14 بايت، وإلا ترفع AT_AUTS المحلية. يجب أن تكون قيمة Milenage وتفشل الجولة

(ERP) إعادة المصادقة السريعة

للمشارك ERP يسمح RFC 6696 وفقًا لـ EAP (ERP) بروتوكول إعادة المصادقة TWAG تدعم EMSK من TWAG كامل. يأتي التوفير من سلسلة مفاتيح تشتقها EAP بإعادة المصادقة دون تبادل خلال المصادقة الكاملة الأولى

:وتخزن مفاتيح إعادة المصادقة TWAG بعد المصادقة الكاملة، تشتق

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

ERP HMAC-SHA-256 تستخدم جميع اشتقاقات مفاتيح

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

1. إلى مصادقة كاملة. ترسل TWAG المخزنة، تعود rIK أو rRK TWAG إذا لم يكن لدى TWAG طلب AKA-Identity جديد.
2. بتحليل الرسالة والتحقق من علامة TWAG المفاتيح، تقوم TWAG إذا كانت لدى rIK المصادقة باستخدام.
3. ورقم rRK من ($rMSK$) إعادة المصادقة TWAG MSK إذا تم التحقق من العلامة، تشتق وتقبل. تصبح ،(EAP 42 نوع) EAP-Finish/Re-auth تسلسل الرسالة، تبني استجابة $rMSK$ MPPE الجديدة لمفاتيح MSK هي.
4. إلى مصادقة كاملة TWAG إذا لم يتم التحقق من ال❖❖ لامة، أو فشل التحليل، تعود.

معالجة الأخطاء ورموز النتائج

EAP نتائج

الشرط	إجراء TWAG
أو المتجهات غير، SWx MAR فشل مكتملة	المشترك TWAG يتم رفض جلب المتجه. ترفض وتسجيل الرفض، EAP-Failure بشكل نظيف مع بدلاً من تعطل.
AT_MAC فشل تحقق	Access-Reject مع EAP-Failure.
XRES مع AT_RES لا يتطابق	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.
AKA- يرسل المشترك Authentication-Reject (النوع الفرعي 0x02)	رفض المشترك الشبكة. Access-Reject.
AKA-Client-Error يرسل المشترك (النوع الفرعي 0xE)	Access-Reject.
بدون طريقة مدعومة EAP-NAK	Access-Reject.
مفقود أو ليس 64 بايت عند MSK القبول	Access-Reject.
غير معالجة EAP رسالة	Access-Reject مع EAP-Failure.

Diameter ل SWx رموز نتائج

Experimental- AVP أساسي. تصل رموز الخطأ أدناه في Result-Code رمز النجاح هو واستكشف SWx الأساسي. راجع ملاحظة إشارات خطأ Result-Code وليس في Result،

.الأخطاء وإصلاحها

الرمز	الاسم	المعنى
2001	DIAMETER_SUCCESS	MAA يحمل متجهًا صالحًا.
5001	DIAMETER_ERROR_USER_UNKNOWN	لا يوجد اشتراك غير 3GPP/SWx لهذا IMSI في HSS. قد يكون المشارك 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 لهذا EPS المشارك.
5450	DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION	لا يوجد اشتراك غير 3GPP للمشارك.
أخرى	(Diameter خطأ)	فشل جلب المتجه. ترفض الجولة.

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

(STa) الأحداث التي تبدأها الشبكة

معرف (3GPP TS 29.273) STa عبر واجهة TWAG إرسال أحداث إلى 3GPP AAA يمكن لخدم
2001 Result-Code على كل حدث بـ TWAG ترد. (التطبيق 16777250

الرسالة	الزناد	TWAG إجراء
ASR (طلب إنهاء الجلسة)	AAA يريد خادم قطع الاتصال.	يقطع جلسة المشترك، ثم ترد على TWAG تقوم ASA.
STR (طلب إنهاء الجلسة)	HSS. فصل بدؤه	يقطع جلسة المشترك، ثم ترد على TWAG تقوم STA.
RAR (طلب إعادة المصادقة)	AAA يريد خادم إعادة المصادقة.	بنجاح وتسجل الطلب. لم RAA على TWAG ترد يتم بعد تشغيل إعادة المصادقة الكاملة للجلسة RAR الحية من.

راجع التكوين. Diameter من هوية Origin-Host وOrigin-Realm تحمل جميع الإجابات الثلاثة

التكوين

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

```
config :omnitwag,  
  # (الاختبار) :local أو (الإنتاج) :swx : مصدر المنتج  
  auth_mode: :swx,  
  
  # أو :eap_aka، (الافتراضي) :eap_aka_prime :المعروضة EAP طريقة  
  :eap_sim  
  eap_method: :eap_aka_prime,  
  
  # إذا لم يتم تعيينه، يتم اشتقاقه من مجال 'EAP-AKA' اسم الشبكة لـ  
  Diameter.  
  network_name: "WLAN:mnc001.mcc001.3gppnetwork.org",  
  
  # حصاد جلسة لا تزال عالقة في مرحلة مصادقة قيد التقدم بعد هذه  
  المدة من  
  # المللي ثانية. الافتراضي 600000 (10 دقائق)  
  identity_timeout_ms: 600_000,  
  
  # عند تعيينها STa DER/AAR تضاف إلى TWAN، حقول معرف  
  twan_ssid: "ons",  
  twan_bssid: "00:11:22:33:44:55",  
  
  # (auth_mode: :local تستخدم فقط عند) مفاتيح اختبار محلية  
  test_keys: %{\br/>    ki: "11111111111111111111111111111111",  
    opc: "22222222222222222222222222222222",  
    amf: "8000",  
    sqn: 1200  
  }  
}
```

المعلمة	النوع	مطلوب	الافتراضي	الوصف
auth_mode	Atom	لا	:local	مصدر المتجه يحصل على H المتجهات من SWx. :local عبر SWx. :local المتجهات من test_keys. :local ي SWX بتعيين الإنتاج.
eap_method	Atom	لا	:eap_aka_prime	EAP طريقة معروضة. واحدة من :eap_aka_prime :eap_aka، :eap_sim. :eap_aka_prime مشترك التفاوض طريقة مدعومة مختلفة باستخدام EAP-NAK.
network_name	String	لا	مشتق من المجال	اسم الشبكة لـ AKA' في AT_KDF_INPU :eap_aka_prime :eap_aka، :eap_sim. :eap_aka_prime مشترك التفاوض طريقة مدعومة مختلفة باستخدام EAP-NAK. ذا لم يتم تعيينه، TWAG مشتق من مجال Diameter لـ TS 24.302.
identity_timeout_ms	Integer	لا	600000	ت بالملي ثانية يمكن أن تبقى جلسة في مرحلة مادية قيد التقدم

الوصف	الافتراضي	مطلوب	النوع	المعلمة
TV قبل أن تقوم بحصادها.				
SSID WLAN. . T تعيينه، تضيف TWAN معرف STa DE رسائل وAAR.	-	لا	String	twan_ssid
BSSID نقطة ول. مجتمعة مع twan_ssid لتشكيل معرف TWAN.	-	لا	String	twan_bssid
Milenage مفاتيح محلية. تستخدم قط عندما يكون auth_mode راجع. local: معلومات مفتاح الاختبار.	القيم الافتراضية الدمجة	لا	Map	test_keys

معلومات مفتاح الاختبار

في الإنتاج test_keys لا تستخدم. local: فقط في وضع test_keys TWAG تقرأ

المعلمة	النوع	مطلوب	الاقتراح	الوصف
ki	String (hex)	نعم (وضع محلي)	1111...	بايت 16 ، Ki مفتاح المشترك ك 32 حرفًا سداسيًا.
opc	String (hex)	نعم (وضع محلي)	2222...	0Pc ، مفتاح متغير المشغل ، بايت ك 32 حرفًا سداسيًا 16.
amf	String (hex)	نعم (وضع محلي)	8000	حقل إدارة المصادقة، 2 بايت ك 4 أحرف سداسية.
sqn	Integer	نعم (وضع محلي)	1200	رقم التسلسل الابتدائي.

الرصد

تعرض نقطة STa ومعالج EAP بإصدار عدادات بيانات استشعار من خلال آلة حالة TWAG تقوم العدادات. راجع [مرجع المقاييس](#) للحصول على نقطة النهاية وأمثلة الاستعلام Prometheus النهاية

EAP مقاييس

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

EAP-SIM (start, auth_success, auth_reject) أيضًا بإصدار أحداث بيانات استشعار لـ TWAG تقوم ERP (initiate, client_error, و AKA auth_reject) لـ

success, fallback, mac_failure). راجع مرجع المقاييس.

RADIUS مقاييس رد

المقياس	المعنى
radius_access_challenge_count	قيد EAP جولة Access-Challenge ردود (التقدم).
radius_access_accept_count	(مصادقة ناجحة) Access-Accept ردود.
radius_access_reject_count	(فشل المصادقة) Access-Reject ردود.

STa مقاييس أحداث

عداد بيانات استشعار لكل حدث يبدأه الشبكة STa يصدر معالج [:sta, :asr, :received, :count], [:sta, :str, :received, :count], و [:sta, :rar, :received, :count], بالإضافة إلى عدادات جلسة disconnect و reauth.

سياق السجل

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

استكشاف الأخطاء وإصلاحها

السبب المحتمل	العرض	
لا يوجد اشتراك 3GPP/SWx غير في IMSI لهذا قد يكون HSS. المشترك معروفًا S6a/EPC على ولكنه غير مفعّل للوصول غير 3GPP.	فشل المصادقة ويظهر السجل DIAMETER_ERROR_USER_UNKNOWN (5001)	مراك غير 3GPP HSS.
ملف تعريف المشترك لا يحتوي على اشتراك غير 3GPP.	فشل المصادقة ويظهر السجل DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION (5450)	مراك غير 3GPP
خطأ SWx أعاد AVP في Experimental- Result، وليس Result- Code الأساسي.	فاشل MAA على Result-Code=nil يظهر السجل	Exl Result ل. تطيع TWAG البشرية
علق المشترك في مرحلة مصادقة قيد التقدم بعد انتهاء مهلة الهوية.	لم تكتمل المصادقة أبدًا وتم حصاد الجلسة	من جانب م بضبط identi زم الأمر
في UE فشل مصادقة الشبكة (AUTN تحقق).	AKA-Authentication-Reject يرسل المشترك	الشبكة OP/OF مع SIM :local

السبب المحتمل	العرض	
		HSS SWX :
SQL انحراف المشترك عن الشبكة SQL.	متكرر AKA فشل إعادة مزامنة	TV تقوم قائماً. إذا معالجة SQL التزامن.
مفقوداً MSK كان أو ليس 64 بايت عند القبول.	Access-Reject مع توقع EAP-Success صالح	ر المتجه ة. تحقق MA المحلية

سر مشترك خاطئ، نقطة) EAP التي تحدث قبل أو حول تبادل RADIUS بالنسبة لرفضات طبقة
ومرجع حالة الجلسات RADIUS راجع الأسرار المشتركة ل، (وصول غير معروفة

تدفقات المكالمات

نظرة عامة

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

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

جدول المحتويات

- الجهات الفاعلة والواجهات
- الاتصال الناجح - محمي، مشحون
- IP مع مجموعة NSWO - الاتصال
- DHCP مع توزيع NSWO - الاتصال
- (AP طائرة بيانات) الاتصال - كسر محلي
- SWx فشل المصادقة - المشترك غير مزود لـ
- 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

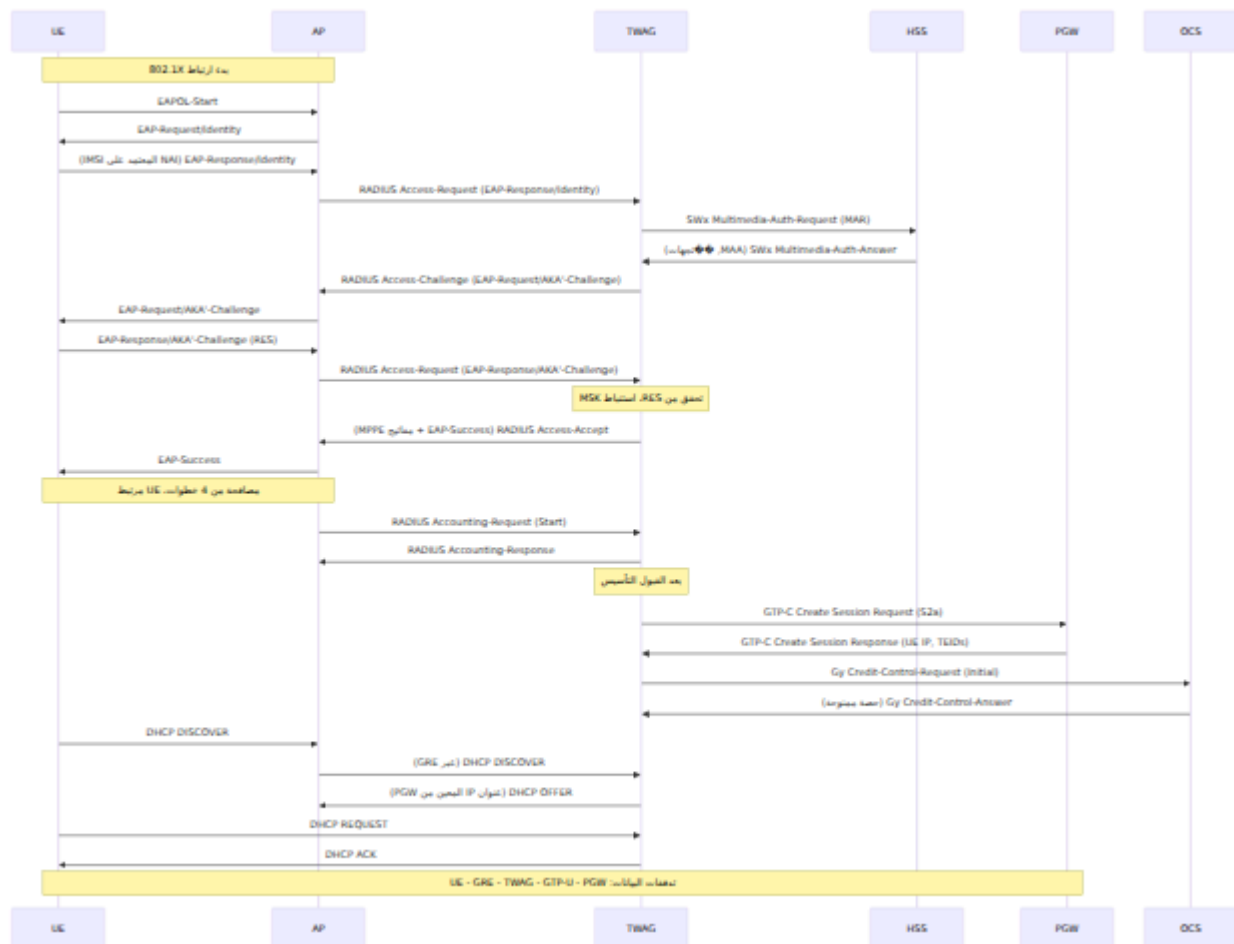
الجهات الفاعلة والواجهات

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

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

الاتصال الناجح - محمي، مشحون

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

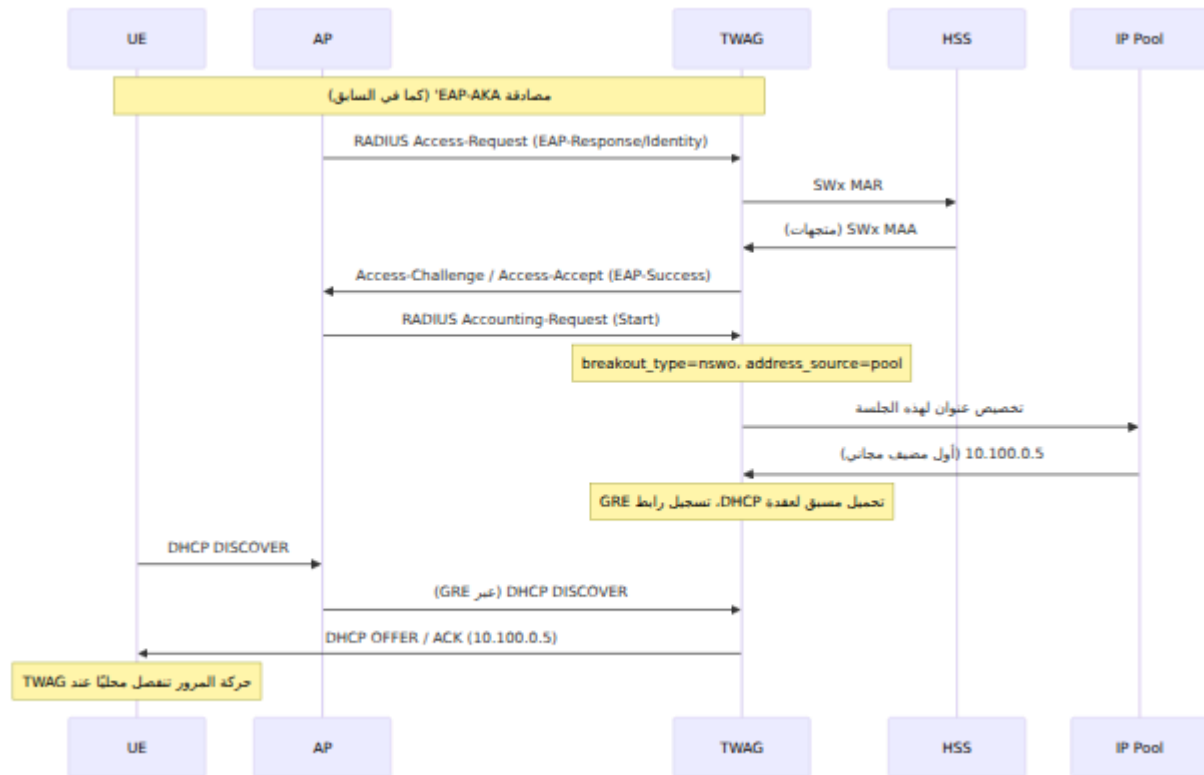


IP مع مجموعة NSW0 - الاتصال

PGW لا يتصل بـ TWAG ، `address_source: pool` و `breakout_type: nsw0` بالنسبة لـ . تنفصل حركة DHCP المرتبطة ويوفره عبر IP بتخصيص عنوان ثابت من مجموعة TWAG يقوم مرور المشترك محليًا .

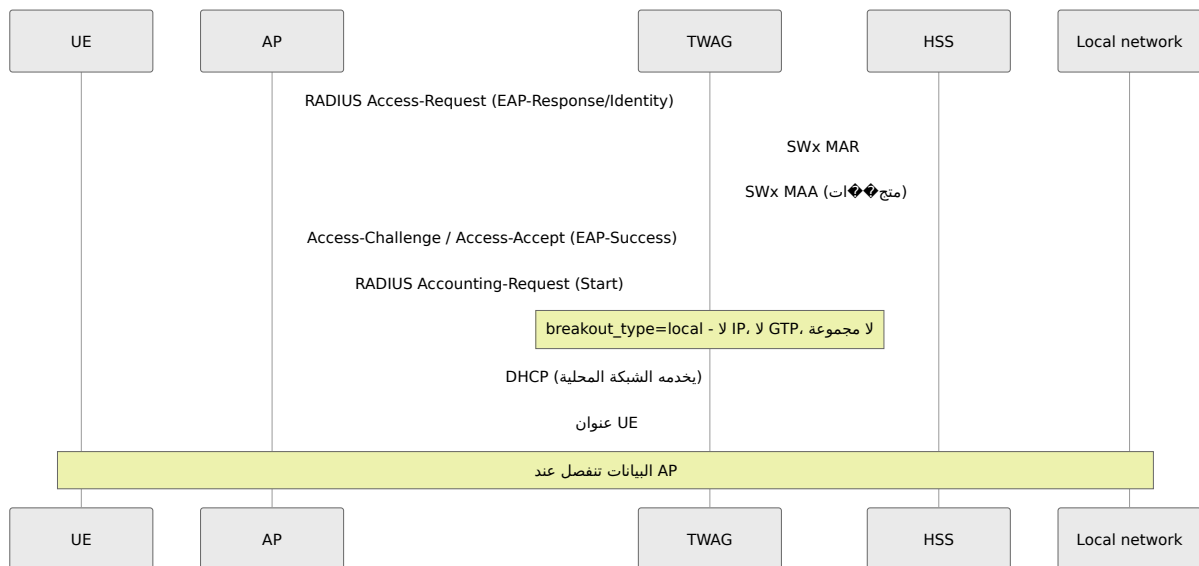


MAC يربط TWAG يقوم ، `address_source: dhcp` و `breakout_type: nswo` بالنسبة لـ بتوزيع العنوان المجاني التالي من نطاق المجموعة عندما DHCP العميل بالمجموعة. يقوم خادم IP. انظر مجموعة UE DISCOVER. يرسل



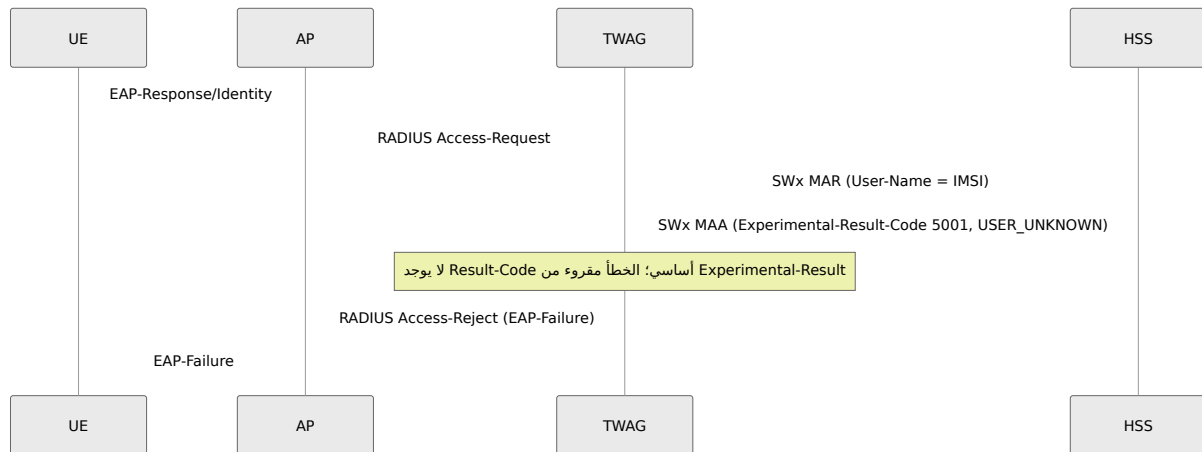
AP (طائرة بيانات) الاتصال - كسر محلي

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



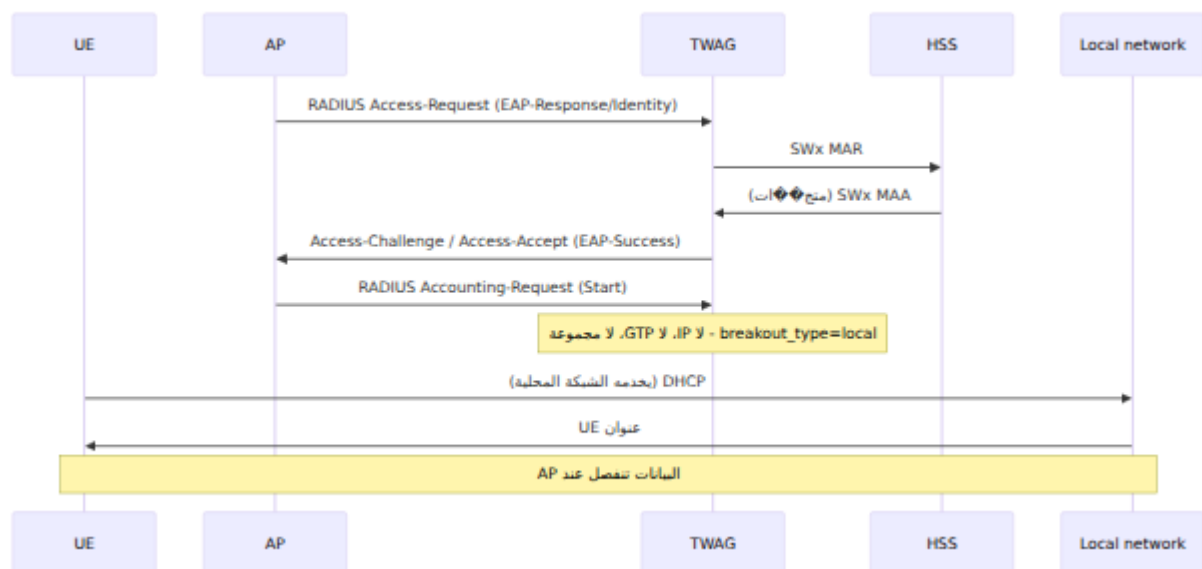
فشل المصادقة - المشترك غير مزود لـ SWx

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



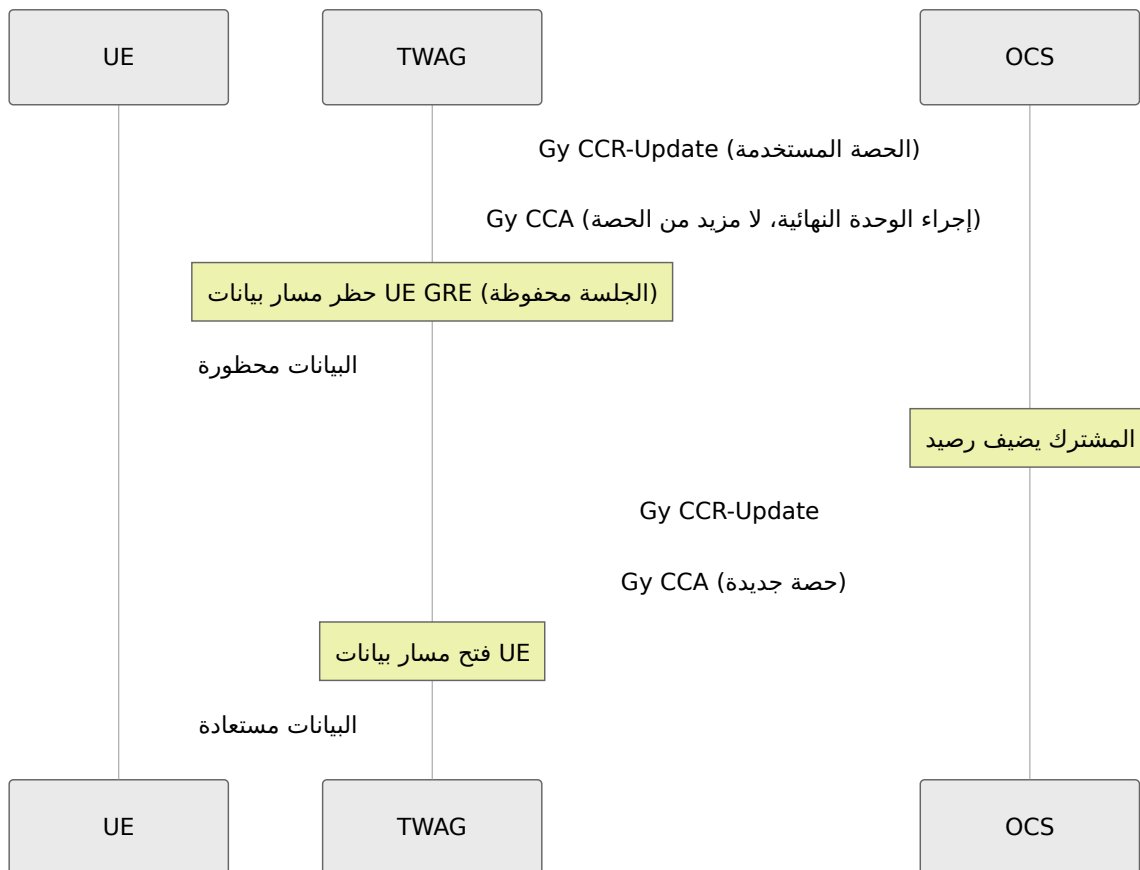
المحاسبة وإبلاغ الاستخدام

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



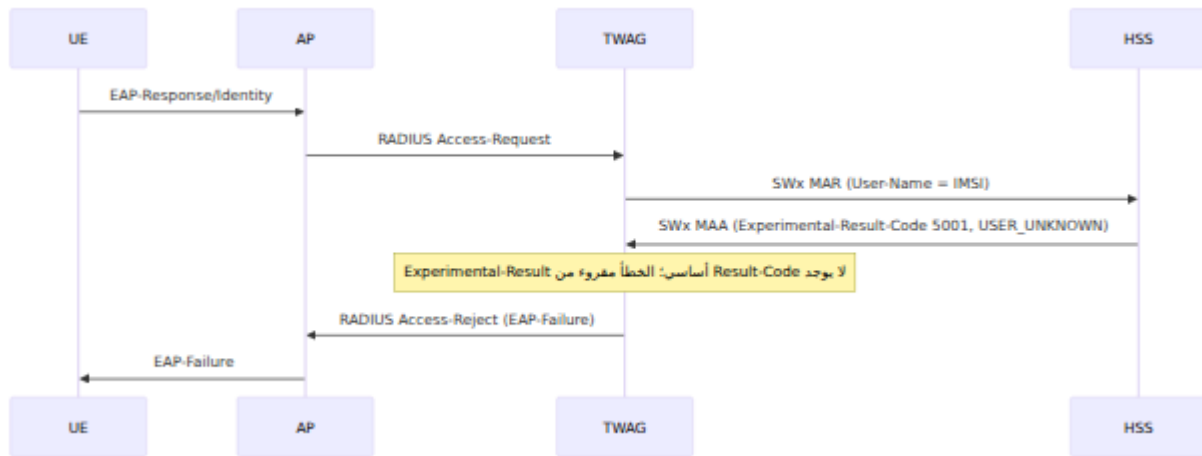
نفاذ الحصة وإعادة المنح

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



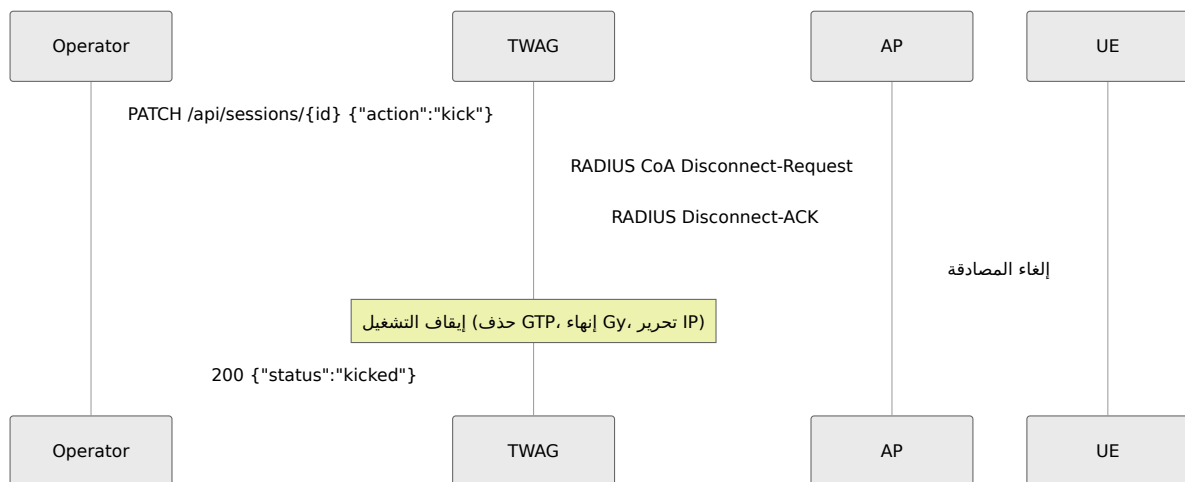
إيقاف التشغيل - فصل المشترك

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



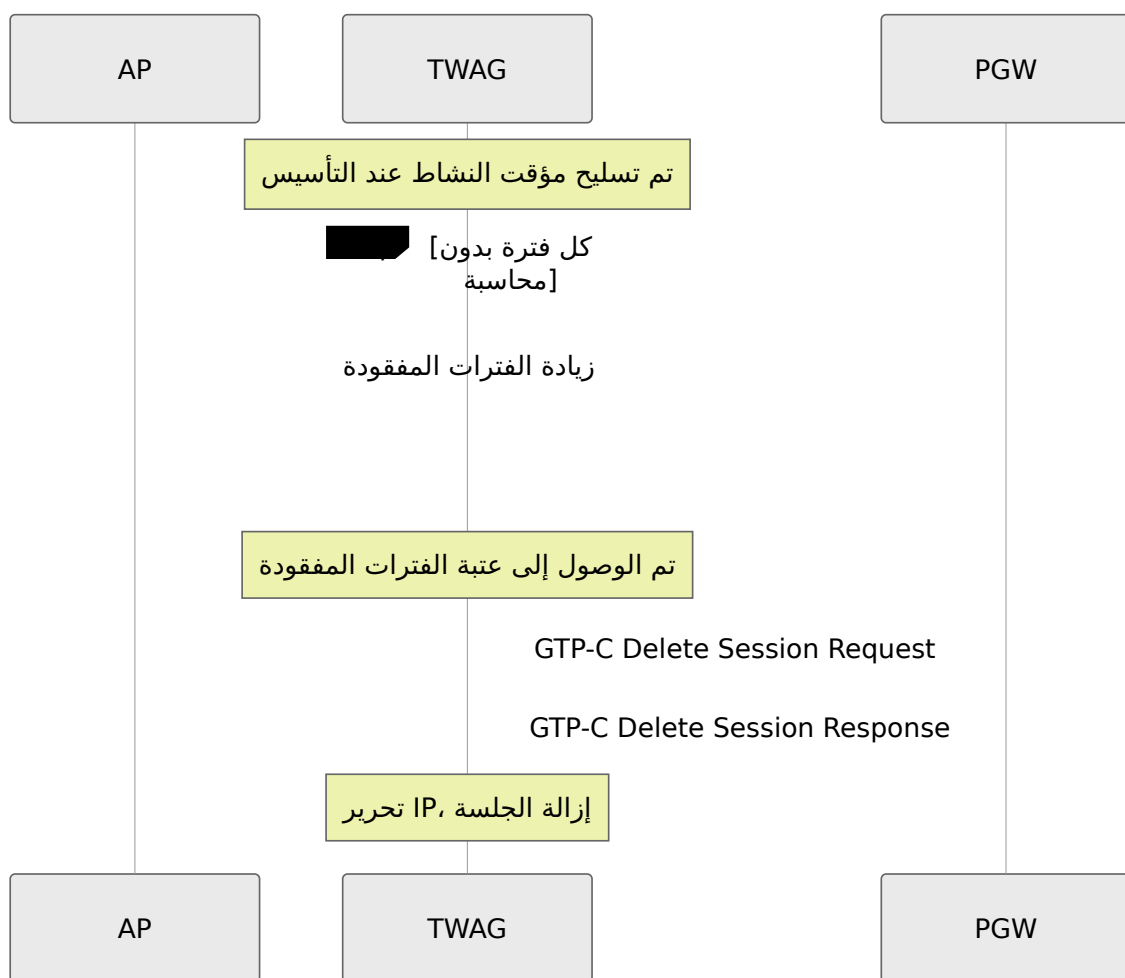
إيقاف التشغيل - طرد المشغل من واجهة برمجة التطبيقات

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



إيقاف التشغيل - مهلة النشاط

جلسة قائمة مع مؤقت نشاط. تعيد تحديثات المحاسبة المؤقتة تعيين المؤقت. إذا لم TWAG يراقب 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**.

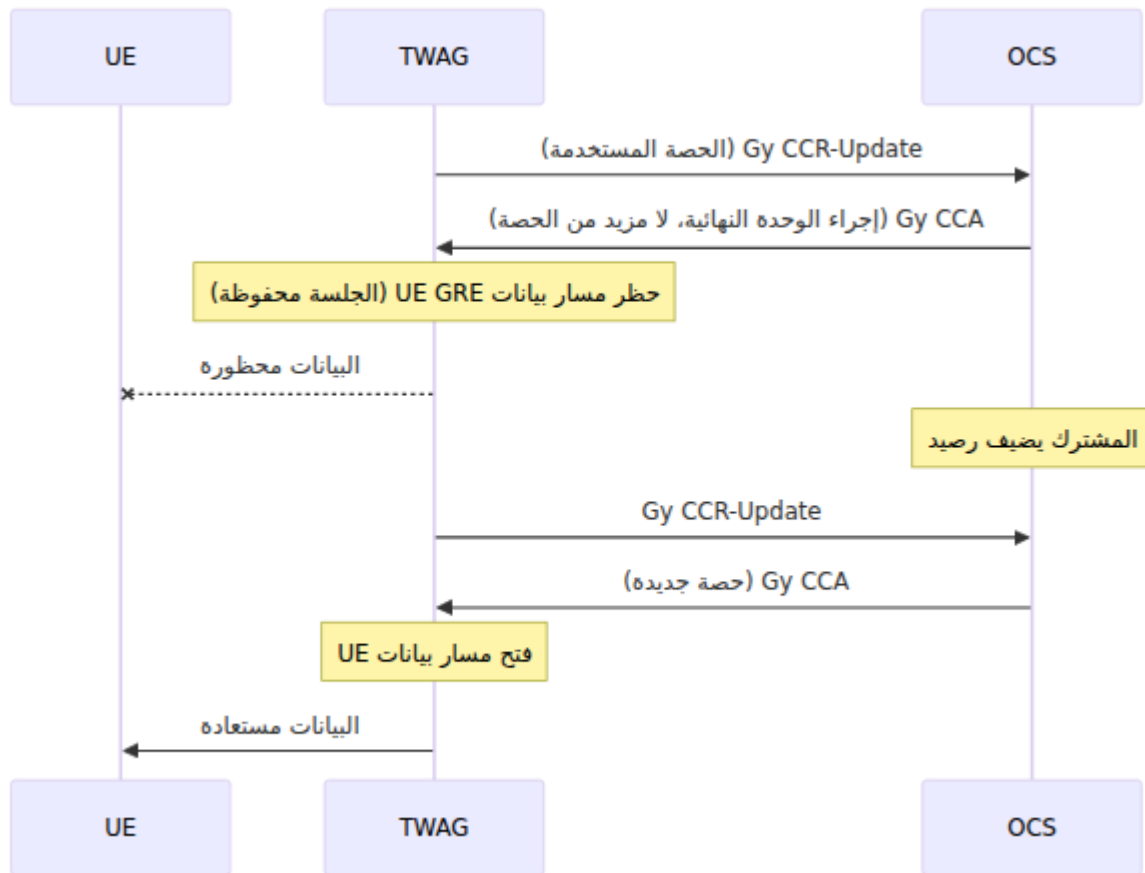


متغيرات وضع الشحن

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

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

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



نظرة عامة

WLC، أوضاع الاتصال والتنقل

نظرة عامة

وسلوك WLAN (WLC)، وبروتوكول التحكم في TWAG، تشرح هذه الوثيقة أوضاع اتصال 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.

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

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

جدول المحتويات

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

نظرة عامة ومقارنة الأوضاع

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

الخاصية	TSCM	SCM	MCM
رمز الوضع	0	1	2
الاسم الكامل	وضع الاتصال الفردي الشفاف	وضع الاتصال الفردي	وضع الاتصال المتعدد
UE لكل PDN اتصالات	واحد	واحد	عدة
IP تسليم عنوان	DHCP	EAP	EAP / WLCP
بالإشارة APN اختيار 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.

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

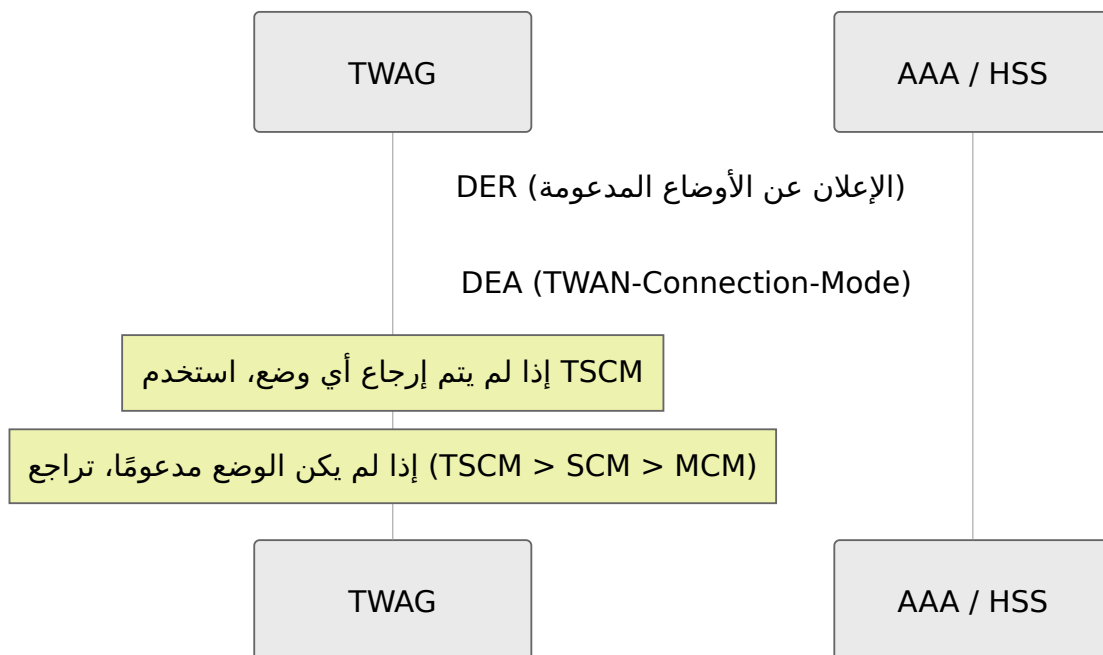


التفاوض على الوضع

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

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

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



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

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

أي شيء DEA عندما لا يحمل TSCM.

الحالة: الوضع المتفاوض عليه غير مفروض على مسار الجلسة الحية. يقوم عميل ويقرأ الوضع المتفاوض عليه من DER بالإعلان عن الوضع المدعوم في (StaClient) STa ليس STa وحدة وضع الاتصال موجودة وتم اختبارها. ومع ذلك، فإن مسار المصادقة عبر DEA. الحي، والعميل الحي لا يطبق أبدًا الوضع المتفاوض علي **❖❖**: RADIUS مسار المصادقة 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 TSCM اليوم، تتبع كل جلسة حية مسار (APN أو UE). انظر **حالة التنفيذ**.

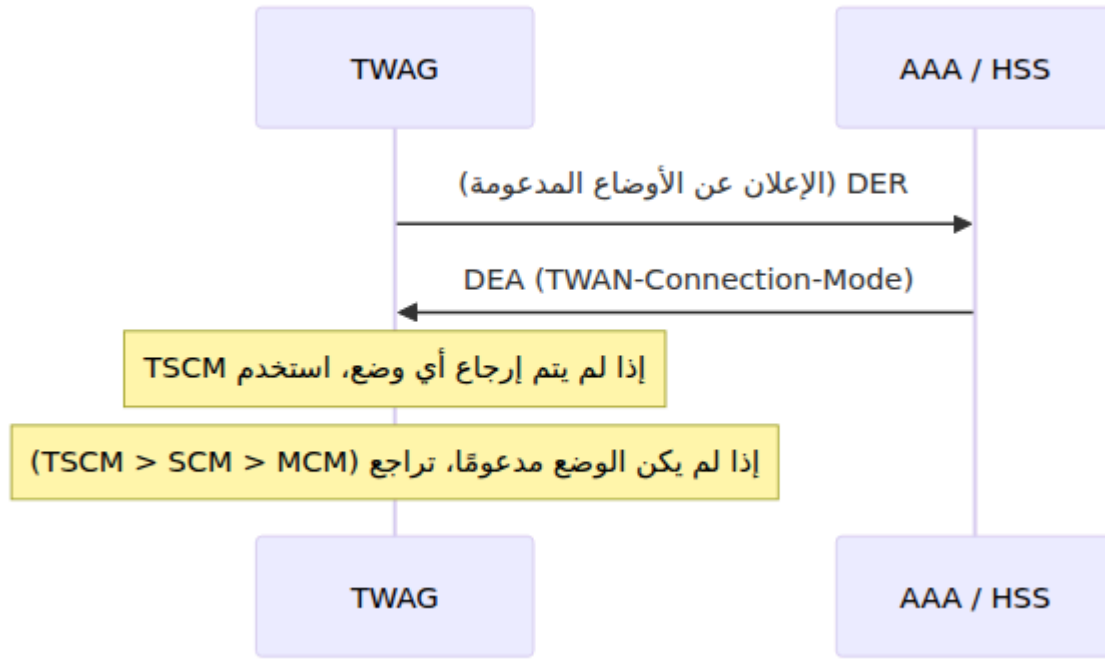
(TSCM) وضع الاتصال الفردي الشفاف

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

TSCM في:

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

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



(SCM) وضع الاتصال الفردي

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

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

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

موجود، لكن كود SCM ليس بعد مسار تشغيل متميز. نموذج القدرة لـ **SCM: الحالة** في SCM 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 في هذا الإصدار SCM لـ UE بالإشارة من APN أو اختيار EAP المقدم عبر IP.

WLCPP و (MCM) وضع الاتصال المتعدد

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

WLCPP نقل

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

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

WLCPP تنسيق رسالة

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

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

له هذا التنسيق IE كل

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

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

WLCF أنواع رسائل

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

WLCF عناصر معلومات

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	IPv4، IPv6، أو IPv4v6) UE المخصص لـ IP عنوان
0x05	الحامل QoS	QCI و MBR / GBR قيم
0x06	TFT	نموذج تدفق البيانات
0x07	السبب	قيمة سبب النتيجة
0x08	معرف الحامل	EPS (EBI) هوية الحامل
0x09	DNS عنوان	DNS عنوان أو أكثر من عناوين خادم

WLCP قيم سبب

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

PDN إعداد اتصال

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

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



PDN إنهاء اتصال

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

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

WLCPP اشتقاق مفتاح

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

$$K_WLCPP = \text{HMAC-SHA-256}(\text{MSK}, \text{FC} \parallel \text{P0} \parallel \text{L0})$$

FC = 0x21

P0 = IPv6 بايت لـ 16، IPv4 بايت لـ 4 TWAG لـ IP عنوان

L0 = big-endian بايت، بنظام 2 P0 طول

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 معروفاً بعد.

WLCPP وخادم WLCPP جزئيان وغير مدمجين. يوجد كود ترميز WLCPP و MCM: الحالة 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:

- العادي UDP يتم التعامل فقط مع WLCPP لـ DTLS حماية.
- لكن TFT IEs و QoS يحمل الترميز قيم MCM. إدارة الحامل المخصص داخل PGW. المعالج لا يتصرف على إنشاء الحامل المخصص الذي بدأه.
- MCM الانتقال داخل.
- يتم تعريف رسالة إشعار بيانات الاتجاه النزولي في الترميز ولكن لا يتم توليدها بواسطة معالج الجلسة.

كمعينة. لا تقم بتمكينه لأجهزة الإنتاج MCM اعتبر

الانتقال والتنقل

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

WiFi الاتصال عبر

OnWLAN

إلى WLAN الانتقال من
حذف الحامل، 3GPP (PGW،
RAT تغيير)

إلى 3GPP الانتقال من 3
HI=1 إنشاء جلسة WLAN
إنهاء الجلسة

LTE

المسار الحي اليوم:
فقط AP التجوال بين
RAT وتغيير HI=1
الفرع غير
يتم استخدامه عند الإرفاق

S2a نفق) AP التجوال بين
(محفوظ

WLAN إلى 3GPP الانتقال من 3

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

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

الحالة: المسار الرئيسي للجلسة لا يضبط علم الانتقال. دائماً 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 3GPP في الانتقال من 3 IP الحفاظ على الإصدار.

3GPP إلى WLAN الانتقال من 3

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

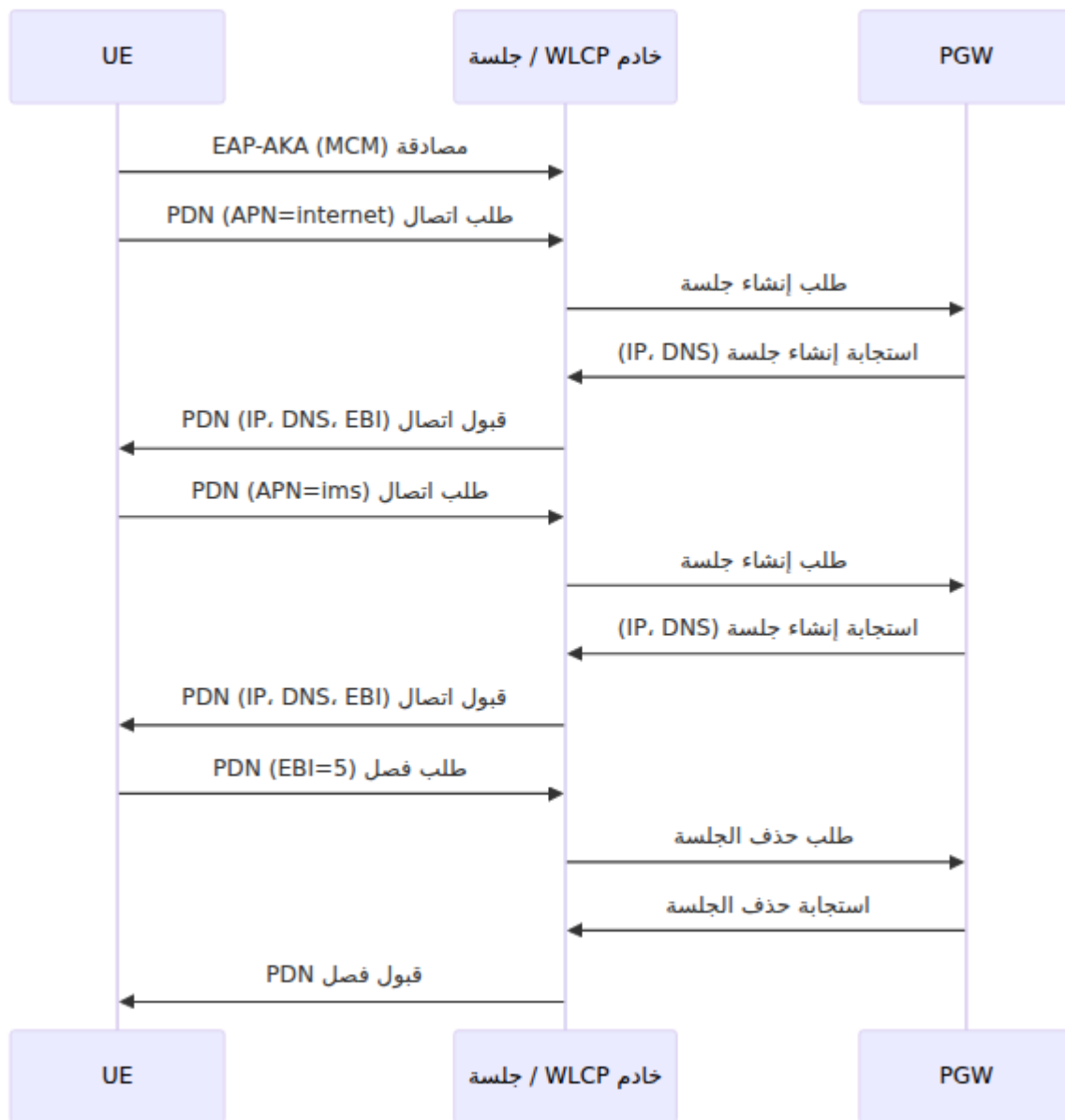
الاسم	رمز السبب
(GPP إلى غير 3 GPP من 3) RAT تم تغيير	4
ISR إلغاء تفعيل	5
GPP إلى 3 GPP تم تغيير الوصول من غير 3	10

محلّيًا. 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، GTP-C جلسة LTE.

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

AP التنقل بين

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 AP عبر تغيير UE الخاص بـ IP استقرار عنوان.



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

التكوين

أوضاع الاتصال

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

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

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

الوضع STa **ملاحظة**. يتم قراءة المجموعة المعلنة بواسطة وحدة وضع الاتصال ويرسل عميل 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)

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

```
config :omnitwag,  
  wlcp: %{\br/>    enabled: true,  
    port: 2156,  
    allowed_apns: :all  
  }
```

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

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

التكوين ذي الصلة

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

الرؤية

ومعالجات **❗❗** لجلسة أحداثًا تتعلق بالقياس. تغذي هذه الأحداث خط أنابيب WLCP يصدر خادم القياسات `latalog` بالقياس. انظر **القياسات** لك

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

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

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.

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

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

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

نظرة عامة

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

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

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

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

جدول المحتويات

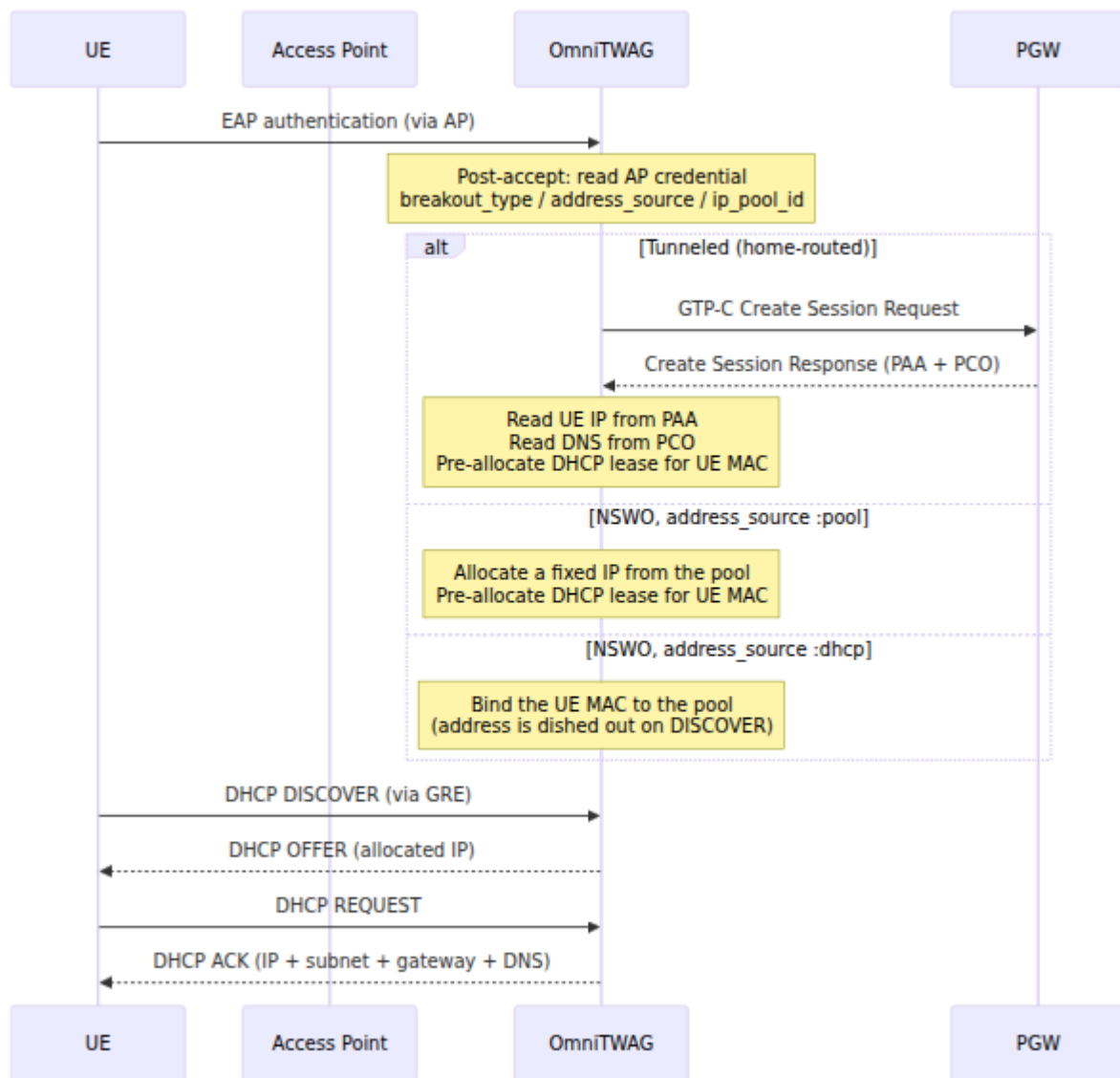
- **نظرة عامة: من يخصص العنوان**
- **مصادر العنوان**
- **PGW الجلسات النفقية: عنوان مخصص من**
- **dhcp المجموعة و: NSWO جلسات**
- **DHCPv4**
- **DHCPv6**

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

نظرة عامة: من يخصص العنوان

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

per-UE يقوم عملية جلسة، 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, :nswو, أو :local.
- address_source: :pool أو :dhcp. ينطبق هذا فقط عندما يكون breakout_type هو :nswو.

الوضع	بيانات الاعتماد	UE من يختار عنوان	كيف يصل إلى UE
نفق (موجه منزلي)	breakout_type: :tunneled	PGW، في استجابة GTP-C إنشاء جلسة PAA.	DHCPv4 عقد إيجار مسبق، DHCPv6، أو IPv6 RA.
NSWO، ثابت	breakout_type: :nswو، address_source: :pool	OmniTWAG، من مجموعة عند ، ip_pool_id إنشاء.	DHCPv4 عقد إيجار مسبق.
NSWO، توزيع	breakout_type: :nswو، address_source: :dhcp	OmniTWAG، من مجموعة عند ، ip_pool_id DISCOVER.	توزيع مجموعة عند DHCPv4 DISCOVER.
AP محلي	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 IP. لمتجر المجموعة، انظر **مجموعات RADIUS اعتماد**.

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 PGW يجب GTP-C. الفرعي:

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

OmniTWAG أي عنوان تقدمه PAA يحدد نوع

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

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

dhcپ المجموعة و: NSWO جلسات

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

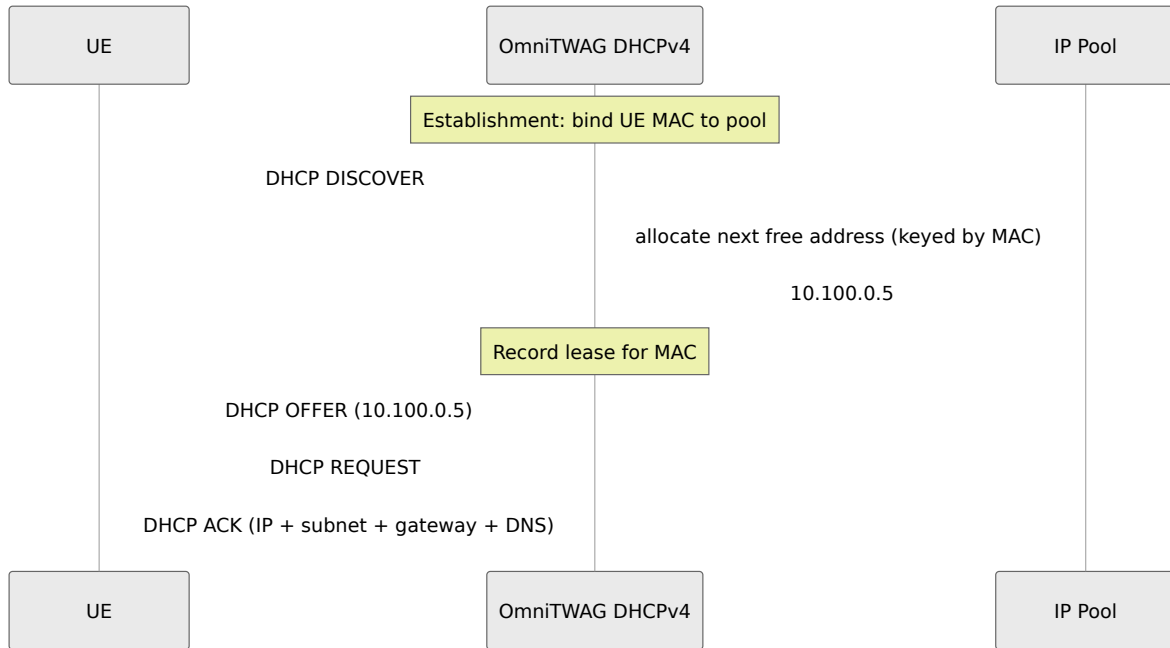
UE في بيانات الاعتماد كيفية وصول عنوان المجموعة إلى address_source يحدد حقل

(ثابت) pool : address_source

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 UE في هذه المرحلة. عندما يرسل GRE في مسار بيانات UE بالمجموعة. كما تسجل DISCOVER، يقدم الخادم العنوان المخصص مسبقًا.

address_source: :dhcp (DISCOVER توزيع عند)

UE الخاص بـ MAC بتخصيص عنوان بعد. إنها ترتبط عنوان OmniTWAG عند الإنشاء، لا تقوم بتخصيص العنوان DHCPv4 يقوم خادم، MAC من ذلك DISCOVER DHCP 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 تخصيص عنوانه بنفسه UE بتخصيص أي عنوان ويتولى OmniTWAG فلا تقوم ، ip_pool_id

DHCPv4

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

- عنواناً PGW مسبق التخصيص. تقوم عملية الجلسة بإدراج عقد إيجار عندما يخصص (NSWO) بتخصيص عنوان ثابت من المجموعة OmniTWAG (نفق) أو عندما تقوم (address_source: :pool).
- تقوم ، address_source: :dhcp NSWO بالنسبة لـ . DISCOVER توزيع عند 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 مرتبط 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 DISCOVER المرتبط، يقوم الخادم بإنشاء عقد الإيجار عند MAC المطلوب. بالنسبة لعنوان MAC . عن طريق توزيعه من المجموعة

```
Parse error on line 2: ...te (PGW PAA or pool :pool) [*] --> B -----^
Expecting 'SPACE', 'NL', 'HIDE_EMPTY', 'scale', 'COMPOSIT_STATE',
'STRUCT_STOP', 'STATE_DESCR', 'ID', 'FORK', 'JOIN', 'CHOICE', 'CONCURRENT',
'note', 'acc_title', 'acc_descr', 'acc_descr_multiline_value', 'CLICK', 'classDef',
'style', 'class', 'direction_tb', 'direction_bt', 'direction_rl', 'direction_lr',
'EDGE_STATE', got 'DESCR'
```

المحاولة مجددًا

DHCP مع هذه الأنواع من رسائل OmniTWAG تتعامل

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

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

محتويات عقد الإيجار

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

وقت `expires_at` ووقت `allocated_at` كما يحتوي سجل عقد الإيجار على 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 ولا ينتهي أبدًا. يتم `expires_at` عقد الإيجار الذي لديه مدة إيجار صفر ليس لديه `expires_at`. أيضًا إزالة عقد الإيجار عند إنهاء الجلسة.

في الرد DHCP خيارات

DHCP مع هذه الخيارات ACK و OFFER كل OmniTWAG تبني

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

GRE عبر DHCP نقل

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

إذا UDP على مقبس (GRE ليس عبر) UDP يصل مباشرة إلى مقبس DHCP يتم الرد على طلب ترد على عنوان المصدر OmniTWAG لم يكن منفذ المصدر هو منفذ العميل القياسي [68]، فإن RFC OmniTWAG 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: 2131 ciaddr إذا تم تعيين هذا العنوان.

DHCPv6

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

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

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

DHCPv6 معالجة رسائل

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

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

DUID الخادم

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

في الرد DHCPv6 خيارات

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

IPv6 (SLAAC) إعلان موجه

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

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

- على مؤقت دوري. الفاصل الزمني الافتراضي هو 30 ثانية.
- على واجهة RA عند الطلب، عندما تطلب طائفة التحكم.

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

محتويات إعلان الموجه

يحمل كل إعلان موجه هذه الحقول والخيارات

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

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

PCO و DNS تسليم

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

PGW من PCO

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

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

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 MTU و DNS IPv4 على سبيل المثال خوادم PGW، أن تعيدها OmniTWAG تريد.

UE إلى DNS تسليم

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

النقل	DNS مصدر	الملاحظات
DHCPv4 (الخيار 6)	DNS IPv4 خوادم من PCO.	تستخدم DNS IPv4 خادم PCO إذا لم يكن لدى OmniTWAG 8.8.8.8.
DHCPv6 (الخيار 23)	DNS قائمة خادم DHCPv6.	أو من PCO PGW يتم تعيينها من Google الافتراضي هو .dhcprv6_dns_servers إذا لم يتم تعيينها Public DNS IPv6.
RA IPv6 (RDNSS، الخيار 25)	DNS IPv6 خوادم المرتبطة بالبادئة المعلنة.	يتم تسليم ❖❖ مع البادئة

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

لا تضيف مسارات PGW من P-CSCF عناوين PCO يقرأ محلل **P-CSCF ملاحظة حول** P- يتم تحليل قيم RA. أو خيار DHCP P-CSCF الحالية خيار RA و DHCPv6 و DHCP تسليم من خلال هذا النظام الفرعي في الشيفرة UE وتكون متاحة، لكنها لا تُسلم إلى CSCF 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 يخصه OmniTWAG تقوم أي عنوان، وتقوم UE فلا يتلقى، PGW PAA نطاق محلي للاستنفاد. إذا لم يعد بتسجيل الحالة OmniTWAG.
- محلية، لذا يمكن أن تنفذ IP بالتخصيص من مجموعة OmniTWAG تقوم **NSWO**. لا يزيد عن 30/. يتخطى المخصص عناوين IPv4 CIDR مجموعة. المجموعة هي الشبكة والبيث ويعطي أول مضيف مجاني. عندما يكون كل مضيف قيد الاستخدام، يعود بعد UE يقوم ، pool: address_source: بالنسبة لـ .pool_exhausted المخصص يذهب ، dhcp: address_source: ذلك بتخصيص عنوانه بنفسه. بالنسبة لـ 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 IP مجموعات.

بإجراء الرياضيات الخاصة بالشبكة للمنصة. تقوم بتحليل سلاسل Twag.Cidr تقوم المساعدة هذه المساعدة RADIUS وتختبر ما إذا كان العنوان داخل شبكة. يستخدم نظام IPv6 و IPv4 CIDR للاشتقاق من قناع الشبكة للمجموعة، ونطاق IP المصدر. يستخدم متجر مجموعة IP لتفويض المضيف القابل للاستخدام، والبوابة الافتراضية.

التكوين

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

```
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
},

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

DHCPv4 (dhcp) معلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
<code>enabled</code>	Boolean	لا	<code>true</code>	تمكين خادم DHCPv4. تعيينه إلى <code>false</code> لتعطيله، على سبيل المثال في بيئة اختبار.
<code>interface</code>	String	لا	<code>wlan0</code>	واجهة الشبكة لخدمة DHCP. <code>gre</code> استخدم لوضع نفق GRE.
<code>server_ip</code>	String	لا	<code>10.0.0.1</code>	معرف خادم DHCP. ترسل OmniTWAG هذه القيمة في خيار DHCP 54 وك مصدر للردود المغلفة بـ GRE.
<code>default_lease_time</code>	Integer	لا	<code>3600</code>	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 (DHCP خيار 3).

RA IPv6 (ipv6_ra) معلمات

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

(المستوى الأعلى) DHCPv6 معلمات

وصف	الافتراضي	مطلوب	النوع	المعلمة
يحدد خوادم DNS IPv6 التي يمكن استخدامها في وقت التشغيل. إذا لم يتم تحديدها، تتجاهل OmniTI الخيار.	Google Public DNS IPv6 (2001:4860:4860::8888, 2001:4860:4860::8844)	لا	قائمة من String	dhcpcv6_dns_servers
يحدد خوادم DNS IPv6 التي يمكن استخدامها في وقت التشغيل. إذا لم يتم تحديدها، تتجاهل OmniTI الخيار.	(غير محدد)	لا	قائمة من String	dhcpcv6_domain_list

الرؤية

واجهة الويب

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

REST واجهة برمجة التطبيقات

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

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

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

يحتوي كل كائن عقد إيجار على هذه الحقول

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

أحداث القياس

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

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

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

استكشاف الأخطاء وإصلاحها

IP على عنوان UE لا يحصل

DHCP تظهر صفحة مجموعة IPv4 بالمصادقة ولكنه لا يحصل على عنوان UE **الأعراض**: يقوم [:dhcp, :discover, :no_allocation] يتم إطلاق حدث UE الخاص بـ MAC عدم وجود إيجار لعنوان [:dhcpv6, :solicit, :received].

الأسباب المحتملة (التفوق):

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

(NSWO) الأسباب المحتملة

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

السبب الشائع:

- غير قيد التشغيل DHCPv4 خادم .

الحل:

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

DNS على عنوان ولكن لا يوجد UE يحصل

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

الأسباب المحتملة

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

الحل:

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

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

UE NAK يتلقى

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

الأسباب المحتملة:

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

الحل:

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

الصفحات ذات الصلة

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

نظرة عامة

IP مجموعات

نظرة عامة

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

لذا تبقى المجموعات، DETS، بتخزينها في ملف OmniTWAG تعريفات المجموعات دائمة. تقوم بإعادة بناء OmniTWAG 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
- REST واجهة برمجة التطبيقات
- واجهة الويب
- استكشاف الأخطاء وإصلاحها

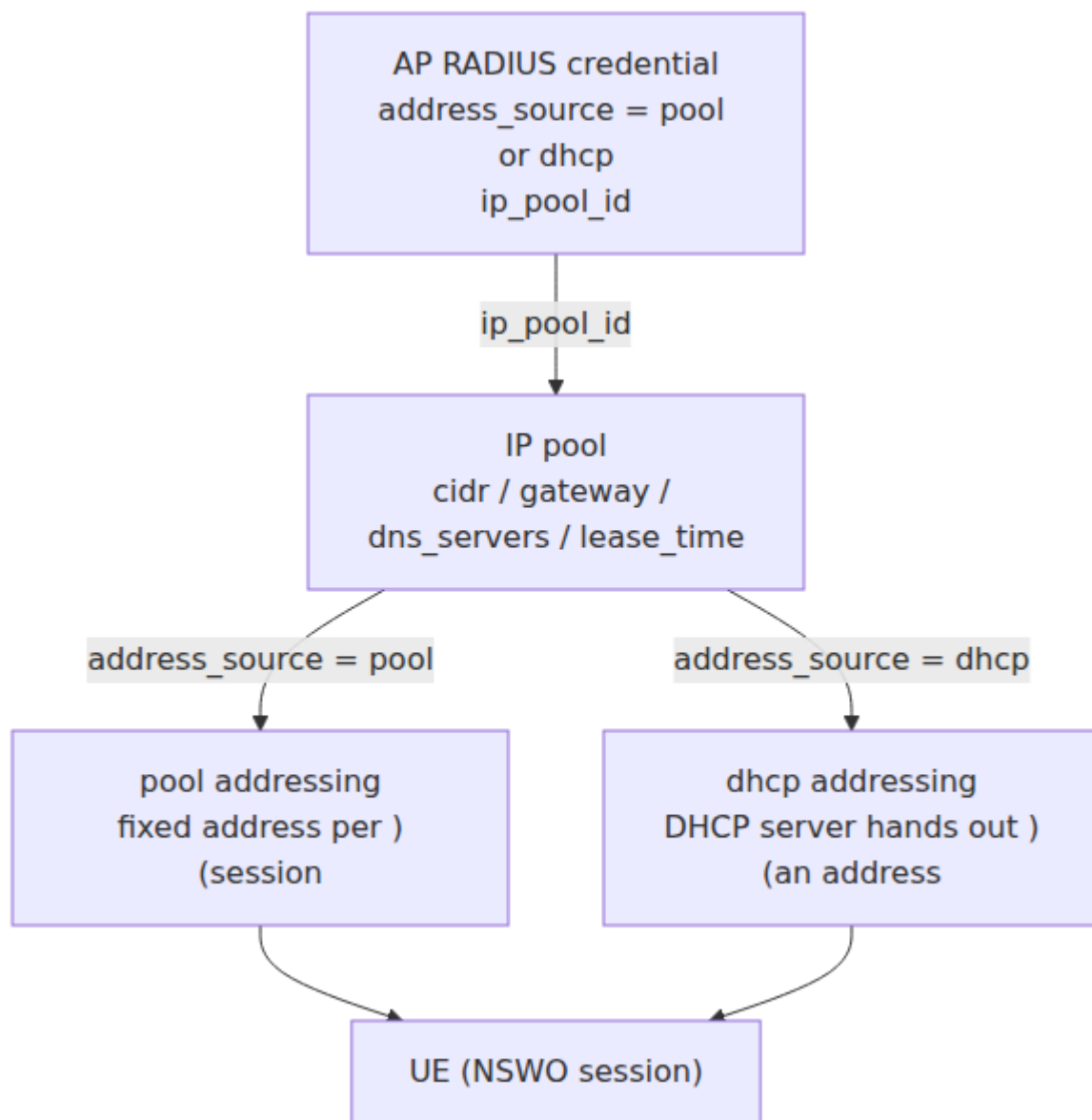
المفاهيم

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

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

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

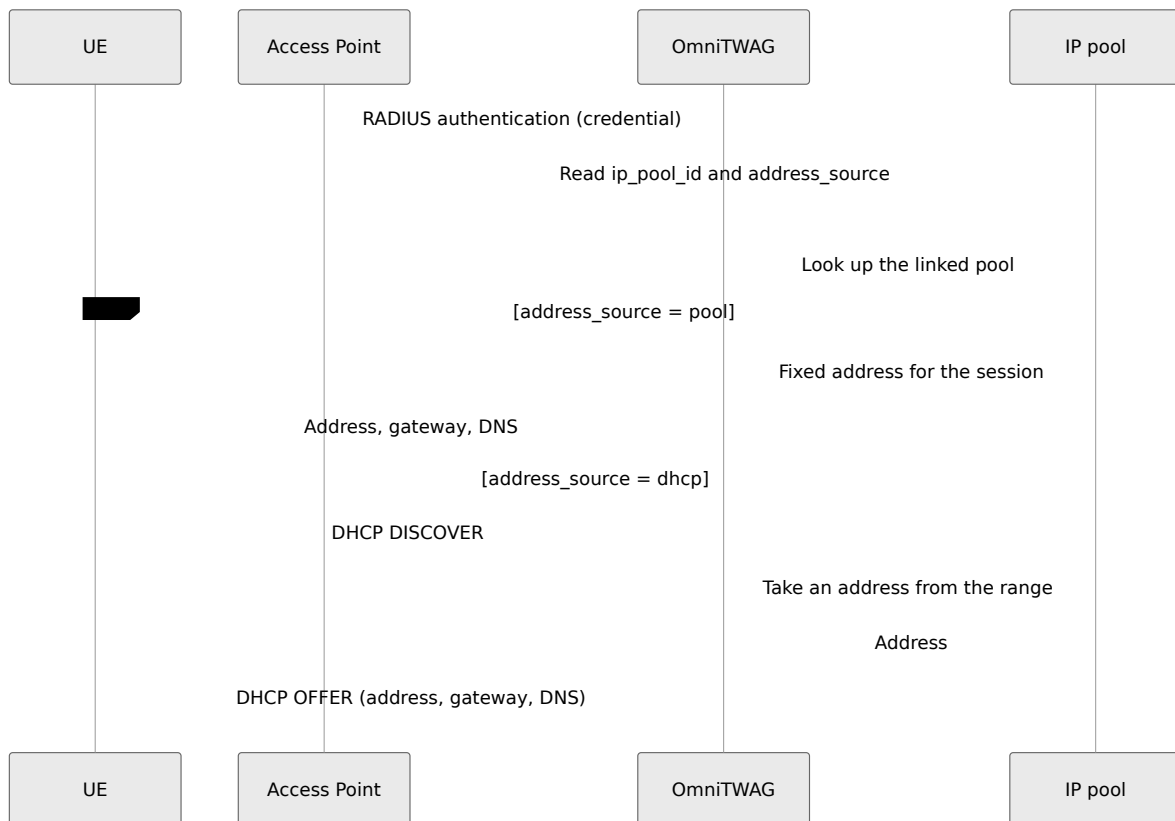
مصدر العنوان	السلوك
pool	بتخصيص عنوان ثابت لكل جلسة من المجموعة. يتم OmniTWAG تقوم اختيار العنوان عند إعداد الجلسة.
dhcp	بتوزيع عنوان من نطاق المجموعة OmniTWAG الخاص بـ DHCP يقوم خادم من جهاز المستخدم يستخدم DHCP DISCOVER ردًا على



كيفية حصول الجلسة على عنوان

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

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



تخصيص العنوان

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

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

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

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

نموذج المجموعة

تحتوي كل مجموعة على هذه الحقول

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

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

REST واجهة برمجة التطبيقات

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

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

جسم الطلب

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

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

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

الاستجابات

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

مثال: قائمة المجموعات

الطلب:

```
GET /ip_pools
```

الاستجابة:

```
{
  "count": 1,
  "ip_pools": [
    {
      "id": "0d1e2f3a-4b5c-6d7e-8f90-1a2b3c4d5e6f",
      "name": "ضيوف ملبورن WiFi",
      "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 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
}
```

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

صغير جدًا CIDR: مثال

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

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

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،

بمسح العلامة على المجموعة الافتراضية السابقة OmniTWAG تقوم

أو، (PGW (tunneled يظهر الإيجار: IP تسجل كل إيجار نشط مصدره. انظر عرض **إيجارات** مسماة، أو المجموعة الافتراضية NSW0 مجموعة

واجهة الويب

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

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

استكشاف الأخطاء وإصلاحها

استنفاد مجموعة

الجديدة من نقطة الوصول الحصول على عنوان. تعيد NSW0 **الأعراض**: لا يمكن لجلسات OmniTWAG pool_exhausted.

الأسباب المحتملة:

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

الحل:

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

نقطة الوصول لا تستخدم مجموعة

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

الأسباب المحتملة:

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

الحل:

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

جهاز المستخدم لا يحصل على عنوان

IPv4. الأعراض: يتصل جهاز المستخدم ولكن لا يتلقى عنوان

الأسباب المحتملة:

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

الحل:

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

نظرة عامة

TWAG مرجع مقاييس

نظرة عامة

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

جدول المحتويات

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

نقطة نهاية المقاييس

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

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

RADIUS مقاييس مصادقة

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

الوصف	التسميات	النوع	المقياس
حزم طلب الوصول RADIUS المستلمة.	لا شيء	عداد	radius_access_request_count
حزم قبول الوصول RADIUS المرسل (مصادقة ناجحة).	لا شيء	عداد	radius_access_accept_count
حزم رفض الوصول RADIUS المرسل (فشل المصادقة).	لا شيء	عداد	radius_access_reject_count
حزم تحدي الوصول RADIUS المرسل (جاري EAP تبادل).	لا شيء	عداد	radius_access_challenge_count

استعلامات مثال:

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

# EAP المفاوضات النشطة) معدل التحديات
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])))
```

ومعدل الحد RADIUS مقاييس تفويض

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

المقياس	النوع	التسميات	
<code>radius_auth_unauthorized_source_count</code>	عداد	<code>source</code>	عنوان مصدر الذي حاول غير الحزمة
<code>radius_auth_bad_secret_count</code>	عداد	<code>source,</code> <code>credential_id</code>	بيانات مصادقة فحص Messa (خاطئ)
<code>radius_access_rate_limited_count</code>	عداد	<code>nas_ip</code>	سقاطها لأن 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]))

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

RADIUS مقاييس محاسبة

[RFC 2866](#) لكل من RADIUS تتبع رسائل محاسبة

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
```

EAP مقاييس

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

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

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

استعلامات مثال:

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

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

# (يجب أن تبقى ثابتة) EAP أعطال معالجة
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
<code>radius_active_clients_count</code>	مقياس	لا شيء	العملاء الذين تم مصادقتهم عمليات) حاليًا <code>Twag.Session.Client</code> (الحية).
<code>radius_access_points_count</code>	مقياس	لا شيء	نقاط الوصول المسجلة <code>APState</code> (مدخلات).
<code>radius_clients_per_ap_count</code>	مقياس	<code>nas_ip</code> , <code>ssid</code>	لعملاء المتصلين بكل نقطة وصول.
<code>radius_active_sessions_count</code>	مقياس	<code>status</code>	الجلسات مجمعة حسب <code>(start</code> , <code>stop</code> , <code>interim_update)</code> .
<code>radius_active_sessions_total</code>	مقياس	لا شيء	<code>start</code> الجلسات في حالة <code>interim_update</code> أو.

استعلامات مثال:

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

# SSID العملاء حسب
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

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

المقياس	النوع	الوحدة	الوصف
<code>radius_data_bytes_in</code>	مقياس	بايت	إجمالي البايتات المستلمة عبر الجلسات (Acct-Input-Octets).
<code>radius_data_bytes_out</code>	مقياس	بايت	إجمالي البايتات المرسله عبر الجلسات (Acct-Output-Octets).
<code>radius_session_total_time</code>	مقياس	ثواني	إجمالي وقت الجلسة عبر الجلسات (Acct-Session-Time).

استعلامات مثال:

```
# إجمالي التدفق بالميغا بايت
(radius_data_bytes_in + radius_data_bytes_out) / 1024 / 1024

# متوسط مدة الجلسة
radius_session_total_time / radius_active_sessions_total
```

ومسار البيانات TWAG مقاييس جلسة

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

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

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

استعلامات مثال:

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

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

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

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

عبر الإنترنت Gy مقاييس شحن

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

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

استعلامات مثال:

```
# حسب النوع CCR معدل إرسال
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]))
```

STa Diameter مقاييس

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

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 STa الجلسة.

Diameter مقياس رسالة

diameter_message_count

النوع: عداد

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

استعلامات مثال:

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

NSWO مقاييس

المقياس	النوع	الوصف
<code>nsw_allocate_count</code>	عداد	NSWO المحلية IP تخصيصات.
<code>nsw_release_count</code>	عداد	NSWO المحلية IP إصدارات.

DHCP مقاييس

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

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

استعلامات مثال:

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

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

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

IPv6 RA و DHCPv6 مقاييس

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

WLCAP مقاييس

المستخدم لوضع الاتصال المتعدد WLAN تتبع هذه العدادات بروتوكول التحكم في

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

Erlang VM مقاييس

BEAM تقدم هذه المقاييس رؤية إلى وقت تشغيل.

الذاكرة

المقياس	الوصف
vm_memory_total	إجمالي الذاكرة المخصصة (بايت).
vm_memory_processes	Erlang الذاكرة المستخدمة بواسطة عمليات
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	حالة الجلسة) ETS الذاكرة المستخدمة بواسطة جداول (ونقطة الوصول

النظام

المقياس	الوصف
vm_system_info_process_count	Erlang العدد الحالي لعمليات
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
<code>vm_statistics_run_queue</code>	إجمالي طول قائمة التشغيل.
<code>vm_total_run_queue_lengths_total</code>	إجمالي قائمة تشغيل المجدول.
<code>vm_total_run_queue_lengths_cpu</code>	CPU قائمة تشغيل المجدول.
<code>vm_total_run_queue_lengths_io</code>	IO قائمة تشغيل المجدول.

استعلامات مثال:

```
# إجمالي الذاكرة بالميغا بايت
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

```
# nas_ip: طلب الوصول ليس لديه تسمية) الطلبات حسب نقطة الوصول  
(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_tearardown_count[1h]))
```

استخدام البيانات

```
# إجمالي التدفق بالميغا بايت  
(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: "EAP-AKA تم الكشف عن فشل مزامنة"

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

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

```
- 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: "GB يتجاوز 1 TWAG استخدام الذاكرة في"

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

صفحات ذات صلة

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

- محاسبة لكل نقطة وصول

نظرة عامة

(Gy) الشحن عبر الإنترنت

نظرة عامة

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

NSWO مسار البيانات، أي TWAG ينطبق الشحن عبر الإنترنت على الجلسات التي يمتلك فيها 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، **(GTP) وضع التوجيه المنزلي** راجع مرجع **خطة المستخدم** لوضعية بيانات الطائرة. **disabled**: الشحن العالمي

معين UE تعمل لجهاز Gy تحدد تحكمان ما إذا كانت

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

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

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
- السلسلة التشغيلية ومعالجة الأخطاء
- قابلية المراقبة
- الجداول المرجعية

المفاهيم

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

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

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

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

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

أوضاع الشحن

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

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

:authorize_only

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

:online_charging

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

وضع الشحن لكل نقطة وصول

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

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

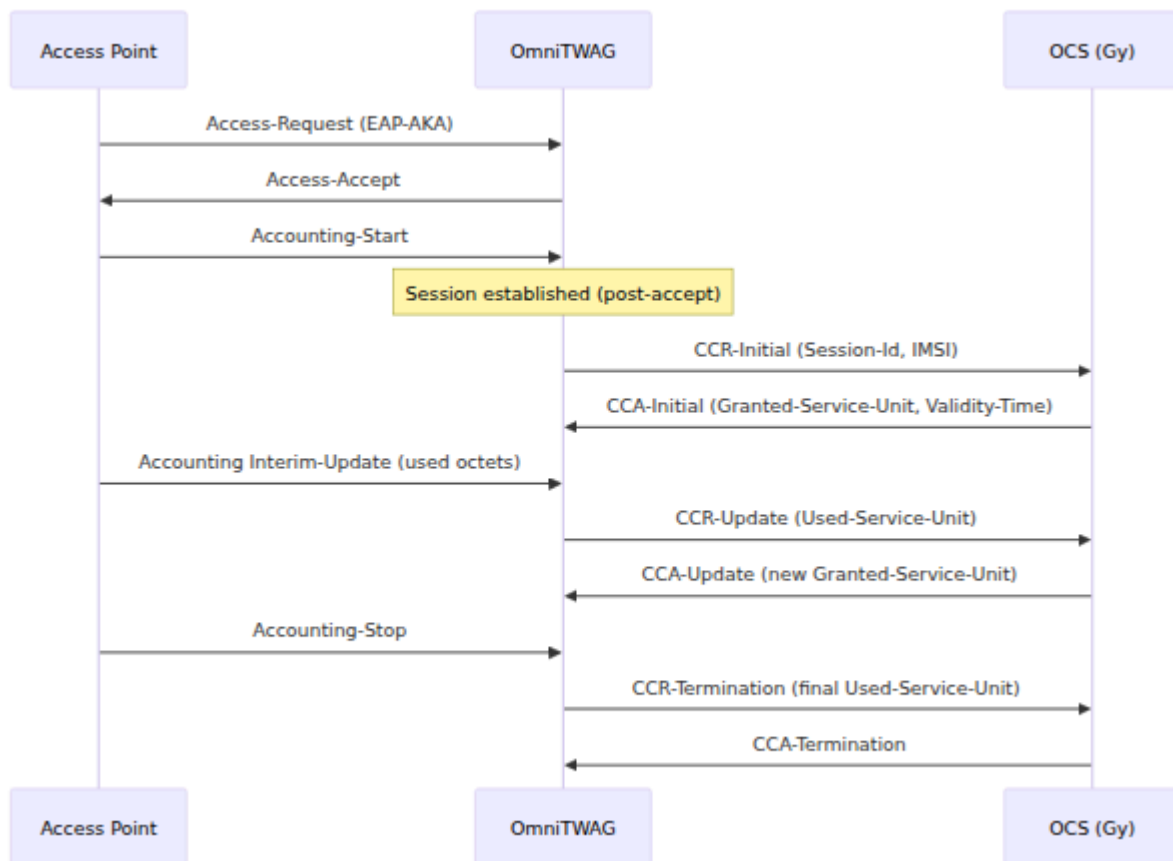
فقط عندما **تتحقق** جميع هذه الشروط OmniTWAG CCR-Initial يرسل

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

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

تدفق التحكم في الائتمان

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



بدء الجلسة (CCR-Initial)

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

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

التحديثات المؤقتة (CCR-Update)

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

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

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 أيضًا CCR-U تتضمن `Used-Service-Unit` AVP الجلسة من سمات المحاسبة ويبلغ عنها في `Requested-Service-Unit` من منح المزيد من الحصة OCS فارغ، حتى تتمكن

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

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

RADIUS سمة	Gy حقل
<code>Acct-Input-Octets</code>	<code>CC-Input-Octets</code>
<code>Acct-Output-Octets</code>	<code>CC-Output-Octets</code>
<code>Acct-Session-Time</code>	<code>CC-Time</code>

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

انتهاء الجلسة (CCR-Termination)

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

الحصة، الاستخدام، وإعادة التفويض

الحصة الممنوحة

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

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

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

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

الإبلاغ عن الاستخدام

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

إعادة التفويض

التفويض على مسارين OmniTWAG يعيد:

- 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.

- **Validity-Time** مؤقت صلاحية الحصة من OmniTWAG **على الوقت**. يشغل 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 يرسل المكونة. مع عدم وجود أي منهما، **quota.validity_time** العودة إلى OmniTWAG. لا يتم تشغيل مؤقت صلاحية.

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

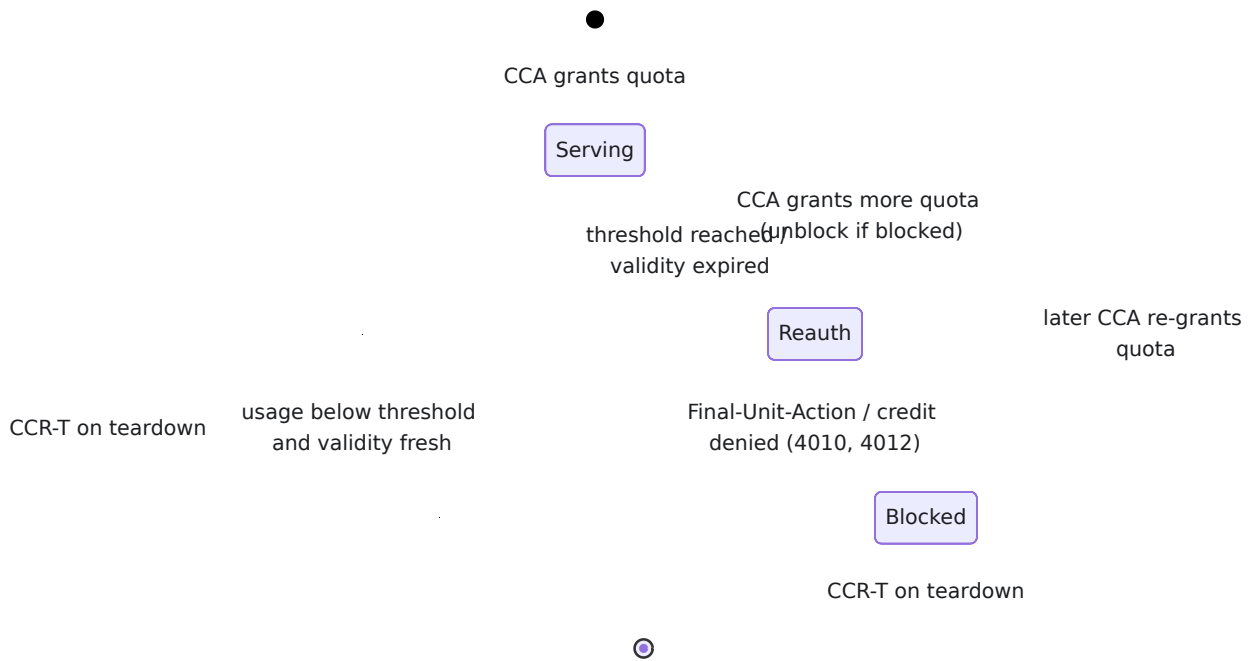
تنفيذ الحصة

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

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

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

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



الذي يفشل في طبقة CCR-U: التنفيذ هو جهد أفضل ويفشل في حالة الأخطاء في النقل 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

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

التكوين

online_charging في كتلة , omnitwag: قم بتعيين معلومات الشحن عبر الإنترنت تحت تطبيق من config/runtime.exs.

```
config :omnitwag,  
  online_charging: %{  
    # وضع الشحن العالمي :disabled, :authorize_only, أو  
:online_charging  
    mode: :disabled,  
  
    # 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,  
  
    # (online_charging: تستخدم في وضع) إدارة الحصص  
    quota: %{  
      # CCR-Update الكسر من الحجم الممنوح الذي يتم عنده تحفيز  
      update_threshold: 0.8,  
  
      # OCS وقت صلاحية النسخة الاحتياطية (بالثواني) عندما لا ترسل  
Validity-Time  
      validity_time: 3600  
    }  
  }  
}
```

المعلومات

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

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 **RADIUS** انظر **بيانات اعتماد AP**.

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

Ro وتطبيق Diameter نقل

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

```
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	-	خدمة يرسل طلبات
host	String	نعم	-	D هوية (host) Origin host
realm	String	نعم	-	المجال يستخدم Origin Destination م تعيين ocs_r
request_timeout	Integer	لا	5000	لانتظار ل على الطلب
application_name	Atom	نعم	-	تطبيق يته إلى
application_dictionary	Atom	نعم	-	قاموس يته إلى :dictionary Gy.
vendor_specific_application_ids	List	نعم	-	تحدد من البائع. vendor auth_4.

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

معلومات الند

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

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

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

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

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

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

ملخص دورة حياة جلسة التحكم في الائتمان

```
Parse error on line 2: ...arging: global mode :disabled OR AP char... -----
-----^ Expecting 'SPACE', 'NL', 'HIDE_EMPTY', 'scale', 'COMPOSIT_STATE',
'STRUCT_STOP', 'STATE_DESCR', 'ID', 'FORK', 'JOIN', 'CHOICE', 'CONCURRENT',
'note', 'acc_title', 'acc_descr', 'acc_descr_multiline_value', 'CLICK', 'classDef',
'style', 'class', 'direction_tb', 'direction_bt', 'direction_rl', 'direction_lr',
'EDGE_STATE', got 'DESCR'
```

المحاولة مجددًا

معالجة رمز النتيجة

رمز النتيجة على مستويين OmniTWAG يقرأ

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

قابلية المراقبة

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

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

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

الجداول المرجعية

CC-Request-Type قيم

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

RFC 4006 §8.3 تم تعريف القيم في

المستخدمة Reporting-Reason قيم

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

رمز النتيجة

الرمز	المستوى	الاسم	OmniTWAG سلوك	ج
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

Final-Unit-Action قيم

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

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

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

Diameter تطبيق

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

مراجع المواصفات

المواصفة	الموضوع
RFC 4006	Diameter تطبيق التحكم في الائتمان
3GPP TS 32.299	Diameter (Ro) تطبيقات الشحن
3GPP TS 32.240	بنية الشحن
3GPP TS 23.402	GPP (S2a, NSW0) الوصول غير 3 / TWAG
RFC 6733	الأساسي Diameter بروتوكول

الصفحات ذات الصلة

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

نظرة عامة

محاسبة لكل نقطة وصول

نظرة عامة

لكل نقطة وصول. يرى المشغل إجمالي الحركة وعدد RADIUS بيانات محاسبة OmniTWAG يجمع الجلسات لكل نقطة وصول. هذه البيانات منفصلة عن سجلات المحاسبة لكل جلسة. يقوم لنقطة الوصول. NAS-IP-Address بتجميع إجماليات كل نقطة وصول بواسطة OmniTWAG 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

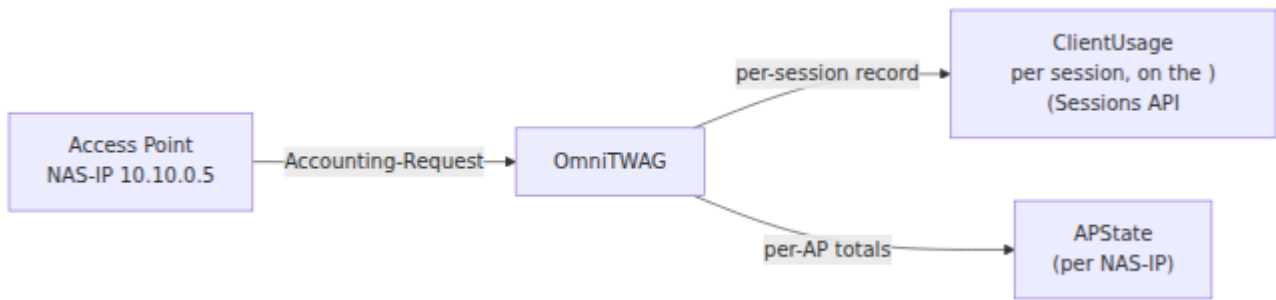
- المفاهيم
- كيفية حساب الإجماليات
- الحقول المسجلة
- عدد العملاء النشطين
- أي؟ يمكن رؤية البيانات
- العلاقة بالبيانات لكل جلسة
- استكشاف الأخطاء وإصلاحها
- صفحات ذات صلة

المفاهيم

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

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

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

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

توقفًا لجلسة لم يرها تبدأ، فإن عدد الجلسات النشطة لا ينخفض إلى أقل OmniTWAG إذا تلقى OmniTWAG يضيف الأوقات والحزم النهائية. إذا تلقى OmniTWAG من صفر. لا يزال 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.



Start (sessions_started
+1, active +1)

Active

Stop (sessions_stopped
+1, active -1, add
octets/packets)

Stopped

Interim-Update (time
only)



الحقول المسجلة

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

الوصف	النوع	الحقل
إجمالي الأوكتات المدخلة، المجمعة عبر الجلسات المتوقفة.	عدد صحيح	acct_input_octets
إجمالي الأوكتات الخارجة، المجمعة عبر الجلسات المتوقفة.	عدد صحيح	acct_output_octets
إجمالي الحزم المدخلة، المجمعة عبر الجلسات المتوقفة.	عدد صحيح	acct_input_packets
إجمالي الحزم الخارجة، المجمعة عبر الجلسات المتوقفة.	عدد صحيح	acct_output_packets
عدد الجلسات التي بدأت على هذه النقطة.	عدد صحيح	acct_sessions_started
عدد الجلسات التي توقفت على هذه النقطة.	عدد صحيح	acct_sessions_stopped
مقياس الجلسات المفتوحة المستمدة من لا تقل ، stopped ناقص started : المحاسبة أبدًا عن صفر. تعكس فقط ما تقارير المحاسبة لذلك يمكن أن تزيد عند فقدان نقطة ، RADIUS 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	عدد صحيح	acct_active_sessions
وقت آخر حزمة محاسبة، بالمللي ثانية منذ بداية Unix.	عدد صحيح	last_accounting_at

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 يتم اشتقاقها من عمليات الجلسات الحية في الذاكرة التي `acct_active_sessions` المحاسبة لنقطة الوصول `NAS-IP-Address` لكل عميل مصادق عليه، مجمعة حسب OmniTWAG يديرها.

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

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

أين يمكن رؤية البيانات

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

- كل `GET /access_points` تعيد نقطة النهاية: **REST واجهة برمجة التطبيقات** `GET` نقطة وصول مع حقول المحاسبة لكل نقطة وصول. تعيد نقطة النهاية الخاص `NAS-IP-Address` نقطة وصول واحدة بواسطة `/access_points/{id}` 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 وصول و `APState` عبارة عن تجميع. لكل طلب محاسبة OmniTWAG بكتابة سجلين:

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

- Acct- ومفاتيحها بواسطة ClientUsage **سجل لكل جلسة**، المحتفظ به في Session-Id. هذا هو عرض حركة المرور والمحاسبة الحية لكل مشترك، وهو .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 لمشارك 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 (المشاركة RADIUS **أسرار** المصدر لم IP لا تظهر نقطة وصول أبدًا إذا تم إسقاط حزمها لأن عنوان Accounting-Request. 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:

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

الحل:

1. OmniTWAG إلى Accounting-Request تأكد من أن نقطة الوصول ترسل حزم.
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. **المشاركة RADIUS المسجلة**. انظر **أسرار**.

يبدو أن عدد الجل؟؟ات النشطة مرتفع جدًا

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

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. الجلسات OmniTWAG قم بتعيين فترة تحديث مؤقت على نقطة الوصول، بحيث يرى النشطة.
3. يصحح العدد النشط نفسه مع وصول حزم التوقف الجديدة. لا ينخفض العدد إلى أقل من صفر.

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

لا تظهر نقطة الوصول

الأعراض: لا تظهر نقطة وصول ترسل المحاسبة في القائمة

الأسباب المحتملة:

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

الحل:

1. انظر مرجع `radius_auth_unauthorized_source_count` تحقق من مقياس RADIUS المقاييس ورفض.
2. المشتركة RADIUS أصف بيانات اعتماد لشبكة نقطة الوصول. انظر أسرار.

صفحات ذات صلة

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

نظرة عامة

OmniTWAG معايير أداء

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

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

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

المصادقة الكاملة (من النهاية إلى النهاية)

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

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

التشفير

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

العملية	السرعة (ips)	المتوسط (μs)	الوسيط (μs)	Mem/op
WLCSP (EMSK - > WLCSP) اشتقاق مفتاح	262,975	3.80	3.54	72 B
EAP-AKA' بناء حزمة التحدي (ترميز)	257,991	3.88	0.87	456 B
EAP-AKA' ل CK'/IK' اشتقاق	225,191	4.44	3.93	328 B
EAP-AKA' ل MAC حساب (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
لـ ERP لـ rMSK اشتقاق (إعادة مصادقة)	113,269	8.83	8.01	376 B
إعادة المصادقة السريعة ERP (rRK -> rIK -> rMSK)	61,496	16.26	14.97	520 B
Milenage_all (RES, CK, IK, AK, MAC-A) حساب	52,451	19.07	16.11	3,560 B
EAP-AKA' اشتقاق المفاتيح لـ (جميع مفاتيح الجلسة -> MK)	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
EAP- بناء حزمة التحدي لـ AKA'	EAP/AKA'-Challenge (AT_RANDOM, AT_AUTN, AT_KDF, AT_MAC).
WLCPP اشتقاق مفتاح	وضع الاتصال) EMSK من WLCPP يشتق مفتاح حماية (المتعدد).
دالة اشتقاق المفاتيح العامة 3GPP	المستخدمة عبر HMAC-SHA-256 دالة اشتقاق المفاتيح تسلسل المفاتيح.
EAP-AKA' لـ MAC حساب	مقطوعة، EAP على حزمة AT_MAC HMAC-SHA-256 إلى 16 بايت.
EAP-AKA' لـ CK'/IK' اشتقاق	مرتبط باسم شبكة الوصول CK'/IK' إلى CK/IK يحول.
ERP لـ rMSK اشتقاق	EAP (RFC 6696) مفتاح جلسة لكل إعادة مصادقة لـ.
إعادة المصادقة السريعة الكاملة	لإعادة مصادقة rRK → rIK → rMSK سلسلة اشتقاق كاملة سريعة.
Milenage_all حساب	RES, CK, IK, AK, MAC-A: واحد AKA متجه مصادقة.
EAP-AKA' اشتقاق المفاتيح لـ	K_encr, K_aut, K_re, MSK, EMSK. يوسع المفتاح الرئيسي إلى.
التشفير الكامل للمصادقة لـ EAP-AKA'	بالإضافة إلى التوسع الكامل لمفاتيح CK'/IK' اشتقاق الجلسة.

ترميز الحزم

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

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

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

المشاركة RADIUS أسرار IP حسب مجموعة عنوان (المصدر)

نظرة عامة

باستخدام سر مشترك. (NAS نقطة وصول، أو) RADIUS بمصادقة كل عميل OmniTWAG تقوم
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

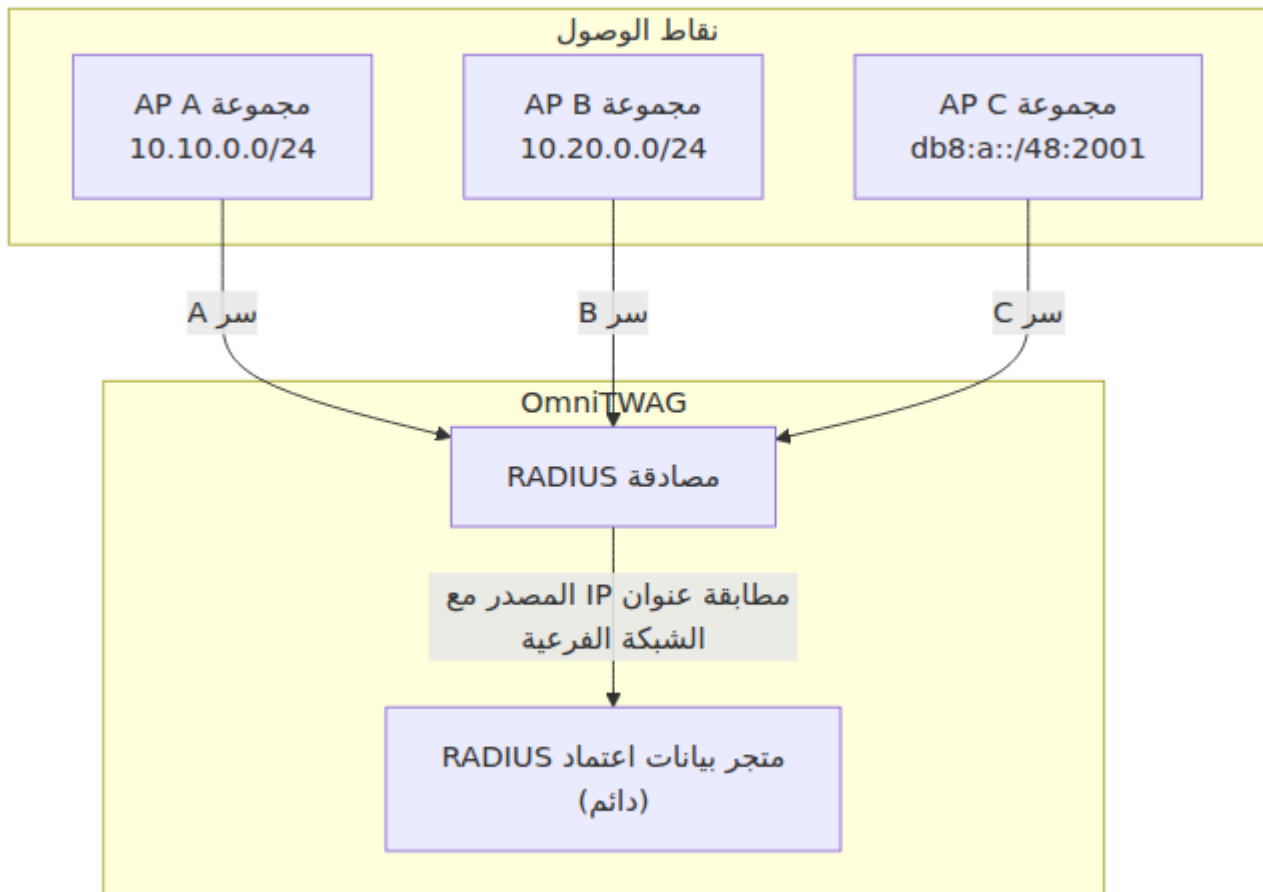
- المفاهيم
- كيف تستخدم المصادقة بيانات الاعتماد
- نموذج بيانات الاعتماد
- التفريغ والشحن لكل نقطة وصول
- REST واجهة برمجة التطبيقات
- واجهة الويب
- التكوين
- الهجرة من سر ثابت واحد
- المقاييس
- استكشاف الأخطاء وإصلاحها

المفاهيم

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

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

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



كيف تستخدم المصادقة بيانات الاعتماد

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

1. المصدر للحزمة IP عنوان OmniTWAG تقرأ.
2. المصدر. إذا IP بيانات الاعتماد التي تتطابق شبكتها الفرعية مع عنوان OmniTWAG تجد الشبكة الفرعية ذات OmniTWAG تطابقت أكثر من شبكة فرعية واحدة، تستخدم 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 . لتوقيع ، MPPE لتشفير مفاتيح ، 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 حافة صالحة عن طريق الخطأ.



نموذج بيانات الاعتماد

.تحتوي كل بيانات اعتماد على هذه الحقول

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

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

TWAG كيفية مغادرة حركة مرور المشتركين ل breakout_type تحدد

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

address_source

تحدد كيفية تعيين nsw هي breakout_type فقط عندما تكون address_source تنطبق IP. انظر مجموعة UE IP.

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

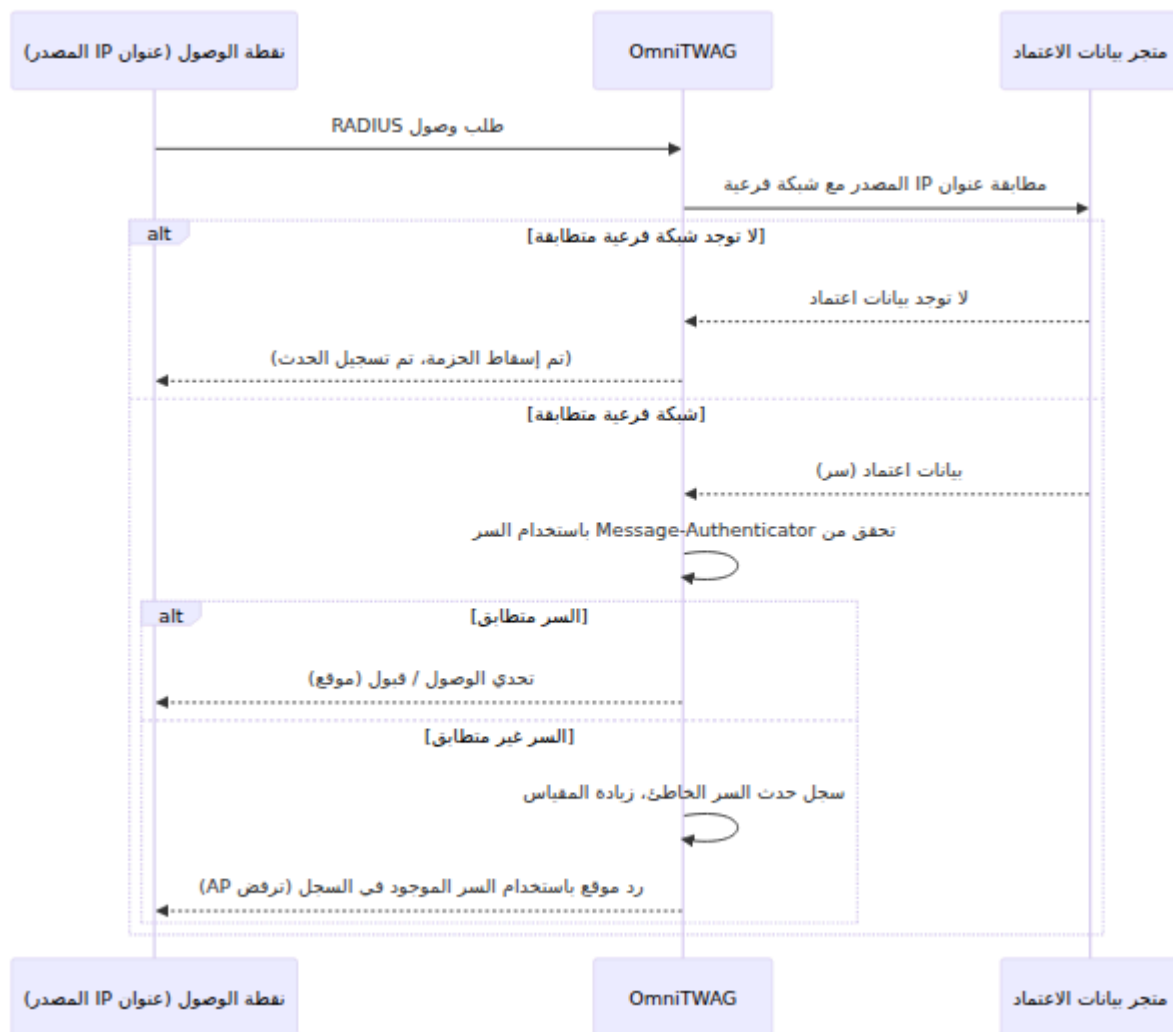
charging_mode

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

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

كيفية تفاعل الحقول

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



REST واجهة برمجة التطبيقات

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

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

جسم الطلب

مع هذه الحقول JSON جسم PUT و POST تقبل

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

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

الردود

الحالة	المعنى
200 OK	(index, show, update, delete). كانت الطلب ناجحة.
201 Created	تم إنشاء بيانات الاعتماد.
404 Not Found	المعطى id لا توجد بيانات اعتماد بال.
422 Unprocessable Entity	صالحة، أو CIDR فارغ، أو شبكة فرعية ليست كتلة secret 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"]
}
```

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

مثال: شبكة فرعية غير صالحة

الطلب:

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

الرد (`422 Unprocessable Entity`):

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

واجهة الويب

تسرد الصفحة `/radius_credentials` في **RADIUS** تحتوي لوحة التحكم على صفحة **أسرار** 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

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

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

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

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

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 `allowed_source_subnets` بتهيئة بيانات اعتماد واحدة من هذه الحقول القديمة. يتم تشغيل التهيئة فقط عندما OmniTWAG يكون كلا الأمرين صحيحين:

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

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

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

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

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 عن هذه العدادات على نقطة نهاية OmniTWAG تكشف للحصول على نقطة النهاية وأمثلة الاستعلام

radius_auth_unauthorized_source_count

النوع: عداد

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

الوصف	التسمية
المصدر للحزمة التي تم إسقاطها IP عنوان	<code>source</code>

radius_auth_bad_secret_count

النوع: عداد

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

الوصف	التسمية
لنقطة الوصول IP عنوان	<code>source</code>
لبيانات الاعتماد المتطابقة	<code>credential_id</code>

استكشاف الأخطاء وإصلاحها

نقطة الوصول لا تتلقى ردًا

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

الأسباب المحتملة:

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

الحل:

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

نقطة الوصول مفوضة ولكن المصادقة تفشل

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

الأسباب المحتملة:

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

الحل:

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

فقدان بيانات الاعتماد بعد إعادة التشغيل

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

الأسباب المحتملة:

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

الحل:

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

RADIUS رفضات

نظرة عامة

التي تم رفض حزمها. يتيح ذلك للمشغل اكتشاف نقطة وصول RADIUS مصادر OmniTWAG تتبع RADIUS غير معروفة أو تم تكوينها بشكل خاطئ بسرعة. هذه الميزة هي صورة مرآة لـ **أسرار** ويسجل متتبع ، OmniTWAG **المشتركة**: تخزين 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
- REST واجهة برمجة التطبيقات
- المقاييس
- استكشاف الأخطاء وإصلاحها

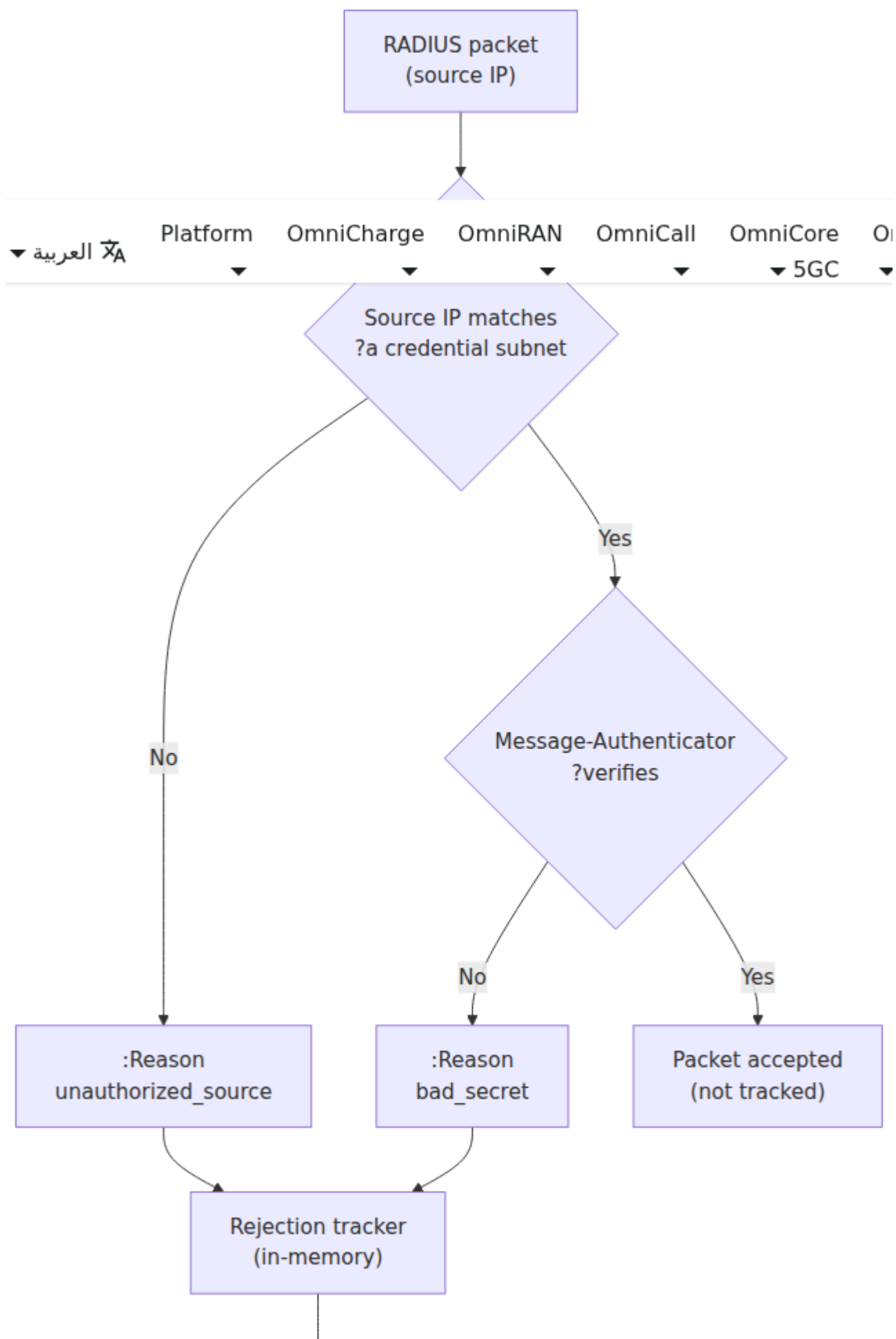
المفاهيم

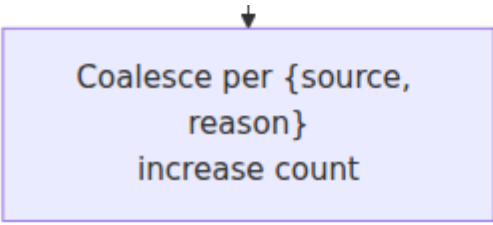
يسجل المتتبع. OmniTWAG لم تقبلها RADIUS أرسل حزمة IP **المصدر المرفوض** هو عنوان إدخالًا واحدًا لكل زوج فريد من **المصدر** و **السبب**. إذا تم رفض نفس المصدر عدة مرات لنفس صفًا جديدًا OmniTWAG عدادًا على الإدخال الموجود. لا تضيف OmniTWAG السبب، تزيد.

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

كيف تصل الحزمة إلى المتتبع

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





أسباب الرفض

يتم رفض المصدر لأحد سببين.

السبب	المعنى
unauthorized_source	المصدر مع أي شبكة فرعية للبيانات IP لم يتطابق عنوان بإسقاط الحزمة. هذه هي حالة OmniTWAG الاعتماد. قامت نقطة الوصول غير المعروفة.
bad_secret	Message- تطابقت شبكة فرعية للبيانات الاعتماد، لكن Authenticator للحرمة 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

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

فارغة لإدخال credential_name و credential_id تكون حقول 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.
- يزيد. reason و source إدخالًا واحدًا لكل زوج من OmniTWAG **مجمعة.** تسجل. لا تضيف صفاً. last_seen ويحدث count الرفض المتكرر من
- **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

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

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

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

الاستجابات

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

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 رفضًا OmniTWAG الوقت الذي تسجل فيه.

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](#) وأمثلة Prometheus [المشتركة](#) لتعريفات العدادات، و [مرجع المقاييس](#) لنقطة نهاية RADIUS الاستعلام.

استكشاف الأخطاء وإصلاحها

تظهر نقطة وصول غير معروفة في القائمة

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

الأسباب المحتملة:

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

الحل:

- من الإدخال `source` اقرأ حقل 1.

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

bad_secret تظهر نقطة وصول معروفة ك

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

الأسباب المحتملة:

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

الحل:

1. من الإدخال. هذه تسمى البيانات `credential_name` و `credential_id` اقرأ حقلي `credential_id` و `credential_name` 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** **المشتركة RADIUS**.
4. لنسيان المصدر `DELETE /radius_rejections/{id}` احذف الإدخال باستخدام.

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

إلى GTP-C / S2a واجهة PGW

نظرة عامة

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

على مستويين S2a تحتوي واجهة:

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

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

جدول المحتويات

- أوضاع الانفصال الثلاثة: S2a أين تناسب
- الدور في دورة حياة الجلسة
- S2a أنواع واجهة
- 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
- GPP مراجع 3

أوضاع الانفصال الثلاثة: S2a أين تناسب

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

الوضع (breakout_type)	IP من يعين لل UE	مستوى البيانات	S2a / GTP المستخدم
tunneled	PGW (في عنصر تخصيص PDN عنوان)	GRE إلى AP من TWAG، إلى S2a على GTP-U ثم ثم إلى الإنترنت، PGW، PGW بواسطة	نعم. هذه الوثيقة.
nswo	من TWAG، IP مجموعة	GRE إلى AP من TWAG، ثم انفصال محلي إلى TWAG في (NAT) الإنترنت	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.

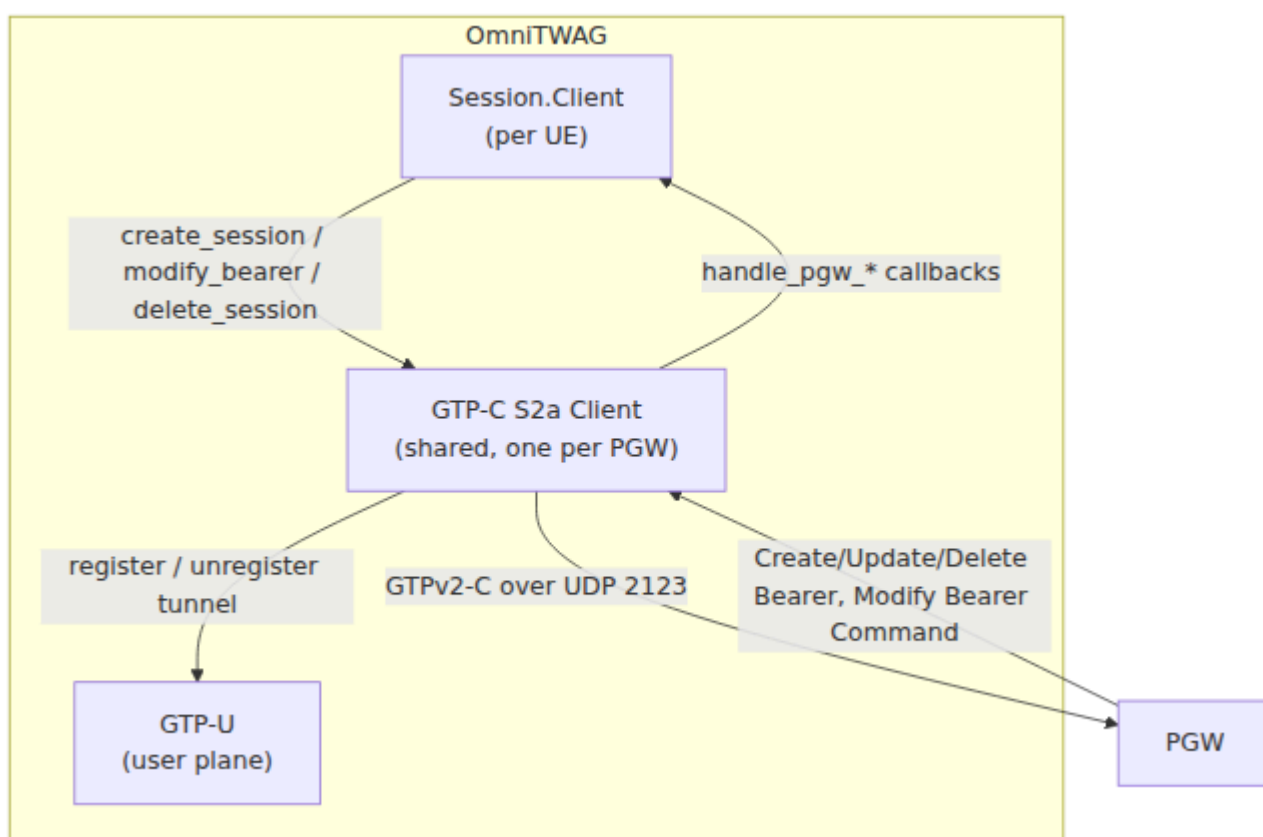
بتخصيص PGW يقوم، tunneled في وضع. فقط في وضع S2a على GTP-C ينطبق بإنشاء TWAG لا يقوم، local و nswo ويطبق السياسة والرسوم. في أوضاع UE لل IP عنوان S2a. لذا لا يتم إرسال أي رسالة، PDN جلسة.

Gy تنطبق الشحنات عبر TWAG وليس PGW بواسطة tunneled تتم عملية الشحن في وضع. في الشحن عبر الإنترنت على الأوضاع المنفصلة محليًا TWAG على جانب

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

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` UE واحد مكون. كل جلسة PGW بنفسها GTPv2-C لا ترسل رسائل GTP-C. لكل جلسة عميل `Session.Client` عملية



S2a أنواع واجهة

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

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

. (القيمة 3) WLAN هو دائمًا RAT نوع

إنشاء الجلسة

التحفيز

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

طلب إنشاء الجلسة

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

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

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

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

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

الناقل الافتراضي

الافتراضي هو 5. لا يحتوي الناقل على EBI. ناقلاً افتراضياً واحداً لكل جلسة TWAG ينشئ على مستوى الناقل في الطلب هذه القيم QoS لذا يحمل كل الحركة. تستخدم، TFT مرشحات الثابتة:

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

الناقلات المخصصة. راجع [إدارة الناقل](#) TWAG لا يدعم

استجابة إنشاء الجلسة

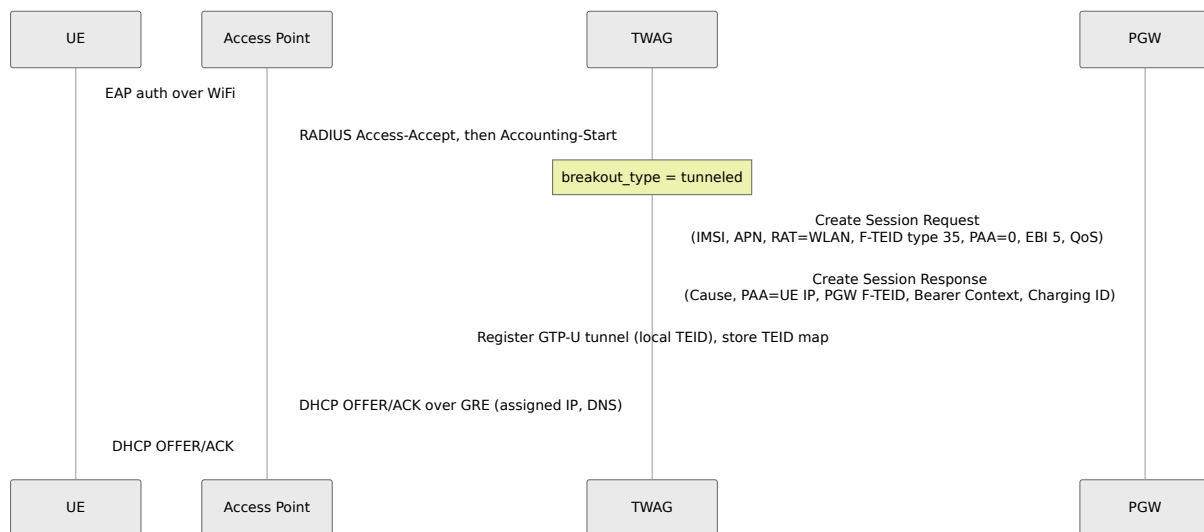
الاستجابة مع الطلب المعلق حسب رقم التسلسل. يتحقق من عنصر السبب. TWAG يتم مطابقة `request_accepted`، الطلب يكون ناجحًا إذا كان السبب هو `new_pdp_type_due_to_network_preference`، أو `new_pdp_type_due_to_single_address_bearer_only`. أي سبب آخر يعيد. `gtpc_error` مع قيمة السبب تلك.

:هذه القيم من الاستجابة TWAG عند النجاح، يقرأ

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

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

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



الجلسات ❖❖ لطائرة

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

إدارة الناقل

الناقل الافتراضي فقط

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

(TWAG من initiated) تعديل الناقل

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

PGW من initiated الإجراءات الم

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

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

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

تدمير الجلسة

(TWAG من initiated) حذف الجلسة

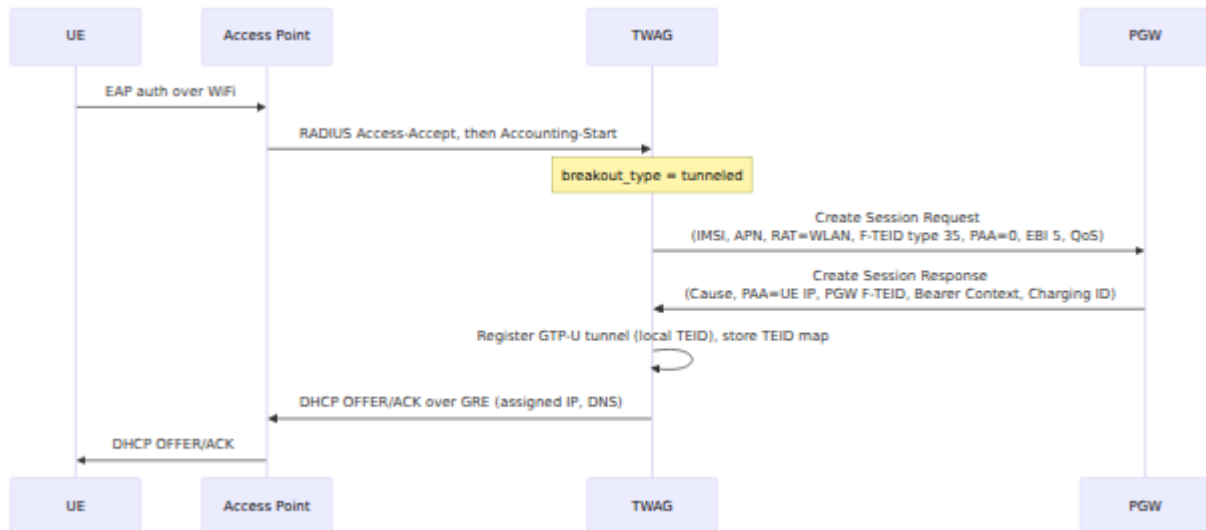
GTP-C تدمير `Session.Client` تستدعي عملية UE. عندما ينفصل PDN جلسة TWAG يحذف: يحمل الطلب PGW. التحكم TEID إلى (TS 29.274 §7.2.9) طلب حذف الجلسة TWAG يرسل

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

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

(PGW من initiated) حذف الناقل

EBI المرتبط، وقائمة EBI TWAG التدمير مع طلب حذف الناقل. يقرأ PGW يمكن أن يبدأ 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 PDN الافتراضي، يتم تدمير الاتصال الكامل لـ



إدارة المسار

صدى

تقوم معلمة (TS 29.274 §6) مع طلب صدى واستجابة صدى GTPV2-C إدارة مسار TWAG يدير PGW طلب صدى إلى TWAG بتنفيذ ذلك. تكون مفعلة بشكل افتراضي. يرسل echo_enabled تحمل كل استجابة صدى عداد استرداد TWAG كل 60 ثانية. يحمل كل طلب صدى رقم تسلسل

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

حالة المسار

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

PGW اكتشاف إعادة تشغيل

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

مهلة الطلب وإعادة الإرسال

لإعادة المحاولات لطلبات التحكم N3-REQUESTS و T3-RESPONSE مؤقت TWAG يستخدم

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

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

TWAG عند بدء التشغيل. إذا لم يتمكن المقبس من الفتح، يعيد GTP-C UDP مقبس TWAG يفتح 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: %{\n    # مطلوبة للانفصال الم (S2a تمكين واجهة tunneled)\n    enabled: true,\n\n    # PGW لـ GTP-C نقطة نهاية\n    pgw_ip: "10.5.198.1",\n    pgw_port: 2123,\n\n    # GTP-U F-TEIDs و GTP-C لـ TWAG المحلي لـ IP\n    local_ip: "10.5.198.200",\n\n    # GTP-U منفذ مستوى المستخدم\n    gtpu_port: 2152,\n\n    # إدارة المسار (صدى)\n    echo_enabled: true,\n\n    الافتراضات لطلب إنشاء الجلسة\n    apn: "internet",\n    pdn_type: :ipv4\n  }\n}
```

GTP معلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
<code>enabled</code>	Boolean	لا	<code>false</code>	تعيين S2a. تمكين واجهة للانفصال الم <code>true</code> إلى <code>tunneled</code> . عندما تكون TWAG لا يبدأ <code>false</code> ، ويتخطى GTP-C عميل لكل جلسة S2a.
<code>pgw_ip</code>	String	نعم (إذا تم تمكينه)	<code>127.0.0.1</code>	GTP-C PGW. ل IP عنوان جميع رسائل TWAG يرسل إلى هذا العنوان GTPv2-C.
<code>pgw_port</code>	Integer	لا	<code>2123</code>	ل GTP-C UDP منفذ PGW. المنفذ القياسي ل GTP-C 2123 هو.
<code>local_ip</code>	String	لا	يتم اكتشافه تلقائيًا	TWAG المحلي ل IP و F-TEIDs يستخدم في GTP-C وكعنوان مصدر ل GTP-U. إذا لم يتم تعيينه، TWAG IP الصادر يكتشف تلقائيًا.
<code>gtpu_port</code>	Integer	لا	<code>2152</code>	GTP-U UDP منفذ لمستوى المستخدم. راجع مستوى المستخدم .
<code>echo_enabled</code>	Boolean	لا	<code>true</code>	GTPv2-C تمكين إدارة مسار PGW. إلى Echo C.
<code>apn</code>	String	لا	<code>internet</code>	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	IMSI أرقام 4-5	رمز الشبكة المحمول لعنصر الشبكة الخادمة.

TWAN معلمات الطوارئ و

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

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

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

جداول المراجع

GTPv2-C (S2a) أنواع رسائل

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

GTPv2-C رموز سبب

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

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

الرصد

أحداث القياس للنشاط ❖❖ لناقل وتدمير الجلسة. تدفع هذه الأحداث المقاييس في TWAG ينشر [مرجع المقاييس](#).

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

حالة العميل

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

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

السجل

كل إجراء. تشمل خطوات السجل الرئيسية GTP-C يسجل عميل

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

استكشاف الأخطاء وإصلاحها

فشل إنشاء الجلسة

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

الأسباب المحتملة:

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

الحل:

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

معطل PGW المسار إلى

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

الأسباب المحتملة:

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

الحل:

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

PGW الجلسات تتقطع بعد إعادة تشغيل

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

الأسباب المحتملة:

- التشغيل وغير عداد الاسترداد الخاص به PGW أعاد.

الحل:

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

الجلسات تتأسس ولكن لا توجد تدفقات بيانات

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

الأسباب المحتملة:

- غير متاح GRE أو مسار GTP-U نفق.

الحل:

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

GPPمراجع 3

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

نظرة عامة

الجلسات

نظرة عامة

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

RADIUS سجل محاسبة OmniTWAG تحمل واجهة الجلسات أيضًا حركة مرور المشترك. يدمج وبالتالي، تعتبر الجلسة المصدر الوحيد لكل من حالة `Acct-Session-Id` في الجلسة بواسطة 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
- REST واجهة برمجة التطبيقات
- إجراءات لكل جلسة
- JSON أمثلة
- واجهة الويب
- استكشاف الأخطاء وإصلاحها

المفاهيم

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

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

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

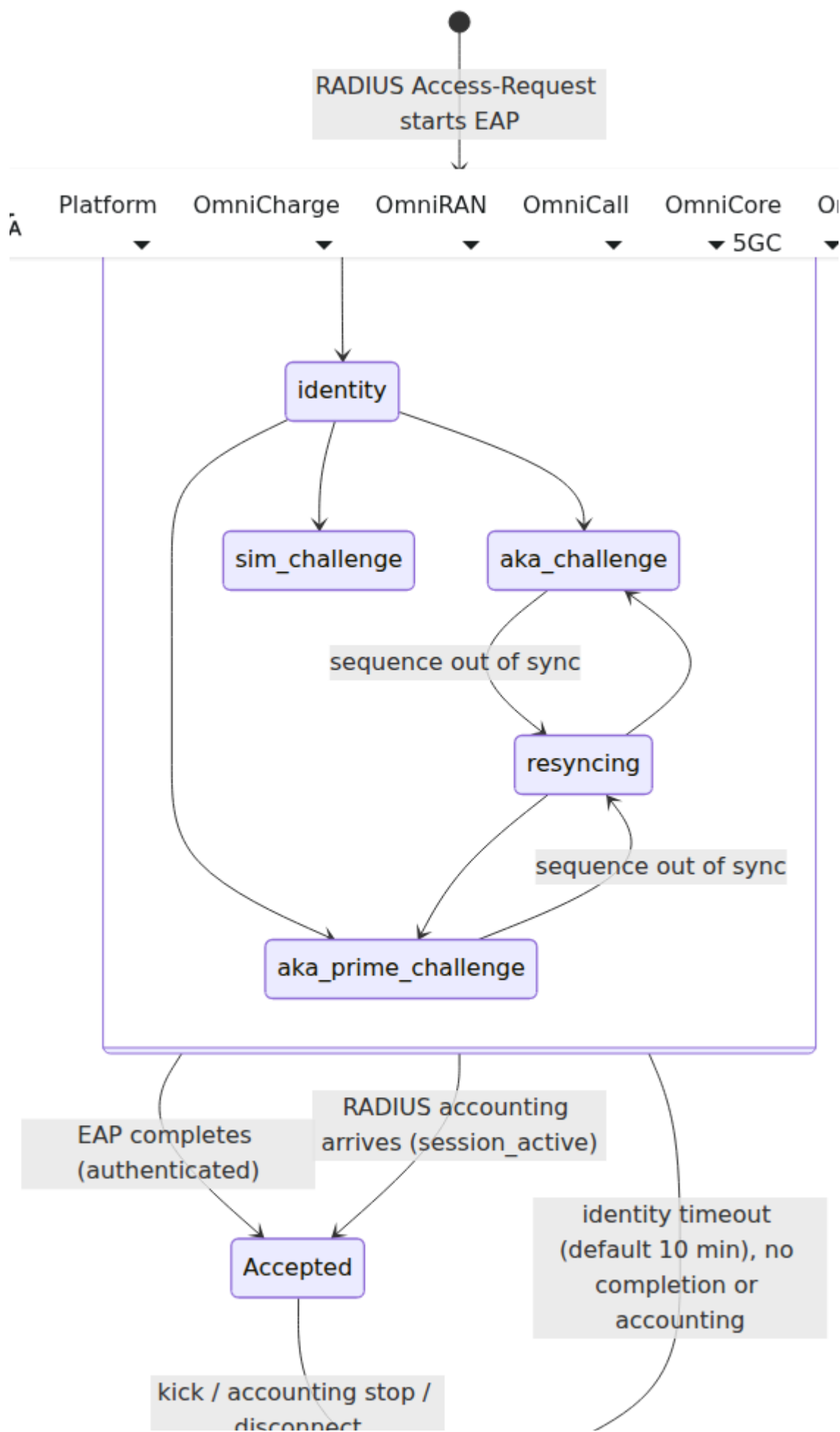
دورة حياة حالة المصادقة

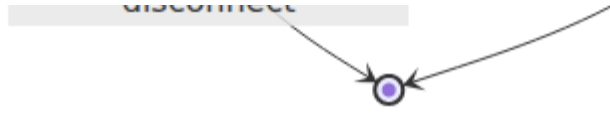
(eap_phase) للجلسة EAP تمتلك الجلسة حالة مصادقة. يتم اشتقاق الحالة من مرحلة

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

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

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





نموذج الجلسة

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

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

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

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

مرجع حالة المصادقة

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

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

.تُعتبر تحت المصادقة eap_phase أي قيمة أخرى لـ

REST واجهة برمجة التطبيقات

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

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

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

البحث والترقيم

معلومات الترقيم والبحث index تقبل نقطة النهاية

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

مع هذه الحقول للجلسة q يتم مطابقة مصطلح

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

جسم طلب الإجراء

يحتوي على حقل واحد JSON جسم PUT و PATCH تقبل.

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

انظر إجراءات لكل جلسة لمعرفة ما يفعله كل إجراء

الاستجابات

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

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

إجراءات لكل جلسة

PATCH لطلب JSON يعمل الإجراء على تنفيذ عملية إدارية ضد جلسة حية. أرسل الإجراء في جسم 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 Accounting-Stop الوصول أرسلت. 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

JSON أمثلة

جلسة مع حركة مرور

الطلب:

```
GET /sessions/0010100000000001
```

الاستجابة:

```
{
  "identity": "0010100000000001",
  "imsi": "0010100000000001",
  "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
}
```

kick إجراء

الطلب:

```
PATCH /sessions/0010100000000001
```

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

الاستجابة (200 OK):

```
{  
  "status": "kicked",  
  "identity": "0010100000000001"  
}
```

إجراء غير معروف

الطلب:

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

الاستجابة (422 Unprocessable Entity):

```
{  
  "error": "Unknown action \"reboot\" (expected  
kick|start_accounting|stop_accounting)",  
  "identity": "0010100000000001"  
}
```

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، أو `identity`، `aka_challenge`، `aka_prime_challenge`، `sim_challenge`، مثل `resyncing`.

الأسباب المحتملة:

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

كيف يتم حلها:

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

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

جلسة لا تظهر حركة مرور

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

الأسباب المحتملة:

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

الحل:

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

انتظر حتى التحديث المؤقت التالى للمحاسبة، ثم اقرأ الجلسة مرة أخرى 3.

نظرة عامة

مسار المستخدم ومسار البيانات

نظرة عامة

بين مستوى التحكم ومستوى المستخدم. يعمل مستوى التحكم على التحقق OmniTWAG يفصل 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 UE. وكيف يعيد توجيه الحزم الهابطة إلى، GTP-U.

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

جدول المحتويات

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

مستوى التحكم ومستوى المستخدم

يعمل مستوى التحكم ومستوى المستخدم كعمليات منفصلة.

يقوم **مستوى التحكم** بالأعمال التالية:

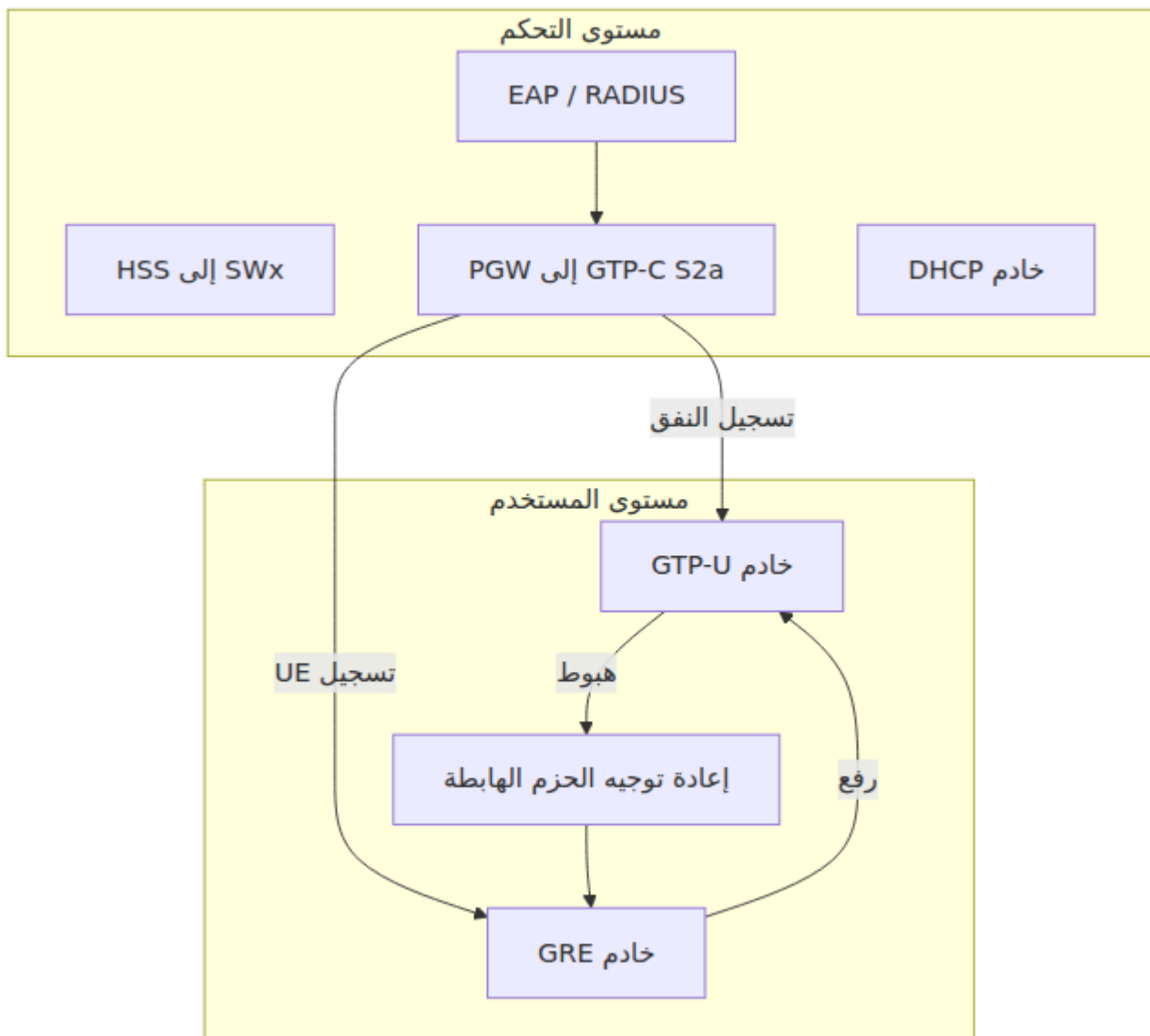
- مع نقطة الوصول RADIUS باستخدام EAP التحقق من الهوية عبر.

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

:يقوم مستوى المستخدم بالأعمال التالية

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

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



أنماط مسار البيانات

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

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

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

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

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

وضع tunneled (GTP-U إلى PGW)

بتخصيص PGW يقوم PGW إلى UE بنفق حركة مرور OmniTWAG يقوم، tunneled في وضع وفقًا S2a ويطبق السياسة والرسوم، ويقدم الوصول إلى الإنترنت. هذه هي واجهة، UE لـ IP عنوان القسم 16 **GPP TS 23.402** لـ 3.

مسار الرفع هو:

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

مسار الهبوط هو العكس:

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

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

(NSWO) خروج محلي

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

NSWO: طريقتين للوصول إلى OmniTWAG يمتلك

1. إلى `breakout_type` AP قم بتعيين بيانات اعتماد: **مفضل AP خروج لكل** إلى `ip_pool_id` المسماة بـ **IP** من مجموعة UE يأتي عنوان `nswo`. يحدد `address_source` في بيانات الاعتماد كيفية ذلك:

- مرة GRE لـ الهبوط UE يخصص عنوان ثابت من المجموعة ويسجل `pool` واحدة.
- بتوزيع TWAG في DHCP بالمجموعة ويسمح لـ خادم UE MAC يربط `dhcp` عندما يكون GRE يتم تسجيل الهبوط. DISCOVER DHCP عنوان في العنوان معروفًا.

2. خروجًا محليًا لكل جلسة `Twag.NSWO.Handler` **العالمي**: يوفر **NSWO معالج** (يطبق) `nswo.enabled: true` يتم تحديده باستخدام GTP. عندما لا يتم استخدام محلية واحدة ويقوم IP يدير المعالج مجموعة (`gtp.enabled: false`) عندما يكون TWAG عن إنشاء الجلسة، يقوم `iptables` باستخدام NAT بتكوين قاعدة تمويه لـ UE ويسجل، عبر DHCP، UE بتخصيص عنوان من المجموعة المحلية، ويوصله إلى. يتم الإفراج عن التخصيص عند إنهاء الجلسة. GTP-C جلسة / PGW دون GRE، الهبوط

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

nswo: العالمي هذه المعلومات من خريطة NSW0 يقرأ معالج

المعلمة	النوع	الافتراضي	الوصف
enabled	Boolean	false	العالمي NSW0 بدء معالج وتوجيه الجلسات عبر الخروج المحلي.
local_pool	String (CIDR)	10.100.0.0/16	المجموعة التي يتم تخصيص منها UE عنوان.
nat_interface	String	eth0	واجهة الخروج لقاعدة تمويه NAT.
dns_servers	List	["8.8.8.8", "8.8.4.4"]	لا UE المعلنة لـ DNS خوادم يحتوي الخروج المحلي على PGW PCO لنقلها.

GRE مسار البيانات

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

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

الوارد GRE تصنيف

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

المعالجة	المعنى	بروتوكول GRE
الداخلي، ثم تصنيفه Ethernet استخراج إطار حسب نوع الإيثر.	Ethernet جسر الشفاف	0x6558
لرفع IPv4 اعتبره حزمة.	IPv4	0x0800

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

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

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

معالجة الرفع

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

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

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

للهبوط UE تسجيل

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

GTP-U نفق

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

TEID معالجة

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

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

:يحتفظ النفق المسجل بهذه الحقول

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

تغليف الرفع

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

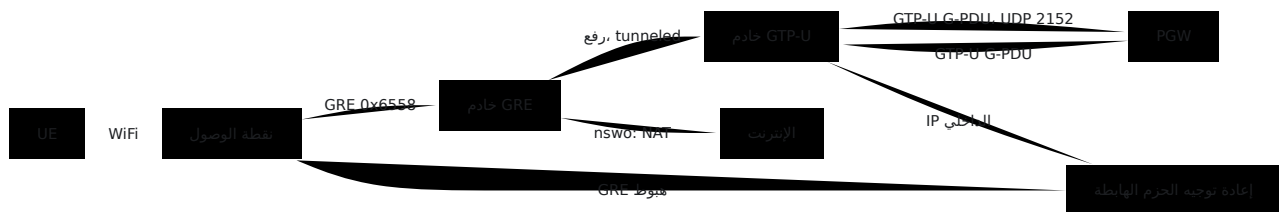
فك تغليف الهبوط

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

الرسالة	النوع	الإجراء
G-PDU	255	IP المحلي، ثم أعد توجيه حزمة TEID ابحث عن النفق بواسطة 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 Twag.Downlink. الداخلية إلى IP ثم يمرر الخادم حزمة. (ونوع رأس الامتداد التالي، N-PDU، 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

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

مسار GRE (مفضل)

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

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

مسار المقبس الخام (خيار احتياطي)

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

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

اختيار المسار

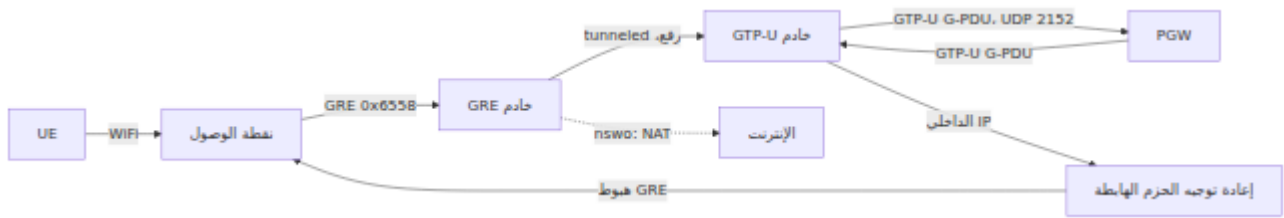
ترتيب اختيار المسار `prefer_gre` تحدد معلمة

- `prefer_gre: true` (افتراضي) أولاً وتعود إلى GRE تحاول إعادة التوجيه نفق: GRE غير متاح أو فشل إرسال GRE المقبس الخام إذا كان
- `prefer_gre: false` تحاول إعادة التوجيه المقبس الخام أولاً لعائلة عنوان الحزمة فقط عندما يكون ذلك المقبس الخام غير متاح GRE وتستخدم

فحوصات الحزمة

تسقط إعادة التوجيه حزمة في هذه الحالات:

- تم تعطيل إعادة التوجيه بواسطة التكوين.
- غير متاح GRE لا يوجد مقبس متاح، و
- الحزمة صغيرة (أقل من 20 بايت)
- الوجهة IP لا تستطيع إعادة التوجيه قراءة عنوان



الحاملات وقوالب تدفق الحركة

الحاملات لجلسة. تتوافق كل حاملة مع هوية (Twag.Bearer.Manager) يدير مدير الحاملات ومرشحات حزمة قالب تدفق الحركة، GTP-U ل TEIDs تحتوي الحاملة على EPS (EBI). حامل GPP TS واحدة من الحاملات هي ♦♦ لحاملة الافتراضية. يتبع هذا 3. QoS (QCI) وفئة (TFT)، القسم 16.1.6.1 23.402.

الحاملات الافتراضية والمخصصة

نوع الحاملة	مرشحات TFT	الغرض
افتراضي	لا شيء	يحمل كل الحركة التي لا تتطابق مع حاملة مخصصة.
مخصص	واحد أو أكثر	TFT يحمل الحركة التي تتطابق مع مرشحات حزمة الخاصة به.

إذا تمت إزالة الحاملة الافتراضية، يقوم مدير الحاملات بإشارة إنهاء الجلسة بالكامل. تؤدي إزالة حاملة مخصصة إلى إزالة تلك الحاملة فقط.

TFT مرشحات حزمة

على TFT القسم 10.5.6.12. تحتوي GPP TS 24.008 قالب تدفق حركة وفقًا ل 3 TFT تعتبر عملية وقائمة من مرشحات الحزمة. يحتوي كل مرشح حزمة على اتجاه، وأولوية، وقائمة من هذه أنواع المكونات TFT المكونات. يدعم محلل

المطابقة	المكون
.عنوان وجهة الحزمة	IPv4 البعيد و القناع IP عنوان
.عنوان مصدر الحزمة	IPv4 المحلي و القناع IP عنوان
.IPv6 عنوان	البعيد/المحلي و البادئة IPv6 عنوان
.IP رقم بروتوكول	معرف البروتوكول
.UE منفذ مصدر	منفذ محلي واحد / نطاق منفذ محلي
.منفذ الوجهة	منفذ بعيد واحد / نطاق منفذ بعيد
.مع قناع، TOS بايت	نوع الخدمة / فئة الحركة
.TWAN لا يتم مطابقته في الرفع	فهرس معلمة الأمان
.(فقط IPv6) لا يتم مطابقته	علامة التدفق

إنشاء، حذف، إضافة مرشحات، استبدال مرشحات، حذف مرشحات، TFT يدعم المحلل عمليات طلب PGW وعدم القيام بأي عملية. يقوم مدير الحاملات بتطبيق هذه العمليات عندما يرسل تحديث الحاملة.

تصنيف الرفع

:يربط مصنف الرفع كل حزمة رفع بحاملة. القواعد هي:

1. من الحزمة TOS الوجهة، والبروتوكول، والمنفذ، و IP المصدر، وعنوان IP اقرأ عنوان.
2. للحاملات المخصصة TFT اختبر الحزمة مقابل مرشحات.
3. AND. يتطابق مرشح فقط إذا تطابق جميع مكوناته. هذه هي منطق.
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.

wildcard. يتطابق مرشح فارغ (مرشح بدون مكونات) مع جميع الحزم. هذه هي

GRE لدعم الحاملات المخصصة. يقوم مسار TFT **ملاحظة:** يتواجد مدير الحاملات ومصنف 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 (S2a / GTP-C). انظر

معالجة الأخطاء

صدى GTP-U

واستجابة الصدى لاختبار مسار النفق. عندما يتلقى GTP-U طلب صدى TWAG و PGW يستخدم على تنفيذ صدى خاص بها S2a GTP-C طلب صدى، يرد باستجابة صدى. تعمل عملية GTP-U خادم (S2a / GTP-C). انظر true هو gtp.echo_enabled عندما يكون

GTP-U إشارة خطأ

مرة أخرى GTP-U إشارة خطأ GTP-U ليس له نفق، يرسل خادم TEID إلى G-PDU إذا وصلت هذا يخبر. TWAG لـ GTP-U غير المعروف وعنوان نظير TEID إلى المصدر. تحمل إشارة الخطأ بالتوقف عن إرسال الحركة على النفق الميت. كما يسقط الخادم الحزمة ويزيد عدد الأخطاء PGW

GTP-U علامة نهاية

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

هو GRE 47 هابطة. رقم بروتوكول GRE الخارجي لكل حزمة IPv4 رأس GRE يبني خادم

لتجنب التجزئة، يجب على نقطة UE بايتات رأس إلى حزمة GRE و GTP-U تضيف كل من تغليف `mss` بتعيين Cisco للنفق. يقوم تكوين نقطة الوصول المرجعي MTU و MSS TCP الوصول تقليل. انظر **الهندسة المعمارية** لتكوين نقطة الوصول GRE. على نفق `mtu 1500` و `1410`.

التكوين

و `gre` و `gtp` الكتل ذات الصلة هي `omnitwag`: تقرأ عمليات مستوى المستخدم تكوين تطبيق `downlink` وليس من هذه الكتل. انظر **بيانات**، RADIUS من بيانات اعتماد AP يأتي وضع خروج. **RADIUS اعتماد**.

```
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 نقطة الوصول
  gre: %{
    enabled: false,
    local_ip: "10.5.198.200"
  },

  # إعادة توجيه الهبوط
  downlink: %{
    enabled: true,
    ip_hdr_incl: true,
    prefer_gre: true
  }
```

GTP معلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
<code>enabled</code>	Boolean	لا 	<code>false</code>	و GTP-C بدء خوادم GTP-U. تعيين <code>true</code> tunneled. لوضع
<code>pgw_ip</code>	String	لا	<code>"10.5.198.1"</code>	ل PGW ل IP عنوان GTP-C و GTP-U.
<code>pgw_port</code>	Integer	لا	<code>2123</code>	ل GTP-C UDP منفذ PGW.
<code>local_ip</code>	String	لا	تلقائي الكشف	المحلي ل IP عنوان يستخدم GTP. ل TWAG GTP-U كمصدر لحزم وعنوان نظير إشارة الخطأ.
<code>gtpu_port</code>	Integer	لا	<code>2152</code>	المحلي UDP المنفذ هذا هو GTP-U. ل خادم GTP- المنفذ القياسي ل U.
<code>echo_enabled</code>	Boolean	لا	<code>true</code>	نحو GTP-C تشغيل صدى PGW. انظر S2a / GTP-C .

GRE معلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
<code>enabled</code>	Boolean	لا	<code>false</code>	<code>true</code> تعيين GRE بدء خادم من نقطة UE لاستقبال إطارات مطلوب لكل GRE الوصول عبر <code>nsw</code> و <code>tunneled</code> من breakout.
<code>local_ip</code>	String	لا	<code>"0.0.0.0"</code>	المحلي لربط المقبس IP عنوان IP هذا هو عنوان GRE الخام لـ الوجهة الذي ترسل إليه نقطة GRE الوصول حركة

معلومات الهبوط

المعلمة	النوع	مطلوب	الافتراضي	الوصف
<code>enabled</code>	Boolean	لا	<code>true</code>	بدء إعادة توجيه الحزم الهابطة. تسقط ، <code>false</code> عندما تكون إعادة التوجيه جميع الحزم الهابطة.
<code>ip_hdr_incl</code>	Boolean	لا	<code>true</code>	و <code>IP_HDRINCL</code> تعيين خيارات <code>IPV6_HDRINCL</code> على المقابس الخام بحيث تزود إعادة التوجيه الرأس الكامل لـ لا يتم ، <code>false</code> عندما تكون IP. ما لم <code>true</code> تعيين الخيار. اترك <code>IP_HDRINCL</code> يرفض النواة.
<code>prefer_gre</code>	Boolean	لا	<code>true</code>	ترتيب اختيار المسار. عندما تحاول إعادة ، <code>true</code> تكون أولاً وتعود إلى GRE التوجيه المقبس الخام. عندما تكون تحاول المقبس الخام ، <code>false</code> فقط عندما GRE أولاً وتستخدم. يكون المقبس الخام غير متاح.

قدرة المضيف

ومسار المقبس الخام للهبوط المقابس الخام. يجب على المضيف منح GRE يستخدم كل من خادم المقبس GRE بدون هذه القدرة، لا تفتح المقابس الخام. يحاول خاد. `CAP_NET_RAW` القدرة كل 10 ثوانٍ. تسقط إعادة توجيه الحزم أو تتراجع، كما هو موضح في **إعادة توجيه الحزم الهابطة**

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. انظر **مرجع المقاييس**، OmniTWAG التي يصدرها Prometheus.

حالة GTP-U

stats وخريطة tunnel_count و local_ip و socket_open عن GTP-U تبلغ حالة متداخلة:

الإحصائية	الوصف
packets_in	GTP-U عدد الحزم المستلمة على مقبس
packets_out	GTP-U عدد الحزم المرسل على مقبس
bytes_in	إجمالي البايتات المستلمة
bytes_out	إجمالي البايتات المرسل
errors	عدد أخطاء فك التشفير وأحداث النفق غير المعروفة
tunnel_count	عدد الأنفاق المسجلة (حقل من المستوى الأعلى)

حالة GRE

و ap_tunnels و local_ip و socket_open و running عن GRE تبلغ حالة متداخلة stats وخريطة registered_ues:

الإحصائية	الوصف
packets_in	المستلمة GRE عدد حزم
packets_out	المرسلة GRE عدد حزم
bytes_in / bytes_out	إجمالي البايتات الداخلة والخارجة
dhcp_in	المستلمة من نقطة الوصول DHCP عدد حزم
uplink_forwarded	GTP-U عدد حزم الرفع التي تم توجيهها إلى
downlink_forwarded	عدد حزم الهبوط المرسلة إلى نقطة الوصول
unknown_protocol	عدد الحزم التي تحتوي على بروتوكول أو نوع إثير غير معروف
errors	عدد الأخطاء في فك التشفير والإرسال
registered_ues	المسجلين (حقل من المستوى الأعلى) UE عدد

إحصائيات الهبوط

الإحصائية	الوصف
forwarded	(الخام IPv4 ومقبس GRE) الموجهة IPv4 عدد حزم
forwarded_v6	الموجهة IPv6 عدد حزم
dropped	عدد الحزم المسقطة
errors	عدد أخطاء الإرسال
bytes	إجمالي البايتات الموجهة
enabled	حالة تمكين إعادة التوجيه
socket_open	الخام IPv4 حالة مقبس

نظرة عامة

