Authentification de la gamme 5x00 SGSN ASR et pratiques recommandées de redistribution PTMSI

Contenu

[Introduction](#)
[Aperçu](#)
[Authentification SGSN et blocs PROCEDURE de signature PTMSI](#)
[Pourquoi l'authentification et redistribution de la signature PTMSI est exigée](#)
[Problème](#)
[Approche de stabilisation](#)
[Plan de difficulté](#)
[Directives de configuration](#)
[Dépannez](#)
[Risques](#)
[Syntaxe de commande](#)

Introduction

Ce document fournit une explication de base des avantages de la configuration de fréquence de procédure d'authentification, de l'identité d'abonné mobile provisoire de paquet (PTMSI), et de la redistribution de signature PTMSI. Spécifiquement, ce document est pour une procédure facultative de gestion de la mobilité de projet de partenariat de troisième-génération pour 2G et 3G sur servir le noeud de support GPRS (SGSN) ce s'exécute sur la gamme 5000 du routeur de service Aggregated (ASR).

Ce document explique ces pratiques recommandées :

- Configuration de fréquence d'authentification
- Redistribution PTMSI
- Redistribution de signature PTMSI
- L'incidence si vous ne configurez pas la configuration de fréquence d'authentification et la redistribution PTMSI et la redistribution de signature (basée sur l'expérience des cas de client)
- Instructions de configuration et l'incidence sur des interfaces externes
- Options de dépanner des questions

Aperçu

L'authentification, cadre de redistribution de signature PTMSI, et PTMSI sous le profil de Contrôle d'appel permet à l'opérateur de configurer l'authentification ou l'allocation de la signature PTMSI et

PTMSI par abonné dans le 2G et le 3G SGSN et l'entité de Gestion mobile (MME.). Dans le SGSN, l'authentification peut actuellement être configurée pour ces procédures - attache, demande de service, routage-zone-mise à jour (RAU), court-Messagerie-service, et détache.

La MME. se sert également du même cadre afin de configurer l'authentification pour les demandes de service et les dépister-zone-mises à jour (TAUs). La redistribution PTMSI est configurable pour l'attache, la demande de service, et le RAUs. La redistribution de signature PTMSI est configurable pour la commande d'attache, de redistribution PTMSI, et le RAUs. L'authentification et la redistribution peuvent être activées pour chaque exemple de ces procédures ou pour chaque nième exemple de la procédure, appelé authentification/redistribution sélectives. Certaines procédures prennent en charge également l'activation de l'authentification ou la redistribution basée sur le temps s'est écoulée (périodicité ou intervalle) depuis la dernière authentification ou redistribution respectivement.

En outre, ceux-ci peuvent être configurés spécifiquement pour seulement l'Universal Mobile Telecommunications System (UMTS) (3G) ou le Service général de radiocommunication par paquets (GPRS) (2G) ou chacun des deux. Cette configuration est vérifiée seulement quand elle est facultative pour que le SGSN authentifie ou pour réapproprie la signature PTMSI/PTMSI d'un abonné. Dans les scénarios où il est obligatoire de faire ces procédures, cette configuration n'est pas vérifiée.

Il y a trois types de CLIs pour la configuration de la fréquence de chaque procédure - un POSITIONNEMENT CLI, un AUCUN CLI, et un RETIRER CLI. Quand vous appelez un POSITIONNEMENT CLI, l'opérateur veut activer l'authentification ou la redistribution pour la procédure spécifique. L'AUCUN CLI n'est de désactiver explicitement l'authentification ou la redistribution PTMSI pour une procédure, et le RETIRER CLI est de restaurer la configuration sur un état où le CLI (PLACEZ ou NON) n'est pas configuré du tout. On assume que toutes les configurations SONT RETIRÉES quand l'arborescence est initialisée dans l'allocation de cc-profil. Par conséquent, REMOVE est la configuration par défaut.

Le POSITIONNEMENT CLI affectera seulement une procédure spécifique dans l'arborescence tandis que l'AUCUN CLI et RETIRE LE CLI affectera le processus actuel et RETIRERA également les Noeuds inférieurs. En outre, si AUCUN CLI ou NE RETIRENT LE CLI affecte l'arborescence commune, l'effet sera propagé sur les Noeuds correspondants dans les arborescences d'Access-particularité également.

Il y a deux types de CLIs pour la configuration de la périodicité de chaque procédure - le POSITIONNEMENT CLI et le RETIRER CLI. Le POSITIONNEMENT et REMOVE terminés contre la périodicité affecteront seulement la configuration de périodicité et laisseront la configuration de fréquence intacte. L'AUCUN CLI exécuté pour la fréquence (pour être précis, l'AUCUN CLI n'est commun parce qu'il ne prend aucun argument de fréquence ou de périodicité, mais est identifié avec la configuration de fréquence intérieurement tout en enregistrant) NE RETIRERA également la configuration de périodicité.

Certains scénarios où l'authentification est terminée sans réserve sont comme suit :

- Attache de l'identité d'abonné mobile internationale (IMSI) - tous les attachés IMSI sont authentifiés
- quand l'abonné n'a pas été authentifié avant et vous n'avez pas un vecteur
- quand il y a une non-concordance de signature PTMSI
- quand il y a une non-concordance du numéro de séquence de clé de chiffrement (CKSN)

Actuellement, l'authentification peut être activée pour ces derniers sous l'appel-contrôle-profil :

- l'attache, demande de service, RAU, détachent, court-Messagerie-service, tout-événements, et TAU
- Le TAU est en service par la MME.
- l'attache et la demande de service sont utilisées par SGSN et MME.
- le repos sont utilisés exclusivement par SGSN

Authentification SGSN et blocs PROCEDURE de signature PTMSI

Cette structure arborescente explique les blocs PROCEDURE que SGSN considère pour des configurations de fréquence.

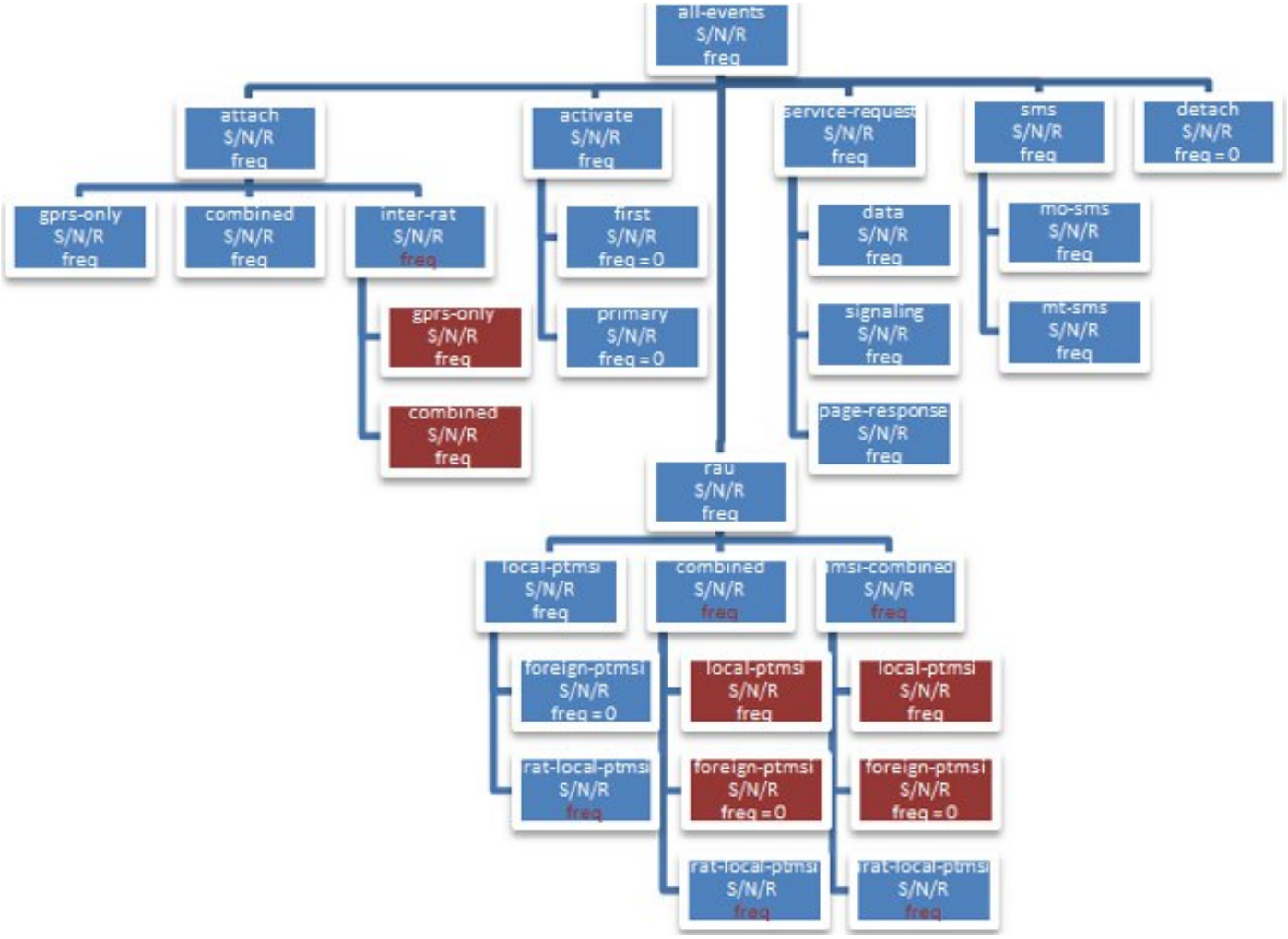

Figure 1 : Les blocs PROCEDURE SGSN considère pour des configurations de fréquence

Les arborescences pour la procédure de redistribution PTMSI sont affichées ici.

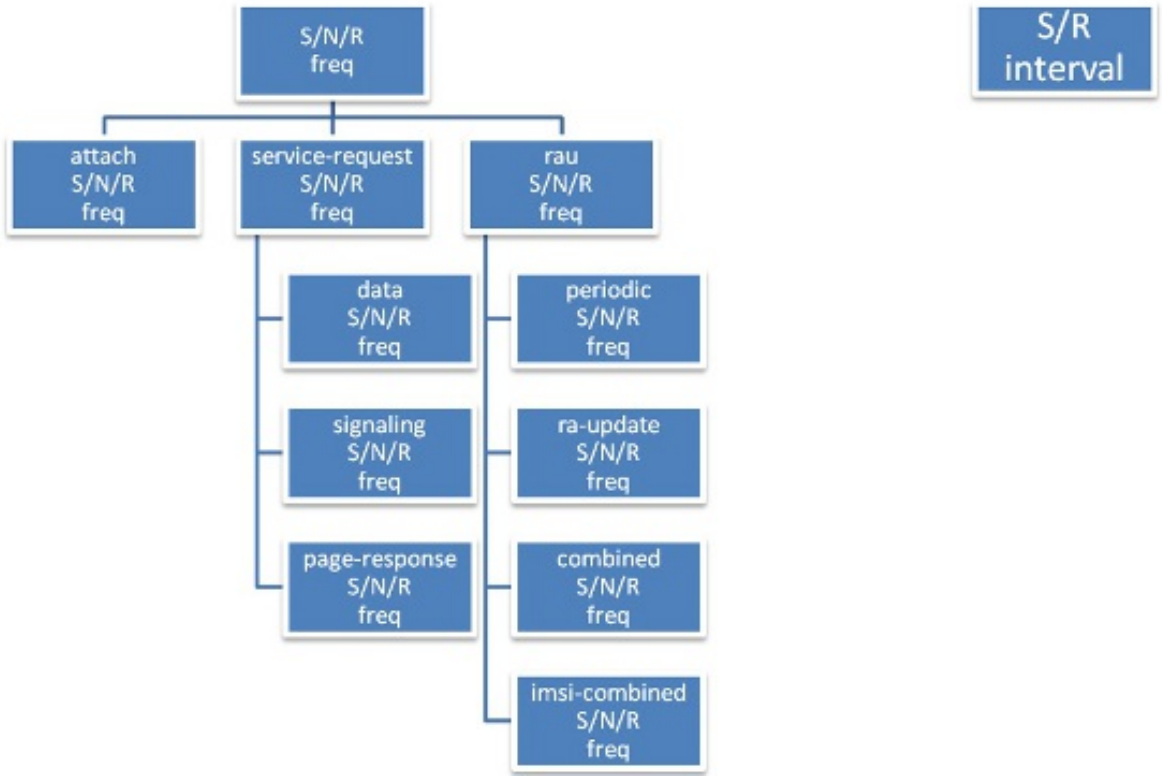

Figure 2 : Arborescence de configuration d'authentification

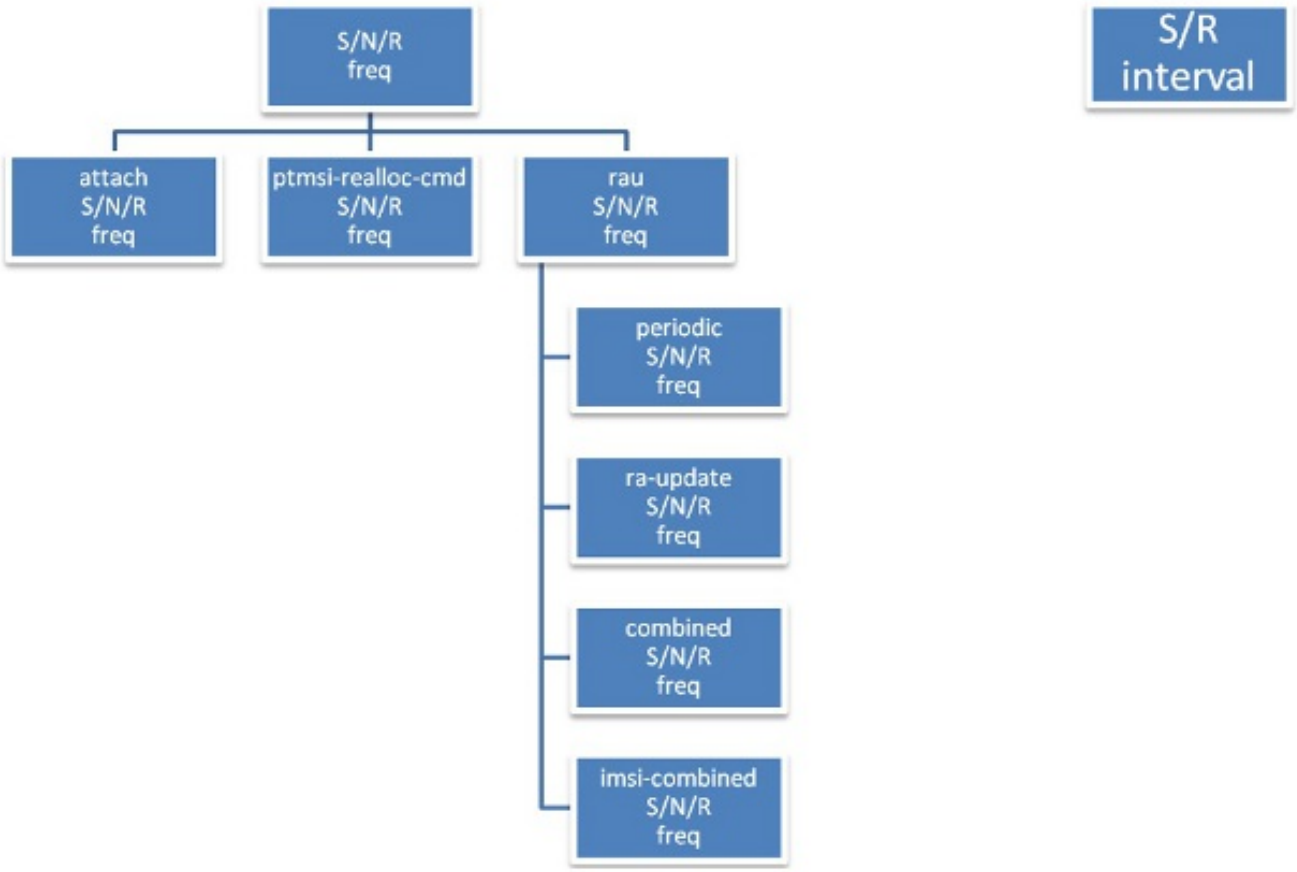

Figure 3 : Arborescence de configuration de redistribution PTMSI

Pourquoi l'authentification et redistribution de la signature PTMSI

est exigée

Par spécifications techniques 3GPP (SOLIDES TOTAUX) 23.060, la section 6.5.2, étape (4), les fonctions d'authentification sont définis dans la clause « fonction de Sécurité ». Si aucun contexte de la gestion de la mobilité (millimètre) pour le poste mobile (MS) n'existe n'importe où dans le réseau, alors l'authentification est obligatoire. Des procédures de chiffrage sont décrites dans la clause « fonction de Sécurité ». Si l'allocation PTMSI sera terminée et les supports réseau chiffrant, le réseau placera le mode de chiffrage.

Comme mentionné, SGSN exécute l'authentification seulement pour de nouvelles demandes d'enregistrement telles que des attachés IMSI et RAUs inter-SGSN dans un certain appel circule où la validation de la signature PTMSI ou du CKSN est mal adaptée avec enregistré. Par exemple, des procédures telles que RAU périodique et intra-RAUs ne sont pas exigés pour être authentifiés car elles ont déjà une base de données existante avec un SGSN enregistré. L'authentification est facultative ici. Ne pas se terminer l'authentification n'est pas toujours tout bon que l'équipement de l'utilisateur (UE) peut rester dans le réseau pendant des jours ensemble sans représentation d'une demande d'enregistrement fraîche. Il y a des occasions que l'installation de contexte de sécurité entre le SGSN et l'UE pourrait obtenir compromis, ainsi il est toujours bon périodiquement d'authentifier et vérifier la validité de l'abonné qui a été enregistré dans SGSN basé sur une certaine fréquence. Ceci est expliqué en détail dans 3GPP 23.060, la section 6.8.

Les fonctions de Sécurité et les références relatives se trouvent dans 33.102, la section 6.8. Par exemple, si l'authentification facultative est activée a basé sur des figures 18 et 19 dans la section 6.8 de 33.102, et si les essais SGSN pour authentifier l'UE avec des paramètres incorrects de contexte de sécurité, l'UE ne pourront jamais apparier la réponse d'envoi (SRES) ou la réponse prévue (XRES) avec SGSN qui a comme conséquence le reattachment au réseau. Ceci empêche l'UE restant dans le réseau avec une base de données fausse pendant un plus long temps.

Afin de fournir l'identité masquant, un SGSN génère une identité provisoire pour un IMSI appelé le PTMSI. Une fois que le MS se relie, le SGSN fournit un nouveau PTMSI au MS. Le MS alors enregistre ce PTMSI et l'emploie afin de s'identifier au SGSN dans n'importe quelle nouvelle future connexion qu'il initie. Puisque le PTMSI est toujours donné au MS dans une connexion chiffrée, personne ne pourra tracer un IMSI au PTMSI dehors, bien qu'ils pourraient voir un message de texte brut avec IMSI allant parfois. (Par exemple, la première fois qu'un IMSI se relie et des identité-réponses avec un IMSI).

La redistribution PTMSI est expliquée dans 3GPP 23.060, la section 6.8 comme procédure autonome. Les mêmes peuvent être terminés en tant qu'élément de n'importe quelle procédure de liaison ascendante afin de réapproprier des signatures PTMSI et PTMSI pour protéger des identités UE. Ceci n'augmentera pas le réseau ne signalant sur aucune interface. La redistribution de signature PTMSI et PTMSI est toujours tout bons que ceux-ci sont les identités principales que SGSN assigne à l'UE dans l'étape initiale d'enregistrement. La redistribution de ces derniers basés sur une certaine fréquence aide SGSN pour masquer l'identité de l'UE avec différentes valeurs pendant un temps prolongé au lieu de l'utilisation de juste une valeur PTMSI. Identité-masquant se rapporte à masquer des informations telles qu'IMSI et IMEI du MS, quand des messages de/au MS sont encore introduits le texte brut et quand le cryptage n'a pas commencé encore.

Problème

Dans quelques réseaux client, on l'a observé que certaines identités principales telles que MSIDN/PTMSI sont mélangées entre différents abonnés et introduites GTPC signalant des messages sur l'interface de la GN et dans les enregistrements de données de l'appel (CDR).

Les id CSCut62632 et CSCuu67401 de bogue Cisco traitent quelques cas faisants le coin de reprise de session, qui tracent l'identité d'un abonné avec des autres. Trois cas sont répertoriés ci-dessous. Tous ces cas sont code passé en revue, équipe d'assurance qualité analysée, et reproduite.

Scénario #1 (double défaut sur le sessmgr ce résultats dans la perte des identités d'abonné)

UE1 - Attache - IMSI1 - Nombre de répertoire d'abonné international de poste mobile (MSISDN) 1 - PTMSI1 - Smgr#1

La double mise à mort de l'exemple de sessmgr, SGSN a perdu les détails UE1.

UE2 - Attache - IMSI2 - MSISDN 2 - PTMSI1 - Smgr#1

PTMSI1 est réutilisé pour UE2.

UE1 - Intra RAU - PTMSI1- SGSN traite cette liaison ascendante, car l'authentification pour intra-RAU n'est pas obligatoire.

Ceci a comme conséquence le mélange des enregistrements de deux sessions différentes.

Scénario #2 l'arrêt de la pièce d'application de capacités de transaction ((TCAP) d'une session cette a en se mélangeant des identités d'abonné)

UE1 - Attache - IMSI1 - UGL réglé (TCAP - en raison intérieurement abandonnés du crash de sessmgr)

UE2 - Attache - IMSI2 - UGL envoyé avec le même TCAP - OTID

HLR envoie le TCAP - suite de la demande précédente, UE1 MSISDN

SGSN met à jour le MSISDN incorrect d'UE1 avec UE2 dans ce cas. Ceci a comme conséquence le mélange des enregistrements de deux sessions différentes.

Scénario #3 (arrêt TCAP d'une session cette résultats en se mélangeant des identités d'abonné)

UE1 - Attache - IMSI1 - SAI envoyé (TCAP - en raison intérieurement abandonnés du crash de sessmgr)

UE2 - Attache - IMSI2 - SAI envoyé avec le même TCAP - OTID

HLR envoie le TCAP - suite de la demande précédente, des vecteurs d'authentification UE1 (des triplets ou des quintuplés)

SGSN met à jour les vecteurs incorrects d'authentification d'UE1 avec UE2

Ceci a comme conséquence SGSN utilisant les vecteurs UE1 pour l'authentification d'UE2.

Approche de stabilisation

Si l'authentification pour intra-RAU est activée ou redistribution PTMSI est activé, SGSN authentifie le client avec un positionnement enregistré de vecteur. Si l'UE est différent que pour ce qu'a été enregistré, UE/SGSN ne passera pas l'étape d'authentification pour poursuivre plus loin dans le réseau. Avec ceci, la possibilité de l'UE restant dans le réseau avec une base de données incorrecte descend. Ce sont quelques zones connues dans le code. L'unité commerciale continuera à analyser plus de cas afin de comprendre cette question mieux.

Plan de difficulté

La difficulté des id de bogue Cisco est une approche de meilleur effort. Analysez plus de zones de code et déployez ceci dans le noeud moins dense pour surveiller avant que vous la prenniez à un noeud à haute densité.

Directives de configuration

L'activation de l'authentification augmente l'interface du GR et unité internationale signalant pendant que SGSN doit chercher le positionnement de vecteur d'authentification à partir du registre d'emplacement de la maison (HLR) et exécuter des procédures supplémentaires d'authentification vers l'accès. Les opérateurs doivent faire attention à choisir les valeurs de fréquence qui affectent le réseau moins.

Les indicateurs de performances de clé de protocole de l'application de la gestion de la mobilité GPRS (GMM) /Mobile (MAP) il est important analyser (ICP) avant que vous dériviez des valeurs de fréquence pour chaque procédure. Basé sur les ICP, vérifiez la procédure qui exécute la haute. Pour cette procédure, placez les valeurs élevées de la fréquence. (C'est la manière de régler avec précision chaque paramètre basé sur un modèle d'appel de réseau).

Une manière idéale de configurer ces paramètres est aux valeurs réglées aux feuilles, mais pas à la racine de l'arborescence. Par exemple, la figure 2 explique l'arborescence de configuration d'authentification. Les opérateurs pourraient choisir de placer la valeur à un niveau plus bas, comme affiché ici, au lieu de la configuration de « authentifier l'attache » directement.

```
authenticate attach attach-type gprs-only frequency 10
authenticate attach attach-type combined frequency 10
```

Il est toujours bon de placer les valeurs à haute fréquence (unités comme 10s) et surveille alors l'interface Gr/Iu signalant des seuils. Si la signalisation est tout à fait en conformité avec les limites, définissez les valeurs jusqu'à ce que la signalisation atteigne un endroit sûr près des seuils que l'opérateur voudrait placer pour leurs réseaux.

Placez la fréquence sur les diverses procédures dans 20/30 et réduisez-les à 5-10 avec la surveillance étroite sur le trafic d'interface externe. On l'exige pour vérifier l'incidence sur la CPU de mémoire de linkmgr et de sessmgr avec ce chargement excédentaire.

Les redistributions de signature PTMSI et PTMSI n'entraîneront pas le pic en signalant directement, mais il est toujours important de placer des valeurs à haute fréquence de sorte que le PTMSIs soient disponible avec des exemples de sessmgr (ce qui se produit rarement). Il n'est pas recommandé pour changer PTMSI pour chaque procédure de liaison ascendante de l'UE, comme ce n'est pas la pratique recommandée. Une valeur de 10 pourrait être convenable. Après tout ces

modifications il est important de surveiller et exécuter les vérifications de l'intégrité standard sur le système.

Comme exemple :

```
Authentication:

authenticate attach ( we can still fine tune this based on KPIs of
Inter RAT attach & attach type).

authenticate rau update-type periodic frequency 10

authenticate rau update-type ra-update frequency 5



PTMSI & PTMSI signature allocation:

ptmsi-reallocate attach

ptmsi-reallocate routing-area-update update-type ra-update

ptmsi-signature-reallocate attach frequency 10

ptmsi-signature-reallocate routing-area-update frequency 20

ptmsi-reallocate routing-area-update update-type periodic frequency 10
```

Dépannez

Quand l'authentification doit être exécutée ou signature PTMSI ou PTMSI doit être alloué, mettez au point les logs sera imprimé pour capturer pourquoi la procédure a été terminée. Ceci aides dans le dépannage en cas de toutes anomalies. Ces logs incluent la configuration du cc-profil et la valeur courante de tous les compteurs et du mouvement de la logique de décision par l'intermédiaire de la divers configuration et compteurs. En outre, les valeurs du compteur en cours par abonné peuvent être visualisées avec les **abonnés d'exposition réservés sgsn** ou des ordres **réservés gprs d'abonnés d'exposition**.

Un résultat témoin de ceci est fourni. Les compteurs de courant et le dernier horodateur authentifié sont ajoutés à la sortie complète d'ordre d'**abonnés d'exposition**.

```
[local]# show subscribers sgsn-only full all
.
.
.
DRX Parameter:
Split PG Cycle Code: 7
SPLIT on CCCH: Not supported by MS
Non-DRX timer: max. 8 sec non-DRX mode after Transfer state
CN Specific DRX cycle length coefficient: Not specified by MS
Authentication Counters
Last authenticated timestamp : 1306427164
Auth all-events UMTS : 0 Auth all-events GPRS : 0
Auth attach common UMTS : 0 Auth attach common GPRS : 0
Auth attach gprs-only UMTS : 0 Auth attach gprs-only GPRS : 0
Auth attach combined UMTS : 0 Auth attach combined GPRS : 0
Auth attach irat UMTS : 0 Auth attach irat GPRS : 0
Auth attach irat-gprs-only UMTS : 0 Auth attach irat-gprs-only GPRS : 0
```

```
Auth attach irat-combined UMTS : 0 Auth attach irat-combined GPRS : 0
Auth UMTS : 0 Auth GPRS : 0
Auth serv-req : 0 Auth serv-req data : 0
Auth serv-req signaling : 0 Auth serv-req page-rsp : 0
Auth rau UMTS : 0 Auth rau GPRS : 0
Auth rau periodic UMTS : 0 Auth rau periodic GPRS : 0
Auth rau ra-upd UMTS : 0 Auth rau ra-upd GPRS : 0
Auth rau ra-upd lcl-ptmsi UMTS : 0 Auth rau ra-upd lcl-ptmsi GPRS : 0
Auth rau ra-upd irat-lcl-ptmsi UMTS : 0 Auth rau ra-upd irat-lcl-ptmsi GPRS : 0
Auth rau comb UMTS : 0 Auth rau comb GPRS : 0
Auth rau comb lcl-ptmsi UMTS : 0 Auth rau comb lcl-ptmsi GPRS : 0
Auth rau comb irat-lcl-ptmsi UMTS : 0 Auth rau comb irat-lcl-ptmsi GPRS : 0
Auth rau imsi-comb UMTS : 0 Auth rau imsi-comb GPRS : 0
Auth rau imsi-comb lcl-ptmsi UMTS : 0 Auth rau imsi-comb lcl-ptmsi GPRS : 0
Auth rau imsi-comb irat-lcl-ptmsi UMTS: 0 Auth rau imsi-comb irat-lcl-ptmsi GPRS: 0
Auth sms UMTS : 0 Auth sms GPRS : 0
Auth sms mo-sms UMTS : 0 Auth sms mo-sms GPRS : 0
Auth sms mt-sms UMTS : 0 Auth sms mt-sms UMTS : 0
PTMSI Realloc Counters
Last allocated timestamp : 1306427165
PTMSI Realloc Freq UMTS : 0 PTMSI Realloc Freq GPRS : 0
PTMSI Realloc Attach UMTS : 0 PTMSI Realloc Attach GPRS : 0
PTMSI Realloc Serv-Req : 0 PTMSI Realloc Serv-Req Data : 0
PTMSI Realloc Serv-Req Signaling : 0 PTMSI Realloc Serv-Req Page-rsp : 0
PTMSI Realloc Rau UMTS : 0 PTMSI Realloc Rau GPRS : 0
PTMSI Realloc Rau Periodic UMTS : 0 PTMSI Realloc Rau Periodic GPRS : 0
PTMSI Realloc Rau Ra-Upd UMTS : 0 PTMSI Realloc Rau Ra-Upd GPRS : 0
PTMSI Realloc Rau Comb-Upd UMTS : 0 PTMSI Realloc Rau Comb-Upd GPRS : 0
PTMSI Realloc Rau Imsi-Comb-Upd UMTS : 0 PTMSI Realloc Rau Imsi-Comb-Upd GPRS : 0
PTMSI Sig Realloc Counters
Last allocated timestamp : 0
PTMSI Sig Realloc Freq UMTS : 0 PTMSI Sig Realloc Freq GPRS : 0
PTMSI Sig Realloc Attach UMTS : 0 PTMSI Sig Realloc Attach GPRS : 0
PTMSI Sig Realloc Ptmsi-rel-cmd UMTS : 0 PTMSI Sig Realloc Ptmsi-rel-cmd GPRS : 0
PTMSI Sig Realloc Rau UMTS : 0 PTMSI Sig Realloc Rau GPRS : 0
PTMSI Sig Realloc Rau Periodic UMTS : 0 PTMSI Sig Realloc Rau Periodic GPRS : 0
PTMSI Sig Realloc Rau Ra-Upd UMTS : 0 PTMSI Sig Realloc Rau Ra-Upd GPRS : 0
PTMSI Sig Realloc Rau Comb-Upd UMTS : 0 PTMSI Sig Realloc Rau Comb-Upd GPRS : 0
PTMSI Sig Realloc Rau Imsi-Comb UMTS : 0 PTMSI Sig Realloc Rau Imsi-Comb GPRS : 0
CAE Server Address:
Subscription Data:
.
.
```

Si la question est vue dans le réseau, sélectionnez ces commandes afin de collecter des informations pour l'unité commerciale pour l'utiliser pour analyser la question plus loin :

```
show subscribers gprs-only full msisdn <msisdn>
show subscribers gprs-only full imsi <imsi>
show subscribers sgsn-only msisdn <msisdn>
show subscribers sgsn-only msisdn <imsi>
show subscribers gprs-debug-info callid <callid> (get o/p for both callid)
show subscribers debug-info callid <callid> (get o/p for both callid)
task core facility sessmgr instance < >
task core facility imsimgr instance < >
Mon sub using MSISDN or pcap traces
SSD during issue.
Syslogs during the issue.
```

Risques

Accru signalant vers des interfaces Gr/Iu plus une légère incidence CPU de processus interne

(linkmgr) si vous authentifiez trop fréquemment.

Syntaxe de commande

Toutes les commandes sont dans la configuration/mode d'appel-contrôle-profil et les privilèges d'opérateur s'appliquent. Un instantané des commandes sous le cc-profil est comme suit :

```
Authentication
1. Attach
authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{frequency <1..16>} {access-type [umts | gprs]}
no authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{access-type [umts | gprs]}
remove authenticate attach {inter-rat} {attach-type [gprs-only | combined ]}
{access-type [umts | gprs]}

2. Service-request
authenticate service-request {service-type [data | signaling | page-response]}
{frequency <1..16> | periodicity <1..10800>}
no authenticate service-request {service-type [data | signaling | page-response]}
remove authenticate service-request {service-type [data | signaling | page-response]}
{periodicity}
3. Rau
authenticate rau {update-type periodic} {frequency <1..16> | periodicity <1..10800>}
{access-type [umts | gprs]}
authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi]} {frequency <1..16> |
periodicity <1..10800>}
{access-type [umts| gprs]}
authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with foreign-ptmsi} {access-type [umts| gprs]}
no authenticate rau {update-type periodic} {access-type [umts | gprs]}
no authenticate rau {update-type [ra-update | combined-update | imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi | foreign-ptmsi]}
{access-type [umts| gprs]}
remove authenticate rau {update-type periodic} {periodicity}
{access-type [umts | gprs]}
remove authenticate rau {update-type [ra-update | combined-update |
imsi-combined-update]}
{with [local-ptmsi | inter-rat-local-ptmsi]} { periodicity} {access-type [umts| gprs]}
remove authenticate rau {update-type [ra-update | combined-update |
imsi-combined-update]}
{with foreign-ptmsi} {access-type [umts| gprs]}
4. Sms
authenticate sms {sms-type [mo-sms | mt-sms]} {frequency <1..16>}
{access-type [umts | gprs]}
no authenticate sms {sms-type [mo-sms | mt-sms]} {access-type [umts | gprs]}
remove authenticate sms {sms-type [mo-sms | mt-sms]} {access-type [umts | gprs]}
5. Detach
authenticate detach {access-type [umts | gprs]}
no authenticate detach {access-type [umts | gprs]}
remove authenticate detach {access-type [umts | gprs]}
6. All-events
authenticate all-events {frequency <1..16>} {access-type [umts | gprs]}
no authenticate all-events {access-type [umts | gprs]}
remove authenticate all-events {access-type [umts | gprs]}

PTMSI Reallocation
1. Attach
ptmsi-reallocate attach {frequency <1..50>} {access-type [umts | gprs]}
```

no ptmsi-reallocate attach {access-type [umts | gprs]}
remove ptmsi-reallocate attach {access-type [umts | gprs]}
2. **Service-request**
ptmsi-reallocate service-request {service-type [data | signaling | page-response]}
{frequency <1..50>} no ptmsi-reallocate service-request
{service-type [data | signaling | page-response]}
remove ptmsi-reallocate service-request {service-type [data | signaling |
page-response]}
3. **Routing-area-update**
ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
4. **Interval/frequency**
ptmsi-reallocate [interval <60..1440> | frequency <1..50>] {access-type [umts | gprs]}
no ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-reallocate [interval | frequency] {access-type [umts | gprs]}

PTMSI-Signature Reallocation
1. Attach
ptmsi-signature-reallocate attach {frequency <1..50>} {access-type [umts | gprs]}
no ptmsi-signature-reallocate attach {access-type [umts | gprs]}
remove ptmsi-signature-reallocate attach {access-type [umts | gprs]}
2. PTMSI Reallocation command
ptmsi-signature-reallocate ptmsi-reallocation-command {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-signature-reallocate ptmsi-reallocation-command {access-type [umts | gprs]}
remove ptmsi-signature-reallocate ptmsi-reallocation-command
{access-type [umts | gprs]}
3. Routing-area-update
ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {frequency <1..50>}
{access-type [umts | gprs]}
no ptmsi-signature-reallocate routing-area-update {update-type [periodic | ra-update |
combined-update | imsi-combined-update]} {access-type [umts | gprs]}
remove ptmsi-signature-reallocate routing-area-update {update-type [periodic |
ra-update | combined-update | imsi-combined-update]} {access-type [umts | gprs]}
4. Interval/frequency
ptmsi-signature-reallocate [interval <60..1440> | frequency <1..50>]
{access-type [umts | gprs]}
no ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}
remove ptmsi-signature-reallocate [interval | frequency] {access-type [umts | gprs]}