ASR 5x00系列SGSN身份验证和PTMSI重新分配最佳实践

目录

[简介](#)
[概述](#)
[SGSN身份验证和PTMSI签名过程块](#)
[为什么需要身份验证和PTMSI签名重新分配](#)
[问题](#)
[稳定方法](#)
[修复计划](#)
[配置指南](#)
[故障排除](#)
[风险](#)
[命令语法](#)

简介

本文档提供身份验证过程频率配置、数据包临时移动用户身份(PTMSI)和PTMSI签名重新分配的优点的基本说明。具体而言，本文档针对在聚合服务路由器(ASR)5000系列上运行的2G和3G服务GPRS支持节点(SGSN)的可选第三代合作伙伴项目移动管理流程。

本文档介绍以下最佳实践：

- 身份验证频率设置
- PTMSI重新分配
- PTMSI签名重新分配
- 如果您未配置身份验证频率设置和PTMSI重新分配和签名重新分配（根据客户案例的经验），将产生影响
- 配置指南和对外部接口的影响
- 排除故障的选项

概述

呼叫控制配置文件下的身份验证、PTMSI和PTMSI签名重新分配框架使运营商能够在2G和3G SGSN和移动管理实体(MME)中为每个用户配置PTMSI和PTMSI签名的身份验证或分配。 在SGSN中，当前可以为以下过程配置身份验证：连接、服务请求、路由区域更新(RAU)、短消息服务和分离。

MME还使用同一框架来配置服务请求和跟踪区域更新(TAU)的身份验证。PTMSI重新分配可配置为附加、服务请求和RAU。PTMSI签名重新分配可配置为附加、PTMSI重新分配命令和RAU。可以为

这些过程的每个实例或该过程的每个第n个实例启用身份验证和重新分配，称为选择性身份验证/重新分配。某些程序还支持基于自上次身份验证或重新分配后经过的时间（周期或间隔）启用身份验证或重新分配。

此外，这些功能可专门配置为仅通用移动电信系统(UMTS)(3G)或通用分组无线业务(GPRS)(2G)或两者。仅当SGSN可选地验证或重新分配用户的PTMSI/PTMSI签名时，才会检查此配置。在必须执行这些步骤的情况下，不检查此配置。

每种过程的频率配置有三种类型的CLI-SET CLI、NO CLI和REMOVE CLI。调用SET CLI时，操作员希望为特定过程启用身份验证或重新分配。NO CLI用于明确禁用某个过程的身份验证或PTMSI重新分配，而REMOVE CLI用于将配置恢复为CLI（SET或NO）根本未配置的状态。在cc-profile分配中初始化树时，所有配置均假设为REMOVED。因此，REMOVE是默认配置。

SET CLI仅影响树中的一个特定过程，而NO CLI和REMOVE CLI则影响当前过程，并且还会删除下部节点。此外，如果NO CLI或REMOVE CLI影响公共树，则影响也应传播到访问特定树中的相应节点。

每种过程的周期性配置有两种类型的CLI-SET CLI和REMOVE CLI。周期性完成的SET和REMOVE只影响周期性配置，不影响频率配置。为频率执行的NO CLI（确切地说，NO CLI的常见之处是它不采用任何频率或周期性参数，但在存储时通过内部频率配置进行标识）也将删除周期性配置。

无条件完成身份验证的某些场景如下：

- 国际移动用户身份(IMSI)连接 — 所有IMSI连接都经过身份验证
- 当用户之前未通过身份验证且您没有矢量时
- 当存在PTMSI签名不匹配时
- 加密密钥序列号(CKSN)不匹配时

目前，可以在call-control-profile下为以下项启用身份验证：

- attach、service-request、RAU、detach、short-messaging-service、all-events和TAU
- MME正在使用TAU
- attach和service-request由SGSN和MME使用
- 其余部分由SGSN专用

SGSN身份验证和PTMSI签名过程块

此树结构说明SGSN为频率设置考虑的过程块。

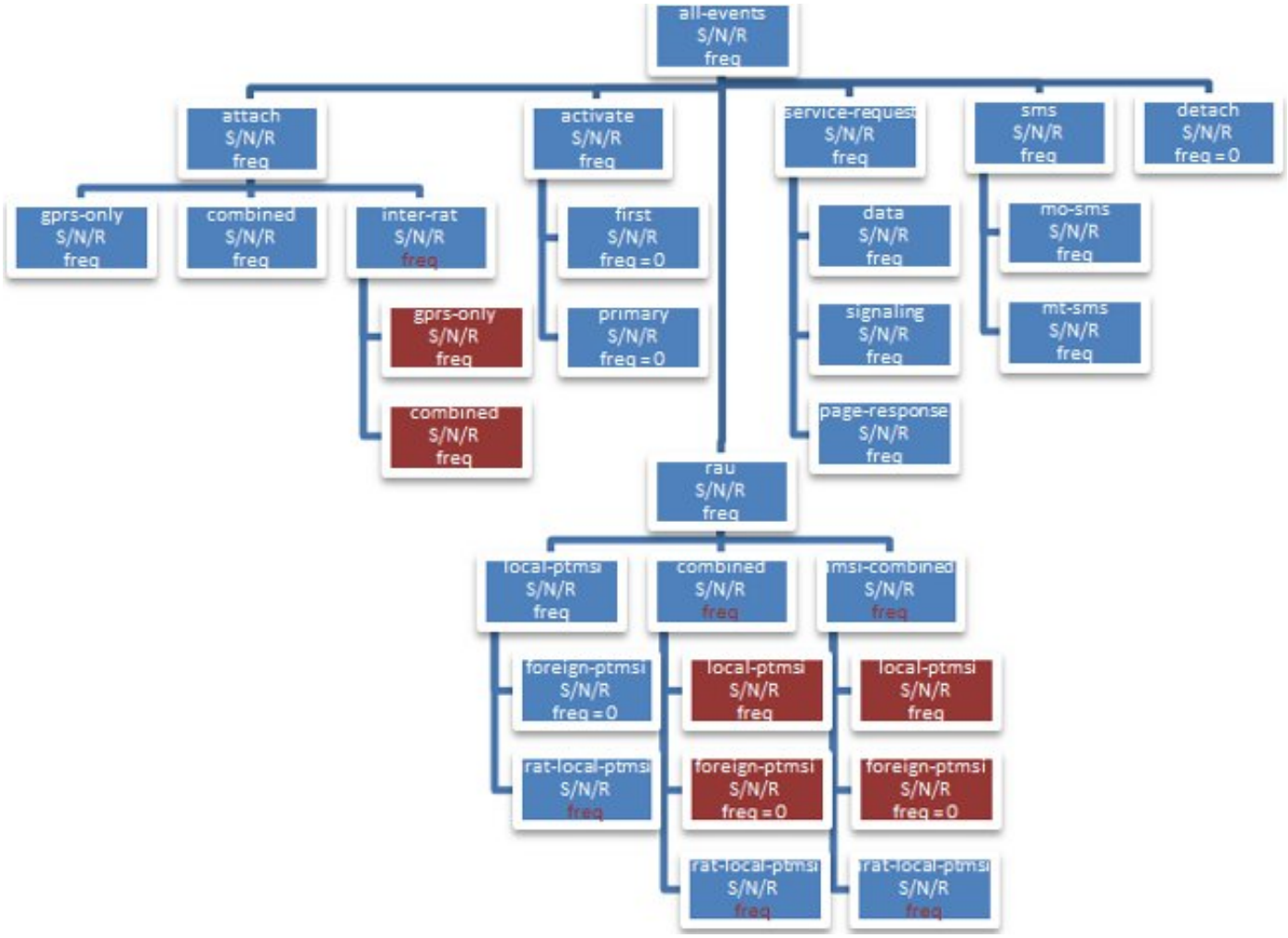

图 1：SGSN考虑的频率设置的程序块

PTMSI重新分配过程的树如下所示。

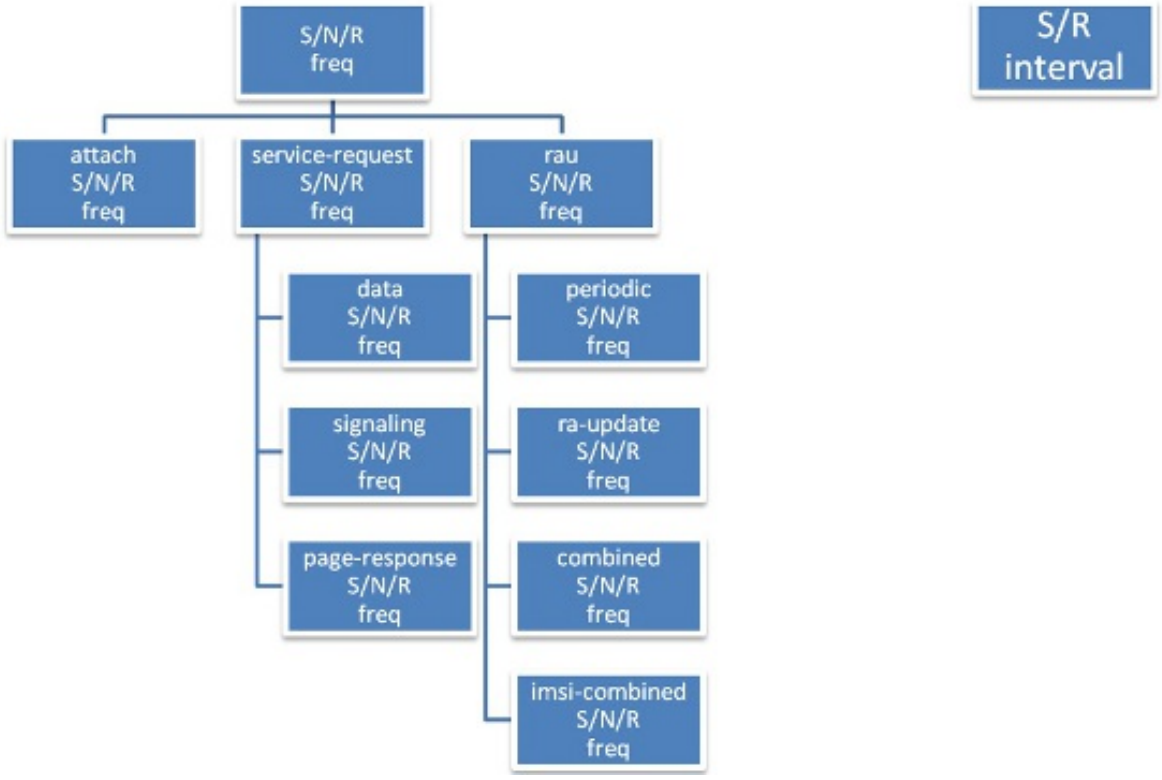

图 2：身份验证配置树

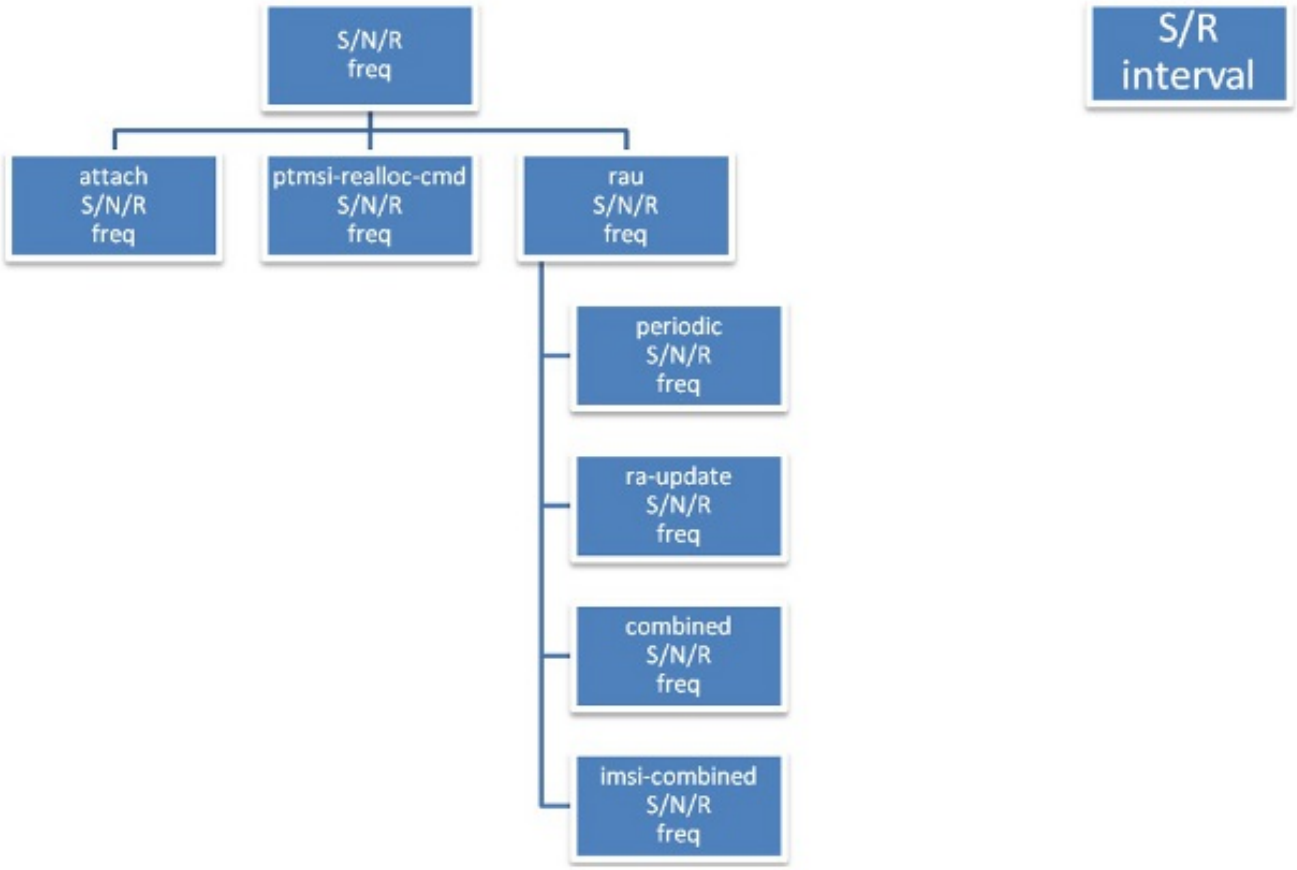

图 3：PTMSI重新分配配置树

为什么需要身份验证和PTMSI签名重新分配

根据3GPP技术规范(TS)23.060，第6.5.2节第(4)步，身份验证功能在“安全功能”子句中定义。 如果移动站(MS)的移动管理(MM)环境在网络的任何位置都不存在，则必须进行身份验证。“安全功能”子句中对加密过程进行了说明。 如果PTMSI分配完成，且网络支持加密，则网络应设置加密模式。

如前所述，SGSN仅对某些呼叫流中的新注册请求（如IMSI连接和SGSN间RAU）执行身份验证，其中PTMSI签名或CKSN的验证与存储的签名不匹配。例如，周期性RAU和RAU内等过程不需要进行身份验证，因为它们已经拥有具有注册SGSN的现有数据库。此处是可选身份验证。不完成身份验证并不总是好的，因为用户设备(UE)可以在网络中停留几天，而无需执行新的注册请求。SGSN和UE之间的安全情景设置可能会受到危害，因此定期进行身份验证并根据某些频率检查在SGSN中注册的用户的有效性总是很好。这在3GPP 23.060第6.8节中有详细说明。

安全功能和相关引用位于33.102第6.8节中。例如，如果根据33.102第6.8节中的图18和19启用了可选身份验证，并且如果SGSN尝试使用不正确的安全上下文参数对UE进行身份验证，UE将永远无法匹配发送响应(SRES))或与SGSN的预期响应(XRES)，导致重新连接到网络。这可防止UE使用错误数据库在网络中停留更长时间。

为了提供身份隐藏，SGSN为称为PTMSI的IMSI生成临时身份。MS连接后，SGSN向MS发出新的PTMSI。然后，MS存储此PTMSI并使用它，以便在SGSN发起的任何未来新连接中识别自身。由于PTMSI始终在加密连接中提供给MS，因此没有人能够将IMSI映射到外部PTMSI，尽管他们可能看到IMSI有时运行的纯文本消息。（例如，IMSI首次与IMSI连接和身份响应）。

PTMSI重新分配在3GPP 23.060第6.8节中作为独立过程进行说明。在任何上行链路过程中，都可以

完成此操作，以重新分配PTMSI和PTMSI签名以保护UE身份。这不会增加任何接口上的网络信令。PTMSI和PTMSI签名重新分配始终良好，因为这些是SGSN在初始注册步骤中分配给UE的密钥身份。根据某些频率重新分配这些值有助于SGSN将UE的标识隐藏一段长时间，而不是仅使用一个PTMSI值。身份隐藏是指当来自/发往MS的消息仍以纯文本形式发送且加密尚未开始时，隐藏MS的IMSI和IMEI等信息。

问题

在某些客户网络中，观察到MSIDN/PTMSI等一些关键标识在不同用户之间混合，并在Gn接口和呼叫数据记录(CDR)中以GTPC信令消息发送。

Cisco Bug ID CSCut62632和CSCuu67401处理某些会话恢复情况，这些情况会将一个用户的身份与另一个用户的身份进行映射。下面列出了三个案例。所有这些案例都经过代码审核、质量保证团队进行分析和复制。

场景#1（会话管理器上出现双重故障，导致用户身份丢失）

UE1 — 连接 — IMSI1 — 移动站国际用户目录号码(MSISDN)1 - PTMSI1 - Smgr#1

会话管理器实例的双终止，SGSN丢失UE1详细信息。

UE2 — 连接 — IMSI2 - MSISDN 2 - PTMSI1 - Smgr#1

PTMSI1被UE2重用。

UE1 - RAU内 — PTMSI1- SGSN处理此上行链路，因为RAU内的身份验证不是必需的。

这会导致两个不同会话的记录混合。

场景#2(事务功能应用部件(TCAP)中止一个会话，导致用户身份混合)

UE1 — 连接 — IMSI1 - UGL集（TCAP — 因会话管理器崩溃而内部中止）

UE2 — 连接 — IMSI2 - UGL已发送，且TCAP相同 — OTID

HLR发送TCAP — 从UE1的MSISDN上一个请求继续

在这种情况下，SGSN使用UE2更新UE1的不正确MSISDN。这会导致两个不同会话的记录混合。

场景#3（TCAP中止一个会话，导致用户身份混合）

UE1 — 连接 — IMSI1 — 已发送SAI（TCAP — 因会话管理器崩溃而内部中止）

UE2 — 连接 — IMSI2 - SAI已发送，且TCAP相同 — OTID

HLR发送TCAP — 从上一个请求继续，UE1的身份验证向量（三个或五个小程序）

SGSN使用UE2更新UE1的不正确身份验证向量

这导致SGSN使用UE1向量对UE2进行身份验证。

稳定方法

如果启用了RAU内的身份验证或启用了PTMSI重新分配，SGSN会使用存储的矢量集对客户端进行身份验证。如果UE与存储的不同，UE/SGSN将不会通过身份验证阶段继续在网络中。这样，UE在网络中使用错误数据库的可能性就会降低。这些是代码中的一些已知区域。业务部门将继续分析更多案例，以便更好地了解此问题。

修复计划

通过思科漏洞ID进行修复是一种尽力而为的方法。分析更多代码区域，并在密度较低的节点中部署此代码，以便在将其带到高密度节点之前进行监控。

配置指南

由于SGSN需要从归属位置寄存器(HLR)获取身份验证矢量集并对接入执行其他身份验证过程，因此启用身份验证会增加Gr和Iu接口信令。运营商需要谨慎选择对网络影响较小的频率值。

GPRS移动管理(GMM)/移动应用协议(MAP)关键性能指标(KPI)在您为每个过程推导频率值之前，对其进行分析非常重要。根据KPI，检查执行高的过程。对于此过程，请设置高频值。（这是根据网络呼叫模型微调每个参数的方法）。

配置这些参数的理想方法是将值设置为枝叶，但不是在树的根上。例如，图2说明了身份验证配置树。操作员可以选择将值设置为较低级别（如图所示），而不是直接配置“验证连接”。

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

设置高频值（单位为10）然后监控Gr/Iu接口信令阈值总是很好的。如果信令完全在限制内，请定义值，直到信令到达接近运营商希望为其网络设置的阈值的安全位置。

在20/30中设置各种过程的频率，并通过对外部接口流量的严密监控将其降至5-10。需要检查此过度负载对linkmgr和sessmgr内存CPU的影响。

PTMSI和PTMSI签名重新分配不会直接导致信令中的尖峰，但始终必须设置高频值，以便PTMSI可用于sessmgr实例（这种情况很少发生）。 不建议更改来自UE的每个上行链路过程的PTMSI，因为这不是最佳实践。10的价值可能不错。在进行所有这些更改后，必须监控并对系统执行标准运行状况检查。

例如：

```
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

当要执行身份验证或分配PTMSI或PTMSI签名时，将打印调试日志以捕获完成过程的原因。这有助于在出现任何差异时进行故障排除。这些日志包括cc-profile的配置和所有计数器的当前值，以及通过各种配置和计数器移动决策逻辑。此外，可以使用show subscribers sgsn-only或**show subscribers gprs-only命令查看每个用户的当前计数**值。

提供了该命令的示例输出。当前计数器和最新经过身份验证的时间戳将添加到**show subscribers**命令的完整输出中。

```
[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:
.
.
```

如果在网络中发现问题，请输入以下命令以收集业务部门用于进一步分析问题的信息：

```
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.
```

风险

向Gr/Iu接口发送的信令增加，如果身份验证过频繁，会对内部进程(linkmgr)CPU产生轻微影响。

命令语法

所有命令都处于配置/呼叫控制配置文件模式，并应用操作员权限。cc-profile下命令的快照如下：

```
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]}
```