

ASR 5x00系列SGSN验证和PTMSI重新分配最佳实践

目录

[简介](#)

[概述](#)

[SGSN验证和PTMSI签名步骤块](#)

[验证和PTMSI签名重新分配为什么要求](#)

[问题](#)

[稳定方法](#)

[修正规划](#)

[配置指南](#)

[故障排除](#)

[风险](#)

[命令语法](#)

简介

本文提供认证程序频率配置、数据包临时移动用户标识(PTMSI)和PTMSI签名重新分配的好处的基本说明。特别地，本文是为2G和3G的一个可选第三代合伙企业项目移动性管理计划在服务GPRS支持节点(SGSN)在Aggregated的该运行服务路由器(ASR) 5000系列。

本文解释这些最佳实践：

- 验证频率设置
- PTMSI重新分配
- PTMSI签名重新分配
- 影响，如果不配置验证频率设置和PTMSI重新分配和签名重新分配(根据从用户案例的体验)
- 配置指南和影响在外部接口
- 选项排除故障问题

概述

验证，PTMSI和PTMSI签名在呼叫控制配置文件下的重新分配框架使操作员配置PTMSI和PTMSI签名的验证或分配每个2G和3G的SGSN和移动管理实体(MME)用户。在SGSN中，验证可能为这些步骤当前配置-附上、服务请求、路由区域更新(RAU)，肖特消息传送服务，并且分开。

MME也利用同一个框架为了配置服务请求和跟踪区域更新的(TAUs)验证。PTMSI重新分配为附上、服务请求和RAUs是可配置。PTMSI签名重新分配为附上，PTMSI重新分配命令和RAUs是可配置。验证和重新分配可以启用为这些步骤每个实例或为步骤的每个第n个实例，呼叫有选择性的验证/重新分配。某些步骤也支持验证的启动或根据时间的重新分配流逝了(周期或间隔)，因为各自最后

验证或重新分配。

此外，这些可以为通用移动通信系统(UMTS) (3G)特别地配置或仅通用分组无线业务(GPRS) (2G)或两个。只有当对于SGSN是可选的验证或再分配用户的PTMSI/PTMSI签名时，此配置被检查。在执行这些步骤的方案中是必须的，此配置没有被检查。

有CLIs的三种类型每个步骤的频率配置的- SET CLI、没有CLI和删除CLI。当您调用SET CLI时，操作员希望对启用认证或重新分配特定步骤的。CLI不是明确地禁用验证或PTMSI重新分配步骤的，并且删除CLI是恢复配置对CLI的状态(SET或不)根本没有配置。当树在CC配置文件分配时，初始化所有配置采取删除。因此，删除是默认配置。

当CLI和删除CLI不会影响当前步骤并且删除更低节点时，SET CLI只将影响在树的一个特定步骤。并且，如果CLI或删除CLI不影响普通的树，效果在访问特定树的对应的节点也将被传播。

有CLIs的两种类型每个步骤的周期配置的- SET CLI和删除CLI。SET和删除完成周期将影响仅周期配置并且留给频率配置未触动过。为频率执行的CLI (是准确的，CLI不普通因为不采取任何频率或周期参数，但是识别与频率配置内部地，虽然存储)不会删除周期配置。

验证绝对地完成的某些方案如下：

- 国际移动用户标识(IMSI)附上-所有IMSI随员验证
- 当用户以前未验证，并且时您没有一矢量
- 当有PTMSI签名不匹配
- 当有一加密的键序列序号(CKSN)不匹配

目前，验证可以为这些启用在呼叫控制下-配置文件：

- 附上，服务请求，RAU，分开，肖特消息传送服务、全事件和TAU
- TAU由MME是在使用中的
- SGSN和MME使用附上和服务请求
- SGSN完全使用其余

SGSN验证和PTMSI签名步骤块

此树型结构解释SGSN为频率设置考虑的步骤块。

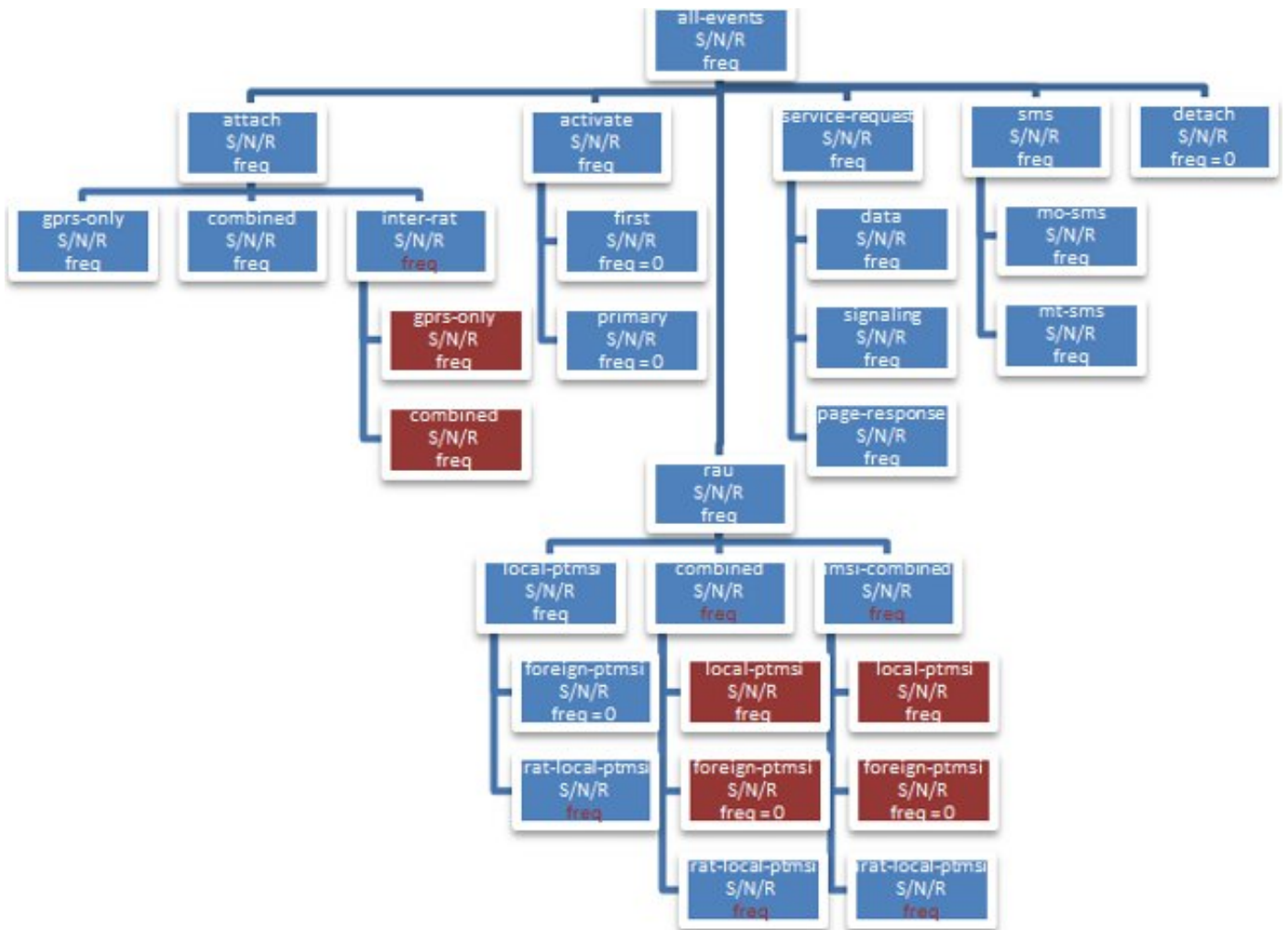


图 1：步骤块SGSN为频率设置考虑

PTMSI重新分配步骤的树显示此处。

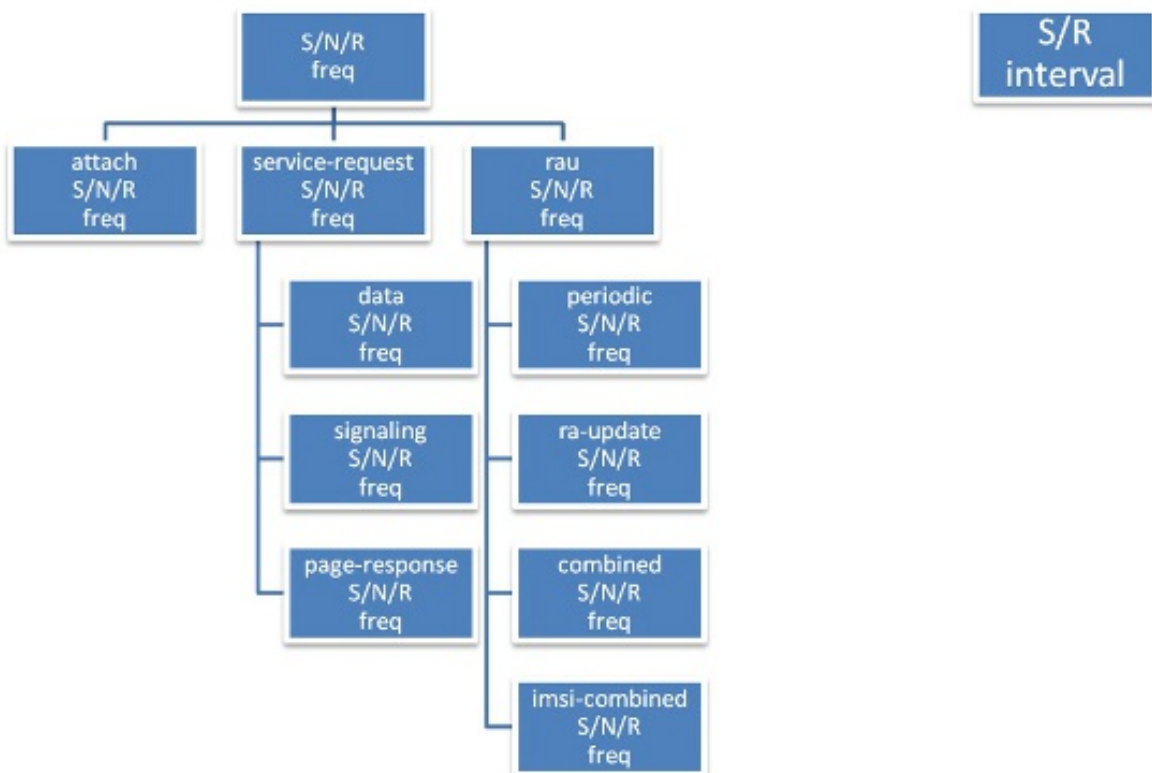


图 2：身份验证配置树

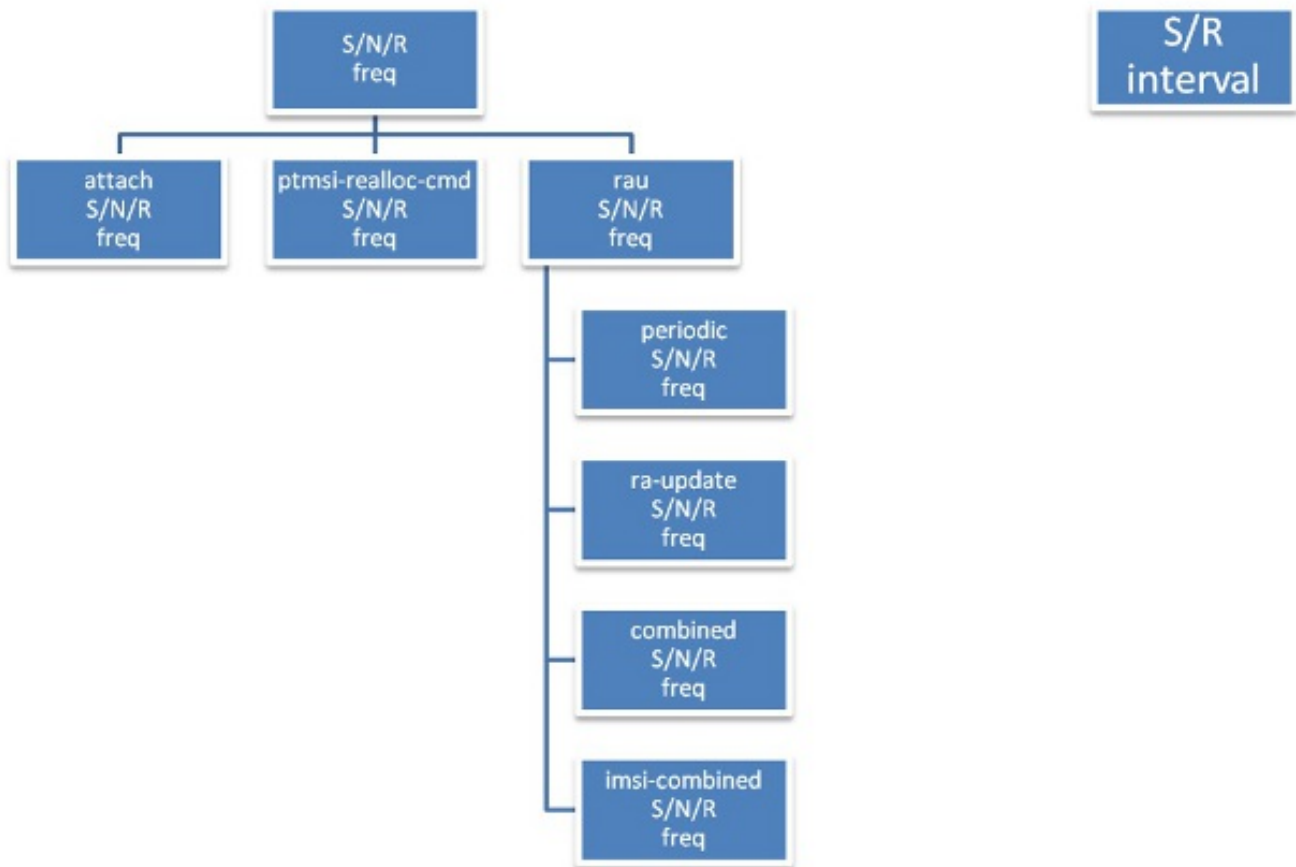


图 3 : PTMSI重新分配配置树

验证和PTMSI签名重新分配为什么要求

每3GPP技术规范(TS) 23.060，第6.5.2部分，步骤(4)，验证功能在条款“安全功能”定义。如果移动站点的(MS)移动管理(MM)上下文任何地方在网络不存在，则验证是必须。加密的步骤在条款“安全功能”描述。如果PTMSI分配将完成，并且网络支持加密，网络将设置加密的模式。

如被提及，SGSN在PTMSI签名或CKSN验证不匹配与存储的一个的有些呼叫流执行仅验证新注册请求的例如IMSI随员和相互的SGSN RAUs。例如，因为他们已经有与已注册SGSN的现有的数据库步骤例如定期RAU和内部RAUs没有要求验证。验证可选在这里。不完成验证总是不是好，虽然用户设备(UE)在网络能一起聚集好几天，不用新注册请求的性能。有机会在SGSN和UE之间的安全上下文设置也许获得折衷，因此周期地验证和检查在根据若干频率的SGSN注册用户的正确性总是好的。这在3GPP 23.060详细解释，第6.8部分。

安全功能和相关参考在33.102查找，第6.8部分。例如，如果可选验证根据在第6.8部分的图18和19启用33.102，并且，如果SGSN设法验证与不正确安全上下文参数的UE，UE不能匹配发送答复(SRES)或期望的响应(XRES)与导致再附着对网络的SGSN。这防止坚持在与一个错误数据库的网络的UE最长时间的。

为了提供隐藏的标识，SGSN生成呼叫PTMSI的IMSI的一临时标识。一旦MS附加，SGSN问题新的PTMSI对MS。MS然后存储此PTMSI并且使用它为了识别到首次在其中任一SGSN新建的将来连接。因为PTMSI总是给对在一加密的连接MS，没人能从外部映射IMSI到PTMSI，虽然他们也许发现与时常去的IMSI的明文消息。(例如，第一次IMSI附加和与IMSI的标识答复)。

PTMSI重新分配在3GPP 23.060解释，第6.8部分作为一个独立步骤。同样可以完成作为所有上行链

路步骤一部分为了再分配PTMSI和PTMSI签名保护UE标识。这不会增加在任何接口的网络信令。PTMSI和PTMSI签名重新分配总是好，虽然这些是SGSN分配到在最初的注册步骤的UE的关键标识。根据若干频率的这些的重新分配帮助SGSN隐藏UE的标识用不同的值的长时期的时间而不是使用一个PTMSI值。标识隐藏是指隐藏信息例如MS的IMSI和IMEI，当信息从/至MS在明文时仍然传送，并且，当加密未开始时。

问题

在一些客户网络中，注意到一些锁上标识例如MSISDN/PTMSI被混合区别用户之间并且发送在Gn接口的GTPC信令消息和在呼叫数据(CDR)。

Cisco Bug ID [CSCut62632](#)和[CSCuu67401](#)处理一些稀有案例会话恢复，映射一个用户标识有别的。三个案件下面是列出的。所有这些案件是查看的代码，质量保证团队被分析和被再生产。

方案#1 (在导致用户标识损耗)的sessmgr的双故障

UE1 -附上- IMSI1 -移动站点国际订户目录号(MSISDN) 1个- PTMSI1 - Smgr#1

sessmgr实例双杀，SGSN丢失UE1详细信息。

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

PTMSI1为UE2被重新使用。

UE1 -内部RAU - PTMSI1- SGSN处理此上行链路，因为内部RAU的验证不是必须。

这导致混合两不同的会话记录。

方案#2 (导致混合用户标识)一会话的事务处理部分(TCAP)中止

UE1 -附上- IMSI1 -设置的UGL (TCAP -内部地中止的由于sessmgr失败)

UE2 -附上- IMSI2 -用同样TCAP传送的UGL - OTID

HLR发送从先前的请求-继续的TCAP，UE1 MSISDN

SGSN在这种情况下更新UE1不正确MSISDN与UE2的。这导致混合两不同的会话记录。

方案#3 (导致混合用户标识)一会话的TCAP中止

UE1 -附上- IMSI1 -发送的SAI (TCAP -内部地中止的由于sessmgr失败)

UE2 -附上- IMSI2 -用同样TCAP传送的SAI - OTID

HLR发送从先前的请求-继续的TCAP，UE1验证向量(三份或五胞胎)

SGSN更新UE1不正确验证向量与UE2的

这导致SGSN使用UE1 UE2的验证的向量。

稳定方法

如果内部RAU的验证启用或PTMSI重新分配启用，SGSN验证有设置的一存储的矢量的客户端。如果UE不同跟什么存储为，UE/SGSN进一步在网络不会通过认证阶段继续。使用此，坚持在与一个不正确数据库的网络的UE的机会下来。这些是代码的一些已知区域。业务部门将继续分析更多案件为了了解更加好此的问题。

修正规划

从Cisco Bug ID的修正是一最佳效果方法。在您采取它对一个高密度节点前，请分析代码更多区域并且部署此在监控的较少密集节点。

配置指南

验证的启动增加Gr和Iu接口信令，当SGSN需要拿来从位置记录器设置的验证矢量(HLR)和执行往访问的另外的认证程序。操作员需要小心选择影响网络的频率值。

GPRS移动管理(GMM) /Mobile应用协议(MAP)关键性能指标(KPIs)是重要分析，在您得到每个步骤的前频率值。凭KPIs，请检查该的步骤高的执行。对于此步骤，设置高值频率。(这是方式优化根据网络呼叫型号的每个参数)。

一个理想的方式配置这些参数是对设置值到分支，但是不在树的根。例如，图2解释身份验证配置树。操作员也许选择设置值为更低级的，如直接地显示此处，而不是“正在验证附上的”配置。

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

设置高频率的值(单元作为10s)总是好的然后监控Gr/Iu接口信令阈值。如果发信号是在限额内，请定义值，直到发信号在阈值附近到达安全的地方操作员希望为他们的网络设置。

设置在多种步骤的频率在20/30并且减少他们到5-10与在外部接口流量的接近的监听。它要求用此超额负载检查在linkmgr和sessmgr内存CPU的影响。

PTMSI和PTMSI签名重新分配的直接发信号不会导致尖峰，但是设置高频率的值总是重要的，以便PTMSIs是可用的与sessmgr实例(哪些很少发生)。没有推荐更改每个上行链路步骤的PTMSI从UE，和这不最佳实践。值为10也许正派。在所有这些更改以后监控和执行在系统的标准的健康检查是重要的。

为例：

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
```

故障排除

当验证将执行或将分配PTMSI或PTMSI签名，调试日志将打印捕获步骤为什么完成。这在故障排除的帮助在任何差异情形下。这些日志通过各种配置和计数器包括从CC配置文件的配置和当前值所有计数器和决策逻辑的移动。并且，当前计数器值每个用户可以用sgsn的**show subscriber**或**show subscriber GPRS**命令查看。

提供此的输出示例:。当前计数器和最新的已验证时间戳被添加到**show subscriber**命令完整输出。

```
[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:
.
.

```

如果问题在网络被看到，请输入这些命令为了收集业务部门的信息能使用进一步分析问题：

```

show subscribers gprs-only full msisdn <msisdn>
show subscribers gprs-only full imsi <imsi>
show subscribers sgsn-only msisdn <msisdn>
show subscribers sgsn-only imsi <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.

```

风险

往Gr/Iu接口的增加的信令加上一轻微的内部进程(linkmgr) CPU影响，如果太频繁地验证。

命令语法

所有命令在配置/call控制中-请描出模式，并且操作员权限应用。命令的快照在CC配置文件下的如下：

```

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]}
```