對ASR5x00系列上的網關和相鄰網路元素實施過載保護

目錄

簡介

本檔案介紹如何在思科聚合服務路由器(ASR)5x00系列上實作閘道(GW)和相鄰網路元素可用的保護功能，以保護整體網路效能。

GW的擁塞控制

擁塞控制是一種通用的自我保護功能。它用於保護系統不受這些資源使用激增的影響：

- 處理卡上的CPU使用率
- 處理卡上的記憶體使用情況

當使用率超過預定義閾值時，所有新呼叫(資料包資料協定(PDP)啟用、資料包資料網路(PDN)會話啟用)都會被丟棄或*拒絕*，具體取決於配置。

以下範例顯示如何監控整體資料處理卡(DPC)的利用率：

```
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
```

附註：系統工程限制是CPU利用率的80%，定義為建議不要超過的工程限制，以便保證系統的正常運行。超出此值的負載可能會影響平台的操作，例如其穩定性和可預測性，在進行適當的容量規劃時應避免這種情況。

附註：思科建議您使用*drop*操作而不是*reject*操作，因為被拒絕的呼叫會導致使用者裝置(UE)立即重複嘗試重新連線。 在丟棄操作的情況下，UE在重複進行重新連線嘗試之前等待幾秒鐘，因此降低了呼叫速率。

適用於輸入GTP-C訊息限制的網路過載保護

此功能可保護封包GW(P-GW)/閘道器GPRS支援節點(GGSN)流程免受傳輸浪湧和網路元素故障的影響。在P-GW/Serving GPRS Support Node(SGSN)中，主要瓶頸與使用者資料處理有關，如會話管理器利用率以及總體DPC CPU和記憶體利用率。

在SGSN/行動管理實體(MME)上配置*No*值，以便在啟用網路過載保護時限制傳入GPRS通道通訊協定控制(GTP-C)訊息。

附註：使用GTP和diameter介面限制需要安裝有效的許可證金鑰。

此功能有助於控制P-GW/GGSN上的入站/出站消息速率，這有助於確保P-GW/GGSN不會被GTP控制計畫消息所淹沒。此外，它有助於確保P-GW/GGSN不會使GTP-C對等體與GTP控制平面消息相重疊。此功能需要在Gn/Gp和S5/S8介面上整形/監管GTP(版本1(v1)和版本2(v2))控制消息。此功能涵蓋P-GW/GGSN節點及其通訊的其他外部節點的過載保護。限制僅針對會話級控制消息完成，因此路徑管理消息根本不受速率限制。

在P-GW/GGSN以比其他節點能夠處理的更高的速率生成信令請求的情形中，可能發生外部節點過載。此外，如果P-GW/GGSN節點的入站速率很高，則可能會泛洪到外部節點。因此，需要限制入站和出站控制消息。為了保護外部節點免受由於P-GW/GGSN控制信令引起的過載，使用框架來形成和管制到外部介面的出站控制消息。

配置輸入GTP-C消息限制

輸入以下命令可設定輸入GTP-C訊息限制：

```
gtpc overload-protection Ingress
```

這會使用在上下文中配置並應用於GGSN和PGW的服務的其他引數，在Gn/Gp(GTPv1)或S5/S8(GTPv2)介面上限制入站GTPv1和GTPv2控制消息，從而配置GGSN/PGW的過載保護。

輸入先前命令時，系統會產生以下提示：

```
[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
```

以下是關於此語法的一些註解：

- **否:**此引數禁用此上下文中GGSN/PGW服務的GTP入站控制消息限制。
- **msg-rate msg_rate**:此引數定義每秒可處理的GTP入站消息數。*msg_rate*是一個介於100和12,000之間的整數。
- **delay-tolerance dur**:此引數定義入站GTP消息在處理之前可以排隊的最大秒數。超出此容差後，郵件將被丟棄。*dur*是一個介於1到10之間的整數。
- **queue-size size**:此引數定義入站GTP-C消息的最大隊列大小。如果隊列超過定義的大小，則會丟棄所有新的入站消息。*size*是一個介於100和10,000之間的整數。

您可以使用此命令為同一上下文中配置的GGSN/PGW服務啟用GTP入站控制消息限制。例如，此命令在消息速率*為1,000*每秒、消息隊列大小*為10,000*和延遲為1秒的上下文中啟用入站GTP控制消息:

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

鄰居網路元素保護

許多鄰居網路元素使用自己的機制來保護自己，可能不需要在ASR5x00端進行額外的網路過載保護。如果僅在出口端應用消息限制時才能達到整體網路穩定性，則可能需要保護鄰居網路元素。

在S6a介面上使用直徑限制的網路過載保護

此功能可保護出口方向的S6a和S13介面。它保護歸屬使用者伺服器(HSS)、Diameter路由代理(DRA)和裝置身份暫存器(EIR)。 此功能使用速率限制函式(RLF)。

在應用diameter端點配置時，請考慮以下重要說明：

- RLF模板必須與對等體關聯。
- RLF僅以每個對等體為基礎（單獨連線）。

在S6a介面上配置直徑限制

以下是在S6a介面上設定diameter throttling所使用的命令語法：

```
[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 ]
```

以下是關於此語法的一些註解：

- **否:**此引數刪除指定的對等配置。

- **[*] peer_name [*]**:此引數將對等體名稱指定為範圍從1到63個字元的字母數字字串（允許使用標點字元）。**附註**：現在，直徑伺服器端點可以是一個萬用字元名稱（使用*字元作為有效的萬用字元）。 滿足通配模式的客戶端對等體被視為有效對等體，連線被接受。萬用字元表示對等體名稱是萬用字元，前面字串中的任何*字元都被視為萬用字元。
- **領域領域名稱**:此引數將此對等體的領域指定為範圍從1到127個字元的字母數字字串。領域名稱可以是公司名稱或服務名稱。

- **地址ipv4/ipv6_address**:此引數指定IPv4點分十進位制或IPv6冒號分隔十六進位制記法中的直徑對等IP地址。此地址必須是機箱與之通訊的裝置的IP地址。

- **fqdn fqdn**:此引數將直徑對等體完全限定域名(FQDN)指定為範圍從1到127個字元的字母數字字串。

- **port port_number**:此引數指定此直徑對等體的埠號。埠號必須是一個介於1和65,535之間的整數。

- **連線應用訪問**:此引數在初始應用程式訪問時啟用對等體。

- **send-dpr-before-disconnect**:此引數傳送Disconnect-Peer-Request(DPR)。

- **disconnect-cause**:此引數以指定的斷開原因將DPR終止到指定的對等體。斷開原因必須是從0到2的整數，對應於以下原因：

  0 ââ重新â啟動

  1âââ忙

  2 ââ âDO_NOT_WANT_TO_TALK_TO_YOU

- **rlf-template rlf_template_name**:此引數指定要與此直徑對等體關聯的RLF模板。*rlf_template_name*必須是範圍從1到127個字元的字母數字字串。

  附註：配置RLF模板需要RLF許可證。

在Gx/Gy介面上使用直徑限制的網路過載保護

此功能可保護出口方向的Gx和Gy介面。它保護策略和計費規則功能(PCRF)和線上計費系統(OCS)並使用RLF。

在應用diameter端點配置時，請考慮以下重要說明：

- RLF模板必須與對等體關聯。

- RLF僅以每個對等體為基礎（單獨連線）。

以下命令是用來設定網路過載保護：

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

附註：配置RLF模板需要RLF許可證

在Gx/Gy介面上配置直徑限制

可以考慮將RLF用於直徑介面。以下是組態範例：

```
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
```

以下是有關此組態的一些說明：

- 稱為peer1*的對等*體繫結到*RFL2*，而端點下的其餘對等體繫結到*RLF1*。
- 對等級RLF模板優先於終端級模板。
- 傳送消息的數量的最大速率為每秒1,000。(msg-rate)。 這些注意事項也適用：

  每100毫秒僅傳送一百條消息（突發大小）（以便達到每秒1,000條消息）。

  如果RLF隊列中的消息數超過消息速率的80%（1,000 = 800的80%），則RLF將轉換為*OVER_THRESHOLD狀*態。

  如果RLF隊列中的消息數超過消息速率(1,000)，則RLF將轉換為*OVER_LIMIT狀*態。

  如果RLF隊列中的消息數減少到消息速率的60%以下（1,000 = 600的60%），則RLF將轉換回*READY*狀態。

  可排隊的最大消息數等於消息速率乘以延遲容限(1,000 x 4 = 4,000)。

  如果應用程式向RLF傳送超過4,000條消息，則前4,000條消息將排隊，其餘消息將被丟棄。

丟棄的消息會在適當的時間內由應用程式重試/重新傳送到RLF。

重試次數由應用程式負責。

- 使用*no rlf-*template引數可從終結點*取消繫結模*板。例如，它會將*RLF1* 與*peer2*解除繫結。
- 請勿在*端點配置*模式下使用*no rlf-template rlf1*引數，因為CLI嘗試刪除RLF模板*RLF1*。此CLI命令是全域性配置的一部分，而不是端點配置。
- 可通過以下命令之一將模板繫結到各個對等體：

```
no peer peer2 realm foo.com

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

- RLF只能用於使用菱形代理的直徑端點。
- 配置的消息速率按數字代理實現。例如，如果消息速率是1,000，而12個diamproxies處於活動狀態(完全填充的機箱= 12個活動的資料包服務卡(PSC)+ 1個解複用器+ 1個待機PSC)，則每秒有效傳輸數(TPS)為12,000。您可以輸入以下命令之一來檢視RLF上下文統計資訊：

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

使用RLF通過頁面限制實現網路過載保護

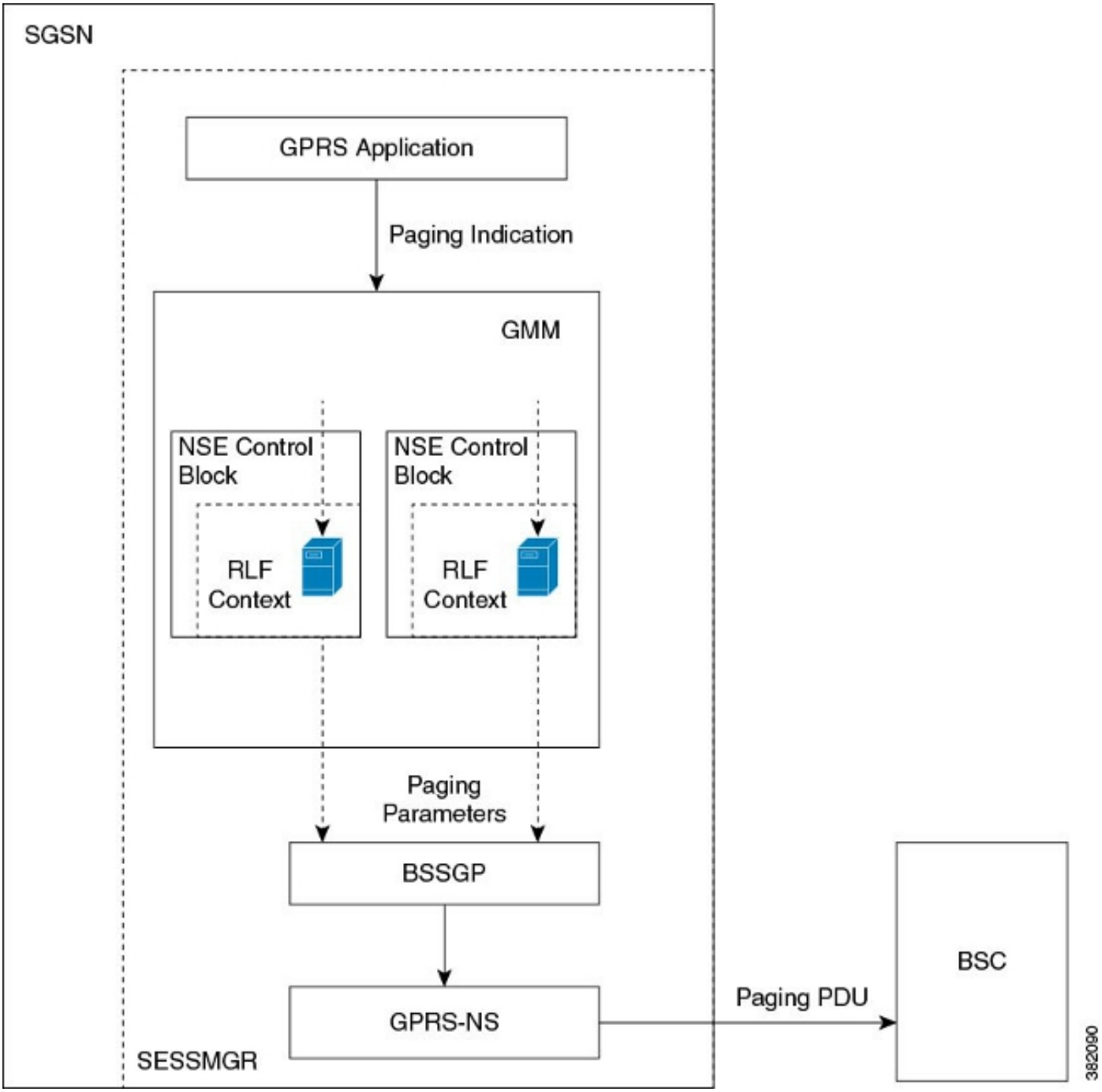
頁面限制功能限制從SGSN發出的尋呼消息的數量。它為運營商提供靈活性和控制，運營商現在可以根據網路條件減少從SGSN發出的尋呼消息的數量。在某些位置，由於無線電條件不良，從SGSN發起的尋呼消息量非常大。尋呼消息數量較多導致網路中頻寬的消耗。此功能提供可設定的速率限制，其中分頁消息限制在以下級別：

- 2G和3G接入的全球級別
- 僅適用於2G接入的網路服務實體(NSE)級別
- 僅適用於3G訪問的無線網路控制器(RNC)級別

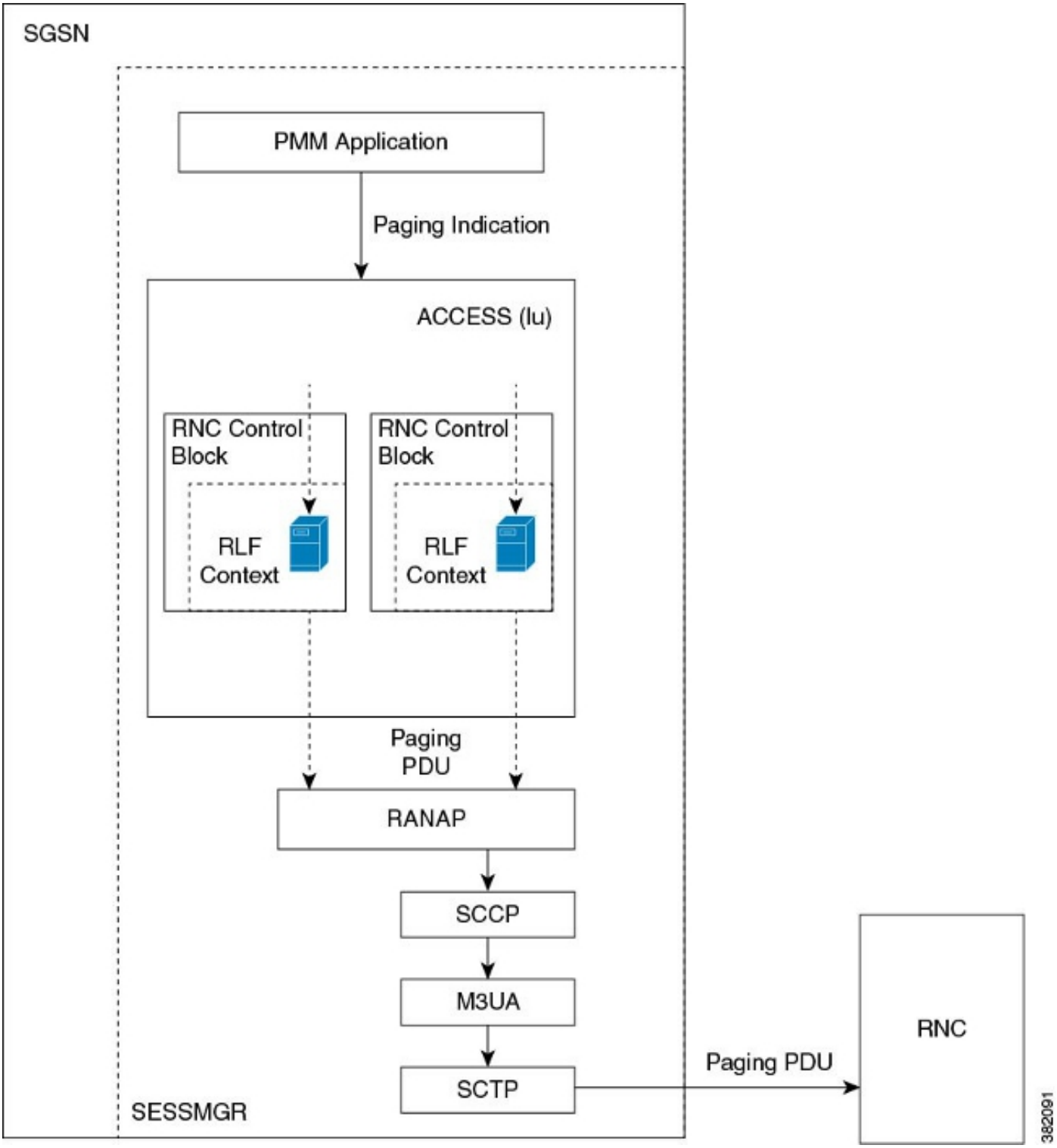
此功能可改善無線電介面上的頻寬消耗。

附註：配置RLF模板需要RLF許可證。

以下是具有2G存取和速率限制的尋呼過程的範例：



以下是具有3G存取和速率限制的尋呼過程的範例：



使用RLF配置頁面限制

本節所述的命令用於設定頁面限制功能。這些CLI命令用於在SGSN上的全域性級別、NSE級別和RNC級別關聯/刪除RLF模板以進行頁面限制。

將RNC名稱對映到RNC識別符號

interface命令用於配置RNC識別符號(ID)和RNC名稱之間的對映。您可以通過RNC名稱或RNC ID配置*paging-rlf-template*。以下是使用的語法：

```
config
```

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

附註：此命令的*no*形式從SGSN中刪除與RNC *paging-rlf-template*配置關聯的對映和其他配置，並將該RNC的行為重置為預設值。

以下是組態範例：

```
[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#
```

關聯尋呼RLF模板

此命令允許SGSN在全域性級別(該級別限制在2G（NSE級別）和3G（RNC級別）訪問中啟動的尋呼消息)或在每個實體級別（在3G訪問的RNC級別或在2G訪問的NSE級別）關聯RLF模板。以下是使用的語法：

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

附註：如果沒有與特定NSE/RNC關聯的RLF模板，則基於關聯的全域性RLF模板（如果存在）限制尋呼負載。 如果沒有關聯全域性RLF模板，則分頁負載不會應用速率限制。

以下是組態範例：

```
[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#
```