Implémenter la protection contre la surcharge pour les passerelles et les éléments de réseau voisins sur la gamme ASR5x00

Contenu

[Introduction](#)
[Contrôle d'encombrement pour GW](#)
[Protection contre la surcharge du réseau pour la limitation des messages GTP-C entrants](#)
[Configurer la limitation des messages GTP-C entrants](#)
[Protection des éléments du réseau voisin](#)
[Protection contre la surcharge du réseau avec limitation du diamètre sur une interface S6a](#)
[Configurer la limitation du diamètre sur une interface S6a](#)
[Protection contre la surcharge du réseau avec limitation du diamètre sur une interface Gx/Gy](#)
[Configurer la limitation du diamètre sur une interface Gx/Gy](#)
[Protection contre la surcharge du réseau via la limitation des pages avec RLF](#)
[Configurer la limitation de page avec RLF](#)

Introduction

Ce document décrit comment mettre en oeuvre les fonctions de protection disponibles pour les passerelles (GW) et les éléments de réseau voisins sur les routeurs à services agrégés (ASR) de la gamme Cisco 5x00 afin de protéger les performances globales du réseau.

Contrôle d'encombrement pour GW

Le contrôle d'encombrement est une fonctionnalité générique d'autoprotection. Il est utilisé afin de protéger le système contre les surtensions d'utilisation de ces ressources :

- Utilisation du processeur sur les cartes de traitement
- Utilisation de la mémoire sur les cartes de traitement

Lorsque l'utilisation dépasse les seuils prédéfinis, tous les nouveaux appels (activations PDP (Packet Data Protocol), activations de session PDN (Packet Data Network) sont *abandonnés* ou *rejetés*, selon la configuration.

Voici un exemple qui montre comment surveiller l'utilisation globale de la carte de traitement des données (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
```

> **Note**: La limite d'ingénierie du système est de 80 % de l'utilisation du processeur, définie comme la limite d'ingénierie recommandée qui ne doit pas être dépassée afin de garantir le fonctionnement régulier du système. La charge au-delà de la valeur peut avoir un impact sur les opérations de la plate-forme, telles que sa stabilité et sa prévisibilité, et doit être évitée avec une planification appropriée de la capacité.

> **Note**: Cisco vous recommande d'utiliser l'action *de suppression* plutôt que l'action de *rejet*, car les appels rejetés provoquent des tentatives de reconnexion répétées immédiates de la part de l'équipement utilisateur (UE). Dans le cas d'une action de suppression, l'UE attend quelques secondes avant de faire des tentatives de reconnexion répétées, de sorte que le taux d'appel est réduit.

Protection contre la surcharge du réseau pour la limitation des messages GTP-C entrants

Cette fonctionnalité protège les processus GGSN (Packet GW)/Gateway GPRS Support Node (GGSN) contre les surtensions de transmission et les pannes d'éléments réseau. Dans un noeud de prise en charge GPRS P-GW/Serving (SGSN), le principal goulot d'étranglement est lié au traitement des données utilisateur, comme l'utilisation du gestionnaire de session et l'utilisation globale du processeur DPC et de la mémoire.

Une *valeur No* est configurée sur le SGSN/MME (Mobility Management Entity) afin de limiter les messages GTP-C (Tunneling Protocol-Control) GPRS entrants lorsque la protection de surcharge réseau est activée.

> **Note**: L'utilisation de GTP et de la limitation d'interface de diamètre nécessite l'installation d'une clé de licence valide.

Cette fonctionnalité permet de contrôler le taux de messages entrants/sortants sur le P-GW/GGSN, ce qui permet de s'assurer que le P-GW/GGSN n'est pas submergé par les messages du plan de contrôle GTP. En outre, il permet de s'assurer que le P-GW/GGSN ne submerge pas l'homologue GTP-C avec les messages du plan de contrôle GTP. Cette fonctionnalité nécessite que les messages de contrôle GTP (version 1 (v1) et version 2 (v2)) soient formatés/contrôlés sur les interfaces Gn/Gp et S5/S8. Cette fonctionnalité couvre la protection contre la surcharge des noeuds P-GW/GGSN et des autres noeuds externes avec lesquels il communique. La limitation est effectuée uniquement pour les messages de contrôle au niveau de la session, de sorte que les messages de gestion des chemins ne sont pas du tout limités en débit.

La surcharge du noeud externe peut se produire dans un scénario où le P-GW/GGSN génère des requêtes de signalisation à un débit supérieur à celui que les autres noeuds peuvent gérer. En

outre, si le débit entrant est élevé au niveau du noeud P-GW/GGSN, il peut inonder le noeud externe. Pour cette raison, la limitation des messages de contrôle entrants et sortants est requise. Pour protéger les noeuds externes d'une surcharge due à la signalisation de contrôle P-GW/GGSN, un cadre est utilisé afin de former et de contrôler les messages de contrôle sortants aux interfaces externes.

Configurer la limitation des messages GTP-C entrants

Entrez cette commande afin de configurer la limitation du message GTP-C d'entrée :

```
gtpc overload-protection Ingress
```

Cela configure la protection contre la surcharge du GGSN/PGW en limitant les messages de contrôle GTPv1 et GTPv2 entrants sur l'interface Gn/Gp (GTPv1) ou S5/S8 (GTPv2) aux autres paramètres des services configurés dans un contexte et appliqués au GGSN et au PGW.

Lorsque vous entrez la commande précédente, cette invite est générée :

```
[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
```

Voici quelques notes sur cette syntaxe :

- **non:** Ce paramètre désactive la limitation des messages de contrôle entrant GTP pour les services GGSN/PGW dans ce contexte.
- **msg-rate msg_rate** : Ce paramètre définit le nombre de messages GTP entrants pouvant être traités par seconde. Le *msg_rate* est un entier compris entre 100 et 12 000.
- **délai-tolérance dur** : Ce paramètre définit le nombre maximal de secondes pendant lesquelles un message GTP entrant peut être mis en file d'attente avant d'être traité. Une fois cette tolérance dépassée, le message est abandonné. Le *dur* est un entier compris entre un et dix.
- **taille de file d'attente** : Ce paramètre définit la taille maximale de file d'attente pour les messages GTP-C entrants. Si la file d'attente dépasse la taille définie, tous les nouveaux messages entrants sont supprimés. La *taille* est un entier compris entre 100 et 10 000.

Vous pouvez utiliser cette commande afin d'activer la limitation des messages de contrôle entrant GTP pour les services GGSN/PGW configurés dans le même contexte. Par exemple, cette commande active les messages de contrôle GTP entrants dans un contexte avec un taux de messages de *1 000* par seconde, une taille de file d'attente de messages de *10 000*, et un délai d'*une* seconde :

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

Protection des éléments du réseau voisin

De nombreux éléments de réseau voisin utilisent leurs propres mécanismes afin de se protéger, et une protection supplémentaire de surcharge réseau du côté ASR5x00 peut ne pas être

nécessaire. La protection des éléments du réseau voisin peut être requise dans les cas où la stabilité globale du réseau ne peut être atteinte que lorsque la limitation des messages est appliquée côté sortie.

Protection contre la surcharge du réseau avec limitation du diamètre sur une interface S6a

Cette fonction protège les interfaces S6a et S13 dans la direction de sortie. Il protège le serveur d'abonné domestique (HSS), l'agent de routage de diamètre (DRA) et le registre d'identité de l'équipement (EIR). La fonction utilise la fonction de limitation de débit (RLF).

Tenez compte de ces remarques importantes lorsque vous appliquez la configuration des points d'extrémité de diamètre :

- Un modèle RLF doit être associé à l'homologue.
- Un RLF est attaché uniquement par homologue (individuellement).

Configurer la limitation du diamètre sur une interface S6a

Voici la syntaxe de commande utilisée afin de configurer la régulation du diamètre sur une interface 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 ]
```

Voici quelques notes sur cette syntaxe :

- **non:** Ce paramètre supprime la configuration d'homologue spécifiée.
- **[*] peer_name [*]** : Ce paramètre spécifie le nom de l'homologue sous la forme d'une chaîne alphanumérique comprise entre un et 63 caractères (les caractères de ponctuation sont autorisés).**Note**: Le terminal du serveur de diamètre peut maintenant être un nom d'homologue générique (avec le caractère * comme caractère générique valide). Les homologues clients qui satisfont au modèle de caractères génériques sont traités comme des homologues valides et la connexion est acceptée. Le jeton à caractères génériques indique que le nom de l'homologue est à caractères génériques, et tout caractère * de la chaîne qui précède est traité comme un caractère générique.
- **realm nom_domaine** : Ce paramètre spécifie le domaine de cet homologue sous la forme d'une chaîne alphanumérique comprise entre un et 127 caractères. Le nom du domaine peut être un nom de société ou de service.
- **adresse ipv4/ipv6_address** : Ce paramètre spécifie l'adresse IP homologue de diamètre en notation décimale à point IPv4 ou en notation hexadécimale séparée par deux points IPv6.

Cette adresse doit être l'adresse IP du périphérique avec lequel le châssis communique.

- **fqdn fqdn** : Ce paramètre spécifie le nom de domaine complet (FQDN) homologue de diamètre sous la forme d'une chaîne alphanumérique de 1 à 127 caractères.

- **port port_number** : Ce paramètre spécifie le numéro de port pour ce homologue de diamètre. Le numéro de port doit être un entier compris entre 1 et 65 535.

- **connect-on-application-access** : Ce paramètre active l'homologue lors de l'accès initial à l'application.

- **send-dpr-before-disconnect** : Ce paramètre envoie le DPR (Disconnect-Peer-Request).

- **cause de déconnexion** : Ce paramètre met fin au DPR à l'homologue spécifié, avec la raison de déconnexion spécifiée. La cause de déconnexion doit être un entier compris entre zéro et deux, qui correspond à ces causes :

  0 âÂ â REDÉMARRAGE

  1 ââ â OCCUPÉ

  2 â - DO_NOT_WANT_TO_TALK_TO_YOU

- **rlf-template rlf_template_name** : Ce paramètre spécifie le modèle RLF à associer à cet homologue de diamètre. Le nom *rlf_template_name* doit être une chaîne alphanumérique comprise entre 1 et 127 caractères.

  Note: Une licence RLF est requise pour configurer un modèle RLF.

Protection contre la surcharge du réseau avec limitation du diamètre sur une interface Gx/Gy

Cette fonction protège les interfaces Gx et Gy en sortie. Il protège la fonction PCRF (Policy and Charging Rules Function) et le système de facturation en ligne (OCS) et utilise RLF.

Tenez compte de ces remarques importantes lorsque vous appliquez la configuration des points d'extrémité de diamètre :

- Un modèle RLF doit être associé à l'homologue.

- Un RLF est attaché uniquement par homologue (individuellement).

Cette commande est utilisée afin de configurer la protection de surcharge du réseau :

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

Note: Une licence RLF est requise pour configurer un modèle RLF

Configurer la limitation du diamètre sur une interface Gx/Gy

Vous pouvez envisager l'utilisation du RLF pour les interfaces de diamètre. Voici un exemple de configuration :

```
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
```

Voici quelques notes sur cette configuration :

- L'homologue appelé *peer1* est lié à *RFL2*, et les autres homologues sous le point de terminaison sont liés à *RLF1*.
- Le modèle RLF de niveau homologue a priorité sur le modèle de niveau terminal.
- Le nombre de messages est envoyé à un débit maximal de 1 000 par seconde.(msg-rate). Ces considérations s'appliquent également :

  Seule une centaine de messages (taille de rafale) sont envoyés toutes les cent millisecondes (afin d'atteindre les 1 000 messages par seconde).

  Si le nombre de messages dans la file d'attente RLF dépasse 80 % du taux de messages (80 % de 1 000 = 800), le RLF passe à l'état *OVER_THRESHOLD*.

  Si le nombre de messages dans la file d'attente RLF dépasse le taux de messages (1 000), le RLF passe à l'état *OVER_LIMIT*.

  Si le nombre de messages dans la file d'attente RLF diminue en dessous de 60 % du taux de messages (60 % de 1 000 = 600), le RLF repasse à l'état *READY*.

  Le nombre maximal de messages pouvant être mis en file d'attente est égal au débit de messages multiplié par la tolérance de délai (1 000 x 4 = 4 000).

Si l'application envoie plus de 4 000 messages au routeur RLF, les 4 000 premiers sont mis en file d'attente et les autres sont abandonnés.

Les messages abandonnés sont retentés/renvoyés par l'application au routeur désigné de sauvegarde dans un délai approprié.

Le nombre de tentatives est la responsabilité de l'application.

- Le modèle peut être indépendant du point de terminaison avec le paramètre *no rlf-template*. Par exemple, il délirait *RLF1* de *peer2*.

- N'utilisez pas le paramètre *no rlf-template rlf1* en mode *de configuration de point de terminaison*, car l'interface de ligne de commande tente de supprimer le modèle RLF *RLF1*. Cette commande CLI fait partie de la configuration globale et non de la configuration des points d'extrémité.

- Le modèle peut être lié à des homologues individuels via l'une des commandes suivantes :

```
no peer peer2 realm foo.com

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

- La valeur RLF ne peut être utilisée que pour les terminaux de diamètre dans lesquels le diamproxy est utilisé.

- Le taux de messages configuré est implémenté par proxy diamantifère. Par exemple, si le taux de messages est de 1 000 et que 12 diamproxies sont actives (châssis entièrement rempli = 12 cartes de services de paquets (PSC) actives + 1 Déux + 1 PSC de secours), les transmissions effectives par seconde (TPS) sont de 12 000. Vous pouvez entrer l'une de ces commandes afin d'afficher les statistiques de contexte RLF :

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Protection contre la surcharge du réseau via la limitation des pages avec RLF

La fonction de limitation de page limite le nombre de messages de pagination envoyés hors du SGSN. Il offre flexibilité et contrôle à l'opérateur, qui peut désormais réduire le nombre de messages de pagination envoyés depuis le SGSN en fonction des conditions du réseau. Dans certains endroits, la quantité de messages de pagination qui sont initiés à partir du SGSN est très élevée en raison de mauvaises conditions radio. Un nombre plus élevé de messages de pagination entraîne la consommation de bande passante sur le réseau. Cette fonctionnalité fournit une limite de débit configurable, dans laquelle le message de pagination est limité aux niveaux suivants :

- Niveau global pour l'accès 2G et 3G

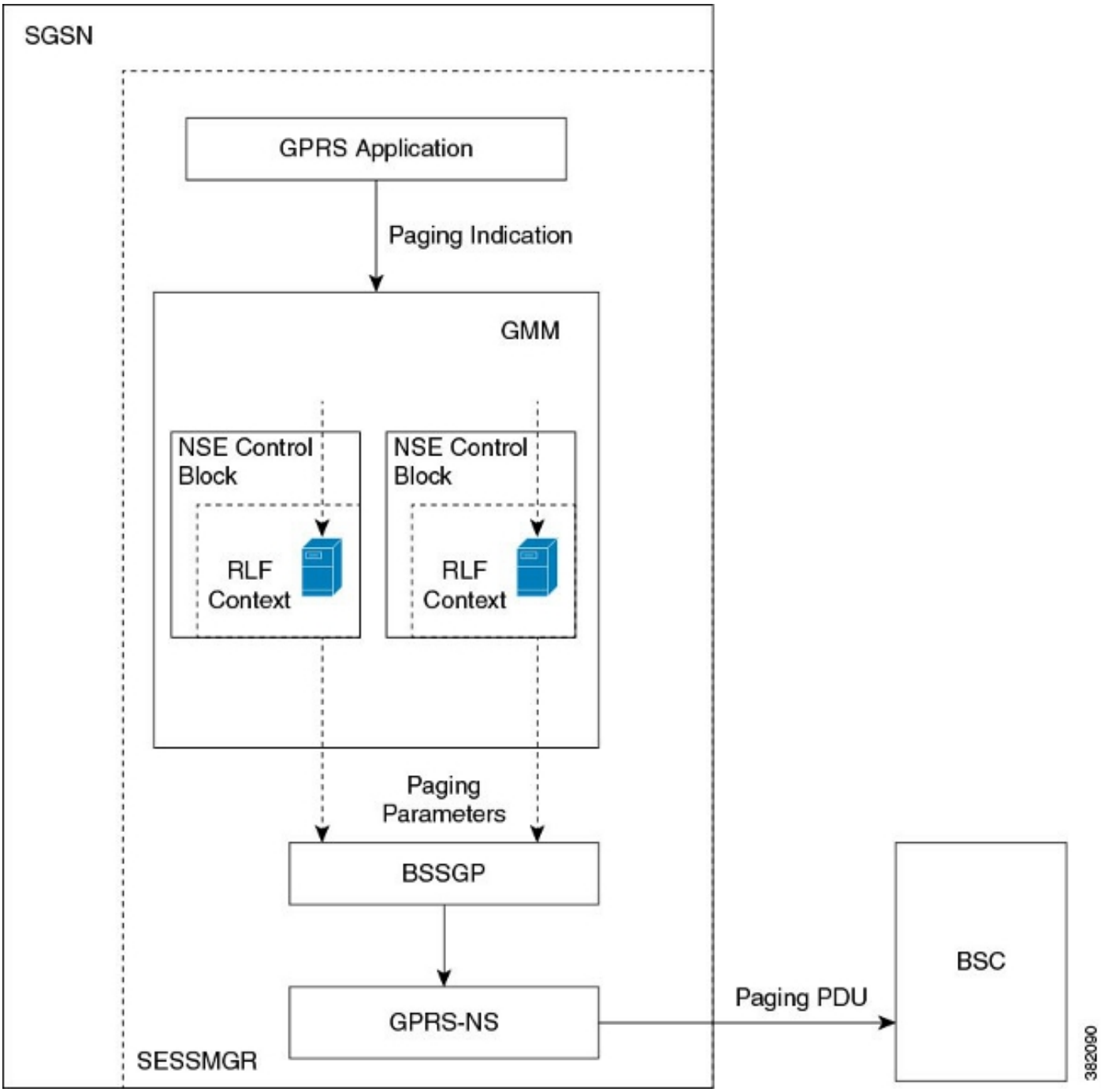
- Niveau NSE (Network Service Entity) pour accès 2G uniquement

- Niveau RNC (Radio Network Controller) pour accès 3G uniquement

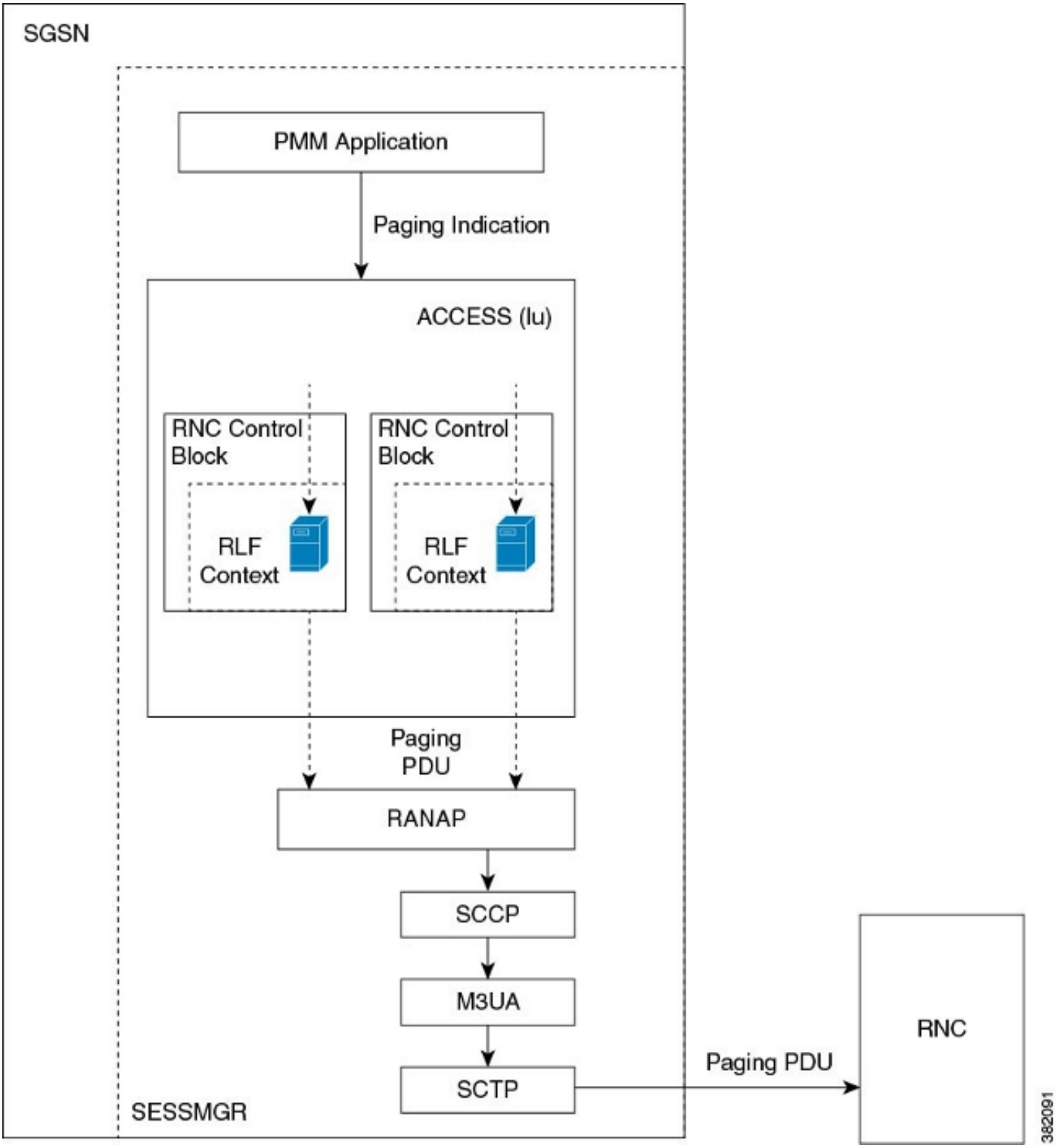
Cette fonctionnalité améliore la consommation de bande passante sur l'interface radio.

Note: Une licence RLF est requise pour configurer un modèle RLF.

Voici un exemple du processus de téléavertissement avec accès 2G et limitation de débit :



Voici un exemple du processus de téléavertissement avec accès 3G et limitation de débit :



Configurer la limitation de page avec RLF

Les commandes décrites dans cette section sont utilisées afin de configurer la fonction de limitation de page. Ces commandes CLI sont utilisées afin d'associer/supprimer le modèle RLF pour la limitation des pages au niveau global, au niveau NSE et au niveau RNC sur le SGSN.

Mapper le nom RNC à l'identificateur RNC

La commande **interface** est utilisée afin de configurer le mappage entre l'identificateur RNC (ID) et le nom RNC. Vous pouvez configurer le *paging-rlf-template* soit par nom RNC, soit par ID RNC. Voici la syntaxe utilisée :

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

Note: La forme *no* de la commande supprime le mappage et toute autre configuration associée à la configuration RNC *paging-rlf-template* du SGSN et réinitialise le comportement par défaut pour ce RNC.

Voici un exemple de configuration :

```
[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#
```

Associer un modèle RLF de pagination

Cette commande permet au SGSN d'associer un modèle RLF soit au niveau global, ce qui limite les messages de pagination qui sont initiés à la fois sur l'accès 2G (niveau NSE) et 3G (niveau RNC), soit au niveau par entité, soit au niveau RNC pour l'accès 3G, soit au niveau NSE pour l'accès 2G. Voici la syntaxe utilisée :

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

Note: Si aucun modèle RLF n'est associé à un NSE/RNC particulier, la charge de pagination est limitée en fonction du modèle RLF global associé (le cas échéant). Si aucun modèle RLF global n'est associé, aucune limite de débit n'est appliquée à la charge de pagination.

Voici un exemple de configuration :

```
[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#
```