Autenticación SGSN de la serie ASR 5x00 y Prácticas Recomendadas de Reasignación de PTMSI

Contenido

Introducción

Este documento proporciona una explicación básica de las ventajas de la configuración de frecuencia del procedimiento de autenticación, la identidad del suscriptor móvil temporal de paquetes (PTMSI) y la reasignación de la firma PTMSI. Específicamente, este documento es para un procedimiento opcional de gestión de movilidad del proyecto de asociación de tercera generación para 2G y 3G en el nodo de soporte de GPRS de servicio (SGSN) que se ejecuta en el router de servicio agregado (ASR) serie 5000.

Este documento explica estas prácticas recomendadas:

- Configuración de la frecuencia de autenticación
- reasignación de PTMSI
- reasignación de firma PTMSI
- Impacto si no configura la configuración de frecuencia de autenticación y la reasignación de firmas y reasignación de PTMSI (según la experiencia de casos de clientes)
- Directrices de configuración e impacto en las interfaces externas
- Opciones para resolver problemas

Overview

El marco de reasignación de firmas de autenticación, PTMSI y PTMSI bajo el perfil de control de llamadas permite al operador configurar la autenticación o asignación de la firma PTMSI y PTMSI

por suscriptor en el SGSN 2G y 3G y en la entidad de administración móvil (MME). En el SGSN, la autenticación se puede configurar actualmente para estos procedimientos: adhesión, solicitud de servicio, actualización de área de routing (RAU), servicio de mensajes cortos y separación.

MME también utiliza el mismo marco para configurar la autenticación para solicitudes de servicio y actualizaciones de área de seguimiento (TAU). La reasignación de PTMSI se puede configurar para adjuntar, solicitar servicio y RAU. La reasignación de la firma PTMSI se puede configurar para la asociación, el comando de reasignación PTMSI y las RAU. La autenticación y la reasignación se pueden habilitar para cada instancia de estos procedimientos o para cada instancia del procedimiento, denominada autenticación/reasignación selectiva. Algunos procedimientos también admiten la habilitación de la autenticación o reasignación en función del tiempo transcurrido (periodicidad o intervalo) desde la última autenticación o reasignación, respectivamente.

Además, pueden configurarse específicamente para el sistema universal de telecomunicaciones móviles (UMTS) (3G) o el servicio general de radio de paquetes (GPRS) (2G) o ambos. Esta configuración se verifica solamente cuando es opcional que el SGSN autentique o reasigne la firma PTMSI/PTMSI de un suscriptor. En los escenarios donde es obligatorio realizar estos procedimientos, esta configuración no está verificada.

Hay tres tipos de CLI para cada configuración de frecuencia de procedimiento: una CLI SET, una CLI NO y una CLI REMOVE. Cuando invoca una CLI SET, el operador desea habilitar la autenticación o reasignación para el procedimiento específico. La CLI NO es para deshabilitar explícitamente la autenticación o la reasignación de PTMSI para un procedimiento, y la CLI REMOVE es para restaurar la configuración a un estado donde la CLI (SET o NO) no está configurada en absoluto. Se supone que se ELIMINAN todas las configuraciones cuando se inicializa el árbol en la asignación de cc-profile. Por lo tanto, REMOVE es la configuración predeterminada.

La CLI SET afectará solamente a un procedimiento específico del árbol, mientras que la CLI NO y la CLI REMOVE afectarán al procedimiento actual y también ELIMINARÁN los nodos inferiores. Además, si NO CLI o REMOVE CLI afecta al árbol común, el efecto se propagará también en los nodos correspondientes en los árboles específicos de acceso.

Hay dos tipos de CLI para la configuración de periodicidad de cada procedimiento: la CLI SET y la CLI REMOVE. El SET y REMOVE completado con periodicidad afectará solamente a la configuración de periodicidad y dejará la configuración de frecuencia intacta. La CLI de NO realizada para la frecuencia (para ser precisos, la CLI de NO es común en el sentido de que no toma ningún argumento de frecuencia o periodicidad, pero se identifica con la configuración de frecuencia internamente mientras se almacena) también ELIMINARÁ la configuración de periodicidad.

Algunos escenarios donde la autenticación se completa incondicionalmente son los siguientes:

- Adhesión de la identidad del suscriptor móvil internacional (IMSI): todos los adjuntos IMSI están autenticados
- cuando el suscriptor no ha sido autenticado antes y usted no tiene un vector
- cuando hay una discordancia de firma PTMSI
- cuando hay una discordancia entre el número de secuencia de clave de cifrado (CKSN)

Actualmente, la autenticación se puede habilitar para estos bajo el call-control-profile:

- attach, service-request, RAU, detach, short-Messaging-service, all-events y TAU

- TAU está en uso por MME
- SGSN y MME utilizan la solicitud de servicio y la adhesión
- el resto lo utiliza exclusivamente SGSN

Bloques de Autenticación SGSN y Procedimiento de Firma PTMSI

Esta estructura de árbol explica los bloques de procedimiento que SGSN considera para la configuración de frecuencia.

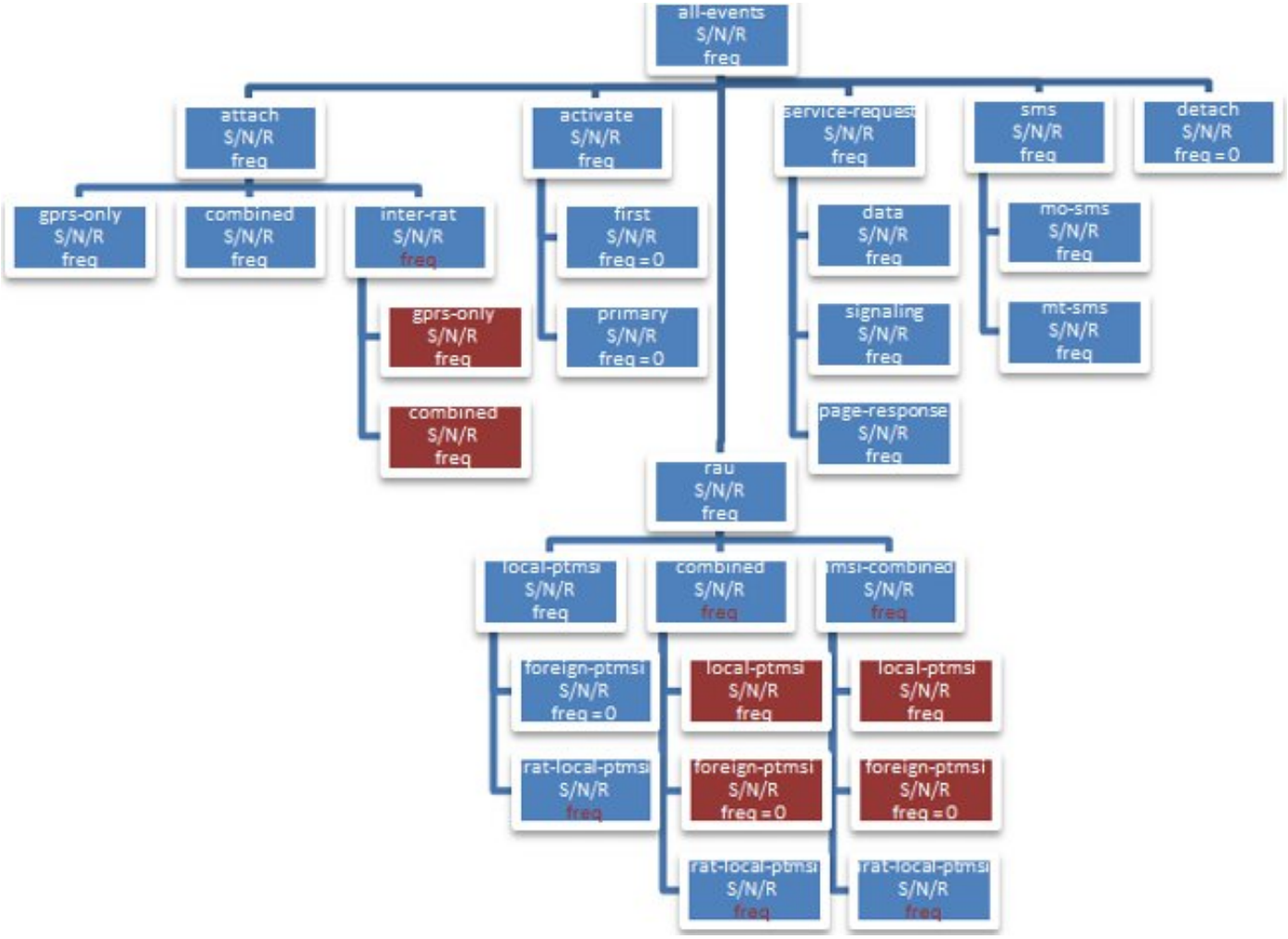

Figura 1: Bloques de procedimiento que SGSN considera para la configuración de frecuencia

Aquí se muestran los árboles para el procedimiento de reasignación de PTMSI.

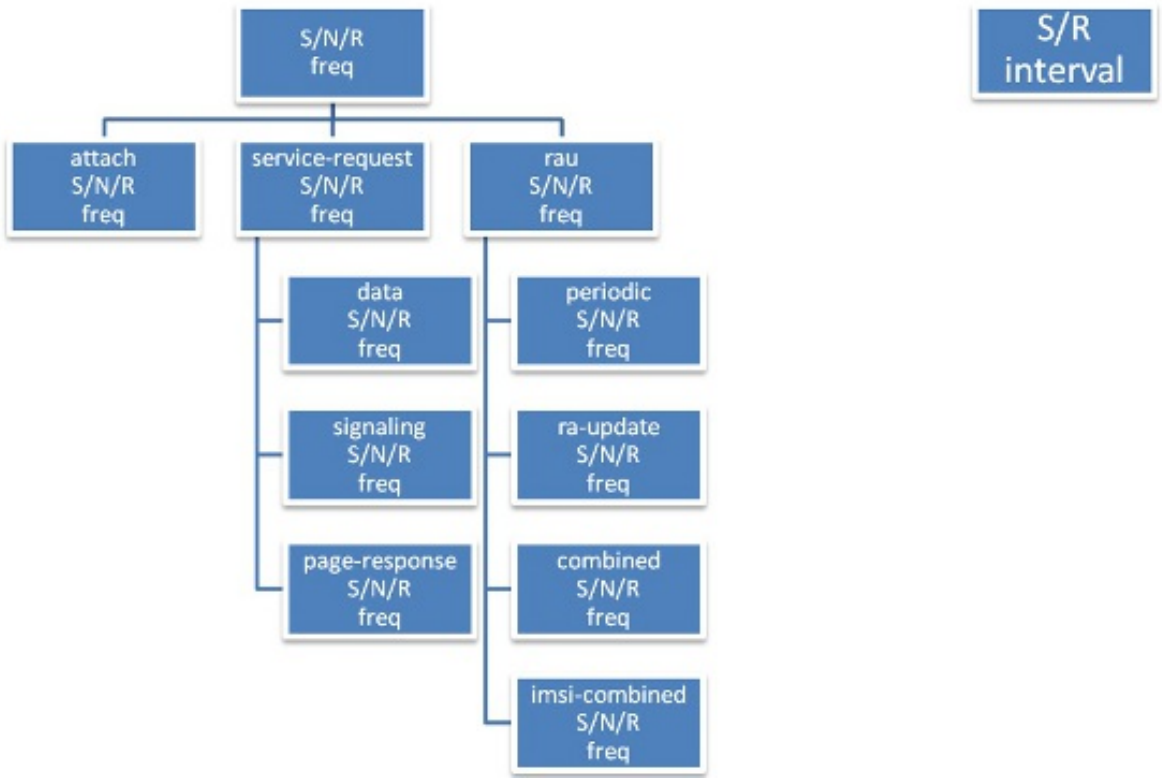

Figura 2: Árbol de configuración de autenticación

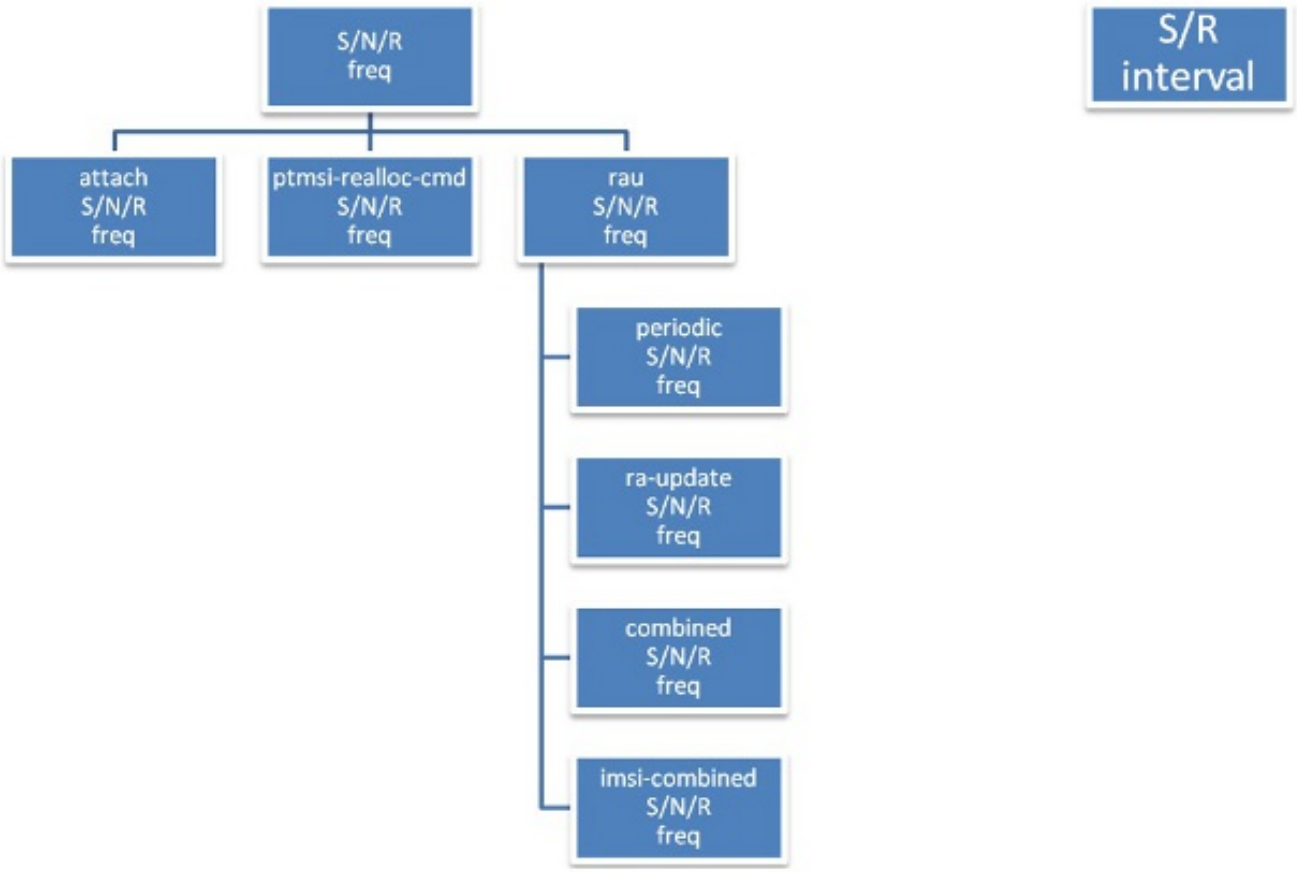

Figura 3: Árbol de Configuración de Reasignación de PTMSI

Por qué se requiere la autenticación y la reasignación de la firma

PTMSI

Según las especificaciones técnicas 3GPP (TS) 23.060, sección 6.5.2, paso 4), las funciones de autenticación se definen en la cláusula "Función de seguridad". Si no existe ningún contexto de gestión de movilidad (MM) para la estación móvil (MS) en ninguna parte de la red, la autenticación es obligatoria. Los procedimientos de cifrado se describen en la cláusula "Función de seguridad". Si se completa la asignación de PTMSI y la red admite el cifrado, la red establecerá el modo de cifrado.

Como se ha mencionado, SGSN realiza la autenticación sólo para las nuevas solicitudes de registro, como las RAU IMSI se conectan y las RAU entre SGSN en algunos flujos de llamada donde la validación de la firma PTMSI o CKSN no coincide con la almacenada. Por ejemplo, no es necesario autenticar procedimientos como RAU periódicas e intrarcada, ya que ya tienen una base de datos existente con una SGSN registrada. La autenticación es opcional aquí. No completar la autenticación no siempre es bueno, ya que el equipo del usuario (UE) puede permanecer en la red durante días sin realizar una nueva solicitud de registro. Hay posibilidades de que la configuración del contexto de seguridad entre el SGSN y la UE se vea comprometida, por lo que siempre es bueno autenticar y verificar periódicamente la validez del suscriptor registrado en SGSN en función de alguna frecuencia. Esto se explica en detalle en 3GPP 23.060, sección 6.8.

Las funciones de seguridad y las referencias conexas se encuentran en la sección 6.8 de la sección 33.102. Por ejemplo, si se habilita la autenticación opcional basada en las figuras 18 y 19 de la sección 6.8 de 33.102, y si SGSN intenta autenticar la UE con parámetros de contexto de seguridad incorrectos, la UE nunca podrá hacer coincidir la respuesta de envío (SRES) o la respuesta esperada (XRES) con SGSN, lo que da lugar a un nuevo acoplamiento a la red. Esto evita que la UE permanezca en la red con una base de datos falsa durante más tiempo.

Para proporcionar ocultación de identidad, una SGSN genera una identidad temporal para un IMSI llamado PTMSI. Una vez que el MS se conecta, el SGSN emite una nueva PTMSI al MS. El MS luego almacena esta PTMSI y la utiliza para identificarse con la SGSN en cualquier nueva conexión futura que inicie. Dado que la PTMSI siempre se da al MS en una conexión cifrada, nadie podrá asignar un IMSI a la PTMSI externa, aunque puede que vean un mensaje de texto simple con IMSI en ocasiones. (Por ejemplo, la primera vez que un IMSI se conecta y responde a la identidad con un IMSI).

La reasignación de PTMSI se explica en 3GPP 23.060, sección 6.8 como procedimiento autónomo. Lo mismo se puede completar como parte de cualquier procedimiento de link ascendente para reasignar las firmas PTMSI y PTMSI para proteger las identidades UE. Esto no aumentará la señalización de red en ninguna interfaz. La reasignación de firmas PTMSI y PTMSI siempre es buena, ya que estas son las identidades clave que SGSN asigna a la UE en el paso inicial de registro. La reasignación de estos datos en función de cierta frecuencia ayuda a SGSN a ocultar la identidad de la UE con valores diferentes durante un tiempo prolongado en lugar de utilizar sólo un valor de PTMSI. La ocultación de identidad se refiere a la ocultación de información como IMSI e IMEI de MS, cuando los mensajes de/a MS se siguen enviando en texto sin formato y cuando todavía no se ha iniciado el cifrado.

Problema

En algunas redes de clientes, se observó que algunas identidades clave como MSIDN/PTMSI se

mezclan entre diferentes suscriptores y se envían en mensajes de señalización GTPC en la interfaz Gn y en los registros de datos de llamadas (CDR).

Los ID de bug de Cisco CSCut62632 y CSCuu67401 tratan de algunos casos esquinales de recuperación de sesión, que asignan la identidad de un suscriptor a otro. A continuación se enumeran tres casos. Todos estos casos se revisan por código, se analiza el equipo de garantía de calidad y se reproducen.

Situación nº 1 (error doble en sessmgr que da lugar a la pérdida de las identidades de suscriptor)

UE1 - Adjuntar - IMSI1 - Número de directorio del suscriptor internacional de la estación móvil (MSISDN) 1 - PTMSI1 - Smgr#1

Doble matanza de la instancia de sessmgr, SGSN perdió los detalles de UE1.

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

PTMSI1 se reutiliza para UE2.

UE1 - Intra RAU - PTMSI1- SGSN procesa este link ascendente, ya que la autenticación para intra-RAU no es obligatoria.

Esto da como resultado la mezcla de registros de dos sesiones diferentes.

Situación n.º 2 (Parte de la aplicación de capacidades de transacción (TCAP) cancelada en una sesión que resulta en la mezcla de identidades de suscriptor)

UE1 - Adjuntar - IMSI1 - conjunto UGL (TCAP - anulado internamente debido al desperfecto de sessmgr)

UE2 - Adjuntar - IMSI2 - UGL enviado con la misma TCAP - OTID

HLR envía TCAP - continúa desde la solicitud anterior, MSISDN de UE1

SGSN actualiza el MSISDN incorrecto de UE1 con UE2 en este caso. Esto da como resultado la mezcla de registros de dos sesiones diferentes.

Situación nº 3 (anulación de TCAP de una sesión que da como resultado la mezcla de identidades de suscriptores)

UE1 - Adjuntar - IMSI1 - SAI enviado (TCAP - Internamente abortado debido al desperfecto de sessmgr)

UE2 - Adjuntar - IMSI2 - SAI enviado con la misma TCAP - OTID

HLR envía TCAP - continúa desde la solicitud anterior, los vectores de autenticación UE1 (trillizos o quintupletas)

SGSN actualiza los vectores de autenticación incorrectos de UE1 con UE2

Esto da como resultado que SGSN utilice vectores UE1 para la autenticación de UE2.

Enfoque de estabilización

Si la autenticación para intra-RAU está habilitada o la reasignación PTMSI está habilitada, SGSN autentica el cliente con un conjunto de vector almacenado. Si la UE es diferente de lo almacenado para, UE/SGSN no pasará la etapa de autenticación para continuar en la red. Con esto, se reduce la posibilidad de que la UE permanezca en la red con una base de datos incorrecta. Estas son algunas áreas conocidas del código. La unidad empresarial seguirá analizando más casos para comprender mejor este problema.

Reparar plan

La solución de los ID de bug de Cisco es un enfoque de mejor esfuerzo. Analice más áreas de código e implemente esto en un nodo menos denso para la supervisión antes de llevarlo a un nodo de alta densidad.

Pautas de Configuración

La habilitación de la autenticación aumenta la señalización de la interfaz Gr e Iu, ya que SGSN necesita obtener el vector de autenticación establecido desde el Registro de ubicación de inicio (HLR) y realizar procedimientos de autenticación adicionales para el acceso. Los operadores deben tener cuidado al elegir los valores de frecuencia que afectan menos a la red.

Los indicadores de rendimiento clave (KPI) GPRS Mobility Management (GMM)/Mobile Application Protocol (MAP) son importantes para analizar antes de derivar los valores de frecuencia para cada procedimiento. En función de los KPI, verifique el procedimiento que se ejecuta en alto. Para este procedimiento, establezca valores altos de frecuencia. (Esta es la forma de ajustar cada parámetro en función de un modelo de llamada de red).

Una forma ideal de configurar estos parámetros es establecer valores en hojas, pero no en la raíz del árbol. Por ejemplo, la Figura 2 explica el árbol de configuración de autenticación. Los operadores pueden optar por establecer el valor en un nivel inferior, como se muestra aquí, en lugar de la configuración de "autentificación de adhesión" directamente.

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

Siempre es bueno establecer valores de alta frecuencia (unidades como 10s) y luego monitorear los umbrales de señalización de interfaz Gr/Iu. Si la señalización está bien dentro de los límites, defina los valores hasta que la señalización alcance un lugar seguro cerca de los umbrales que el operador desea establecer para sus redes.

Establezca la frecuencia en los diversos procedimientos en 20/30 y bajarlos a 5-10 con una estrecha supervisión del tráfico de interfaz externa. Es necesario verificar el impacto en la CPU de memoria de linkmgr y sessmgr con esta carga excesiva.

Las reasignaciones de firmas PTMSI y PTMSI no causarán el pico en la señalización directamente, pero siempre es importante establecer valores de alta frecuencia para que las PTMSI estén disponibles con instancias de sessmgr (lo que sucede raramente). No se recomienda cambiar la PTMSI para cada procedimiento de enlace ascendente desde la UE, ya que esta no es la mejor práctica. Un valor de 10 podría ser decente. Después de todos estos

cambios, es importante monitorear y realizar controles de estado estándar en el sistema.

Por ejemplo:

```
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
```

Troubleshoot

Cuando se realiza la autenticación o se asigna la firma PTMSI o PTMSI, se imprimirán los registros de depuración para capturar por qué se completó el procedimiento. Esto ayuda en la resolución de problemas en caso de discrepancias. Estos registros incluyen la configuración de cc-profile y el valor actual de todos los contadores y el movimiento de la lógica de decisión a través de las diversas configuraciones y contadores. Además, los valores de contador actuales por suscriptor se pueden ver con los comandos **show subscribers sgsn-only** o **show subscribers gprs-only**.

Se proporciona un ejemplo de salida de esto. Los contadores actuales y la última marca de tiempo autenticada se agregan al resultado completo del comando **show subscribers**.

```
[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 el problema se ve en la red, ingrese estos comandos para recolectar información para que la unidad de negocio lo utilice para analizar el problema más a fondo:

```
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.
```

Riesgos

Mayor señalización hacia las interfaces Gr/Iu, además de un ligero impacto en la CPU del proceso interno (linkmgr) si se autentica con demasiada frecuencia.

Sintaxis del comando

Todos los comandos están en el modo configuration/call-control-profile y se aplican los privilegios de operador. Una instantánea de los comandos bajo el cc-profile es la siguiente:

```
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]}
```