Внедрите защиту от перегрузок для шлюзов и элементов соседней сети на серии ASR5x00

Содержание

Введение

Этот документ описывает, как внедрить защитные функции, которые доступны для шлюзов (GW) и элементы соседней сети на маршрутизаторе Cisco Aggregated Services (ASR) 5x00 Серия для защиты полной производительности сети.

Управление перегрузкой для GW

Управление перегрузкой является функцией самозащиты общего назначения. Это используется для защиты системы против скачков использования этих ресурсов:

- Использование ЦПУ при обработке карт
- Использование памяти при обработке карт

Когда использование превышает предустановленные пороги, все новые требования (активации Протокола коммутации пакетов (PDP), активация сеанса Пакетной сети передачи данных (PDN)) *отброшены* или *отклонены*, зависят от конфигурации.

Вот пример, который показывает, как контролировать полное использование Карты обработки данных (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
```

> **Примечание:** Предел системного проектирования составляет 80% загрузки ЦПУ, которая определена как рекомендуемый технический предел, который не должен быть превышен для гарантии обычного использования системы. Загрузка вне значения могла бы повлиять на использование платформы, такое как ее устойчивость и предсказуемость, и должна избежаться с надлежащим планированием мощности.

> **Примечание:** Cisco рекомендует использовать *действие сброса*, а не действие *отклонения*, поскольку отклоненные вызовы вызывают непосредственные повторные попытки повторного соединения от Пользовательского оборудования (UE). В случае действия сброса UE ждет за несколько секунд до того, как он предпримет повторенные попытки повторного соединения, таким образом, уменьшена скорость вызова.

Защита перегрузки сети для входной регулировки сообщения GTP-C

Эта функция защищает Пакетный GW (PGW) / GPRS шлюза, Поддерживающий Узел (GGSN) процессы от скачков передачи и сбоев сетевого элемента. В Узле Поддержки GPRS P-GW/Serving (SGSN) основное узкое место отнесено к обработке пользовательских данных, такой как использование менеджера сеанса и полный ЦП DPC и загруженность памяти.

Когда защита перегрузки сети активирована, *Никакое значение* не настроено на Объекте управления SGSN/Mobility (MME) для регулировки входящего GPRS, Туннелирующего Контроль протокола (GTP-C) сообщения.

> **Примечание:** Использование GTP и регулировка интерфейса диаметра требуют, чтобы был установлен допустимый лицензионный ключ.

Эта функция помогает управлять скоростью входящих / исходящих сообщений на P-GW/GGSN, который помогает гарантировать, что P-GW/GGSN не разбит сообщениями плана контроля за GTP. Кроме того, это помогает гарантировать, что P-GW/GGSN не сокрушает узел GTP-C с сообщениями уровня управления GTP. Эта функция требует, чтобы GTP (Версия 1 (v1) и Версия 2 (v2)) управляющие сообщения формировались/определялись политику по интерфейсам Gn/Gp и S5/S8. Эта функция покрывает защиту от перегрузок узлов P-GW/GGSN и других внешних узлов, с которыми это связывается. Регулировка сделана только для управляющих сообщений сеансового уровня, таким образом, сообщения управления пути не являются скоростью, ограниченной вообще.

Перегрузка внешнего узла может произойти в сценарии, где P-GW/GGSN генерирует запросы сигнализации на более высокой скорости, чем другие узлы могут обработать. Кроме того, если входящая скорость высока в узле P-GW/GGSN, она могла бы лавинно разослать внешний узел. Поэтому регулировка и входящих и исходящих управляющих сообщений требуется. Для защиты внешних узлов от перегрузки из-за сигнализации контроля за P-GW/GGSN, используется платформа, чтобы сформировать и определить

политику исходящих управляющих сообщений к внешним интерфейсам.

Настройте входную регулировку сообщения GTP-C

Введите эту команду для настройки входной регулировки сообщения GTP-C:

```
gtpc overload-protection Ingress
```

Это настраивает защиту от перегрузок GGSN/PGW путем регулировки входящего GTPv1 и управляющих сообщений GTPv2 по Gn/Gp (GTPv1) или S5/S8 (GTPv2) интерфейс с другими параметрами для сервисов, которые настроены в контексте и применены к GGSN и PGW.

При вводе предыдущей команды это приглашение генерируется:

```
gtpc overload-protection Ingress
```

Вот некоторые примечания об этом синтаксисе:

- **нет:** Этот параметр отключает входящую регулировку управляющего сообщения GTP для сервисов GGSN/PGW в этом контексте.
- **скорость сообщения message_rate**: Этот параметр определяет количество входящих сообщений GTP, которые могут быть обработаны в секунду. *Message_rate* является целым числом, которое колеблется от сто до 12,000.
- **допустимая задержка dur**: Этот параметр определяет максимальное число секунд, что входящее сообщение GTP может быть помещено в очередь, прежде чем это будет обработано. После того, как этот допуск превышен, сообщение отброшено. *dur* является целым числом, которое колеблется от один до десять.
- **размер размера очереди**: Этот параметр определяет максимальный размер очереди для входящих сообщений GTP-C. Если очередь превышает определенный размер, то любые новые входящие сообщения отброшены. *Размер* является целым числом, которое колеблется от сто до 10,000.

Можно использовать эту команду для включения входящей регулировки управляющего сообщения GTP для сервисов GGSN/PGW, которые настроены в том же контексте. Как пример, эта команда включает входящие управляющие сообщения GTP в контексте со скоростью передачи сообщений *1,000* в секунду, размер очереди сообщений *10,000* и задержка *одной секунды*:

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

Защита элемента соседней сети

Много элементов соседней сети используют свои собственные механизмы для защиты себя, и дополнительная защита перегрузки сети на стороне ASR5x00 не могла бы быть необходима. Защита элементов соседней сети могла бы требоваться в случаях, где полная устойчивость сети может быть достигнута только, когда регулировка сообщения применена на выходную сторону.

Защита перегрузки сети с регулировкой диаметра на интерфейсе S6a

Эта функция защищает интерфейсы S6a и S13 в выходном направлении. Это защищает Абонентский сервер Дом (HSS), Агента маршрутизации диаметра (DRA) и Регистр идентичности оборудования (EIR). Функция использует Функцию ограничения скорости (RLF).

Рассмотрите эти важные замечания при применении конфигурации оконечной точки диаметра:

- Шаблон RLF должен быть привязан к узлу.
- RLF подключен только на основе на узел (индивидуально).

Настройте регулировку диаметра на интерфейсе S6a

Вот синтаксис команды, который используется для настройки регулировки диаметра на интерфейсе S6a:

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

Вот некоторые примечания об этом синтаксисе:

- **нет:** Этот параметр удаляет указанную конфигурацию одноранговой узла.
- **[*] peer_name [*]**: Этот параметр задает одноранговое название как алфавитно-цифровую строку, которая колеблется от одного до 63 символов (символы пунктуации позволены).**Примечание:** Оконечная точка сервера диаметра может теперь быть дико чесавшим одноранговым названием (с * символ как допустимый подстановочный знак). Клиентские узлы, которые удовлетворяют дико чесавший образец, рассматриваются как допустимые одноранговые узлы, и соединение принято. Дико чесавший маркер указывает, что одноранговое название дико чешется, и любой *, символ в строке, которая предшествует, рассматривается как подстановочный знак.
- **область realm_name**: Этот параметр задает область этого узла как алфавитно-цифровая строка, которая колеблется от одного до 127 символов. Имя области может быть компанией или именем сервиса.
- **адрес ipv4/ipv6_address**: Этот параметр задает IP-адрес diameter peer в десятичном представлении с точкой IPv4 или IPv6 colon-separated-hexadecimal нотация. Этим адресом должен быть IP-адрес устройства, с которым связывается шасси.
- **fqdn fqdn**: Этот параметр задает Полное доменное имя (FQDN) diameter peer как алфавитно-цифровую строку, которая колеблется от одного до 127 символов.
- **[port port-number]:** Этот параметр задает номер порта для этого diameter peer. Номер порта должен быть целым числом, которое колеблется от одного до 65,535.
- **connect-on-application-access**: Этот параметр активирует узел на доступ начального приложения.

- **send-dpr-before-disconnect**: Этот параметр передает Запрос от равноправного участника разъединения (DPR).

- **disconnect-cause**: Этот параметр заканчивает DPR к указанному узлу с указанной причиной разъединения. Причина разъединения должна быть целым числом, которое колеблется от нуля до два, которые соответствуют этим причинам:

  ПЕРЕЗАГРУЗКА **0** Г¦¦

  1 ЗАНЯТЫЙ Г¦¦

  2 Г¦¦ DO_NOT_WANT_TO_TALK_TO_YOU

- **rlf-шаблон rlf_template_name**: Этот параметр задает шаблон RLF, который будет привязан к этому diameter peer. *rlf_template_name* должен быть алфавитно-цифровой строкой, которая колеблется от одного до 127 символов.

  Примечание: Лицензия RLF требуется для настройки шаблона RLF.

Защита перегрузки сети с регулировкой диаметра на интерфейсе Gx/Gy

Эта функция защищает интерфейсы Gx и Gy в выходном направлении. Это защищает Политику и Заряжающую Функцию Правил (PCRF) и Онлайновую тарификационную систему (OCS) и использует RLF.

Рассмотрите эти важные замечания при применении конфигурации оконечной точки диаметра:

- Шаблон RLF должен быть привязан к узлу.

- RLF подключен только на основе на узел (индивидуально).

Эта команда используется для настройки защиты перегрузки сети:

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

Примечание: Лицензия RLF требуется для настройки Шаблона RLF

Настройте регулировку диаметра на интерфейсе Gx/Gy

Вы могли бы рассмотреть использование RLF для интерфейсов диаметра. Вот пример конфигурации:

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

Вот некоторые примечания об этой конфигурации:

- Узел, названный *peer1*, связан с *RFL2*, и остаток узлов под оконечной точкой связан с *RLF1*.

- Одноранговый уровень шаблон RLF имеет приоритет по шаблону уровня оконечной точки.

- Количество сообщений отослано в максимальном значении 1,000 в секунду. (скорость сообщения). Эти факторы также применяются:

  Только сто сообщений (размер пакета) отосланы каждые сотни миллисекунд (для достижения 1,000 сообщений в секунду).

  Если количество сообщений в очереди RLF превышает 80% скорости передачи сообщений (80% из 1,000 = 800), переходы RLF к состоянию *OVER_THRESHOLD*.

  Если количество сообщений в очереди RLF превышает скорость передачи сообщений (1,000), переходы RLF к состоянию *OVER_LIMIT*.

  Если количество сообщений в очереди RLF уменьшается ниже 60% скорости передачи сообщений (60% из 1,000 = 600), переходы RLF назад к *Состоянию готовности*.

  Максимальное число сообщений, которые могут быть помещены в очередь, равняется скорости передачи сообщений, умноженной на допустимую задержку (1,000 x 4 = 4,000).

  Если приложение передает больше чем 4,000 сообщений к RLF, первые 4,000 помещены в очередь, и остальные отброшены.

  Сообщения, которые отброшены, являются retried/re-sent приложением к RLF в соответствующем периоде времени.

  Количество повторных попыток является ответственностью приложения.

- Шаблон может быть развязан от оконечной точки ни с *каким* параметром *rlf-шаблона*. Например, это развязало бы *RLF1* от *peer2*.

- Не используйте *rlf-шаблон rlf1* параметр в *режиме конфигурации оконечной точки*, поскольку CLI пытается удалить шаблон RLF *RLF1*. Эта команда CLI является частью глобальной конфигурации, не конфигурацией оконечной точки.

- Шаблон может быть связан с отдельными узлами через одну из этих команд:
  `no peer peer2 realm foo.com`

  `peer peer2 realm foo.com address 10.55.22.1 port 3867`
- RLF может только использоваться для оконечных точек диаметра, в которых используется diamproxy.

- Настроенная скорость передачи сообщений внедрена на - diamproxy. Например, если скорость передачи сообщений 1,000, и 12 diamproxies активны (полностью заполненное шасси = 12 активных Карт служб пакетной передачи (PSC) + 1 Демультиплексор + 1 резервный PSC), эффективные Передачи в секунду (TPS) 12,000. Можно ввести одну из

этих команд для просмотра статистики контекста RLF:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Защита перегрузки сети посредством регулировки страницы с RLF

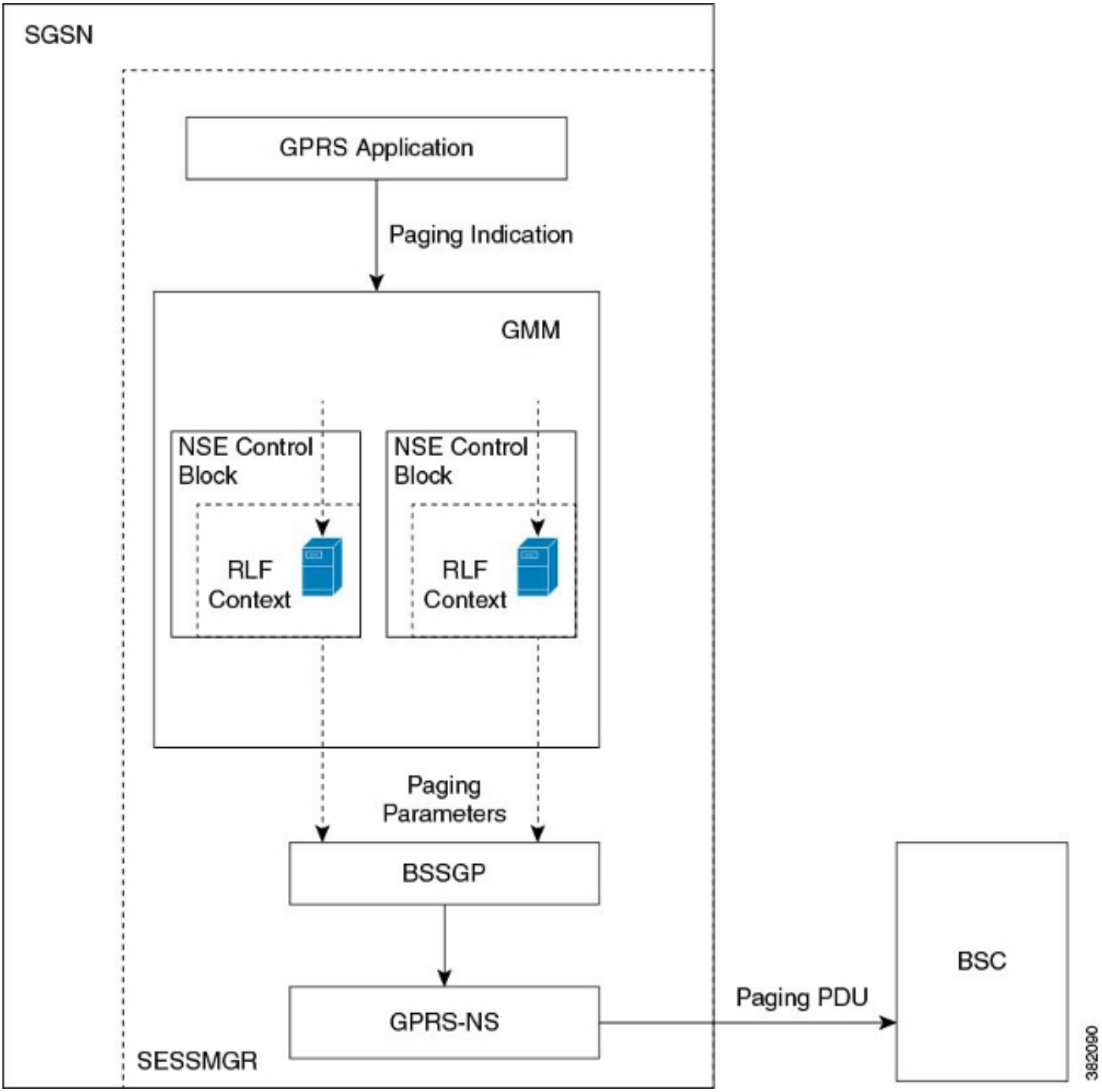
Страница, регулирующая функцию, ограничивает количество пейджинговых сообщений, которые передаются из SGSN. Это предоставляет гибкость и контроль оператору, который может теперь сократить количество пейджинговых сообщений, которые передаются из SGSN на основе состояний сети. В некоторых местоположениях сумма пейджинговых сообщений, которые инициируются от SGSN, является очень причиной высокой загрузки к плохим радио-условиям. Более высокое количество пейджинговых сообщений приводит к потреблению пропускной способности в сети. Эта функция предоставляет конфигурируемое ограничение скорости, в котором пейджинговое сообщение регулируют на этих уровнях:

- Глобальный уровень и для 2G и для доступа 3G
- Уровень Объекта сетевого сервиса (NSE) для 2G обращается только
- Уровень Контроллера радиосети (RNC) для 3G обращается только

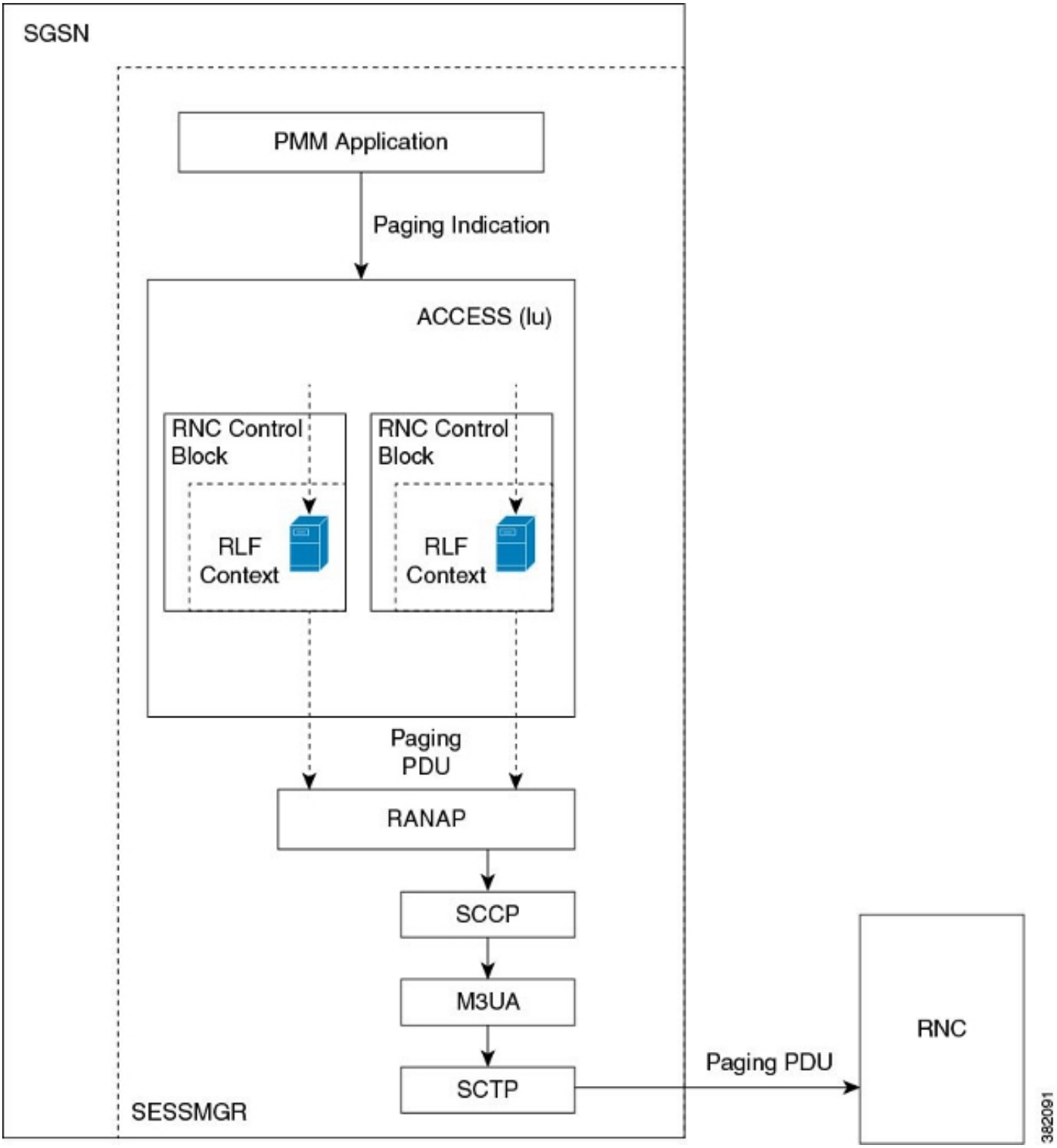
Эта функция улучшает потребляемую полосу пропускания относительно радиоинтерфейса.

Примечание: Лицензия RLF требуется для настройки шаблона RLF.

Вот пример процесса пейджинга с доступом 2G и ограничения скорости:



Вот пример процесса пейджинга с доступом 3G и ограничения скорости:



Регулировка страницы настройки с RLF

Команды, которые описаны в этом разделе, используются для настройки функции регулировки страницы. Эти команды CLI используются для соединения шаблона RLF для регулировки страницы на глобальном уровне, уровне NSE и уровне RNC на SGSN.

Сопоставьте название RNC к идентификатору RNC

Интерфейсная команда используется для настройки сопоставления между Идентификатором RNC (ID) и названием RNC. Можно настроить *paging-rlf-template* или названием RNC или ID RNC. Вот синтаксис, который используется:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

> **Примечание:** *Никакая* форма команды не удаляет сопоставление и другую конфигурацию, которая привязана к RNC *paging-rlf-template* конфигурация от SGSN и перезагружает поведение к по умолчанию для того RNC.

Вот пример конфигурации:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

Привяжите разбивку на страницы шаблон RLF

Эта команда позволяет, что SGSN для соединения RLF обрабатывают по шаблону или на глобальном уровне, который ограничивает пейджинговые сообщения, которые инициируются и через 2G (уровень NSE) и через 3G (уровень RNC) доступ, или на уровне на объект, который является или на уровне RNC для доступа 3G или на уровне NSE для доступа 2G. Вот синтаксис, который используется:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```

> **Примечание:** Если нет никакого шаблона RLF, привязанного к определенному NSE/RNC, то загрузка разбивки на страницы ограничена на основе глобального шаблона RLF, который привязан (если есть). Если никакой глобальный шаблон RLF не привязан, то никакое ограничение скорости не применено на загрузку разбивки на страницы.

Вот пример конфигурации:

```
show rlf-context-statistics diamproxy

show rlf-context-statistics diamproxy verbose
```