Implemente la protección contra sobrecargas para gateways y elementos de red vecinos en la serie ASR5x00

Contenido

Introducción

Este documento describe cómo implementar las funciones de protección disponibles para Gateways (GW) y elementos de red vecinos en el router de servicios agregados (ASR) de Cisco serie 5x00 para proteger el rendimiento general de la red.

Control de congestión para GW

Control de congestión es una función genérica de autoprotección. Se utiliza para proteger el sistema frente a los aumentos de utilización de estos recursos:

- Uso de CPU en tarjetas de procesamiento
- Uso de memoria en tarjetas de procesamiento

Cuando la utilización excede los umbrales predefinidos, todas las llamadas nuevas (activaciones de protocolo de datos de paquetes (PDP), activaciones de sesión de red de datos de paquetes (PDN)) se *eliminan* o *rechazan*, según la configuración.

A continuación se muestra un ejemplo que muestra cómo supervisar el uso general de la tarjeta de procesamiento de datos (DPC):

```
congestion-control threshold system-cpu-utilization 85

congestion-control threshold system-memory-utilization 85

congestion-control policy ggsn-service action drop

congestion-control policy sgw-service action drop

congestion-control policy pgw-service action drop
```

> **Nota:** El límite de ingeniería del sistema es el 80% de la utilización de la CPU, que se define como el límite de ingeniería recomendado que no se debe exceder para garantizar el funcionamiento regular del sistema. La carga más allá del valor podría afectar a las operaciones de la plataforma, como su estabilidad y previsibilidad, y debería evitarse con una planificación adecuada de la capacidad.

> **Nota:** Cisco recomienda que utilice la acción de *descarte* en lugar de la *acción de rechazo*, ya que las llamadas rechazadas provocan intentos de reconexión repetida inmediata del Equipo del usuario (UE). En el caso de una acción de caída, la UE espera unos segundos antes de realizar repetidos intentos de reconexión, por lo que la velocidad de llamada disminuye.

Protección contra sobrecarga de red para la aceleración de mensajes GTP-C de entrada

Esta función protege los procesos de Packet GW (P-GW)/Gateway GPRS Supporting Node (GGSN) de las sobrecargas de transmisión y las fallas de elementos de red. En un nodo de soporte de P-GW/Serving GPRS (SGSN), el principal cuello de botella está relacionado con el procesamiento de datos del usuario, como la utilización del administrador de sesiones y la utilización general de la CPU y la memoria de DPC.

Se configura un *valor No* en la SGSN/Mobility Management Entity (MME) para limitar los mensajes entrantes de control de protocolo de túnel GPRS (GTP-C) cuando se activa la protección contra sobrecarga de red.

> **Nota:** El uso de GTP y la regulación de la interfaz de diámetro requiere que se instale una clave de licencia válida.

Esta función ayuda a controlar la velocidad de los mensajes entrantes/salientes en el P-GW/GGSN, lo que ayuda a asegurar que el P-GW/GGGSN no se vea abrumado por los mensajes del plan de control GTP. Además, ayuda a asegurar que el P-GW/GGSN no supere al GTP-C peer con los mensajes del plano de control GTP. Esta función requiere que los mensajes de control GTP (versión 1 (v1) y versión 2 (v2)) se modelen/regulen sobre las interfaces Gn/Gp y S5/S8. Esta función cubre la protección contra sobrecarga de los nodos P-GW/GGSN y los otros nodos externos con los que se comunica. La aceleración se realiza sólo para los mensajes de control de nivel de sesión, por lo que los mensajes de administración de trayectoria no se limitan en absoluto a la velocidad.

La sobrecarga del nodo externo puede ocurrir en un escenario donde el P-GW/GGSN genera solicitudes de señalización a una velocidad mayor que la que pueden manejar los otros nodos.

Además, si la velocidad de entrada es alta en el nodo P-GW/GGSN, podría inundar el nodo externo. Por esta razón, se requiere la regulación de los mensajes de control tanto entrantes como salientes. Para la protección de los nodos externos de una sobrecarga debido a la señalización de control P-GW/GGSN, se utiliza un marco para modelar y vigilar los mensajes de control de salida a las interfaces externas.

Configuración de la Regulación de Mensajes GTP-C de Ingreso

Ingrese este comando para configurar la limitación de mensajes GTP-C de ingreso:

gtpc overload-protection Ingress

Esto configura la protección de sobrecarga de GGSN/PGW mediante la regulación de los mensajes de control GTPv1 y GTPv2 entrantes a través de la interfaz Gn/Gp (GTPv1) o S5/S8 (GTPv2) con los demás parámetros para los servicios configurados en un contexto y aplicados a GGGSN y PGW.

Cuando ingresa el comando anterior, se genera este mensaje:

```
[context_name]host_name(config-ctx)# gtpc overload-protection ingress
{msg-rate msg_rate} [delay-tolerance dur] [queue-size size]
[no] gtpc overload-protection Ingress
```

A continuación se muestran algunas notas sobre esta sintaxis:

- **no:** Este parámetro inhabilita la regulación de mensajes de control de entrada GTP para los servicios GGSN/PGW en este contexto.
- **msg-rate msg_rate**: Este parámetro define el número de mensajes entrantes GTP que se pueden procesar por segundo. *msg_rate* es un número entero que va de ciento a 12.000.
- **límite de tolerancia de retraso**: Este parámetro define el número máximo de segundos que un mensaje GTP entrante puede ser puesto en cola antes de ser procesado. Después de que se exceda esta tolerancia, se descarta el mensaje. El *dur* es un entero que va de uno a diez.
- **tamaño de cola**: Este parámetro define el tamaño máximo de cola para los mensajes GTP-C entrantes. Si la cola excede el tamaño definido, se descartan los mensajes entrantes nuevos. El *tamaño* es un entero que va de ciento a 10.000.

Puede utilizar este comando para habilitar la regulación de mensajes de control entrante GTP para los servicios GGSN/PGW configurados en el mismo contexto. Como ejemplo, este comando habilita los mensajes de control GTP entrantes en un contexto con una velocidad de mensajes de *1,000* por segundo, un tamaño de cola de mensajes de *10,000*, y una demora de *un* segundo:

gtpc overload-protection ingress msg-rate 1000 delay-tolerance 1 queue-size 10000

Protección de elementos de red vecinos

Muchos elementos de red vecinos utilizan sus propios mecanismos para protegerse, y es posible que no sea necesaria una protección adicional de sobrecarga de red en el lado ASR5x00. Es

posible que se requiera la protección de los elementos de red vecinos en los casos en los que la estabilidad de la red global sólo se puede alcanzar cuando se aplica la regulación de mensajes en el lado de salida.

Protección contra sobrecarga de red con aceleración de diámetro en una interfaz S6a

Esta función protege las interfaces S6a y S13 en la dirección de salida. Protege el servidor de suscriptor doméstico (HSS), el agente de routing de diámetro (DRA) y el registro de identidad del equipo (EIR). La función utiliza la función de limitación de velocidad (RLF).

Tenga en cuenta estas notas importantes cuando aplique la configuración del punto final del diámetro:

- Se debe asociar una plantilla RLF con el par.
- Un RLF se adjunta sólo por peer (individualmente).

Configuración de la Regulación del Diámetro en una Interfaz S6a

Esta es la sintaxis del comando que se utiliza para configurar la regulación del diámetro en una interfaz S6a:

```
[context_na>me]host_name(config-ctx-diameter)#>peer [*] peer_name [*]
[ realm realm_name ] { address ipv4/ipv6_address [ [ port port_number ]
[connect-on-application-access] [ send-dpr-before-disconnect disconnect-cause
disconnect_cause ] [ sctp ] ] + | fqdn fqdn [ [ port port_number ]
[ send-dpr-before-disconnect disconnect-cause disconnect_cause ]
[ rlf-template rlf_template_name ] ] }

no peer peer_name [ realm realm_name ]
```

A continuación se muestran algunas notas sobre esta sintaxis:

- **no:** Este parámetro quita la configuración de peer especificada.
- **[*] nombre_peer [*]**: Este parámetro especifica el nombre del par como una cadena alfanumérica que oscila entre uno y 63 caracteres (se permiten caracteres de puntuación).**Nota:** El punto final del servidor de diámetro ahora puede ser un nombre de peer comodín (con el carácter * como carácter comodín válido). Los pares cliente que satisfacen el patrón comodín se tratan como pares válidos y se acepta la conexión. El token comodín indica que el nombre de peer es comodín y cualquier carácter * de la cadena anterior se trata como comodín.
- **realm realm_name**: Este parámetro especifica el rango de este par como una cadena alfanumérica que va de uno a 127 caracteres. El nombre de rango puede ser una empresa o un nombre de servicio.
- **address ipv4/ipv6_address**: Este parámetro especifica la dirección IP del par de diámetro en la notación hexadecimal con puntos IPv4 o hexadecimal con dos puntos IPv6. Esta dirección debe ser la dirección IP del dispositivo con el que se comunica el chasis.

- **fqdn fqdn**: Este parámetro especifica el par de diámetro Nombre de dominio completo (FQDN) como una cadena alfanumérica que oscila entre uno y 127 caracteres.

- **port port_number**: Este parámetro especifica el número de puerto para este par de diámetro. El número de puerto debe ser un número entero que oscile entre uno y 65.535.

- **connect-on-application-access**: Este parámetro activa el par en el acceso inicial a la aplicación.

- **send-dpr-before-disconnect**: Este parámetro envía la petición de par de desconexión (DPR).

- **disconnect-cause**: Este parámetro finaliza el DPR al par especificado, con el motivo de desconexión especificado. La causa de desconexión debe ser un entero que oscile entre cero y dos, lo que corresponde a estas causas:

  0 Â REINICIO

  1. .. OCUPADO

  2 Â DO_NOT_WANT_TO_TALK_TO_USTED

- **rlf-template rlf_template_name**: Este parámetro especifica la plantilla RLF que se asociará con este par de diámetro. El *rlf_template_name* debe ser una cadena alfanumérica que tenga entre uno y 127 caracteres.

  Nota: Se requiere una licencia RLF para configurar una plantilla RLF.

Protección contra sobrecarga de red con aceleración de diámetro en una interfaz Gx/Gy

Esta función protege las interfaces Gx y Gy en la dirección de salida. Protege la función de reglas de cobro y políticas (PCRF) y el sistema de carga en línea (OCS) y utiliza RLF.

Tenga en cuenta estas notas importantes cuando aplique la configuración del punto final del diámetro:

- Se debe asociar una plantilla RLF con el par.

- Un RLF se adjunta sólo por peer (individualmente).

Este comando se utiliza para configurar la protección de sobrecarga de red:

```
[context_name]host_name(config-ctx-diameter)# rlf-template rlf_template_name
```

Nota: Se requiere una licencia RLF para configurar una plantilla RLF

Configuración de la Regulación del Diámetro en una Interfaz Gx/Gy

Puede considerar el uso del RLF para interfaces de diámetro. A continuación se muestra un ejemplo de configuración:

```
rlf-template rlf1

msg-rate 1000 burst-size 100

threshold upper 80 lower 60

delay-tolerance 4

#exit


diameter endpoint Gy

use-proxy

origin host Gy address 10.55.22.3

rlf-template rlf1

peer peer1 realm foo.com address 10.55.22.1 port 3867 rlf-template rlf2

peer peer2 realm fo.com address 10.55.22.1 port 3870

#exit
```

A continuación se muestran algunas notas sobre esta configuración:

- El peer llamado *peer1* está enlazado a *RFL2*, y el resto de los peers bajo el punto final están enlazados a *RLF1*.
- La plantilla de RLF de nivel de peer tiene prioridad sobre la plantilla de nivel de punto final.
- El número de mensajes se envía a una velocidad máxima de 1.000 por segundo.(msg-rate). Estas consideraciones también se aplican:

  Sólo se envían cien mensajes (tamaño de ráfaga) cada cien milisegundos (para alcanzar los 1000 mensajes por segundo).

  Si el número de mensajes en la cola RLF supera el 80% de la velocidad de mensajes (80% de 1000 = 800), el RLF pasa al estado *OVER_THRESHOLD*.

  Si el número de mensajes en la cola RLF supera la velocidad de mensajes (1000), el RLF pasa al estado *OVER_LIMIT*.

  Si el número de mensajes en la cola RLF disminuye por debajo del 60% de la velocidad de mensajes (60% de 1.000 = 600), el RLF vuelve al estado *PREPARADO*.

  El número máximo de mensajes que se pueden poner en cola es igual a la velocidad de mensajes multiplicada por la tolerancia de retardo (1000 x 4 = 4000).

Si la aplicación envía más de 4.000 mensajes al RLF, los primeros 4.000 se ponen en cola y se suprime el resto.

La aplicación vuelve a intentar/reenviar los mensajes descartados al RLF en un tiempo adecuado.

El número de reintentos es responsabilidad de la aplicación.

- La plantilla se puede liberar del extremo con el parámetro *no rlf-template*. Por ejemplo, desenlazaría *RLF1* del *peer2*.
- No utilice el parámetro *no rlf-template rlf1* en el *modo de configuración del terminal* mientras la CLI intenta eliminar la plantilla de RLF *RLF1*. Este comando CLI es parte de la configuración global, no de la configuración del terminal.
- La plantilla se puede enlazar a peers individuales a través de uno de estos comandos:

```
no peer peer2 realm foo.com

peer peer2 realm foo.com address 10.55.22.1 port 3867
```

- El RLF sólo se puede utilizar para los puntos finales de diámetro en los que se utiliza el diamproxy.
- La velocidad de mensajes configurada se implementa por proxy de diamante. Por ejemplo, si la velocidad del mensaje es de 1000 y hay 12 diamproxies activos (chasis totalmente rellenado = 12 Packet Services Card (PSC) activos + 1 Demux + 1 PSC en espera), la Transmisiones por segundo (TPS) efectiva es de 12 000. Puede ingresar uno de estos comandos para ver las estadísticas de contexto de RLF:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Protección contra sobrecarga de red mediante aceleración de páginas con RLF

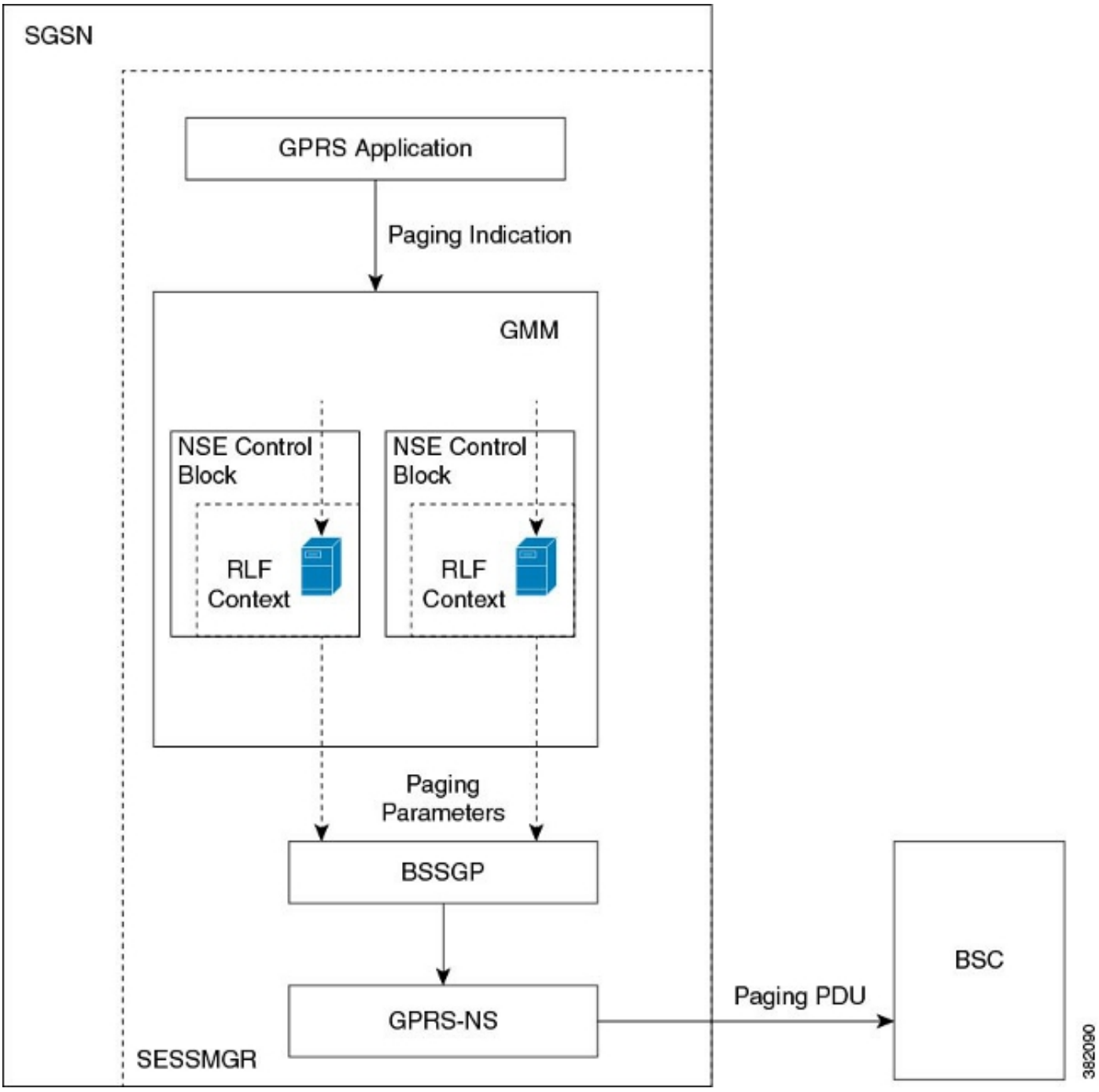
La función de limitación de páginas limita el número de mensajes de paginación que se envían desde SGSN. Proporciona flexibilidad y control al operador, que ahora puede reducir el número de mensajes de paginación enviados desde el SGSN en función de las condiciones de la red. En algunas ubicaciones, la cantidad de mensajes de paginación que se inician desde el SGSN es muy alta debido a las malas condiciones de radio. Un mayor número de mensajes de paginación produce el consumo de ancho de banda en la red. Esta función proporciona un límite de velocidad configurable, en el que el mensaje de paginación se limita a estos niveles:

- Nivel global para el acceso 2G y 3G
- El nivel de entidad de servicio de red (NSE) para acceso 2G solamente
- Nivel de controlador de red de radio (RNC) para acceso 3G solamente

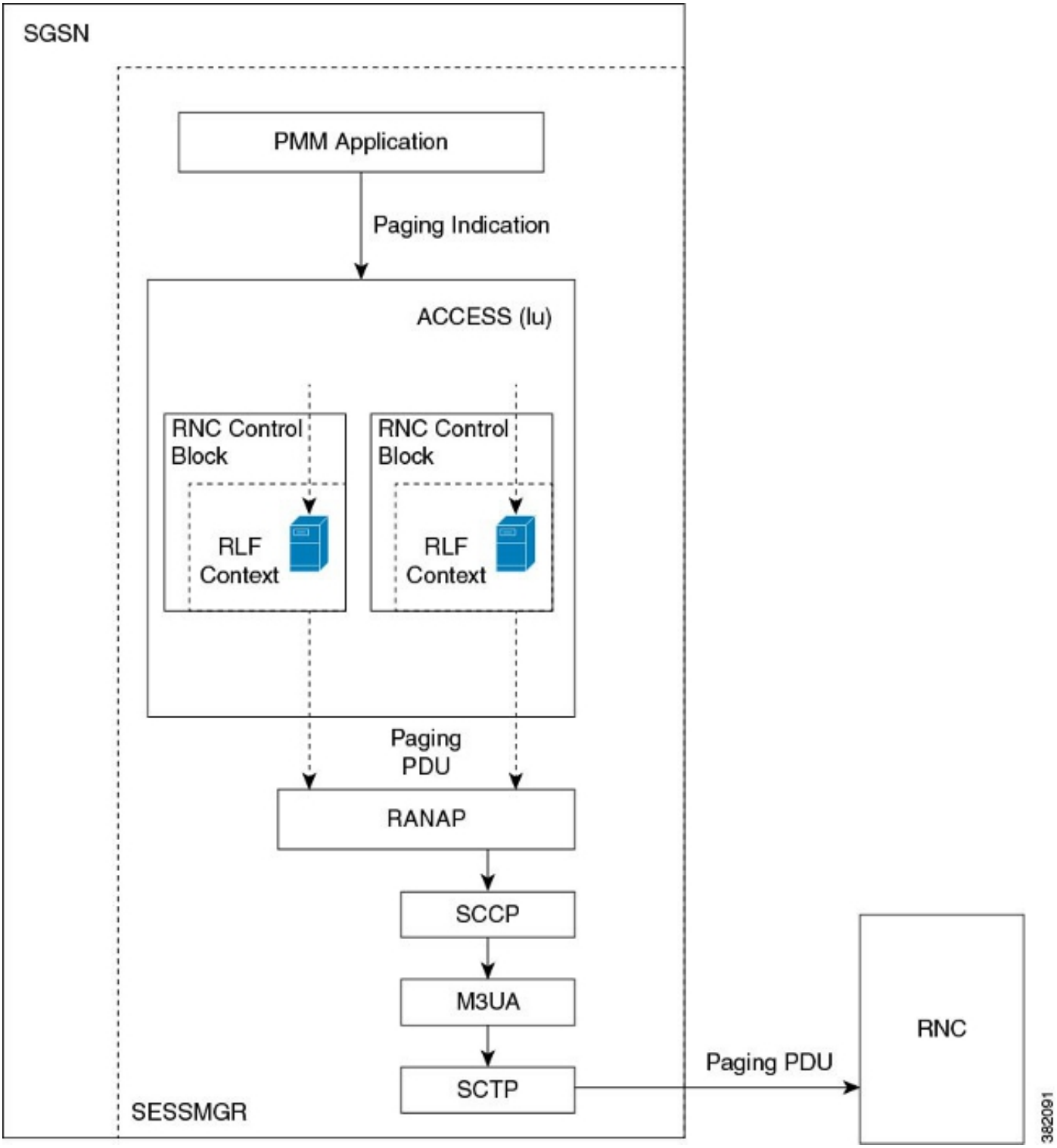
Esta función mejora el consumo de ancho de banda en la interfaz de radio.

Nota: Se requiere una licencia RLF para configurar una plantilla RLF.

A continuación se muestra un ejemplo del proceso de paginación con acceso 2G y limitación de velocidad:



Este es un ejemplo del proceso de paginación con acceso 3G y limitación de velocidad:



Configuración de la Regulación de Páginas con RLF

Los comandos que se describen en esta sección se utilizan para configurar la función de regulación de páginas. Estos comandos de CLI se utilizan para asociar/quitar la plantilla de RLF para la regulación de páginas en el nivel global, el nivel NSE y el nivel RNC en el SGSN.

Asignar el nombre RNC al identificador RNC

El comando **interface** se utiliza para configurar la asignación entre el Identificador RNC (ID) y el nombre RNC. Puede configurar el *paging-rlf-template* bien por el nombre RNC o por el ID RNC. Esta es la sintaxis utilizada:

```
config
sgsn-global
interface-management
[ no ] interface {gb
peer-nsei | iu peer-rnc} {name <value> | id <value>}
exit
```

Nota: La forma *no* del comando quita la asignación y otra configuración asociada con la configuración de la *paginación-rlf-template* RNC del SGSN y restablece el comportamiento al valor predeterminado para ese RNC.

A continuación se muestra un ejemplo de configuración:

```
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# interface
iu peer-rnc id 250 name bng_rnc1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
```

Asociar una plantilla RLF de búsqueda

Este comando permite al SGSN asociar una plantilla RLF ya sea a nivel global, lo que limita los mensajes de paginación que se inician en el acceso 2G (nivel NSE) y 3G (nivel RNC), o en el nivel por entidad, que se encuentra en el nivel RNC para el acceso 3G o en el nivel NSE para el acceso 2G. Esta es la sintaxis utilizada:

```
config
sgsn-global
interface-management
[no] paging-rlf-template {template-name <template-name>} {gb
peer-nsei | iu peer-rnc} {name <value> | id <value>}
exit
```

Nota: Si no hay ninguna plantilla de RLF asociada a un NSE/RNC determinado, la carga de paginación se limita según la plantilla de RLF global asociada (si está presente). Si no se asocia ninguna plantilla RLF global, no se aplica ningún límite de velocidad en la carga de paginación.

A continuación se muestra un ejemplo de configuración:

```
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf2 gb peer-nsei id 1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
```

```
[local]asr5000# configure
[local]asr5000(config)# sgsn-global
[local]asr5000(config-sgsn-global)# interface-management
[local]asr5000(config-sgsn-interface-mgmt)# paging-rlf-template
template-name rlf2 iu peer-rnc name bng_rnc1
[local]asr5000(config-sgsn-interface-mgmt)# end
[local]asr5000#
```