Implemente la protección de la sobrecarga para los gatewayes y los elementos de red vecina en las ASR5x00 Series

Contenido

Introducción

Este documento describe cómo implementar las funciones de telefonía que están disponibles para los gatewayes (GW) y los elementos de red vecina en las 5x00 Series agregadas Cisco del router de los servicios (ASR) para proteger el rendimiento de la red total.

Control de la congestión para los GW

El control de la congestión es una característica genérica de la autopretección. Se utiliza para proteger el sistema contra las oleadas de la utilización de estos recursos:

- USO de la CPU en el proceso de los indicadores luminosos LED amarillo de la placa muestra gravedad menor
- Uso de la memoria en el proceso de los indicadores luminosos LED amarillo de la placa muestra gravedad menor

Cuando la utilización excede los umbrales predefinidos, *se caen* o *se rechazan* todas las nuevas llamadas las activaciones (del protocolo de datos de paquete (PDP), las activaciones de sesión de la red de datos del paquete (PDN)), dependiente sobre la configuración.

Aquí está un ejemplo que muestra cómo monitorear la utilización total del indicador luminoso LED amarillo de la placa muestra gravedad menor de proceso 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 la ingeniería de sistemas es el 80% de la utilización de la CPU, que se define como el límite que dirige recomendado que no se debe exceder para garantizar la operación regular del sistema. La carga más allá del valor pudo afectar las operaciones de la plataforma, tales como su estabilidad y previsibilidad, y se debe evitar con la planificación de capacidad apropiada.

> Nota: Cisco recomienda que usted utiliza la *acción de descarte* bastante que la acción del *rechazo*, pues la reconexión relanzada inmediata de la causa de las llamadas rechazadas intenta del equipo del usuario (UE). En el caso de una acción de descarte, el UE espera algunos segundos antes de que haga relanzara las tentativas de la reconexión, así que se disminuye el porcentaje de llamadas.

Protección de la sobrecarga de red para estrangular del mensaje del ingreso GTP-C

Esta característica protege el paquete GW (P-GW) /Gateway GPRS que soporta los procesos del nodo (GGSN) contra las oleadas de la transmisión y los errores del elemento de redes. En un P-GW/un GPRS de servicio que soportan el nodo (SGSN), el embotellamiento principal se relaciona con la informática del usuario, tal como la utilización y el DPC total CPU y utilización de la memoria del administrador de sesión.

No se configura un *ningún valor* en la entidad de administración SGSN/Mobility (MME) para estrangular los mensajes entrantes del control del protocolo del tunneling GPRS (GTP-C) cuando se activa la protección de la sobrecarga de red.

> Nota: El uso de GTP y de estrangular de la interfaz del diámetro requiere que una clave de licencia válida esté instalada.

Esta característica ayuda al control el índice de entrante/de mensajes de salida en el P-GW/GGSN, que ayuda a asegurarse de que el P-GW/GGSN no es abrumado por los mensajes del plan del control GTP. Además, ayuda a asegurarse de que el P-GW/GGSN no abruma al par GTP-C con los mensajes del avión del control GTP. Esta característica requiere que el GTP (versión 1 (v1) y versión 2 (el v2)) controle los mensajes se forme/se limpia sobre las interfaces Gn/Gp y S5/S8. Esta característica cubre la protección contra sobrecarga de los Nodos P-GW/GGSN y de los otros nodos externos con los cuales comunica. El estrangular se hace solamente para los mensajes del control del sesión-nivel, así que los mensajes de administración de la trayectoria no son tarifa limitada en absoluto.

La sobrecarga del nodo externo puede ocurrir en un escenario donde el P-GW/GGSN genera las peticiones de señalización a una tarifa más alta que los otros Nodos pueden dirigir. También, si la

tarifa entrante es alta en el nodo P-GW/GGSN, puede ser que inunde el nodo externo. Por este motivo, el estrangular de los mensajes entrantes y salientes del control se requiere. Para la protección de los nodos externos contra una sobrecarga debido a la señalización de control P-GW/GGSN, un marco se utiliza para formar y limpiar los mensajes salientes del control a las interfaces externas.

El estrangular del mensaje del ingreso GTP-C de la configuración

Ingrese este comando para configurar estrangular del mensaje del ingreso GTP-C:

```
gtpc overload-protection Ingress
```

Esto configura la protección contra sobrecarga del GGSN/PGW estrangulando los mensajes del control entrante GTPv1 y GTPv2 sobre la interfaz Gn/Gp (GTPv1) o S5/S8 (GTPv2) con los otros parámetros para los servicios que se configuran en un contexto y se aplican al GGSN y al PGW.

Cuando usted ingresa el comando anterior, se genera este prompt:

```
gtpc overload-protection Ingress
```

Aquí están algunas notas sobre este sintaxis:

- no: Este parámetro inhabilita estrangular de mensaje de control entrante GTP para los servicios GGSN/PGW en este contexto.
- msg_rate de la MSG-tarifa: Este parámetro define el número de mensajes entrantes GTP que se puedan procesar por segundo. *El msg_rate* es un número entero que se extiende a partir de la ciento a 12,000.
- dur de la tolerancia de retraso: Este parámetro define el número máximo de segundos que un mensaje entrante GTP pueda ser hecho cola antes de que se procese. Después de que se exceda esta tolerancia, se cae el mensaje. *El dur* es un número entero que se extiende a partir del uno a diez.
- tamaño del tamaño de la cola: Este parámetro define el tamaño máximo de cola para los mensajes entrantes GTP-C. Si la cola excede el tamaño definido, después se cae cualquier nuevo mensaje entrante. *El tamaño* es un número entero que se extiende a partir de la ciento a 10,000.

Usted puede utilizar este comando para habilitar estrangular de mensaje de control entrante GTP para los servicios GGSN/PGW que se configuran en el mismo contexto. Como un ejemplo, este comando habilita los mensajes entrantes del control GTP en un contexto con un índice del mensaje de *1,000* por segundo, un tamaño de la cola de mensaje de *10,000*, y un retardo del *segundo*:

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

Protección del elemento de red vecina

Muchos elementos de red vecina utilizan sus propios mecanismos para protegerse, y la protección adicional de la sobrecarga de red en el lado ASR5x00 no pudo ser necesaria. La protección de los elementos de red vecina pudo ser requerida en caso de que la estabilidad de la

red total pueda ser alcanzada solamente cuando el estrangular del mensaje se aplica en el lado de la salida.

Protección de la sobrecarga de red con el diámetro que estrangula en una interfaz S6a

Esta característica protege las interfaces S6a y S13 en la dirección de salida. Protege el servidor del suscriptor casero (HS), el agente de la encaminamiento del diámetro (DRACMA), y el registro de identidad de equipo (EIR). La característica utiliza la función de limitación de la tarifa (RLF).

Considere estas NOTAS IMPORTANTES cuando usted aplica la configuración del punto final del diámetro:

- Una plantilla RLF se debe asociar al par.
- Un RLF se asocia solamente sobre una base del por-par (individualmente).

Diámetro de la configuración que estrangula en una interfaz S6a

Aquí está la sintaxis de los comandos que se utiliza para configurar el diámetro que estrangula en una interfaz S6a:

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

Aquí están algunas notas sobre este sintaxis:

- **no**: Este parámetro quita la configuración de peer especificada.
- **[*]del peer_name del [*]**: Este parámetro especifica el nombre del par como cadena alfanumérica que se extienda a partir de la una a 63 caracteres (se permiten los caracteres de puntuación).Nota: El punto final del servidor del diámetro puede ahora ser un nombre salvaje-cardado del par (con * el carácter como carácter comodín válido). Validan al cliente que tratan a los pares que satisfacen el modelo salvaje-cardado como los peeres válidos, y la conexión. El token salvaje-cardado indica que el nombre del par salvaje-está cardado, y * el carácter en la cadena que precede se trata como comodín.
- **realm_name del reino**: Este parámetro especifica el reino de este par como cadena alfanumérica que se extienda a partir de la una a 127 caracteres. El Nombre de terreno puede ser una compañía o mantener el nombre.
- **direccionamiento ipv4/ipv6_address**: Este parámetro especifica el IP Address de Peer del diámetro en el decimal punteado del IPv4, o la notación dos puntos-separar-hexadecimal del IPv6. Este direccionamiento debe ser la dirección IP del dispositivo con el cual el chasis comunica.
- **FQDN FQDN**: Este parámetro especifica el nombre de dominio completo (FQDN) del par del diámetro como cadena alfanumérica que se extienda a partir de la una a 127 caracteres.
- **port_number del puerto**: Este parámetro especifica el número del puerto para este par del diámetro. El número del puerto debe ser un número entero que se extiende a partir del uno a

65,535.

- **conectar-en-aplicación-acceso**: Este parámetro activa al par sobre el acceso de la aplicación inicial.
- **enviar-DPR-antes-desconexión**: Este parámetro envía la Desconexión-Par-petición (DPR).
- **Desconectar causa**: Este parámetro termina el DPR al par especificado, con el motivo de desconexión especificado. El Desconectar causa debe ser un número entero que se extiende a partir de la cero a dos, que corresponden a estas causas:

  el 0 REINICIAR del del Â del âÂ

  1 del Â del âÂ OCUPADO

  2 DO_NOT_WANT_TO_TALK_TO_YOU del Â del âÂ

- **rlf_template_name de la rlf-plantilla**: Este parámetro especifica la plantilla RLF que se asociará a este par del diámetro. *El rlf_template_name* debe ser una cadena alfanumérica que se extiende a partir de la una a 127 caracteres.

  Nota: Una licencia RLF se requiere para configurar una plantilla RLF.

Protección de la sobrecarga de red con el diámetro que estrangula en una interfaz Gx/Gy

Esta característica protege las interfaces de Gx y GY en la dirección de salida. Protege la directiva y cargando gobierna la función (PCRF) y el sistema de carga en línea (OCS) y utiliza RLF.

Considere estas NOTAS IMPORTANTES cuando usted aplica la configuración del punto final del diámetro:

- Una plantilla RLF se debe asociar al par.
- Un RLF se asocia solamente sobre una base del por-par (individualmente).

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

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

Nota: Una licencia RLF se requiere para configurar una plantilla RLF

Diámetro de la configuración que estrangula en una interfaz Gx/Gy

Usted puede ser que considere el uso del RLF para las interfaces del diámetro. Aquí está un ejemplo de configuración:

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

Aquí están algunas notas sobre esta configuración:

- El par llamado *peer1* está limitado a *RFL2*, y el resto de los pares conforme al punto final está limitado a *RLF1*.
- La plantilla del par-nivel RLF toma la precedencia sobre la plantilla del punto final-nivel.
- El número de mensajes se envía hasta una tasa máxima de 1,000 por segundo. (MSG-tarifa). Estas consideraciones también se aplican:

  Solamente cientos mensajes (tamaño de ráfaga) se envían todos los cientos de milisegundos (para alcanzar los 1,000 mensajes por segundo).

  Si el número de mensajes en la cola RLF excede del 80% de la tarifa del mensaje (el 80% de 1,000 = 800), las transiciones RLF al estado *OVER_THRESHOLD*.

  Si el número de mensajes en la cola RLF excede la tarifa del mensaje (1,000), las transiciones RLF al estado *OVER_LIMIT*.

  Si el número de mensajes en la cola RLF disminuye debajo del 60% de la tarifa del mensaje (el 60% de 1,000 = 600), las transiciones RLF de nuevo al *estado Ready (Listo)*.

  El número máximo de mensajes que puedan ser hechos cola iguala la tarifa del mensaje multiplicada por la tolerancia de retraso (1,000 x 4 = 4,000).

  Si la aplicación envía más de 4,000 mensajes al RLF, se hacen cola los primeros 4,000 y se cae el resto.

  Los mensajes se caen que son retried/re-sent por la aplicación al RLF en una cantidad de tiempo apropiada.

  El número de recomprobaciones es la responsabilidad de la aplicación.
- La plantilla puede ser desatada del punto final con el *ningún* parámetro de la rlf-*plantilla*. Por ejemplo, desataría *RLF1 de peer2*.
- No utilice el *ningún* parámetro de la rlf-*plantilla rlf1* en el *modo de configuración del punto final*, como el CLI intenta borrar la plantilla *RLF1* RLF. Este comando CLI es una parte de la configuración global, no la configuración del punto final.
- La plantilla se puede limitar a los pares individuales vía uno de estos comandos:
  no peer peer2 realm foo.com

  peer peer2 realm foo.com address 10.55.22.1 port 3867
- El RLF se puede utilizar solamente para los puntos finales del diámetro en los cuales se utiliza el diamproxy.
- La tarifa configurada del mensaje se implementa por-diamproxy. Por ejemplo, si es la tarifa

del mensaje 1,000, y 12 diamproxies son activas (chasis completamente poblado de = el indicador luminoso LED amarillo de la placa muestra gravedad menor activo 12 servicios de paquetes (PSC) + 1 Demux + 1 PSC espera), las transmisiones eficaces por segundo (los TP) son 12,000. Usted puede ingresar uno de estos comandos para ver las estadísticas del contexto RLF:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Protección de la sobrecarga de red a través de la página que estrangula con RLF

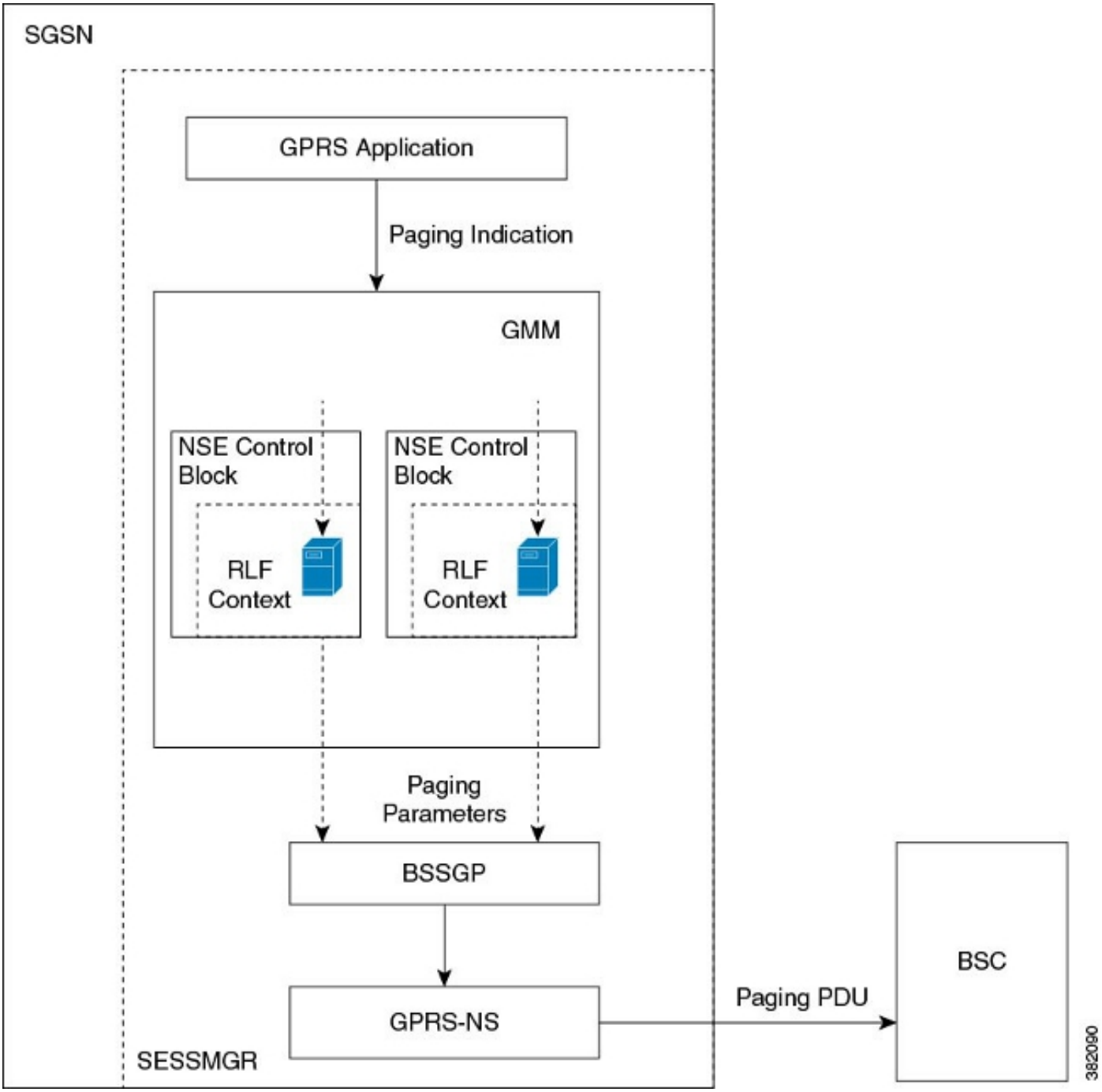
La característica que estrangula de la página limita el número de mensajes de la paginación que se envíen el de los SGSN. Proporciona la flexibilidad y el control al operador, que puede ahora reducir el número de mensajes de la paginación que se envíen del SGSN basado en los estados de la red. En algunas ubicaciones, la cantidad de mensajes de la paginación que se inicien del SGSN es mismo elevado debido a las malas condiciones de radio. Un número más elevado de los mensajes de la paginación da lugar al consumo de ancho de banda en la red. Esta característica proporciona un límite de velocidad configurable, en el cual el mensaje de la paginación se estrangula en estos niveles:

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

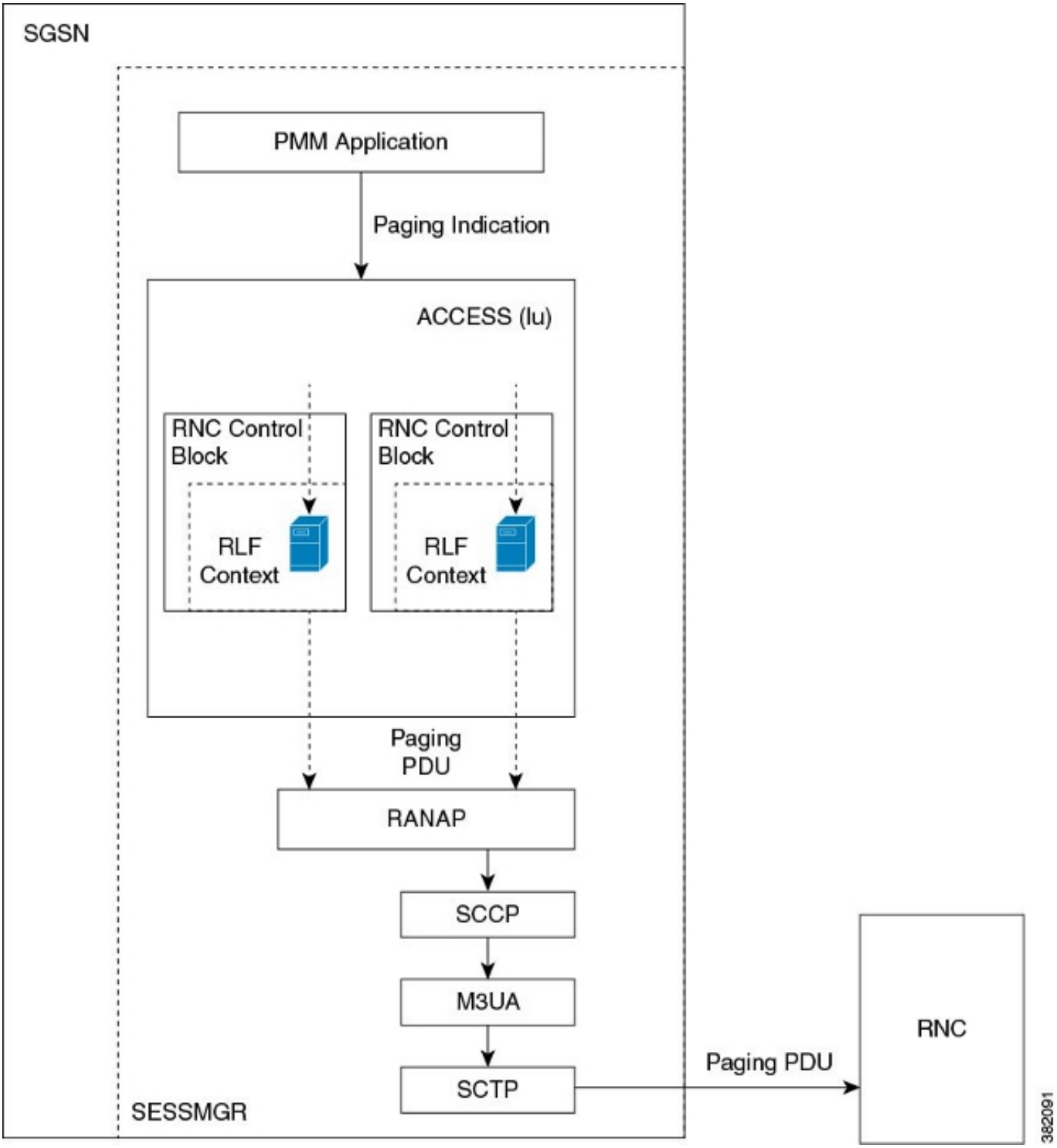
Esta característica mejora el consumo de ancho de banda en la interfaz radio.

Nota: Una licencia RLF se requiere para configurar una plantilla RLF.

Aquí está un ejemplo del proceso de la paginación con el acceso 2G y valora la limitación:



Aquí está un ejemplo del proceso de la paginación con el acceso 3G y valora la limitación:



Página de la configuración que estrangula con RLF

Los comandos que se describen en esta sección se utilizan para configurar la característica que estrangula de la página. Utilizan para asociarse/quitan a estos comandos CLI la plantilla RLF para la página que estrangula en el nivel global, el nivel NSE, y el nivel RNC en el SGSN.

Asocie el nombre RNC al identificador RNC

Utilizan al **comando interface** para configurar la asignación entre el identificador RNC (ID) y el nombre RNC. Usted puede configurar la paginación-rlf-*plantilla* por el nombre o RNC ID RNC. Aquí está el sintaxis se utiliza que:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Nota: *La ninguna* forma del comando quita la asignación y la otra configuración que se asocia a la configuración de la paginación-rlf-*plantilla* RNC del SGSN y reajusta el comportamiento al valor por defecto para eso RNC.

Aquí está un ejemplo de configuración:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Asocie una plantilla RLF que pagina

Este comando permite que el SGSN asocie una plantilla RLF cualquiera en el nivel global, que limita los mensajes de la paginación que se inician a través del 2G (NSE-nivel) y el acceso 3G (RNC-nivel), o en el nivel de la por-entidad, que está en el nivel RNC para el acceso 3G o en el nivel NSE para el acceso 2G. Aquí está el sintaxis se utiliza que:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Nota: Si no hay plantilla RLF asociada a un NSE/RNC determinado, después la carga de la paginación es limitada basada en la plantilla global RLF que es asociada (si presente). Si no hay plantilla global RLF asociada, después no se aplica ninguna limitación de la tarifa en la carga de la paginación.

Aquí está un ejemplo de configuración:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```