

在ASR5x00系列上为网关和相邻网络元素实施过载保护

目录

[简介](#)

[GW的拥塞控制](#)

[入口GTP-C消息限制的网络过载保护](#)

[配置入口GTP-C消息限制](#)

[邻居网元保护](#)

[在S6a接口上通过直径限制实现网络过载保护](#)

[在S6a接口上配置直径限制](#)

[在Gx/Gy接口上通过直径限制实现网络过载保护](#)

[在Gx/Gy接口上配置直径限制](#)

[使用RLF通过页面限制实现网络过载保护](#)

[使用RLF配置页面限制](#)

简介

本文档介绍如何在思科聚合服务路由器(ASR)5x00系列上实施网关(GW)和相邻网络元素可用的保护功能，以保护整体网络性能。

GW的拥塞控制

拥塞控制是一种通用的自保护功能。它用于保护系统免受这些资源的利用率激增的影响：

- 处理卡上的CPU使用率
- 处理卡上的内存使用

当利用率超过预定义的阈值时，所有新呼叫(分组数据协议(PDP)激活、分组数据网络(PDN)会话激活)将根据配置被丢弃或拒绝。

以下示例展示如何监控整体数据处理卡(DPC)利用率：

```
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

注意：系统工程限制是CPU利用率的80%，这被定义为不应超出的建议工程限制，以保证系统的正常运行。超出价值的负载可能会影响平台的操作，例如其稳定性和可预测性，应通过适当的容量规划来避免。

注意：Cisco建议您使用丢弃操作，而不是拒绝操作，因为拒绝的呼叫会导致用户设备(UE)立即重复重新连接尝试。在发生丢弃操作时，UE会等待几秒钟，然后再重复尝试重新连接，因此呼叫率会降低。

入口GTP-C消息限制的网络过载保护

此功能可保护数据包GW(P-GW)/网关GPRS支持节点(GGSN)进程免受传输浪涌和网元故障的影响。在P-GW/服务GPRS支持节点(SGSN)中，主要瓶颈与用户数据处理有关，例如会话管理器利用率以及整体DPC CPU和内存利用率。

在SGSN/移动管理实体(MME)上配置“否”值，以在激活网络过载保护时限制入站GPRS隧道协议控制(GTP-C)消息。

注意：使用GTP和直径接口限制需要安装有效的许可证密钥。

此功能有助于控制P-GW/GGSN上入站/出站消息的速率，这有助于确保P-GW/GGSN不会被GTP控制计划消息压垮。此外，它有助于确保P-GW/GGSN不会使用GTP控制平面消息压垮GTP-C对等体。此功能要求GTP(版本1(v1)和版本2(v2))控制消息通过Gn/Gp和S5/S8接口整形/管制。此功能包括P-GW/GGSN节点及其通信的其他外部节点的过载保护。限制仅对会话级控制消息执行，因此路径管理消息的速率完全不受限制。

外部节点过载可以在P-GW/GGSN以比其他节点可以处理的更高速率生成信令请求的场景中发生。此外，如果P-GW/GGSN节点的入站速率较高，则可能泛洪外部节点。因此，需要限制入站和出站控制消息。为了保护外部节点免受由于P-GW/GGSN控制信令而引起的过载，使用框架以形成和管制到外部接口的出站控制消息。

配置入口GTP-C消息限制

输入以下命令以配置入口GTP-C消息限制：

```
gtpc overload-protection Ingress
```

这通过在Gn/Gp(GTPv1)或S5/S8(GTPv2)接口上使用在情景中配置并应用于GGSN和PGW的服务的其他参数限制入站GTPv1和GTPv2控制消息来配置GGSN/PGW的过载保护。

输入上一命令时，将生成以下提示：

```
[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
```

以下是有关此语法的一些说明：

- **否**：此参数在此情景中禁用GGSN/PGW服务的GTP入站控制消息限制。
- **msg-rate msg_rate**:此参数定义每秒可处理的GTP入站消息数。*msg_rate*是一个介于100到12,000之间的整数。
- **延迟容差持续时间**:此参数定义入站GTP消息在处理前可以排队的最大秒数。超过此容差后，消息将被丢弃。*dur*是一个介于1到10之间的整数。
- **队列大小**:此参数定义入站GTP-C消息的最大队列大小。如果队列超过定义的大小，则丢弃任何新的入站消息。大小是介于100到10,000之间的整数。

您可以使用此命令为在同一情景中配置的GGSN/PGW服务启用GTP入站控制消息限制。例如，此命令在消息速率为1,000/秒、消息队列大小为10,000、延迟为1秒的情景中启用入站GTP控制消息：

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

邻居网元保护

许多邻居网络元素使用自己的机制来保护自己，而ASR5x00端可能不需要额外的网络过载保护。在只有在出口端应用消息限制时才能达到整体网络稳定性的情况下，可能需要保护邻居网络元素。

在S6a接口上通过直径限制实现网络过载保护

此功能可保护S6a和S13接口在出口方向。它可保护家庭用户服务器(HSS)、Diameter路由代理(DRA)和设备身份注册(EIR)。该功能使用速率限制功能(RLF)。

在应用直径终端配置时，请考虑以下重要注意事项：

- RLF模板必须与对等体关联。
- RLF仅按对等体（单独）连接。

在S6a接口上配置直径限制

以下是用于在S6a接口上配置直径限制的命令语法：

```
[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 ]
```

以下是有关此语法的一些说明：

- **否**：此参数删除指定的对等配置。
- **[*] peer_name [*]**:此参数将对等体名称指定为一个字母数字字符串，范围为1到63个字符（允许

标点字符)。注意：现在，直径服务器终端可以是通配符的通配符对等体名称（*字符作为有效通配符）。满足通配符模式的客户端对等体被视为有效对等体，并接受连接。通配符表示对等体名称为通配符，而字符串中前面的任何*字符都被视为通配符。

- **realm realm_name**:此参数将此对等体的领域指定为一个字母数字字符串，范围为1到127个字符。领域名称可以是公司或服务名称。
- **地址ipv4/ipv6_address**:此参数以IPv4点分十进制或IPv6冒号分隔的十六进制记法指定直径对等体IP地址。此地址必须是机箱与之通信的设备的IP地址。
- **fqdn fqdn**:此参数将直径对等体完全限定域名(FQDN)指定为一个字母数字字符串，范围为1到127个字符。
- **port port_number**:此参数指定此直径对等体的端口号。端口号必须是一个介于1和65,535之间的整数。
- **连接应用访问**:此参数在初始应用访问时激活对等体。
- **send-dpr-before-disconnect**:此参数发送Disconnect-Peer-Request(DPR)。
- **disconnect-cause**:此参数将DPR结束到指定的对等体，具有指定的断开原因。断开原因必须是介于0和2之间的整数，其对应于以下原因：

0 重启

1 占线

2 DO_NOT_WANT_TO_TALK_TO_YOU

- **rlf-template rlf_template_name**:此参数指定要与此直径对等体关联的RLF模板。
*rlf_template_name*必须是一个字母数字字符串，范围为1到127个字符。

注意：配置RLF模板需要RLF许可证。

在Gx/Gy接口上通过直径限制实现网络过载保护

此功能可保护Gx和Gy接口在出口方向。它保护策略和计费规则功能(PCRF)和在线计费系统(OCS)，并使用RLF。

在应用直径终端配置时，请考虑以下重要注意事项：

- RLF模板必须与对等体关联。
- RLF仅按对等体（单独）连接。

此命令用于配置网络过载保护：

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

注意：配置RLF模板需要RLF许可证

在Gx/Gy接口上配置直径限制

您可以考虑将RLF用于直径接口。以下是配置示例：

```
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
```

以下是有关此配置的一些说明：

- 名为peer1的对等体绑定到RFL2，终端下的其余对等体绑定到RLF1。
- 对等级RLF模板优先于终端级模板。
- 以每秒1,000的最大速率发送邮件数。(msg-rate)。这些注意事项也适用：

每100毫秒只发送100条消息（突发大小）（以便每秒传输1,000条消息）。

如果RLF队列中的消息数超过消息速率的80%（1,000 = 800的80%），则RLF将转换到OVER_THRESHOLD状态。

如果RLF队列中的消息数超过消息速率(1,000)，则RLF将转换到OVER_LIMIT状态。

如果RLF队列中的消息数减少到消息速率的60%以下（1,000 = 600的60%），则RLF将转换回“就绪”状态。

可排队的最大消息数等于消息速率乘以延迟容限(1,000 x 4 = 4,000)。

如果应用程序向RLF发送超过4,000条消息，则前4,000条将排入队列，其余将被丢弃。

应用会在适当的时间内重试/重新发送被丢弃的消息到RLF。

重试次数是应用程序的责任。

- 可以使用no rlf-template参数从终端解除模板。例如，它会从peer2解除RLF 1绑定。
- 请勿在终端配置模式下使用no rlf-template rlf1参数，因为CLI尝试删除RLF模板RLF1。此CLI命令是全局配置的一部分，而不是终端配置的一部分。
- 模板可以通过以下命令之一绑定到各个对等体：

```
no peer peer2 realm foo.com
```

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

- RLF只能用于使用diamproxy的直径端点。
- 配置的消息速率按DiamProxy实现。例如，如果消息速率为1,000，而12个双面代理处于活动状态(完全填充的机箱= 12个主用数据包服务卡(PSC)+ 1个解复用器+ 1个备用PSC)，则有效每秒传输(TPS)为12,000。您可以输入以下命令之一以查看RLF情景统计信息：

```
show rlf-context-statistics diamproxy
```

```
show rlf-context-statistics diamproxy verbose
```

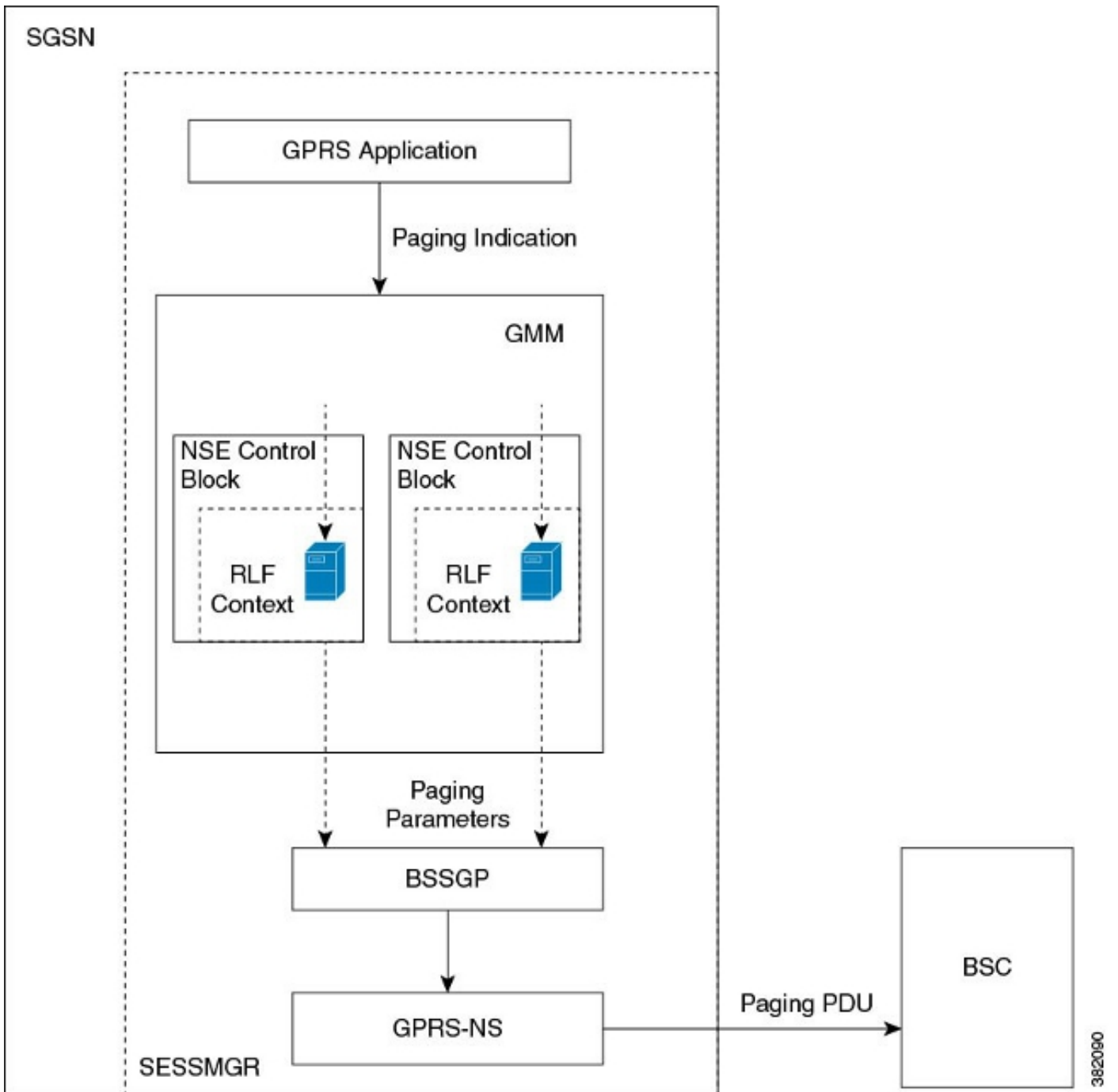
使用RLF通过页面限制实现网络过载保护

页面限制功能限制从SGSN发送的寻呼消息数。它为运营商提供灵活性和控制，运营商现在可以根据网络条件减少从SGSN发送的寻呼消息数。在某些位置，由于无线电条件不良，从SGSN发起的寻呼消息量非常大。寻呼消息数量越多，网络带宽消耗就越大。此功能提供可配置的速率限制，在此限制中，寻呼消息在以下级别被限制：

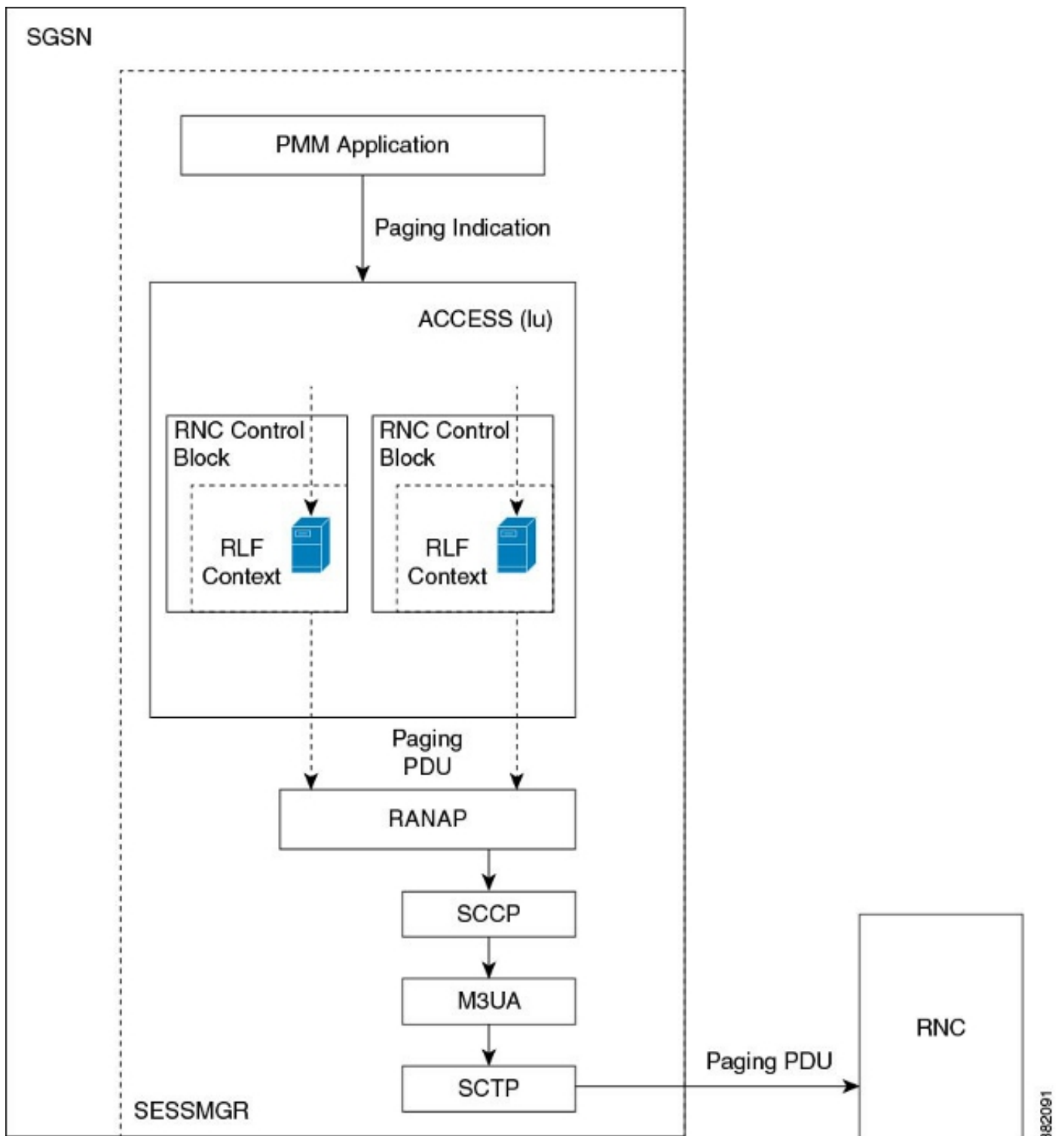
- 2G和3G接入的全球级别
 - 仅用于2G访问的网络服务实体(NSE)级别
 - 无线网络控制器(RNC)级别，仅用于3G接入
- 此功能可提高无线电接口的带宽消耗。

注意：配置RLF模板需要RLF许可证。

以下是具有2G访问和速率限制的寻呼过程的示例：



以下是具有3G访问和速率限制的寻呼过程的示例：



使用RLF配置页面限制

本节介绍的命令用于配置页面限制功能。这些CLI命令用于关联/删除SGSN上全局级、NSE级和RNC级的页限制的RLF模板。

将RNC名称映射到RNC标识符

使用interface命令可配置RNC标识符(ID)和RNC名称之间的映射。您可以按RNC名称或RNC ID配置寻呼 — rlf-template。以下是使用的语法：

```
config
```



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

注意：该命令的`no`形式从SGSN中删除与RNC分页 — `rlf-template`配置关联的映射和其他配置，并将该RNC的行为重置为默认值。

以下是配置示例：

```
[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#
```

关联寻呼RLF模板

此命令允许SGSN在全局级别(限制2G (NSE级) 和3G (RNC级) 访问中发起的寻呼消息)或在每个实体级别 (在3G访问的RNC级别或在2G访问的NSE级别) 关联RLF模板。以下是使用的语法：

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

注意：如果没有与特定NSE/RNC关联的RLF模板，则寻呼负载会基于关联的全局RLF模板 (如果存在) 进行限制。如果未关联全局RLF模板，则不对分页负载应用速率限制。

以下是配置示例：

```
[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#
```