ASR 5x00系列SGSN身份驗證和PTMSI重新分配最佳實踐

目錄

簡介

本檔案將提供驗證程式頻率組態、封包臨時行動使用者身分(PTMSI)和PTMSI簽名重新分配的優點的基本說明。具體而言，本文檔針對在聚合服務路由器(ASR)5000系列上運行的2G和3G服務GPRS支援節點(SGSN)上的可選第三代合作夥伴專案移動性管理過程。

本檔案將說明以下最佳實踐：

- 身份驗證頻率設定
- PTMSI重新分配
- PTMSI簽名重新分配
- 如果不配置身份驗證頻率設定和PTMSI重新分配以及簽名重新分配的影響（基於客戶案例的經驗）
- 配置准則及對外部介面的影響
- 故障排除選項

概觀

在呼叫控制配置檔案下的身份驗證、PTMSI和PTMSI簽名重新分配框架使運營商能夠在2G和3G SGSN以及移動管理實體(MME)中為每個使用者配置PTMSI和PTMSI簽名的身份驗證或分配。 在SGSN中，當前可以為以下過程配置身份驗證：attach、service-request、routing-area-update(RAU)、short-messaging-service和detach。

MME也使用相同的框架來設定服務請求和追蹤區域更新(TAU)的驗證。PTMSI重新分配可針對連線、服務請求和RAU進行配置。PTMSI簽名重新分配可配置用於attach、PTMSI reallocation命令和

RAU。可以為這些過程的每個例項或過程的每個第n個例項啟用身份驗證和重新分配，稱為選擇性身份驗證/重新分配。某些過程還支援分別基於自上次驗證或重新分配以來經過的時間（週期或間隔）啟用驗證或重新分配。

此外，這些配置可以專門為通用移動電信系統(UMTS)(3G)或通用分組無線服務(GPRS)(2G)或兩者配置。只有當SGSN可以驗證或重新分配訂閱者的PTMSI/PTMSI簽名時，才會檢查此配置。在必須執行這些步驟的情況下，不會檢查此配置。

每個過程的頻率配置有三種型別的CLI - SET CLI、NO CLI和REMOVE CLI。當您呼叫SET CLI時，操作員希望為特定過程啟用身份驗證或重新分配。NO CLI是顯式禁用某個過程的身份驗證或PTMSI重新分配，REMOVE CLI是將配置恢復到未配置CLI（SET或NO）的狀態。當在cc配置檔案分配中初始化樹時，假定所有配置都將被刪除。因此，REMOVE是預設配置。

SET CLI將只影響樹中的一個特定過程，而NO CLI和REMOVE CLI將影響當前過程並刪除較低節點。此外，如果沒有CLI或刪除CLI影響公共樹，則此影響也應在訪問特定樹中的相應節點上傳播。

每個過程的週期性配置有兩種型別的CLI - SET CLI和REMOVE CLI。針對週期而完成的SET和REMOVE應僅影響週期配置，且保持頻率配置不變。對頻率執行的NO CLI（確切地說，NO CLI是常見的，因為它不採用任何頻率或週期引數，但在儲存時由內部頻率配置標識）也將刪除週期配置。

無條件完成身份驗證的某些方案如下：

- 國際移動使用者標識(IMSI)連線 — 所有IMSI連線均通過身份驗證
- 如果使用者之前未通過身份驗證，並且您沒有向量
- 存在PTMSI簽名不匹配時
- 加密金鑰序列號(CKSN)不匹配時

目前，可以在呼叫控制配置檔案下為這些裝置啟用身份驗證：

- attach、service-request、RAU、detach、short-messaging-service、all-events和TAU
- TAU正被MME使用
- sgsn和MME都使用attach和service-request
- 其餘部分僅由SGSN使用

SGSN身份驗證和PTMSI簽名過程塊

此樹結構說明SGSN為頻率設定考慮的過程塊。

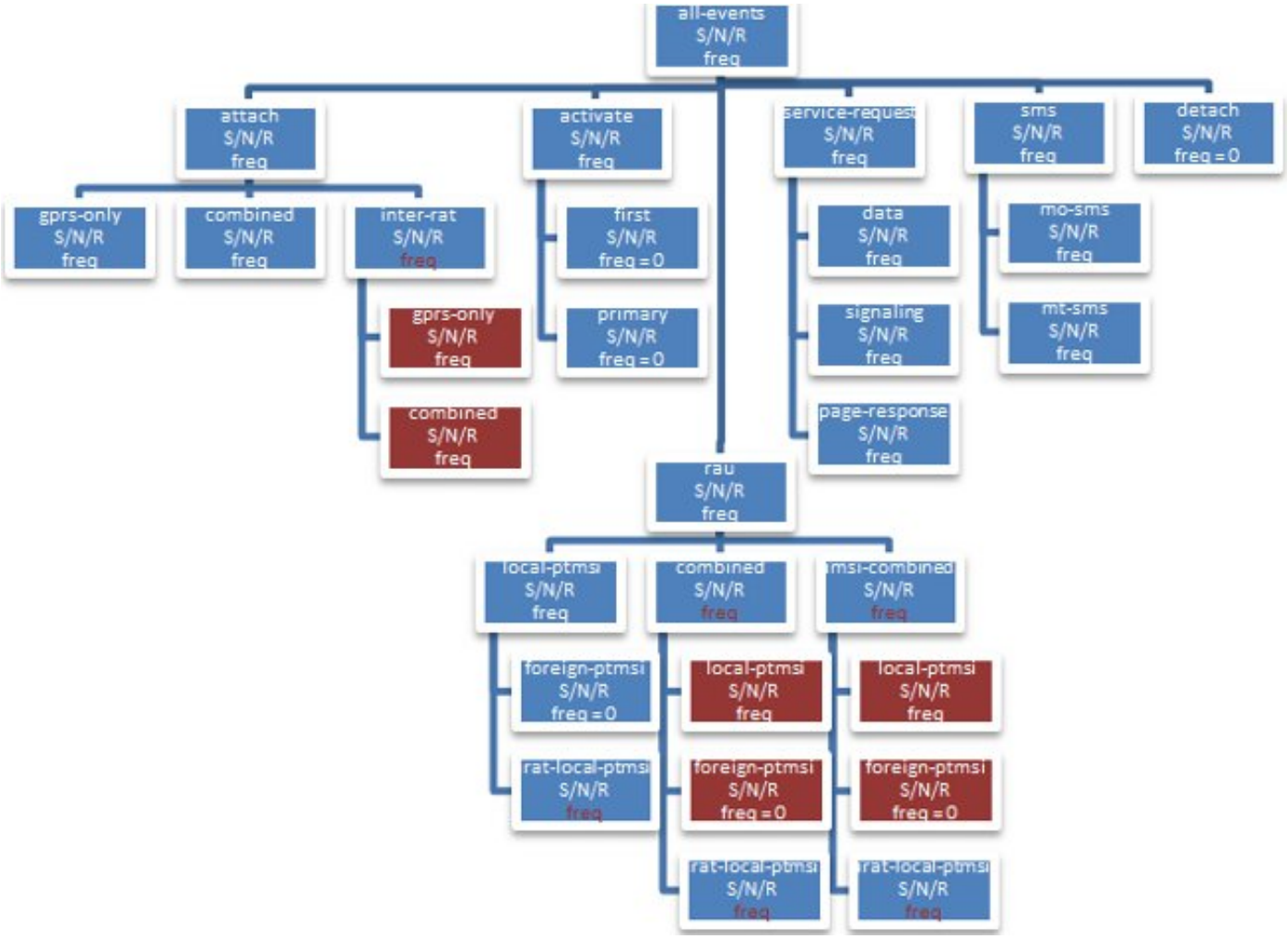

圖1:過程塊SGSN考慮頻率設定

此處顯示了PTMSI重新分配過程的樹。

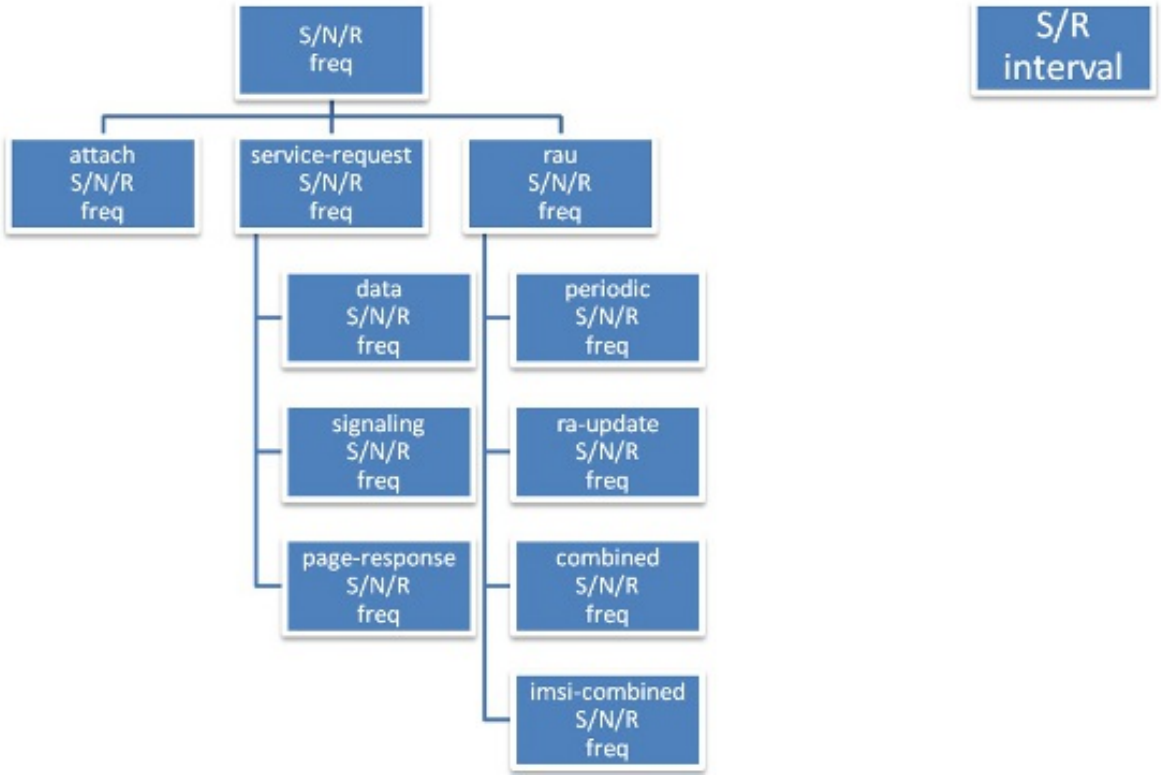

圖2:身份驗證配置樹

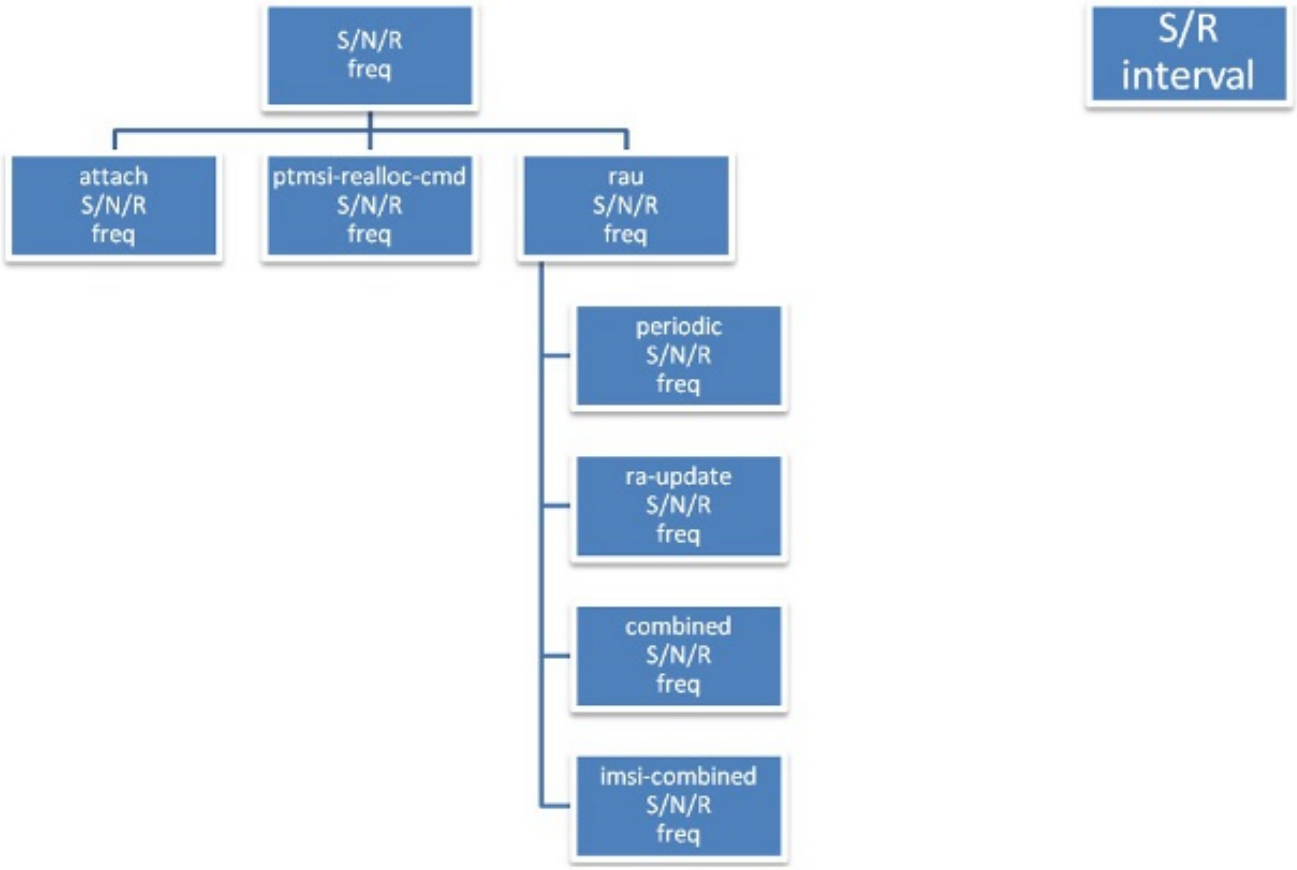

圖3:PTMSI重新分配配置樹

為什麼需要身份驗證和PTMSI簽名重新分配

根據3GPP Technical Specifications(TS)23.060第6.5.2節（步驟4），身份驗證函式在「Security Function」子句中定義。 如果網路中任何位置都沒有行動站(MS)的行動管理(MM)內容，則驗證是強制性的。加密過程在「安全功能」子句中描述。 如果PTMSI分配將完成並且網路支援加密，則網路應設定加密模式。

如前所述，SGSN僅對新的註冊請求執行身份驗證，例如IMSI連線和PTMSI簽名或CKSN的驗證與儲存簽名不匹配的一些呼叫流中的SGSN RAU。例如，定期RAU和RAU內部等過程不需要進行身份驗證，因為它們已經有一個已註冊SGSN的現有資料庫。此處可選擇身份驗證。未完成身份驗證並非總是好事，因為使用者裝置(UE)可能會在網路中待上幾天，而不執行新的註冊請求。SGSN和UE之間的安全上下文設定可能會受到危害，因此定期驗證和檢查在SGSN中註冊的使用者的有效性總是很好的。這在3GPP 23.060第6.8節中詳細解釋。

安全函式和相關引用位於33.102的6.8節。例如，如果根據33.102的6.8節中的圖18和圖19啟用了可選身份驗證，並且如果SGSN嘗試使用錯誤的安全上下文引數對UE進行身份驗證，則UE將永遠無法與SGSN匹配導致重新連線到網路的傳送響應(SRES)或預期響應(XRES)。這可以防止UE與錯誤的資料庫在網路中停留更長時間。

為了提供身份隱藏，SGSN為名為PTMSI的IMSI生成臨時身份。一旦MS附著，SGSN向MS發佈新的PTMSI。然後MS儲存此PTMSI並使用該資訊以在其發起的任何新的未來連線中向SGSN標識自身。由於PTMSI總是以加密連線方式提供給MS，因此沒有人能夠將IMSI對映到PTMSI外部，儘管他們有時可能會看到帶IMSI的純文字檔案消息。（例如，IMSI第一次附加IMSI和身份響應）。

PTMSI重新分配在3GPP 23.060第6.8節中作為獨立步驟說明。這也可以作為任何上行鏈路過程的一部分完成，以便重新分配PTMSI和PTMSI簽名以保護UE身份。這不會增加任何介面上的網路訊號。PTMSI和PTMSI簽名重新分配總是好的，因為這些是SGSN在初始註冊步驟中分配給UE的關鍵標識。根據某種頻率重新分配這些值有助於SGSN在較長的時間內以不同的值隱藏UE的身份，而不是僅使用一個PTMSI值。身份隱藏是指當來自/發往MS的消息仍然以純文字檔案形式傳送並且尚未開始加密時，隱藏MS的IMSI和IMEI等資訊。

問題

在一些客戶網路中，發現某些關鍵標識（例如MSIDN/PTMSI）被混合在不同的使用者之間，並在Gn介面的GTPC信令消息和呼叫資料記錄(CDR)中傳送。

思科錯誤ID CSCut62632和CSCuu67401處理某些會話恢復角案例，這些案例將一個使用者的身份對映到另一個使用者。下面列出三個案例。所有這些案例均經過代碼審查、品質保證小組分析，並且均已複製。

案例#1（sessmgr上發生雙重故障，導致使用者標識丟失）

UE1 — 連線 — IMSI1 — 移動站國際使用者目錄號碼(MSISDN)1 - PTMSI1 - Smgr#1

兩次終止sessmgr例項，SGSN丟失UE1詳細資訊。

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

PTMSI1重新用於UE2。

UE1 - RAU內 — PTMSI1- SGSN處理此上行鏈路，因為RAU內身份驗證不是強制性的。

這導致兩個不同會話的記錄混合。

案例#2(交易能力應用部分(TCAP)中止導致使用者身份混合的一個作業階段)

UE1 — 附加 — IMSI1 - UGL設定（TCAP — 由於sessmgr崩潰而在內部中止）

UE2 - Attach - IMSI2 - UGL使用同一TCAP - OTID傳送

HLR傳送TCAP — 繼續上一請求，UE1的MSISDN

在這種情況下，SGSN會通過UE2更新UE1的不正確的MSISDN。這導致兩個不同會話的記錄混合。

案例#3（導致使用者身份混合的一個作業階段的TCAP中止）

UE1 — 連線 — IMSI1 — 已傳送SAI（TCAP — 由於sessmgr崩潰而在內部中止）

UE2 — 附加 — IMSI2 — 使用同一TCAP傳送的SAI - OTID

HLR傳送TCAP — 繼續之前請求，UE1的身份驗證向量（三重或五重組）

SGSN通過UE2更新UE1的錯誤認證向量

這會導致SGSN使用UE1向量對UE2進行身份驗證。

穩定方法

如果啟用了RAU內身份驗證或啟用了PTMSI重新分配，則SGSN會使用儲存的向量集對客戶端進行身份驗證。如果UE與儲存的UE不同，則UE/SGSN將不會通過身份驗證階段，從而在網路中進一步繼續。這樣，UE在使用不正確的資料庫的情況下留在網路中的機會就減少了。這些是代碼中的一些已知區域。業務部門將繼續分析更多案例，以更好地瞭解此問題。

修復計畫

思科錯誤ID的修正是盡力而為的方法。分析更多代碼區域，並將其部署在不太密集的節點中進行監控，然後再將其部署到高密度節點。

配置指南

身份驗證的啟用增加了Gr和Iu介面信令，因為SGSN需要從歸屬位置暫存器(HLR)獲取身份驗證向量集並執行額外的訪問身份驗證過程。操作員需要小心選擇對網路影響較小的頻率值。

GPRS移動性管理(GMM)/移動應用協定(MAP)在匯出每個過程的頻率值之前，必須分析主要績效指標(KPI)。根據KPI檢查執行率高的過程。對於此過程，請設定較高的頻率值。（這是根據網路呼叫模型微調每個引數的方法）。

配置這些引數的理想方法是將值設定為枝葉，而不是在樹的根部。例如，圖2說明了身份驗證配置樹。操作員可以選擇將值設定為較低級別（如此處所示），而不是直接進行「身份驗證連線」的配置。

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

設定高頻值（單位為10）然後監控Gr/Iu介面信令閾值始終是好的。如果信令完全在限制範圍內，請定義值，直到信令到達運營商為其網路設定的閾值附近的安全位置。

在20/30中設定各種過程的頻率，通過密切監視外部介面流量將它們降到5-10。需要檢查此超負荷對linkmgr和sessmgr記憶體CPU的影響。

PTMSI和PTMSI簽名重新分配不會直接導致信令的峰值，但設定高頻值始終非常重要，以使PTMSI可用於sessmgr例項（這種情況很少發生）。 建議不要從UE為每個上行鏈路過程更改PTMSI，因為這不是最佳實踐。值10可能會比較好。在所有這些更改之後，監視和對系統執行標準運行狀況檢查是非常重要的。

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
```

疑難排解

當要執行身份驗證或分配PTMSI或PTMSI簽名時，將列印調試日誌以捕獲該過程完成的原因。這有助於在發生任何差異時進行故障排除。這些日誌包括cc-profile中的配置以及所有計數器的當前值，以及通過各種配置和計數器移動決策邏輯。此外，還可以使用**show subscribers sgsn-only**或**show subscribers gprs-only**命令檢視每個訂戶的當前計數器值。

提供了此示例輸出。當前計數器和最新的驗證時間戳將新增到**show subscribers**命令完整輸出中。

```
[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:
.
.
```

如果在網路中發現問題，請輸入以下命令以收集資訊供業務部門用於進一步分析問題：

```
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.
```

風險

向Gr/Iu介面傳送的信令增加，如果您身份驗證過於頻繁，則可能會輕微影響內部進程(linkmgr)CPU。

指令語法

所有命令均處於配置/呼叫控制配置檔案模式並應用操作員許可權。cc-profile下的命令快照如下：

```
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]}