Meilleures pratiques d'authentification SGSN et de réallocation PTMSI de la gamme ASR 5x00

Contenu

[Introduction](#)
[Aperçu](#)
[Blocs de procédure d'authentification SGSN et de signature PTMSI](#)
[Pourquoi l'authentification et la réallocation des signatures PTMSI sont nécessaires](#)
[Problème](#)
[Approche de stabilisation](#)
[Plan de réparation](#)
[Directives de configuration](#)
[Dépannage](#)
[Risques](#)
[Syntaxe de commande](#)

Introduction

Ce document fournit une explication de base des avantages de la configuration de la fréquence de la procédure d'authentification, de l'identité PTMSI (Packet Temporaire Mobile Subscriber Identity) et de la réallocation des signatures PTMSI. Plus précisément, ce document concerne une procédure facultative de gestion de la mobilité du projet de partenariat de troisième génération pour 2G et 3G sur le noeud de support GPRS (SGSN) de service qui s'exécute sur la gamme ASR 5000.

Ce document explique les meilleures pratiques suivantes :

- Paramètre de fréquence d'authentification
- Réallocation PTMSI
- Réallocation de signature PTMSI
- L'impact si vous ne configurez pas le paramètre de fréquence d'authentification et la réallocation PTMSI et la réallocation de signature (en fonction de l'expérience des cas client)
- Directives de configuration et impact sur les interfaces externes
- Options de dépannage

Aperçu

L'infrastructure d'authentification, de PTMSI et de réallocation des signatures 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 SGSN 2G et 3G et l'entité de gestion mobile (MME). Dans le SGSN, l'authentification peut actuellement être configurée pour ces procédures :

attachement, demande de service, mise à jour de la zone de routage (RAU), service de messagerie courte et détachement.

MME utilise également le même cadre afin de configurer l'authentification pour les demandes de service et les mises à jour de zone de suivi (TAU). La réallocation PTMSI est configurable pour l'attachement, la demande de service et les unités de rack. La réallocation des signatures PTMSI est configurable pour les fonctions d'attachement, de réallocation PTMSI et RAU. L'authentification et la réallocation peuvent être activées pour chaque instance de ces procédures ou pour chaque instance nth de la procédure, appelée authentification/réallocation sélective. Certaines procédures prennent également en charge l'activation de l'authentification ou de la réallocation en fonction du temps écoulé (périodicité ou intervalle) depuis la dernière authentification ou réallocation, respectivement.

En outre, ils peuvent être configurés spécifiquement pour le système UMTS (Universal Mobile Telecommunications System) (3G) ou le service GPRS (General Packet Radio Service) (2G) ou les deux. Cette configuration est vérifiée uniquement lorsqu'il est facultatif pour le SGSN d'authentifier ou de réallouer la signature PTMSI/PTMSI d'un abonné. Dans les scénarios où ces procédures sont obligatoires, cette configuration n'est pas vérifiée.

Il existe trois types de CLI pour chaque configuration de fréquence de procédure : une CLI SET, une CLI NO et une CLI REMOVE. Lorsque vous appelez une CLI SET, l'opérateur veut activer l'authentification ou la réallocation pour la procédure spécifique. L'interface de ligne de commande NO doit désactiver explicitement l'authentification ou la réallocation PTMSI pour une procédure, et l'interface de ligne de commande REMOVE doit restaurer la configuration dans un état où l'interface de ligne de commande (SET ou NO) n'est pas configurée du tout. Toutes les configurations sont supposées SUPPRIMÉES lorsque l'arborescence est initialisée dans l'allocation cc-profile. Par conséquent, REMOVE est la configuration par défaut.

L'interface de ligne de commande SET n'affecte qu'une seule procédure spécifique dans l'arborescence, tandis que l'interface de ligne de commande NO CLI et l'interface de ligne de commande REMOVE CLI affectent la procédure actuelle et SUPPRIMENT également les noeuds inférieurs. En outre, si NO CLI ou REMOVE CLI affecte l'arbre commun, l'effet doit être propagé sur les noeuds correspondants dans les arbres spécifiques à l'accès également.

Il existe deux types de CLI pour chaque configuration de périodicité de procédure : la CLI SET et la CLI REMOVE. L'ENSEMBLE et l'ENREGISTREMENT terminés par rapport à la périodicité n'affectent que la configuration de la périodicité et ne modifient pas la configuration de la fréquence. L'interface de ligne de commande NO exécutée pour la fréquence (pour être précis, l'interface de ligne de commande NO est courante en ce sens qu'elle ne prend aucun argument de fréquence ou de périodicité, mais qu'elle est identifiée avec la configuration de fréquence en interne lors du stockage) SUPPRIME également la configuration de périodicité.

Certains scénarios dans lesquels l'authentification est effectuée sans condition sont les suivants :

- Association d'identité d'abonné mobile international (IMSI) - toutes les pièces jointes IMSI sont authentifiées
- lorsque l'abonné n'a pas été authentifié auparavant et que vous n'avez pas de vecteur
- En cas de non-correspondance de signature PTMSI
- En cas de non-correspondance de CKSN (Ciphering Key Sequence Number)

Actuellement, l'authentification peut être activée pour ceux-ci sous call-control-profile :

- attachement, demande de service, RAU, détachement, service de messagerie courte, tous les

événements et TAU
- La TAU est utilisée par MME
- La connexion et la demande de service sont utilisées à la fois par SGSN et MME
- Les autres sont utilisés exclusivement par SGSN

Blocs de procédure d'authentification SGSN et de signature PTMSI

Cette structure d'arborescence explique les blocs de procédure que le SGSN prend en compte pour les paramètres de fréquence.

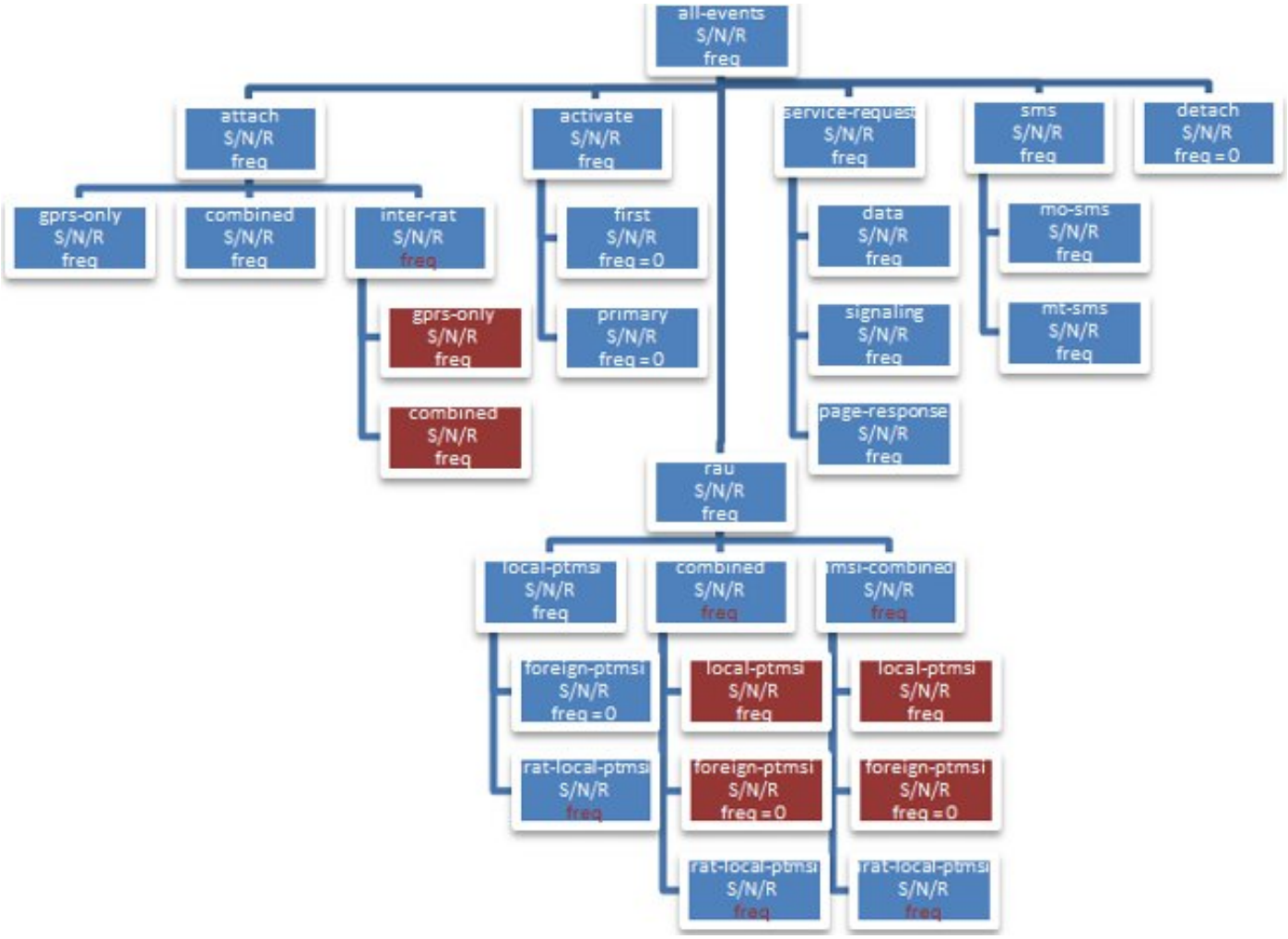

Figure 1 : Blocs de procédure SGSN pris en compte pour les paramètres de fréquence

Les arborescences de la procédure de réallocation PTMSI sont indiquées ici.

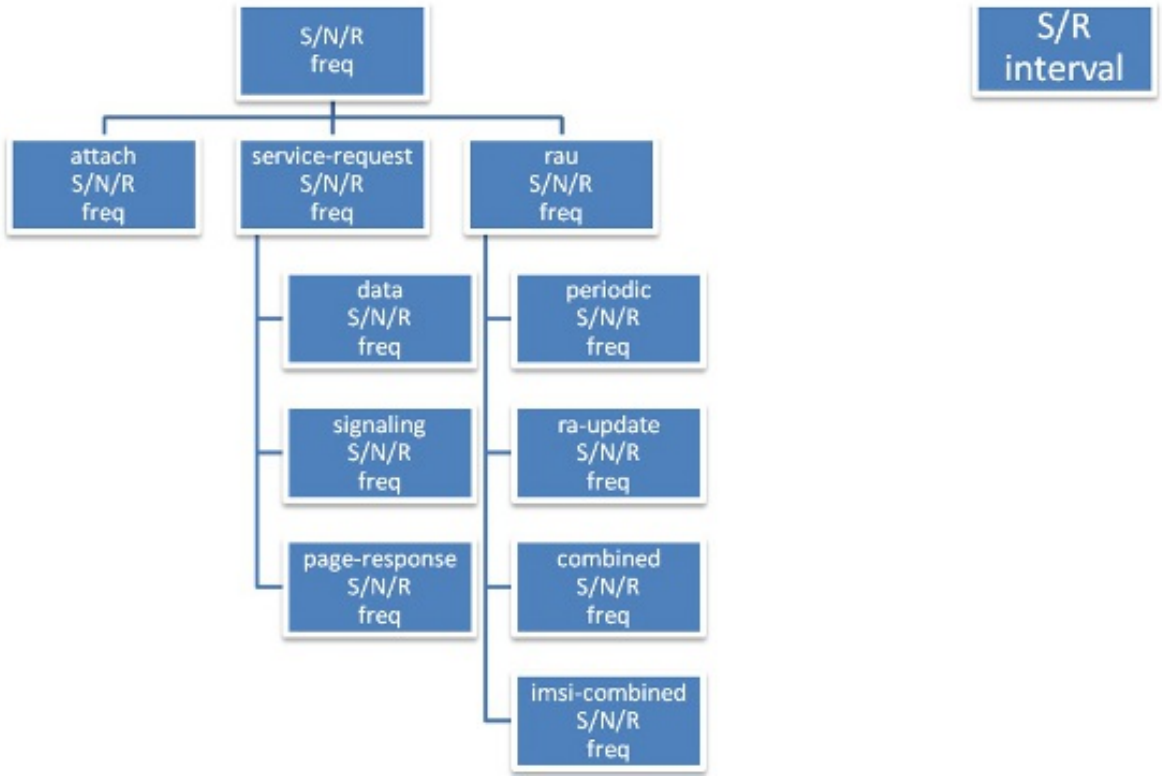

Figure 2 : Arborescence de configuration d'authentification

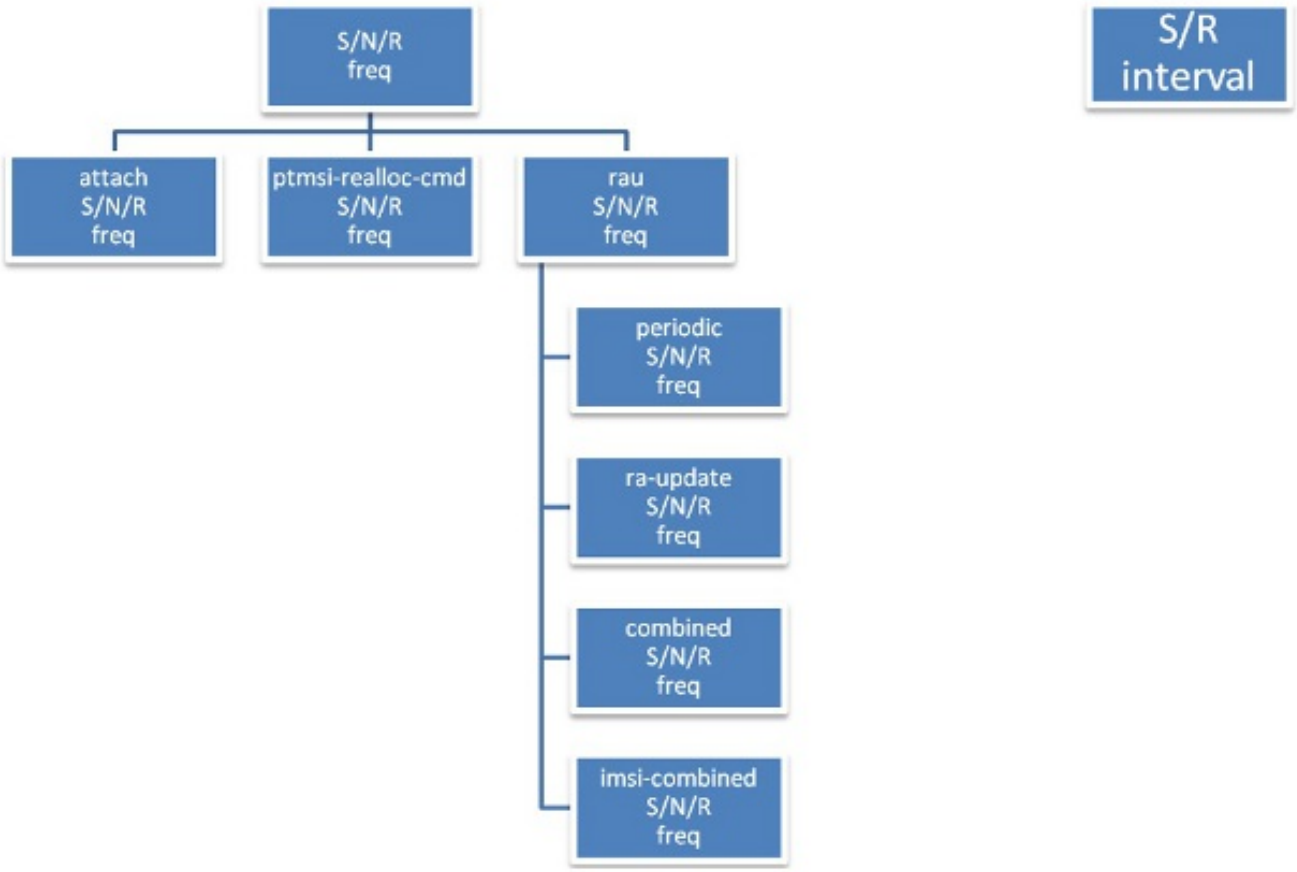

Figure 3 : Arborescence de configuration de réallocation PTMSI

Pourquoi l'authentification et la réallocation des signatures

PTMSI sont nécessaires

Selon les spécifications techniques (TS) 23.060 de 3GPP, section 6.5.2, étape (4), les fonctions d'authentification sont définies dans la clause « Fonction de sécurité ». Si aucun contexte de gestion de la mobilité (MM) pour la station mobile (MS) n'existe sur le réseau, l'authentification est obligatoire. Les procédures de chiffrement sont décrites dans la clause « Fonction de sécurité ». Si l'allocation PTMSI est terminée et que le réseau prend en charge le chiffrement, le réseau doit définir le mode de chiffrement.

Comme mentionné, SGSN effectue l'authentification uniquement pour les nouvelles demandes d'enregistrement telles que les pièces jointes IMSI et les RAU inter-SGSN dans certains flux d'appels où la validation de la signature PTMSI ou du CKSN ne correspond pas à celle stockée. Par exemple, les procédures telles que les RAU périodiques et les intra-RAU ne sont pas obligatoires pour être authentifiées car elles ont déjà une base de données existante avec un SGSN enregistré. L'authentification est facultative ici. L'échec de l'authentification n'est pas toujours une bonne chose, car l'équipement utilisateur (UE) peut rester sur le réseau pendant des jours sans qu'une nouvelle demande d'enregistrement ne soit effectuée. Il y a des chances que la configuration du contexte de sécurité entre le SGSN et l'UE soit compromise, il est donc toujours bon de s'authentifier périodiquement et de vérifier la validité de l'abonné qui a été enregistré dans le SGSN en fonction d'une certaine fréquence. Ceci est expliqué en détail à la section 6.8 de la section 3GPP 23.060.

Les fonctions de sécurité et les références connexes se trouvent à la section 6.8 de la section 33.102. Par exemple, si l'authentification facultative est activée sur la base des Figures 18 et 19 de la section 6.8 de 33.102, et si SGSN tente d'authentifier l'UE avec des paramètres de contexte de sécurité incorrects, l'UE ne pourra jamais faire correspondre la réponse d'envoi (SRES) ou la réponse attendue (XRES) avec le SGSN, ce qui entraîne une réattachement au réseau. Cela empêche l'UE de rester sur le réseau avec une fausse base de données pendant plus longtemps.

Afin de fournir une masquage d'identité, un SGSN génère une identité temporaire pour un IMSI appelé PTMSI. Une fois que le MS est joint, le SGSN émet un nouveau PTMSI à l'MS. Le MS stocke ensuite ce PTMSI et l'utilise afin de s'identifier au SGSN dans toute nouvelle connexion future qu'il initiera. Puisque l'ISTSM est toujours donnée à l'ÉM dans une connexion chiffrée, personne ne pourra mapper un IMSI à l'ISTSM à l'extérieur, même s'il peut y avoir un message en texte clair avec l'IMSI en cours. (Par exemple, la première fois qu'un IMSI joint et répond par identité à un IMSI).

La réaffectation de PTMSI est expliquée à la section 6.8 de la section 3GPP 23.060 comme procédure autonome. La même chose peut être effectuée dans le cadre de toute procédure de liaison ascendante afin de réallouer les signatures PTMSI et PTMSI pour protéger les identités UE. Cela n'augmentera la signalisation réseau sur aucune interface. La réallocation des signatures PTMSI et PTMSI est toujours bonne, car il s'agit des identités clés que le SGSN attribue à l'UE lors de l'étape d'enregistrement initiale. La réaffectation de ces valeurs en fonction d'une certaine fréquence aide SGSN à cacher l'identité de l'UE avec différentes valeurs pendant une longue période au lieu d'utiliser une seule valeur PTMSI. Le masquage d'identité désigne le masquage d'informations telles que IMSI et IMEI de l'État membre, lorsque les messages de/vers l'État membre sont toujours envoyés en texte brut et lorsque le chiffrement n'a pas encore commencé.

Problème

Dans certains réseaux de clients, il a été observé que certaines identités clés telles que MSIDN/PTMSI sont mélangées entre différents abonnés et envoyées dans des messages de signalisation GTPC sur l'interface Gn et dans les enregistrements de données d'appel (CDR).

Les ID de bogue Cisco CSCut62632 et CSCuu67401 traitent certains cas de récupération de session en coin, qui mappent l'identité d'un abonné à un autre. Trois cas sont énumérés ci-dessous. Tous ces cas sont examinés, analysés et reproduits par l'équipe d'assurance de la qualité.

Scénario 1 (Double erreur sur sessmgr qui entraîne la perte des identités des abonnés)

UE1 - Attach - IMSI1 - Mobile Station International Subscriber Directory Number (MSISDN) 1 - PTMSI1 - Smgr#1

Double suppression de l'instance de sessmgr, SGSN a perdu des détails UE1.

UE2 - Attacher - 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.

Il en résulte un mélange des enregistrements de deux sessions différentes.

Scénario 2 (abandon de la partie Application des capacités de transaction (TCAP) d'une session qui entraîne le mélange des identités des abonnés)

UE1 - Attach - IMSI1 - UGL set (TCAP - abandonné en interne en raison d'un plantage de sessmgr)

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

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

Le SGSN met à jour le MSISDN incorrect de UE1 avec UE2 dans ce cas. Il en résulte un mélange des enregistrements de deux sessions différentes.

Scénario 3 (abandon TCAP d'une session qui entraîne le mélange des identités des abonnés)

UE1 - Attach - IMSI1 - SAI envoyé (TCAP - Abandon interne en raison d'un plantage de sessmgr)

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

HLR envoie TCAP - suite de la demande précédente, vecteurs d'authentification de l'UE1 (triplets ou quintuplets)

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

Cela donne lieu à l'utilisation de vecteurs UE1 par SGSN pour l'authentification UE2.

Approche de stabilisation

Si l'authentification pour l'intra-RAU est activée ou si la réallocation PTMSI est activée, le SGSN authentifie le client avec un ensemble de vecteurs stockés. Si l'UE est différente de ce pour quoi elle a été stockée, UE/SGSN ne passera pas l'étape d'authentification pour continuer dans le réseau. Ainsi, la probabilité que l'UE reste dans le réseau avec une base de données incorrecte diminue. Ce sont des zones connues dans le code. L'unité opérationnelle continuera d'analyser davantage de cas afin de mieux comprendre cette question.

Plan de réparation

La correction à partir des ID de bogue Cisco est une approche au mieux. Analysez plus de zones de code et déployez-les dans un noeud moins dense pour la surveillance avant de l'amener à un noeud haute densité.

Directives de configuration

L'activation de l'authentification augmente la signalisation de l'interface Gr et Iu, car le SGSN doit récupérer le jeu de vecteurs d'authentification à partir du Registre de localisation résidentielle (HLR) et exécuter des procédures d'authentification supplémentaires pour l'accès. Les opérateurs doivent faire attention à choisir des valeurs de fréquence qui affectent moins le réseau.

Les indicateurs de performance clés (KPI) GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) sont importants à analyser avant de calculer les valeurs de fréquence pour chaque procédure. En fonction des indicateurs de performance clés, vérifiez la procédure qui s'exécute en haut. Pour cette procédure, définissez des valeurs élevées de fréquence. (Il s'agit de la manière de régler chaque paramètre en fonction d'un modèle d'appel réseau).

Une façon idéale de configurer ces paramètres est de définir des valeurs sur des feuilles, mais pas à la racine de l'arborescence. Par exemple, la Figure 2 explique l'arborescence de configuration de l'authentification. Les opérateurs peuvent choisir de définir la valeur à un niveau inférieur, comme indiqué ici, au lieu de configurer l'authentification de la connexion directement.

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

Il est toujours utile de définir des valeurs de haute fréquence (unités par 10), puis de surveiller les seuils de signalisation d'interface Gr/Iu. Si la signalisation est bien à l'intérieur des limites, définissez des valeurs jusqu'à ce que la signalisation atteigne un endroit sûr près des seuils que l'opérateur souhaite définir pour ses réseaux.

Réglez la fréquence des différentes procédures en 20/30 et réduisez-les à 5-10 avec une surveillance étroite du trafic d'interface externe. Il est nécessaire de vérifier l'impact sur linkmgr et le CPU mémoire de sessmgr avec cette charge excessive.

Les réallocations de signature PTMSI et PTMSI ne provoqueront pas de pic dans la signalisation directe, mais il est toujours important de définir des valeurs de haute fréquence afin que les PTMSI soient disponibles avec les instances sessmgr (ce qui arrive rarement). Il n'est pas recommandé de modifier PTMSI pour chaque procédure de liaison ascendante à partir de l'UE, car ce n'est pas la meilleure pratique. Une valeur de 10 peut être décente. Après toutes ces modifications, il est important de surveiller et d'effectuer des contrôles d'intégrité standard sur le système.

Par 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
```

Dépannage

Lorsque l'authentification doit être effectuée ou que la signature PTMSI ou PTMSI doit être attribuée, les journaux de débogage sont imprimés pour saisir la raison pour laquelle la procédure a été terminée. Cela facilite le dépannage en cas d'incompatibilité. Ces journaux incluent la configuration à partir de cc-profile et la valeur actuelle de tous les compteurs, ainsi que le déplacement de la logique de décision via les différentes configurations et compteurs. En outre, les valeurs de compteur actuelles par abonné peuvent être affichées à l'aide des commandes **show users sgsn-only** ou **show subscribe gprs-only**.

Un exemple de résultat est fourni. Les compteurs actuels et le dernier horodatage authentifié sont ajoutés à la sortie complète de la commande **show abonnés**.

```
[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 le problème apparaît sur le réseau, entrez ces commandes afin de collecter des informations que l'unité commerciale doit utiliser pour analyser le problème plus en détail :

```
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

Signalisation accrue vers les interfaces Gr/Iu plus un impact léger sur le processeur du processus

interne (linkmgr) si vous vous authentifiez trop souvent.

Syntaxe de commande

Toutes les commandes sont en mode configuration/call-control-profile et les privilèges d'opérateur s'appliquent. Voici un instantané des commandes sous le profil cc :

```
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]}
```