Proteção da sobrecarga do implementar para gateways e elementos de rede de vizinhança no ASR5x00 Series

Índice

Introdução

Este documento descreve como executar os recursos de proteção que estão disponíveis para os gateways (GW) e os elementos de rede de vizinhança no 5x00 Series agregado Cisco do roteador dos serviços (ASR) a fim proteger o desempenho da rede total.

Controle de congestionamento para GW

O controle de congestionamento é uma característica genérica da autoproteção. É usado a fim proteger o sistema contra impulsos da utilização destes recursos:

- USO de CPU em processar cartões
- Utilização de memória em processar cartões

Quando a utilização excede os pontos iniciais predefinidos, todos os atendimentos novos (ativações do protocolo de dados de pacote (PDP), ativações de sessão da rede de dados do pacote (PDN)) *estão deixados cair* ou *rejeitados*, dependente da configuração.

Está aqui um exemplo que mostre como monitorar a utilização total do cartão de processo de dados (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: O limite da engenharia de sistema é 80% da utilização CPU, que é definida como o limite de planejamento recomendado que não deve ser excedido a fim garantir a operação regular do sistema. A carga além do valor pôde impactar funcionamentos da plataforma, tais como suas estabilidade e previsibilidade, e deve ser evitada com planejamento da capacidade apropriado.

> Nota: Cisco recomenda que você usa a *ação de queda* um pouco do que a ação da *rejeição*, porque a re-conexão repetida imediata da causa das chamadas rejeitadas tenta do equipamento de usuário (UE). No caso de uma ação de queda, o UE espera alguns segundos antes que faça repetir tentativas da re-conexão, assim que a taxa de chamada está diminuída.

Proteção da sobrecarga de rede para o estrangulamento da mensagem do ingresso GTP-C

Esta característica protege os processos de apoio do nó do pacote GW (P-GW) /Gateway GPRS (GGSN) das falhas dos impulsos e do elemento de rede da transmissão. Em um P-GW/em servir o nó de apoio GPRS (SGSN), o gargalo principal é relacionado ao processo de dados do usuário, tal como a utilização da gerente de sessão e o DPC total CPU e utilização de memória.

Nenhum valor é configurado na entidade de gerenciamento SGSN/Mobility (MME) a fim estrangular as mensagens de entrada do controle de protocolo da escavação de um túnel GPRS (GTP-C) quando a proteção da sobrecarga de rede é ativada.

> Nota: O uso de GTP e do estrangulamento da relação do diâmetro exige que uma chave de licença válida esteja instalada.

Esta característica ajuda o controle a taxa de entrada/mensagens externa no P-GW/GGSN, que ajuda a se assegurar de que o P-GW/GGSN não esteja oprimido pelas mensagens do plano do controle GTP. Além, ajuda a assegurar-se de que o P-GW/GGSN não oprima o par GTP-C com as mensagens do plano do controle GTP. Esta característica exige que o GTP (versão 1 (v1) e versão 2 (v2)) controle mensagens seja dado forma/policiado sobre as relações Gn/Gp e S5/S8. Esta característica cobre a proteção da sobrecarga dos Nós P-GW/GGSN e dos outros nós externos com que se comunica. Estrangular é feito somente para mensagens do controle do sessão-nível, assim que os mensagens de gerenciamento do trajeto não são taxa limitada de todo.

A sobrecarga do nó externo pode ocorrer em uma encenação onde o P-GW/GGSN gerencia solicitações de sinalização em uma taxa mais alta do que os outros Nós podem segurar. Também, se a taxa de entrada é alta no nó P-GW/GGSN, pôde inundar o nó externo. Por este motivo, o estrangulamento de mensagens de entrada e de partida do controle é exigido. Para a

proteção dos nós externos de uma sobrecarga devido ao P-GW/GGSN controle a sinalização, uma estrutura é usada a fim dar forma e policiar às mensagens de partida do controle às interfaces externas.

Configurar o estrangulamento da mensagem do ingresso GTP-C

Incorpore este comando a fim configurar o estrangulamento da mensagem do ingresso GTP-C:

```
gtpc overload-protection Ingress
```

Isto configura a proteção da sobrecarga do GGSN/PGW estrangulando mensagens do controle GTPv1 e GTPv2 de entrada sobre (GTPv2) a relação Gn/Gp (GTPv1) ou S5/S8 com os outros parâmetros para os serviços que são configurados em um contexto e aplicados ao GGSN e ao PGW.

Quando você incorpora o comando precedente, esta alerta está gerada:

```
[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
```

Estão aqui algumas notas sobre esta sintaxe:

- **não**: Este parâmetro desabilita a mensagem de entrada do controle GTP que estrangula para os serviços GGSN/PGW neste contexto.
- **msg_rate da MSG-taxa**: Este parâmetro define o número de mensagens de entrada GTP que podem ser processadas por segundo. *O msg_rate* é um inteiro que varie de cem a 12,000.
- **dur da tolerância de retardo**: Este parâmetro define o número máximo de segundos que uma mensagem de entrada GTP pode ser enfileirada antes que esteja processada. Depois que esta tolerância é excedida, a mensagem está deixada cair. *O dur* é um inteiro que varie de um a dez.
- **tamanho do tamanho da fila**: Este parâmetro define o tamanho máximo de fila para as mensagens de entrada GTP-C. Se a fila excede o tamanho definido, a seguir todas as mensagens de entrada novas estão deixadas cair. *O tamanho* é um inteiro que varie de cem a 10,000.

Você pode usar este comando a fim permitir a mensagem de entrada do controle GTP que estrangula para os serviços GGSN/PGW que são configurados no mesmo contexto. Como um exemplo, este comando permite as mensagens de entrada do controle GTP em um contexto com uma taxa da mensagem de *1,000* por segundo, um tamanho da fila de mensagem de *10,000*, e um atraso do *segundo*:

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

Proteção do elemento de rede vizinha

Muitos elementos de rede vizinha usam seus próprios mecanismos a fim proteger-se, e a proteção adicional da sobrecarga de rede no lado ASR5x00 não pôde ser precisada. A proteção dos elementos de rede vizinha pôde ser exigida nos casos onde a estabilidade de rede total pode

ser alcançada somente quando o estrangulamento da mensagem é aplicado no lado de saída.

Proteção da sobrecarga de rede com o diâmetro que estrangula em uma relação S6a

Esta característica protege as relações S6a e S13 na direção de saída. Protege o servidor de assinante home (HS), o agente do roteamento do diâmetro (DRACMA), e o registro de identidade de equipamento (EIR). A característica usa a função de limitação da taxa (RLF).

Considere estas observações importantes quando você aplica a configuração do valor-limite do diâmetro:

- Um molde RLF deve ser associado com o par.
- Um RLF é anexado somente em uma base do por-par (individualmente).

Configurar o diâmetro que estrangula em uma relação S6a

Está aqui a sintaxe de comando que é usada a fim configurar o diâmetro que estrangula em uma relação 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 ]
```

Estão aqui algumas notas sobre esta sintaxe:

- **não**: Este parâmetro remove a configuração de peer especificada.
- **[*]do peer_name do [*]**: Este parâmetro especifica o nome do par como uma corda alfanumérica que varie de uma a 63 caráteres (os caráteres de pontuação são permitidos).Nota: O valor-limite do server do diâmetro pode agora ser um nome selvagem-cardado do par (com * o caráter como um caractere wildcard válido). O cliente que os pares que satisfazem o teste padrão selvagem-cardado são tratados como peer válidos, e a conexão é aceitado. O token selvagem-cardado indica que o nome do par selvagem-está cardado, e * o caráter na corda que precede é tratado como um convite.
- **realm_name do reino**: Este parâmetro especifica o reino deste par como uma corda alfanumérica que varie de uma a 127 caráteres. O nome de esfera pode ser uma empresa ou prestar serviços de manutenção ao nome.
- **endereço ipv4/ipv6_address**: Este parâmetro especifica a notação do endereço IP do peer do diâmetro no ponto decimal do IPv4, ou do dois pontos-separar-hexadecimal do IPv6. Este endereço deve ser o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo com que o chassi se comunica.
- **FQDN FQDN**: Este parâmetro especifica o nome de domínio totalmente qualificado do par do

diâmetro (FQDN) como uma corda alfanumérica que varie de uma a 127 caráteres.

- **port_number da porta**: Este parâmetro especifica o número de porta para este par do diâmetro. O número de porta deve ser um inteiro que varie de um a 65,535.
- **conectar-em-aplicativo-acesso**: Este parâmetro ativa o par em cima do acesso de aplicativo inicial.
- **enviar-DPR-antes-disconexão**: Este parâmetro envia o Disconexão-Par-pedido (DPR).
- **causa da desconexão**: Este parâmetro termina o DPR ao par especificado, com o motivo de desconexão especificado. A causa da desconexão deve ser um inteiro que varie de zero a dois, que correspondem a estas causas:

  0 REPARTIÇÕES do do Â do âÂ

  1 do Â do âÂ OCUPADO

  2 DO_NOT_WANT_TO_TALK_TO_YOU do Â do âÂ

- **rlf_template_name do rlf-molde**: Este parâmetro especifica o molde RLF a ser associado com este par do diâmetro. *O rlf_template_name* deve ser uma corda alfanumérica que varie de uma a 127 caráteres.

  Nota: Uma licença RLF é exigida a fim configurar um molde RLF.

Proteção da sobrecarga de rede com o diâmetro que estrangula em uma relação Gx/Gy

Esta característica protege as relações de Gx e GY na direção de saída. Protege a política e carregando ordena a função (PCRF) e o sistema de carregamento em linha (OC) e usa RLF.

Considere estas observações importantes quando você aplica a configuração do valor-limite do diâmetro:

- Um molde RLF deve ser associado com o par.
- Um RLF é anexado somente em uma base do por-par (individualmente).

Este comando é usado a fim configurar a proteção da sobrecarga de rede:

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

Nota: Uma licença RLF é exigida a fim configurar um molde RLF

Configurar o diâmetro que estrangula em uma relação Gx/Gy

Você pôde considerar o uso do RLF para relações do diâmetro. Está aqui um exemplo de

configuração:

```
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
```

Estão aqui algumas notas sobre esta configuração:

- O par chamado *peer1* é limitado a *RFL2*, e o resto dos pares sob o valor-limite é limitado a *RLF1*.
- O molde do par-nível RLF toma a precedência sobre o molde do valor--nível.
- O número de mensagens é mandado a uma taxa máxima de 1,000 por segundo. (MSG-taxa). Estas considerações igualmente aplicam-se:

  Somente cem mensagens (tamanho de intermitência) são mandadas cada cem milissegundos (a fim alcançar por segundo as 1,000 mensagens).

  Se o número de mensagens na fila RLF excede 80% da taxa da mensagem (80% de 1,000 = de 800), as transições RLF ao estado *OVER_THRESHOLD*.

  Se o número de mensagens na fila RLF excede a taxa da mensagem (1,000), as transições RLF ao estado *OVER_LIMIT*.

  Se o número de mensagens na fila RLF diminui abaixo de 60% da taxa da mensagem (60% de 1,000 = de 600), as transições RLF de volta ao *estado pronto*.

  O número máximo de mensagens que podem ser enfileiradas iguala a taxa da mensagem multiplicada pela tolerância de retardo (1,000 x 4 = 4,000).

  Se o aplicativo envia mais de 4,000 mensagens ao RLF, os primeiros 4,000 estão enfileirados e o resto é deixado cair.

As mensagens que são deixadas cair são retried/re-sent pelo aplicativo ao RLF em uma quantidade de tempo apropriada.

O número de novas tentativas é a responsabilidade do aplicativo.

- O molde pode ser desatado do valor-limite com *nenhum* parâmetro do rlf-*molde*. Por exemplo, desataria *RLF1 de peer2*.

- Não use *nenhum* parâmetro do rlf-*molde rlf1 no modo de configuração do valor-limite*, como o CLI tenta suprimir do molde *RLF1* RLF. Este comando CLI é parte da configuração global, não a configuração do valor-limite.

- O molde pode ser limitado aos pares individuais através de um destes comandos:
  no peer peer2 realm foo.com

  peer peer2 realm foo.com address 10.55.22.1 port 3867
- O RLF pode somente ser usado para os valores-limite do diâmetro em que o diamproxy é usado.

- A taxa configurada da mensagem é executada por-diamproxy. Por exemplo, se a taxa da mensagem é 1,000, e 12 diamproxies são ativas (chassi inteiramente povoado = cartão ativo de 12 serviços de pacote de informação (PSC) + 1 Demux + 1 PSC à espera), as transmissões eficazes por segundo (TP) são 12,000. Você pode incorporar um destes comandos a fim ver as estatísticas do contexto RLF:
  show rlf-context-statistics diamproxy

  show rlf-context-statistics diamproxy verbose

Proteção da sobrecarga de rede através da página que estrangula com RLF

A característica de estrangulamento da página limita o número de mensagens da paginação que são enviadas fora do SGSN. Fornece a flexibilidade e o controle ao operador, que pode agora reduzir o número de mensagens da paginação que são mandadas do SGSN baseado nas condições de rede. Em alguns lugar, a quantidade de mensagens da paginação que são iniciadas do SGSN é muito alta devido às circunstâncias de rádio ruins. Um número mais alto de mensagens da paginação conduz ao consumo de largura de banda na rede. Esta característica fornece um limite de taxa configurável, em que a mensagem da paginação é estrangulada a estes níveis:

- O nível global para 2G e 3G alcança

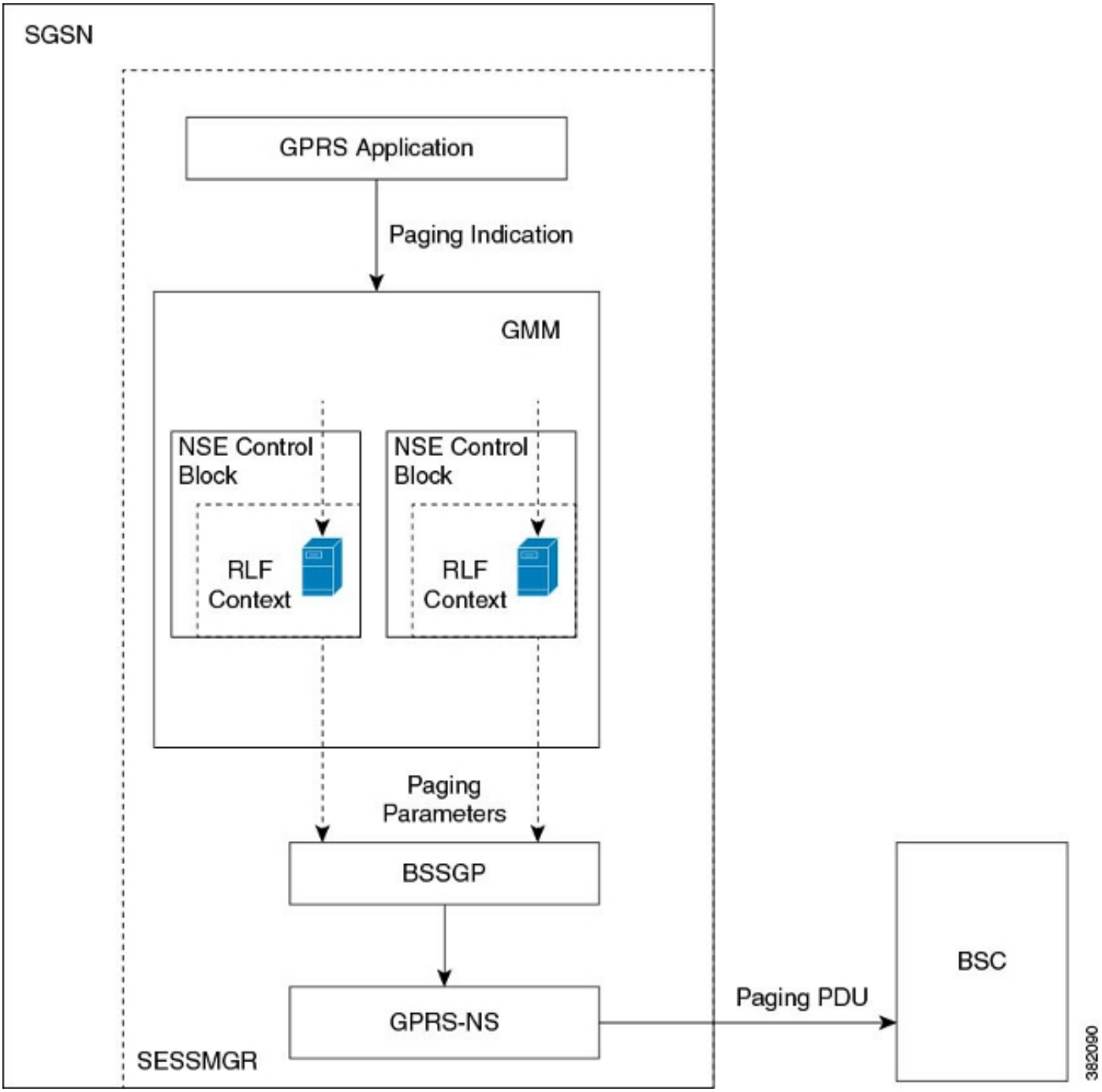
- O nível da entidade do serviço de rede (NSE) para 2G alcança somente

- O nível do controlador da rede de rádio (RNC) para 3G alcança somente

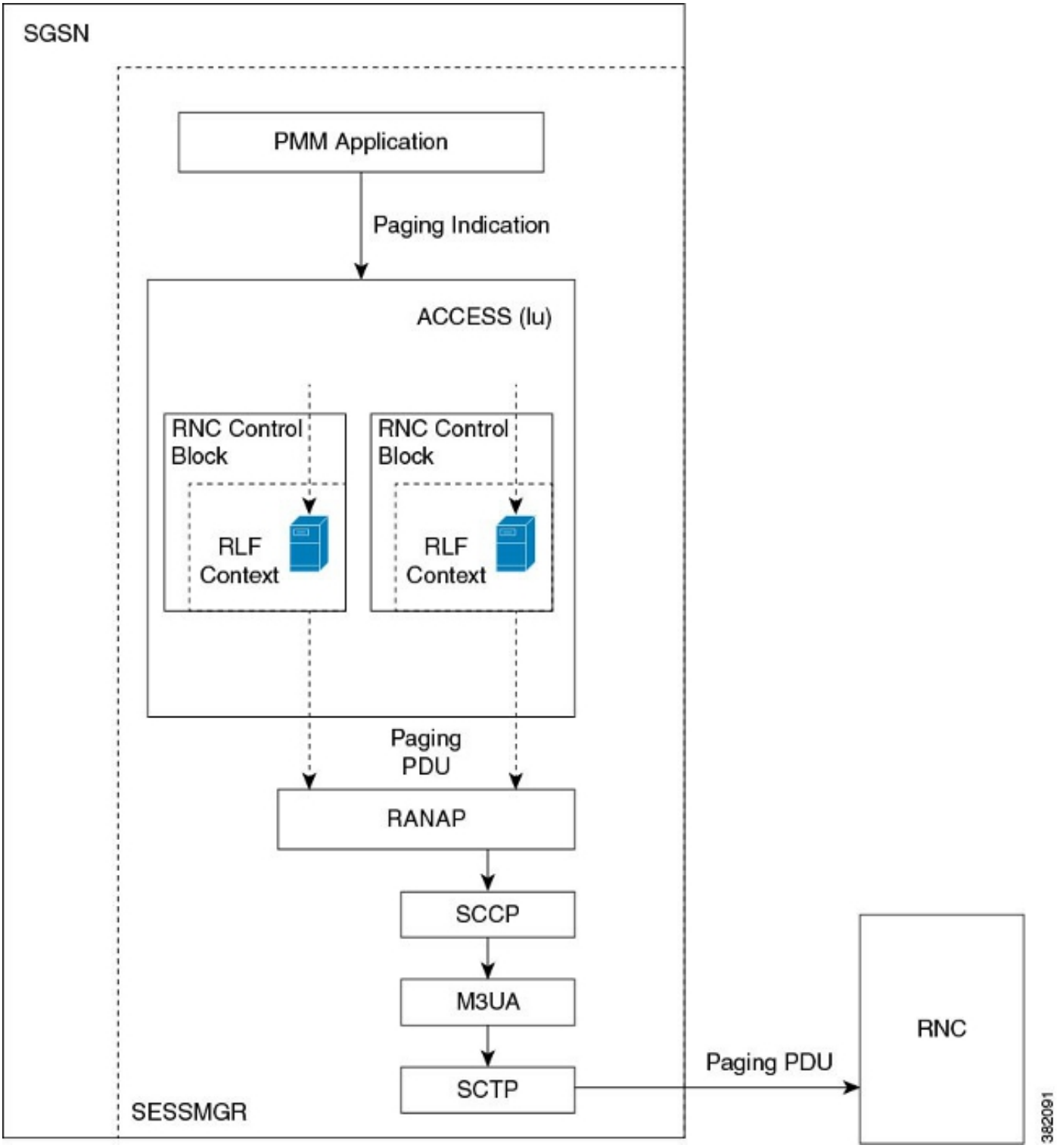
Esta característica melhora o consumo de largura de banda na interface de rádio.

Nota: Uma licença RLF é exigida a fim configurar um molde RLF.

Aqui está um exemplo do processo da paginação com acesso 2G e avalia a limitação:



Aqui está um exemplo do processo da paginação com acesso 3G e avalia a limitação:



Configurar a página que estrangula com RLF

Os comandos que são descritos nesta seção são usados a fim configurar a característica de estrangulamento da página. Estes comandos CLI são usados a fim associar/removem o molde RLF para a página que estrangula a nível global, nível NSE, e nível RNC no SGSN.

Trace o nome RNC ao identificador RNC

O comando interface é usado a fim configurar o mapeamento entre o identificador RNC (ID) e o nome RNC. Você pode configurar o paginação-rlf-*molde pelo* nome RNC ou pelo RNC ID. Está aqui a sintaxe que é usada:

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

Nota: *Nenhum* formulário do comando remove o mapeamento e a outra configuração que é associada com a configuração do paginação-rlf-*molde* RNC do SGSN e restaura o comportamento ao padrão para aquele RNC.

Está aqui um exemplo de configuração:

```
[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#
```

Associe um molde de paginação RLF

Este comando permite que o SGSN associe um molde RLF qualquer um a nível global, que limita as mensagens da paginação que são iniciadas através do 2G (NSE-nível) e (RNC-nível) acesso 3G, ou a nível da por-entidade, que está a nível RNC para o acesso 3G ou a nível NSE para o acesso 2G. Está aqui a sintaxe que é usada:

```
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: Se não há nenhum molde RLF associado com um NSE/RNC particular, a seguir a carga da paginação é limitada baseada no molde global RLF que é associado (se presente). Se nenhum molde global RLF é associado, a seguir nenhuma limitação da taxa está aplicada na carga da paginação.

Está aqui um exemplo de configuração:

```
[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#
```