Overloadbescherming voor gateways en aangrenzende netwerkelementen implementeren op de ASR5x00 Series

Inhoud

Inleiding

Dit document beschrijft hoe de beveiligingsfuncties die beschikbaar zijn voor gateways (GW's) en aangrenzende netwerkelementen moeten worden geïmplementeerd op de Cisco Aggregated Services Router (ASR) 5x00 Series om de algemene netwerkprestaties te beschermen.

Congestion Control voor GW's

Congestion Control is een generieke zelfbeveiligingsfunctie. Deze middelen worden gebruikt om het systeem te beschermen tegen een toename van het gebruik van deze middelen:

- CPU-gebruik bij verwerkingskaarten
- Geheugengebruik op verwerkingskaarten

Wanneer het gebruik de vooraf gedefinieerde drempels overschrijdt, worden alle nieuwe oproepen (Packet Data Protocol (PDP)-activering, Packet Data Network (PDN)-sessieactivering) *ingetrokken* of *afgewezen*, afhankelijk van de configuratie.

Hier is een voorbeeld dat laat zien hoe u het algemene gebruik van de Gegevensverwerkingskaart (DPC) kunt controleren:

```
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
```

> **Opmerking:** De technische limiet van het systeem is 80% van het CPU-gebruik, dat wordt gedefinieerd als de aanbevolen technische limiet die niet mag worden overschreden om een regelmatige werking van het systeem te garanderen. Laad boven de waarde kan gevolgen hebben voor de activiteiten van het platform, zoals zijn stabiliteit en voorspelbaarheid, en moet vermeden worden door middel van een goede capaciteitsplanning.

> **Opmerking:** Cisco raadt u aan de actie van de *uitrollijst* te gebruiken in plaats van de actie van de *afstoting*, aangezien de afgewezen oproepen onmiddellijke heraansluitingspogingen van de Gebruiker Apparatuur (UE) veroorzaken. In het geval van een druppelactie wacht de UE een paar seconden voordat ze opnieuw probeert verbinding te maken, dus wordt de aanroep verlaagd.

Protection voor Network Overload Protection voor Ingress GTP-C Berichtrouting

Deze functie beschermt de Packet GW (P-GW)/Gateway GPRS-processen ter ondersteuning van knooppunt (GGN) tegen transmissiesnelheden en fouten in netwerkelementen. In een IP-GW/Serving GPRS-ondersteuningsknooppunt (SGSN) is het belangrijkste knelpunt gerelateerd aan de verwerking van gebruikersgegevens, zoals het gebruik van de sessiebeheerder en de totale DPC CPU- en geheugenbenutting.

Er wordt *geen waarde* ingesteld op de SGN/Mobility Management Entiteit (MME) om de inkomende GPRS Tunneling Protocol-Control (GTP-C) berichten te blokkeren wanneer de netwerkoverload Protection is geactiveerd.

> **Opmerking:** Het gebruik van het wentelen van de GTP- en de diameter van de interface vereist dat een geldige licentiesleutel wordt geïnstalleerd.

Deze eigenschap helpt de snelheid van inkomende/uitgaande berichten op de P-GW/GGSN te controleren, wat helpt te verzekeren dat de P-GW/GGSN niet overweldigd wordt door de berichten van het GTP controleplan. Bovendien helpt het om ervoor te zorgen dat de P-GW/GGSN de GTP-C-peer niet overweldigt met de GTP-besturingsplane berichten. Voor deze optie moeten de GTP-controlevers (versie 1 (v1) en versie 2 (v2) via de Gn/Gp- en S5/S8-interfaces worden vormgegeven/geordend. Deze functie bestrijkt de overload bescherming van de P-GW/GGN-knooppunten en de andere externe knooppunten waarmee de communicatie plaatsvindt. Throtting wordt alleen uitgevoerd voor sessielaag control-berichten, dus de path management-berichten zijn helemaal niet snelheidsbeperkt.

De externe knooppunten overload kunnen voorkomen in een scenario waar de P-GW/GGSN signaleringsverzoeken genereert met een hogere snelheid dan de andere knooppunten kunnen

verwerken. Als de inkomende snelheid hoog is bij het P-GW/GGSN-knooppunt, kan dit het externe knooppunt verplaatsen. Om deze reden is het wentelen van zowel inkomende als uitgaande controleberichten vereist. Voor bescherming van de externe knooppunten tegen overbelasting door de P-GW/GGSN-controle signalering wordt een kader gebruikt om de uitstroomregelberichten naar de externe interfaces te vormen en te controleren.

Ingrepen GTP-C boodschap sturen

Voer deze opdracht in om het ingesloten GTP-C-bericht te configureren:

gtpc overload-protection Ingress

Dit vormt de overloadbescherming van de GGN/PGW door het doorsijpelen van inkomende GTPv1 en GTPv2-regelberichten via de GN/Gp (GTPv1) of S5/S8 (GTPv2) interface met de andere parameters voor de services die in een context zijn geconfigureerd en van toepassing zijn op GGSN en PGW.

Wanneer u de vorige opdracht invoert, wordt deze melding gegenereerd:

```
[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
```

Hier volgen wat opmerkingen over de syntax:

- **neen**: Deze parameter schakelt de GTP inkomende controlebericht bundeling voor de GGN/PGW diensten in deze context uit.
- **msg-tarief msg_rate**: Deze parameter definieert het aantal GTP inkomende berichten die per seconde kunnen worden verwerkt. De *msg_rate* is een integer die varieert van honderd tot 12.000.
- **vertragingstolerantie**: Deze parameter definieert het maximale aantal seconden dat een inkomend GTP-bericht in de wachtrij kan worden geplaatst voordat het wordt verwerkt. Nadat deze tolerantie is overschreden, wordt het bericht ingetrokken. Het *dur* is een integer dat varieert van één tot tien.
- **rijgrootte**: Deze parameter definieert de maximale rijgrootte voor de inkomende GTP-C berichten. Als de rij de gedefinieerde grootte overschrijdt, worden alle nieuwe inkomende berichten laten vallen. De *grootte* is een getal dat varieert van 10 tot 10.000.

U kunt deze opdracht gebruiken om het GTP-bericht van inkomende controle in te schakelen voor de GGSN/PGW-services die in dezelfde context zijn geconfigureerd. Als voorbeeld, laat deze opdracht de inkomende GTP controleberichten in een context toe met een berichttarief van *1.000* per seconde, een berichtrijgrootte van *10.000*, en een vertraging van *één* seconde:

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

Bescherming van buurnetwerkelementen

Veel buurnetwerkelementen maken gebruik van hun eigen mechanismen om zichzelf te beschermen en extra bescherming tegen overbelasting aan de ASR5x00-zijde is wellicht niet nodig. De bescherming van de aangrenzende netwerkelementen kan nodig zijn in gevallen waarin de algehele netwerkstabiliteit alleen kan worden bereikt wanneer de berichtgeving aan de bovenzijde wordt gedraaid.

Bescherming tegen overbelasting van netwerk met Diameter-switching op een S6a-interface

Deze optie beschermt de S6a- en S13-interfaces in de richting van de uitgang. Hiermee beschermt u de Home Subscriber Server (HSS), de Diameter Routing Agent (DROA) en het Equipment Identity Registreer (EIR). Deze functie gebruikt de functie Snelheidsbeperking (RLF).

Neem deze belangrijke nota's in overweging wanneer u de configuratie van het dichte eindpunt toepast:

- Een RLF-sjabloon moet aan de peer zijn gekoppeld.
- Een RLF wordt alleen per peer-basis (afzonderlijk) aangesloten.

Diameter-switching op een S6a-interface configureren

Hier is de syntax van commando's die wordt gebruikt om de diameter van een drukte op een S6a-interface te configureren:

```
[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 ]
```

Hier volgen wat opmerkingen over de syntax:

- **neen**: Deze parameter verwijdert de gespecificeerde peer configuratie.
- **[*] peer_name [*]**: Deze parameter specificeert de peer naam als een alfanumerieke string die varieert van één tot 63 tekens (leestekens zijn toegestaan).**Opmerking:** Het uiteinde van de diameter server kan nu een wild-kaard peer naam zijn (met het * teken als geldig wilde kaart teken). De client-peers die voldoen aan het wild-kaard patroon worden behandeld als geldige peers en de verbinding wordt geaccepteerd. Het wild-kaard token geeft aan dat de peer naam wild-kaard is en elk * teken in de string dat voorafgaat wordt behandeld als een jokerteken.
- **realm realm_name**: Deze parameter specificeert het rijk van deze peer als een alfanumerieke string die van één tot 127 tekens varieert. De naam van het gebied kan een bedrijf of een servicenaam zijn.
- **adres ipv4/ipv6_adres**: Deze parameter specificeert de diameter van IP-adres in IPv4 decimale of IPv6 colon-gescheiden-hexadecimale notatie. Dit adres moet het IP-adres zijn

van het apparaat waarmee het chassis communiceert.

- **fqdn** : Deze parameter specificeert de diameter van Fully Qualified Domain Name (FQDN) als een alfanumerieke string die varieert van één tot 127 tekens.

- **port_number**: Deze parameter specificeert het poortnummer voor deze diameter peer. Het poortnummer moet een integer zijn die varieert van één tot 65.535.

- **Connect-on-application-toegang**: Deze parameter activeert de peer bij eerste applicatie toegang.

- **verzenden-dpr-voor-ontkoppeling**: Deze parameter verstuurt het desconnect-peer-request (DPR).

- **oorzaak van verbroken verbinding**: Deze parameter eindigt de DPR aan de gespecificeerde peer, met de gespecificeerde disconnect reden. De scheidingsoorzaak moet een integer zijn die van nul tot twee varieert, wat overeenkomt met deze oorzaken:

  0--- REBOOTING

  1ßHE

  2--- DO_NOT_WANT_TO_TALK_TO-U

- **rlf-sjabloon rlf_sjabloon_name**: Deze parameter specificeert de RLF-sjabloon die aan deze diameterpeer wordt gekoppeld. De *rlf_sjabloon_name* moet een alfanumerieke string zijn die varieert van 1 tot 127 tekens.

  Opmerking: Er is een RLF-licentie vereist om een RLF-sjabloon te kunnen configureren.

Network Overload Protection met Diameter-switching op een GX/Gy-interface

Deze optie beschermt de interfaces Gx en Gy in de richting van de uitgang. Het beschermt de beleids- en heffingsfunctie (PCRF) en het online heffingssysteem (OCS) en gebruikt RLF.

Neem deze belangrijke nota's in overweging wanneer u de configuratie van het dichte eindpunt toepast:

- Een RLF-sjabloon moet aan de peer zijn gekoppeld.

- Een RLF wordt alleen per peer-basis (afzonderlijk) aangesloten.

Deze opdracht wordt gebruikt om de beveiliging van het netwerk te configureren:

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

Opmerking: Er is een RLF-licentie vereist om het RLF-sjabloon te kunnen configureren

Diameter-DING op een GX/Gy-interface configureren

U kunt het gebruik van RLF voor diameterinterfaces overwegen. Hier is een voorbeeldconfiguratie:

```
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
```

Hier volgen wat opmerkingen over de configuratie:

- De peer die *peer1* wordt genoemd is gebonden aan *RFL2*, en de rest van de peers onder het eindpunt is gebonden aan *RLF1*.
- De RLF-sjabloon op peer-niveau heeft voorrang op de sjabloon op endpointniveau.
- Het aantal berichten wordt verstuurd tegen een maximum van 1000 per seconde (msg-tarief). Deze overwegingen gelden ook:

  Slechts honderd berichten (burst-size) worden verzonden elke honderd milliseconden (om de 1.000 berichten per seconde te bereiken).

  Als het aantal berichten in de RLF-wachtrij meer dan 80% van de berichtsnelheid bedraagt (80% van 1.000 = 800), gaat de RLF over naar de *OVER_THRESHOLD*-status.

  Als het aantal berichten in de RLF wachtrij de berichtsnelheid (1.000) overschrijdt, gaat de RLF over naar de status *OVER_LIMIT*.

  Als het aantal berichten in de RLF-wachtrij daalt tot minder dan 60% van het bericht (60% van 1.000 = 600), gaat de RLF terug naar de *READY*-status.

  Het maximale aantal berichten dat in de wachtrij kan worden geplaatst, is gelijk aan het berichttarief vermenigvuldigd met de vertragingstolerantie (1,000 x 4 = 4,000).

Als de applicatie meer dan 4.000 berichten naar RLF verstuurt, staan de eerste 4.000 berichten in de wachtrij en gaan de overige berichten naar beneden.

De berichten die worden gedropt, worden binnen een bepaalde tijd opnieuw geprobeerd/opnieuw verstuurd door de applicatie naar de RLF.

Het aantal herhalingen valt onder de verantwoordelijkheid van de aanvraag.

- De sjabloon kan niet worden gebonden aan het eindpunt met de *geen rlf-sjabloon* parameter. Bijvoorbeeld, zou het *RLF1* van *peer2* loskoppelen.

- Gebruik de *geen rlf-sjabloon rlf1* parameter in de configuratiemodus van *eindpunt*, omdat de CLI probeert de RLF-sjabloon *RLF1* te verwijderen. Deze CLI-opdracht maakt deel uit van de mondiale configuratie en niet van de configuratie van endpoints.

- De sjabloon kan via een van deze opdrachten aan de afzonderlijke peers worden gebonden:

```
no peer peer2 realm foo.com

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

- RLF kan alleen worden gebruikt voor doorsnede-eindpunten waarin diamanten worden gebruikt.

- Het geconfigureerde berichtpercentage wordt per-diamantheretie uitgevoerd. Als het bericht bijvoorbeeld 1.000 is en 12 diamproxies actief zijn (volledig bevolkt chassis = 12 actieve Packet Services Card (PSC) + 1 Demux + 1 standby PSC), is de effectieve transmissie per seconde (TPS) 12.000. U kunt één van deze opdrachten invoeren om de RLF-contextstatistieken te bekijken:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Bescherming tegen overbelasting van netwerken door pagina's te wijzigen met RLF

De functie voor het koppelen van pagina's beperkt het aantal pagina's dat uit de SGN wordt verzonden. Het voorziet in flexibiliteit en controle voor de exploitant, die nu het aantal semafoonberichten kan verminderen die op basis van de netwerkvoorwaarden uit het SGSN worden verstuurd. Op sommige plaatsen is de hoeveelheid semafoonberichten die vanuit het SGSN geïnitieerd worden zeer hoog door slechte radioomstandigheden. Een hoger aantal pagina's resulteert in het verbruik van bandbreedte in het netwerk. Deze optie biedt een instelbare snelheidsbeperking, waarbij het pagineren bericht op deze niveaus wordt gedraaid:

- Het mondiale niveau voor toegang tot zowel 2G als 3G

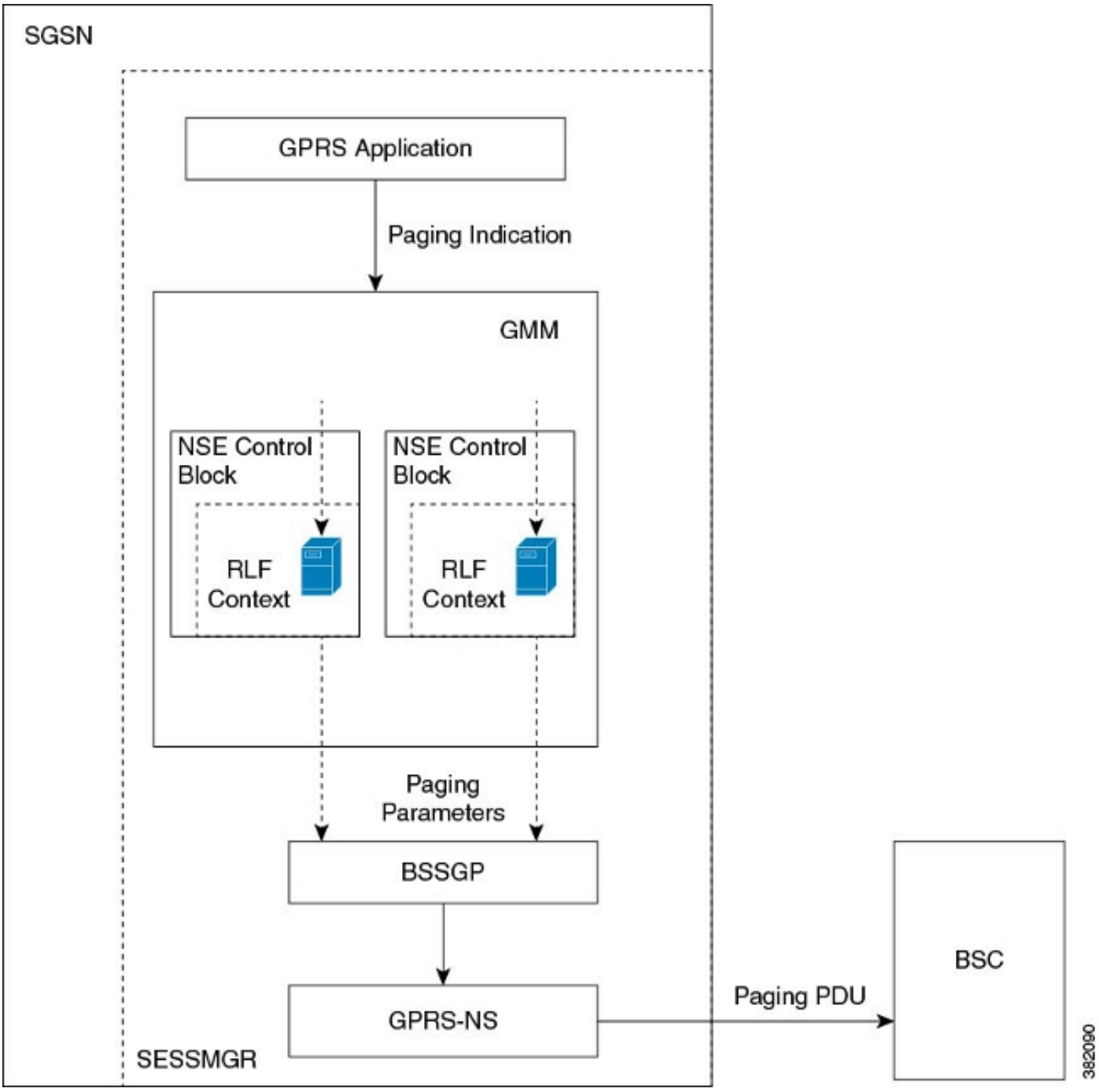
- Het niveau van de Netwerkservicetechnicus (NSE) voor alleen 2G-toegang

- Het niveau van Radio Network Controller (RNC) voor alleen 3G-toegang

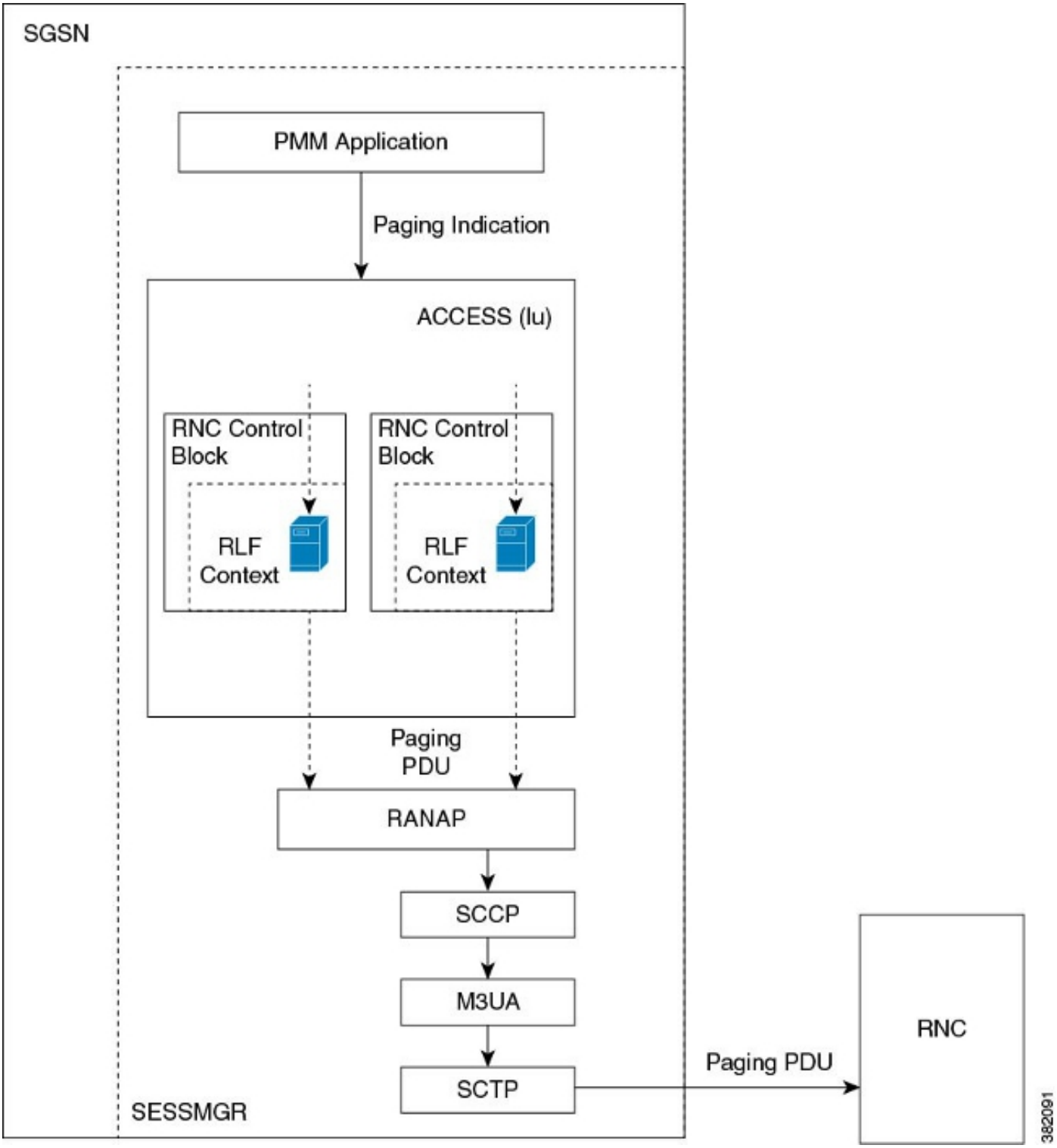
Deze functie verbetert het bandbreedteverbruik op de radio interface.

Opmerking: Er is een RLF-licentie vereist om een RLF-sjabloon te kunnen configureren.

Hier is een voorbeeld van het piepproces met 2G toegang en snelheidsbeperking:



Hier is een voorbeeld van het semafoonproces met 3G-toegang en snelheidsbeperking:



Paginabereik configureren met RLF

De opdrachten die in deze sectie worden beschreven, worden gebruikt om de functie voor het koppelen van pagina's te configureren. Deze CLI-opdrachten worden gebruikt om de RLF-sjabloon te associëren of te verwijderen voor het bladeren door pagina's op mondiaal niveau, op het NSE-niveau en op het RNC-niveau op het SGN.

Stel de RNC-naam in op de RNC-identificator

De opdracht **van de interface** wordt gebruikt om de afbeelding tussen de RNC Identifier (ID) en de naam RNC te configureren. U kunt de *paging-rlf-sjabloon* configureren door RNC-naam of RNC-

ID. Hier wordt de syntaxis gebruikt:

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

> **Opmerking:** De opdracht verwijdert de mapping en andere configuratie die is gekoppeld aan de RNC *paging-rlf-sjabloon* configuratie uit de SGSN en stelt het gedrag voor die RNC in op de standaard.

Hier is een voorbeeldconfiguratie:

```
[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#
```

Een RLF-sjabloon toevoegen

Deze opdracht stelt het SGSN in staat een RLF-sjabloon te associëren op mondiaal niveau, wat de paginering-berichten beperkt die geïnitieerd worden voor zowel de 2G (NSE-niveau) als de 3G (RNC-niveau) toegang, of op het niveau per entiteit, dat op RNC-niveau voor 3G-toegang of op NSE-niveau voor 2G-toegang is. Hier wordt de syntaxis gebruikt:

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

> **Opmerking:** Als er geen RLF-sjabloon gekoppeld is aan een bepaalde NSE/RNC dan is de paginasnelheid beperkt op basis van het wereldwijde RLF-sjabloon dat gekoppeld is (indien aanwezig). Als er geen mondiaal RLF-sjabloon is gekoppeld, wordt er geen snelheidsbeperking toegepast op de paginabereis.

Hier is een voorbeeldconfiguratie:

```
[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#
```