Implement Overload Protection for Gateways and Neighboring Network Elements on the ASR5x00 Series

Document ID: 119196

Contributed by Krishna Kishore DV, Cisco TAC Engineer, and Albert
Zagrobskiy, Cisco Advanced Services.
Jul 24, 2015

Contents

Introduction

This document describes how to implement the protection features that are available for Gateways (GWs) and neighboring network elements on the Cisco Aggregated Services Router (ASR) 5x00 Series in order to protect the overall network performance.

Congestion Control for GWs

Congestion Control is a generic self−protection feature. It is used in order to protect the system against utilization surges of these resources:

- CPU usage on processing cards
- Memory usage on processing cards

When the utilization exceeds the pre−defined thresholds, all of the new calls (Packet Data Protocol (PDP) activations, Packet Data Network (PDN) session activations) are *dropped* or *rejected*, dependent upon the configuration.

Here is an example that shows how to monitor the overall Data Processing Card (DPC) utilization:

```
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: The system engineering limit is 80% of the CPU utilization, which is defined as the recommended engineering limit that should not be exceeded in order to guarantee regular operation of the system. Load beyond the value might impact operations of the platform, such as its stability and predictability, and should be avoided with proper capacity planning.

Note: Cisco recommends that you use the *drop* action rather than the *reject* action, as the rejected calls cause immediate repeated re−connection attempts from the User Equipment (UE). In the case of a drop action, the UE waits a few seconds before it makes repeated re−connection attempts, so the call rate is decreased.

Network Overload Protection for Ingress GTP−C Message Throttling

This feature protects the Packet GW (P−GW)/Gateway GPRS Supporting Node (GGSN) processes from transmission surges and network element failures. In a P−GW/Serving GPRS Supporting Node (SGSN), the main bottleneck is related to the user data processing, such as the session manager utilization and the overall DPC CPU and memory utilization.

A *No value* is configured on the SGSN/Mobility Management Entity (MME) in order to throttle the inbound GPRS Tunnelling Protocol−Control (GTP−C) messages when the network overload protection is activated.

Note: The use of GTP and diameter interface throttling requires that a valid license key be installed.

This feature helps control the rate of inbound/outbound messages on the P−GW/GGSN, which helps to ensure that the P−GW/GGSN is not overwhelmed by the GTP control plan messages. In addition, it helps to ensure that the P−GW/GGSN does not overwhelm the GTP−C peer with the GTP control plane messages. This feature requires that the GTP (Version 1 (v1) and Version 2 (v2)) control messages be shaped/policed over the Gn/Gp and S5/S8 interfaces. This feature covers the overload protection of the P−GW/GGSN nodes and the other external nodes with which it communicates. Throttling is done only for session−level control messages, so the path management messages are not rate limited at all.

The external node overload can occur in a scenario where the P−GW/GGSN generates signaling requests at a higher rate than the other nodes can handle. Also, if the inbound rate is high at the P−GW/GGSN node, it might flood the external node. For this reason, the throttling of both inbound and outbound control messages is required. For protection of the external nodes from an overload due to the P−GW/GGSN control signaling, a framework is used in order to shape and police the outbound control messages to the external interfaces.

Configure Ingress GTP−C Message Throttling

Enter this command in order to configure the ingress GTP−C message throttling:

```
gtpc overload−protection Ingress
```

This configures the overload protection of the GGSN/PGW by throttling inbound GTPv1 and GTPv2 control messages over the Gn/Gp (GTPv1) or S5/S8 (GTPv2) interface with the other parameters for the services that are configured in a context and applied to the GGSN and PGW.

When you enter the previous command, this prompt is generated:

```
[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
```

Here are some notes about this syntax:

- ***no***: This parameter disables the GTP inbound control message throttling for the GGSN/PGW services in this context.
- ***msg−rate msg_rate***: This parameter defines the number of GTP inbound messages that can be processed per second. The *msg_rate* is an integer that ranges from one hundred to 12,000.
- ***delay−tolerance dur***: This parameter defines the maximum number of seconds that an inbound GTP message can be queued before it is processed. After this tolerance is exceeded, the message is dropped. The *dur* is an integer that ranges from one to ten.
- ***queue−size size***: This parameter defines the maximum queue size for the inbound GTP−C messages. If the queue exceeds the defined size, then any new inbound messages are dropped. The *size* is an integer that ranges from one hundred to 10,000.

You can use this command in order to enable the GTP inbound control message throttling for the GGSN/PGW services that are configured in the same context. As an example, this command enables the inbound GTP control messages in a context with a message rate of *1,000* per second, a message queue size of *10,000*, and a delay of *one* second:

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

Neighbor Network Element Protection

Many neighbor network elements use their own mechanisms in order to protect themselves, and additional network overload protection on the ASR5x00 side might not be needed. Protection of the neighbor network elements might be required in cases where the overall network stability can be reached only when message throttling is applied on the egress side.

Network Overload Protection with Diameter Throttling on an S6a Interface

This feature protects the S6a and S13 interfaces in the egress direction. It protects the Home Subscriber Server (HSS), the Diameter Routing Agent (DRA), and the Equipment Identity Register (EIR). The feature uses the Rate Limiting Function (RLF).

Consider these important notes when you apply the diameter endpoint configuration:

- An RLF template must be associated with the peer.
- An RLF is attached only on a per−peer basis (individually).

Configure Diameter Throttling on an S6a Interface

Here is the command syntax that is used in order to configure diameter throttling on an S6a interface:

```
[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 ]
```

Here are some notes about this syntax:

- ***no***: This parameter removes the specified peer configuration.
- ***[*] peer_name [*]***: This parameter specifies the peer name as an alphanumeric string that ranges from one to 63 characters (punctuation characters are allowed).

  Note: The diameter server endpoint can now be a wild−carded peer name (with the * character as a valid wildcard character). The client peers that satisfy the wild−carded pattern are treated as valid peers, and the connection is accepted. The wild−carded token indicates that the peer name is wild−carded, and any * character in the string that precedes is treated as a wildcard.
- ***realm realm_name***: This parameter specifies the realm of this peer as an alphanumeric string that ranges from one to 127 characters. The realm name can be a company or service name.
- ***address ipv4/ipv6_address***: This parameter specifies the diameter peer IP address in IPv4 dotted−decimal, or IPv6 colon−separated−hexadecimal notation. This address must be the IP address of the device with which the chassis communicates.
- ***fqdn fqdn***: This parameter specifies the diameter peer Fully Qualified Domain Name (FQDN) as an alphanumeric string that ranges from one to 127 characters.
- ***port port_number***: This parameter specifies the port number for this diameter peer. The port number must be an integer that ranges from one to 65,535.
- ***connect−on−application−access***: This parameter activates the peer upon initial application access.
- ***send−dpr−before−disconnect***: This parameter sends the Disconnect−Peer−Request (DPR).
- ***disconnect−cause***: This parameter ends the DPR to the specified peer, with the specified disconnect reason. The disconnect cause must be an integer that ranges from zero to two, which correspond to these causes:
  - ***0*** REBOOTING
  - ***1*** BUSY
  - ***2*** DO_NOT_WANT_TO_TALK_TO_YOU
- ***rlf−template rlf_template_name***: This parameter specifies the RLF template to be associated with this diameter peer. The *rlf_template_name* must be an alphanumeric string that ranges from one to 127 characters.

Note: An RLF license is required in order to configure an RLF template.

Network Overload Protection with Diameter Throttling on a Gx/Gy Interface

This feature protects the Gx and Gy interfaces in the egress direction. It protects the Policy and Charging Rules Function (PCRF) and the Online Charging System (OCS) and uses RLF.

Consider these important notes when you apply the diameter endpoint configuration:

- An RLF template must be associated with the peer.
- An RLF is attached only on a per−peer basis (individually).

This command is used in order to configure the network overload protection:

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

Note: An RLF license is required in order to configure an RLF Template

Configure Diameter Throttling on a Gx/Gy Interface

You might consider the use of the RLF for diameter interfaces. Here is an example 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
```

Here are some notes about this configuration:

- The peer called *peer1* is bound to *RFL2*, and the rest of the peers under the endpoint are bound to *RLF1*.
- The peer−level RLF template takes precedence over the endpoint−level template.
- The number of messages are sent out at a maximum rate of 1,000 per second.(msg−rate). These considerations also apply:
  - Only one hundred messages (burst−size) are sent out every one hundred milliseconds (in order to reach the 1,000 messages per second).
  - If the number of messages in the RLF queue exceeds 80% of the message rate (80% of 1,000 = 800), the RLF transitions to the *OVER_THRESHOLD* state.
  - If the number of messages in the RLF queue exceeds the message rate (1,000), the RLF transitions to the *OVER_LIMIT* state.

    - If the number of messages in the RLF queue decreases below 60% of the message rate (60% of 1,000 = 600), the RLF transitions back to the *READY* state.
    - The maximum number of messages that can be queued equals the message rate multiplied by the delay tolerance (1,000 x 4 = 4,000).
    - If the application sends more than 4,000 messages to the RLF, the first 4,000 are queued and the rest are dropped.
    - The messages that are dropped are retried/re−sent by the application to the RLF in an appropriate amount of time.
    - The number of retries is the responsibility of the application.
- The template can be unbound from the endpoint with the *no rlf−template* parameter. For example, it would unbind *RLF1* from *peer2*.
- Do not use the *no rlf−template rlf1* parameter in *endpoint configuration* mode, as the CLI attempts to delete the RLF template *RLF1*. This CLI command is a part of the global configuration, not the endpoint configuration.
- The template can be bound to the individual peers via one of these commands:

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

  ```
  peer peer2 realm foo.com address 10.55.22.1 port 3867
  ```
- The RLF can only be used for diameter endpoints in which diamproxy is used.
- The configured message rate is implemented per−diamproxy. For example, if the message rate is 1,000, and 12 diamproxies are active (fully populated chassis = 12 active Packet Services Card (PSC) + 1 Demux + 1 standby PSC), the effective Transmissions Per Second (TPS) is 12,000. You can enter one of these commands in order to view the RLF context statistics:

  ```
  show rlf−context−statistics diamproxy
  ```

  ```
  show rlf−context−statistics diamproxy verbose
  ```

Network Overload Protection Through Page Throttling with RLF

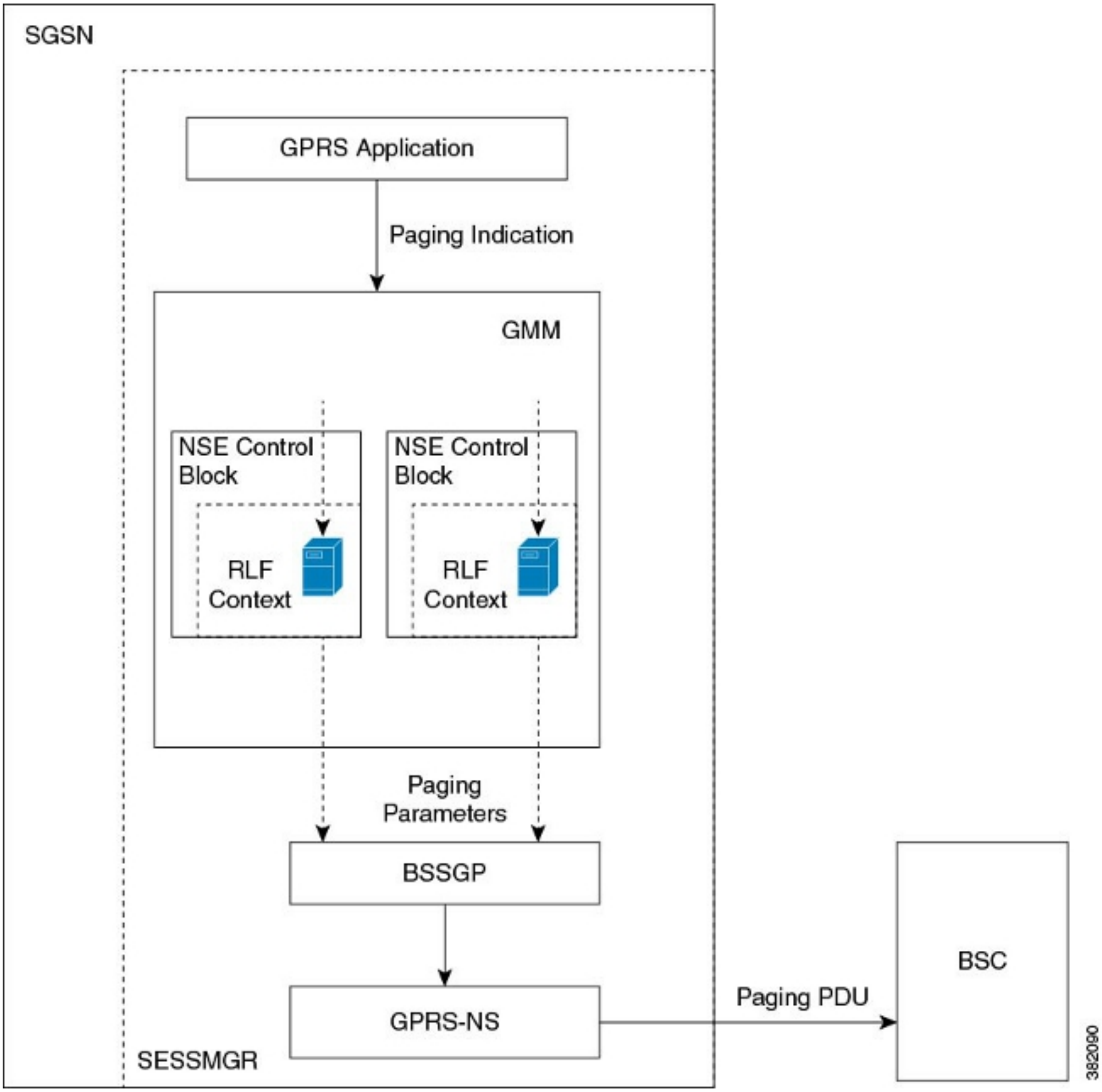
The page throttling feature limits the number of paging messages that are sent out of the SGSN. It provides flexibility and control to the operator, who can now reduce the number of paging messages that are sent out from the SGSN based on the network conditions. In some locations, the amount of paging messages that are initiated from the SGSN is very high due to bad radio conditions. A higher number of paging messages results in the consumption of bandwidth in the network. This feature provides a configurable rate limit, in which the paging message is throttled at these levels:

- The global level for both 2G and 3G access
- The Network Service Entity (NSE) level for 2G access only
- The Radio Network Controller (RNC) level for 3G access only

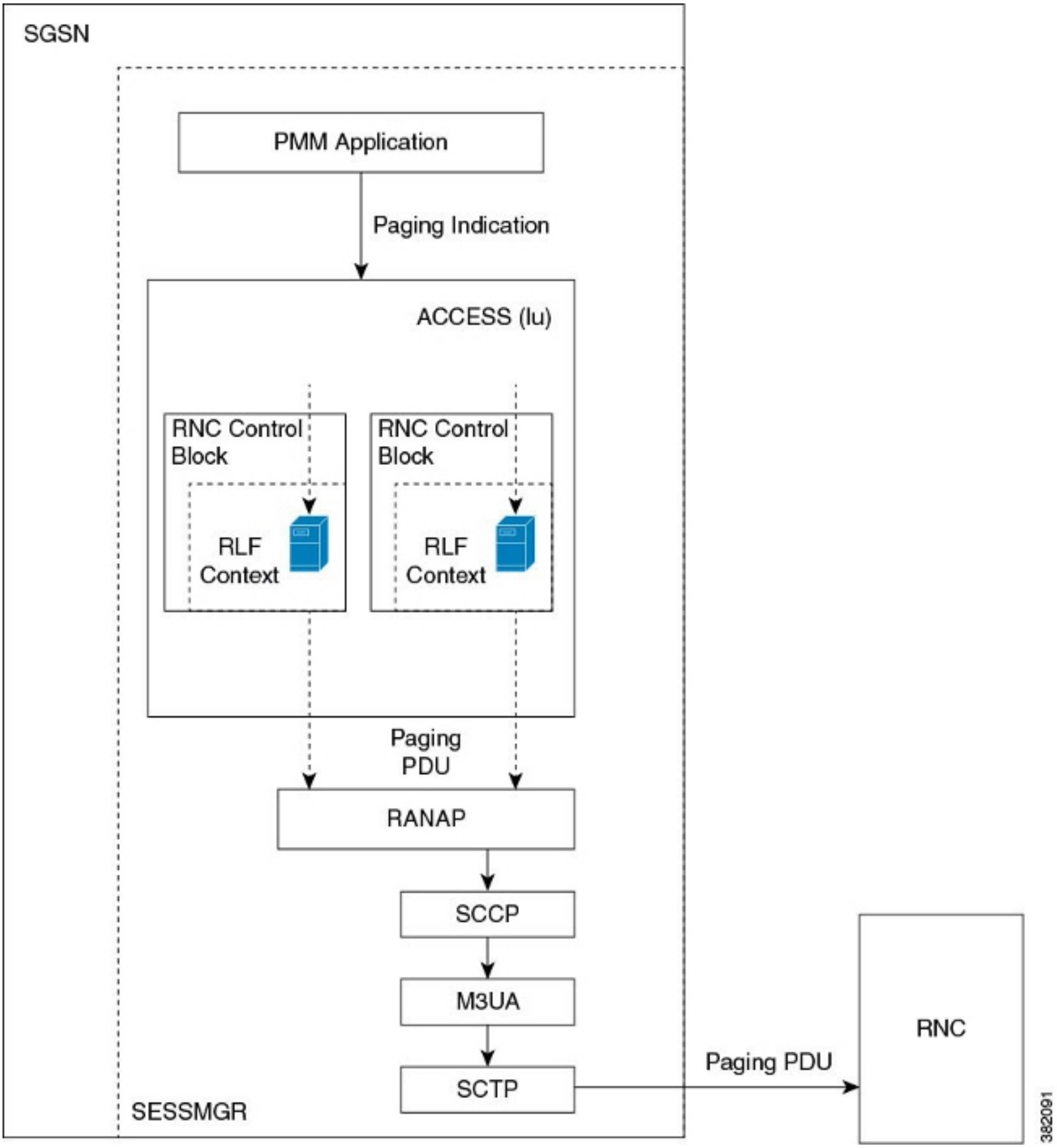
This feature improves the bandwidth consumption on the radio interface.

Note: An RLF license is required in order to configure an RLF template.

Here is an example of the paging process with 2G access and rate limiting:



Here is an example of the paging process with 3G access and rate limiting:



Configure Page Throttling with RLF

The commands that are described in this section are used in order to configure the page throttling feature. These CLI commands are used in order to associate/remove the RLF template for page throttling at the global level, the NSE level, and the RNC level on the SGSN.

Map the RNC Name to the RNC Identifier

The ***interface*** command is used in order to configure the mapping between the RNC Identifier (ID) and the RNC name. You can configure the *paging−rlf−template* either by RNC name or RNC ID. Here is the syntax that is used:

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

Note: The *no* form of the command removes the mapping and other configuration that is associated with the RNC *paging-rlf-template* configuration from the SGSN and resets the behavior to the default for that RNC.

Here is an example 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#
```

Associate a Paging RLF Template

This command allows the SGSN to associate an RLF template either at the global level, which limits the paging messages that are initiated across both the 2G (NSE-level) and 3G (RNC-level) access, or at the per-entity level, which is either at the RNC level for 3G access or at the NSE level for 2G access. Here is the syntax that is used:

```
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: If there is no RLF template associated with a particular NSE/RNC, then the paging load is limited based on the global RLF template that is associated (if present). If no global RLF template is associated, then no rate limiting is applied on the paging load.

Here is an example 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#
```