

在ASR 5X00上配置擁塞控制機制

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[擁塞控制概述](#)

[MME/SGSN擁塞控制](#)

[基於APN的會話管理擁塞控制](#)

[基於APN的MM擁塞控制](#)

[常規NAS級擁塞控制](#)

[S1-MME介面上的MME過載降低](#)

[過載的PGW控制](#)

[ASR 5x00上的擁塞控制操作](#)

[過載時呼叫斷開連線](#)

[擁塞條件閾值](#)

[服務擁塞策略](#)

[設定](#)

[啟用擁塞控制](#)

[擁塞控制過載斷開連線](#)

[擁塞控制策略配置](#)

[擁塞控制策略](#)

[策略過載重定向](#)

[MME服務的擁塞控制策略](#)

[MME擁塞控制策略操作配置檔案](#)

[17.0及更新版本的SGSN擁塞控制策略](#)

[SGSN擁塞控制策略操作配置檔案](#)

[擁塞控制閾值](#)

[MME和SGSN的擁塞控制閾值](#)

[驗證](#)

[擁塞控制組態驗證](#)

[啟用前的擁塞控制](#)

[啟用後的擁塞控制](#)

[過載斷開連線啟用後的擁塞控制](#)

[啟用除SGSN和MME以外的策略後的擁塞控制](#)

[主要和次要配置檔案的擁塞控制閾值](#)

[針對SGSN的擁塞控制策略啟用](#)

[針對MME的擁塞控制策略啟用](#)

[擁塞控制統計資訊](#)

簡介

本文描述如何在思科聚合服務路由器(ASR)5x00系列上配置擁塞控制機制。本文所述的擁塞控制功能主要應用於服務通用封包無線服務(GPRS)支援節點(SGSN)和行動管理實體(MME)網路功能。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

擁塞控制概述

有時，網路中可能會出現過大的負載，這可能會導致許可證漏洞、高CPU利用率、高埠利用率或高記憶體利用率。這會導致重負載下的節點效能下降，但這些情況通常是臨時的，並且很快就會解決。擁塞控制用於協助識別此類狀況，以及在這些重負載狀況持續存在或存在大量該等狀況時，呼叫處理該狀況的策略。

本節介紹第3代合作夥伴計畫(3GPP)中SGSN和MME中的擁塞控制機制。

MME/SGSN擁塞控制

MME提供了非接入起點(NAS)級別的擁塞控制機制，該機制基於接入點名稱(APN)或通用NAS級別移動管理(MM)控制。

基於APN的擁塞控制機制可以處理與具有特定APN和UE的使用者裝置(UE)相關聯的演化分組系統(EPS)會話管理(ESM)和EPS移動管理(EMM)信令。網路應支援此擁塞控制功能。MME檢測與APN關聯的NAS級擁塞控制，並根據以下標準啟動和停止基於APN的擁塞控制：

- 每個APN的活動EPS承載的最大數量
- 每個APN的最大EPS承載啟用數

- APN上的一個或多個封包資料網路(PDN)閘道(PGW)無法連線或表示到MME擁塞
- 與具有特定APN訂閱的裝置相關聯的最大MM信令請求數
- 網路管理設定

附註：MME不應將擁塞控制應用於高優先順序訪問和緊急服務。通用的NAS級MM控制可用於在一般擁塞條件下拒絕NAS級MM信令請求。

基於APN的會話管理擁塞控制

基於APN的會話管理擁塞控制可以由於擁塞情況、由OAM或通過重新啟動/恢復PGW在MME上啟用。MME可以拒絕來自UE的ESM請求，該請求可以包含在PDN連線、承載資源分配或承載資源修改請求中。MME還可以在擁塞條件期間停用當前PDN連線，並且向UE傳送會話回退計時器。如果包括此計時器，則不應啟用重新啟用請求。

在擁塞期間，MME可以儲存特定UE和APN的會話管理(SM)回退計時器，並立即拒絕來自該APN所針對的UE的任何後續SM消息，直到該計時器耗盡。對於不支援SM回退計時器的UE（對於版本10之前的UE版本），這是必需的。MME如果想要向計時器已運行的UE傳送SM消息，則首先清除此計時器。

UE可以在計時器運行時完成以下操作：

- 如果在拒絕的EPS SM請求消息中提供APN，或者如果在NAS停用EPS承載上下文請求消息中接收了SM回退計時器，則UE不應為擁塞的APN啟動任何SM過程。
- 如果被拒絕的EPS SM請求消息中未提供APN，則UE將不發起沒有APN的任何SM請求。
- 這些更改不會停止回退計時器：

單元格

跟蹤區域(TA)

公共土地行動網路(PLAMN)

無線電存取技術(RAT)

- 即使SM回退計時器運行，UE也可以啟動用於高優先順序接入和緊急服務的SM過程。
- 如果UE在SM回退計時器運行時接收到針對擁塞APN的網路發起的EPS SM請求消息，則UE停止與該APN相關聯的SM回退計時器並響應MME。
- 如果UE被配置為覆蓋低接入優先順序的許可權，並且SM回退計時器由於響應於低接入優先順序的請求而接收的拒絕消息而運行，則UE中的上層可以請求啟動沒有低接入優先順序的單播過程。

- 允許UE發起PDN斷開過程，但它不刪除相關SM回退計時器。
- 所述回退計時器不停止UE傳送資料或發起針對擁塞APN啟用使用者平面承載的服務請求。

基於APN的MM擁塞控制

與SM過程類似，MME也有一個MM回退計時器，可以拒絕連線過程。MME應在拒絕連線過程之後保留使用者資料一段時間，以便相同使用者後續請求的拒絕可在不與HSS互動的情況下完成。

當回退計時器運行時，UE不應為MM過程發起任何NAS請求，高優先順序訪問或緊急服務除外。然而，如果UE已經處於連線模式，則允許UE執行跟蹤區域更新(TAU)。

MME應選擇回退計時器，使得所有UE不應具有此計時器的相同值，且UE應同時發起延遲請求。當接收到移動性回退計時器時，UE行為不是APN特定的。

常規NAS級擁塞控制

一般的NAS級擁塞控制對一般的過載情況很有幫助。其工作方式與基於APN的擁塞控制類似，並且與回退計時器具有類似的概念。當回退計時器運行時，UE可以發起分離請求、高優先順序請求和TAU(當處於連線模式)。

即使在UE從網路中分離之後，回退計時器仍繼續運行。如果MME要尋呼回退計時器已經運行的UE，則MME應停止回退計時器，並且UE應在收到MME的尋呼請求並發起服務請求之後停止回退計時器。

MM回退計時器不會影響Cell/RAT和PLMN更改。TA更改不會停止此計時器。當選擇了與PLMN不等效的新PLMN時，此計時器停止。

當UE接收到切換命令時，它應該繼續切換，而不管回退計時器狀態如何。

如果MME用大於UE定期TAU計時器加上隱式分離計時器的總和的MM後退計時器拒絕TAU請求或服務請求，則MME應調整移動可達計時器和/或隱式分離計時器，使得在MM後退計時器運行時MME不會隱式地分離UE。

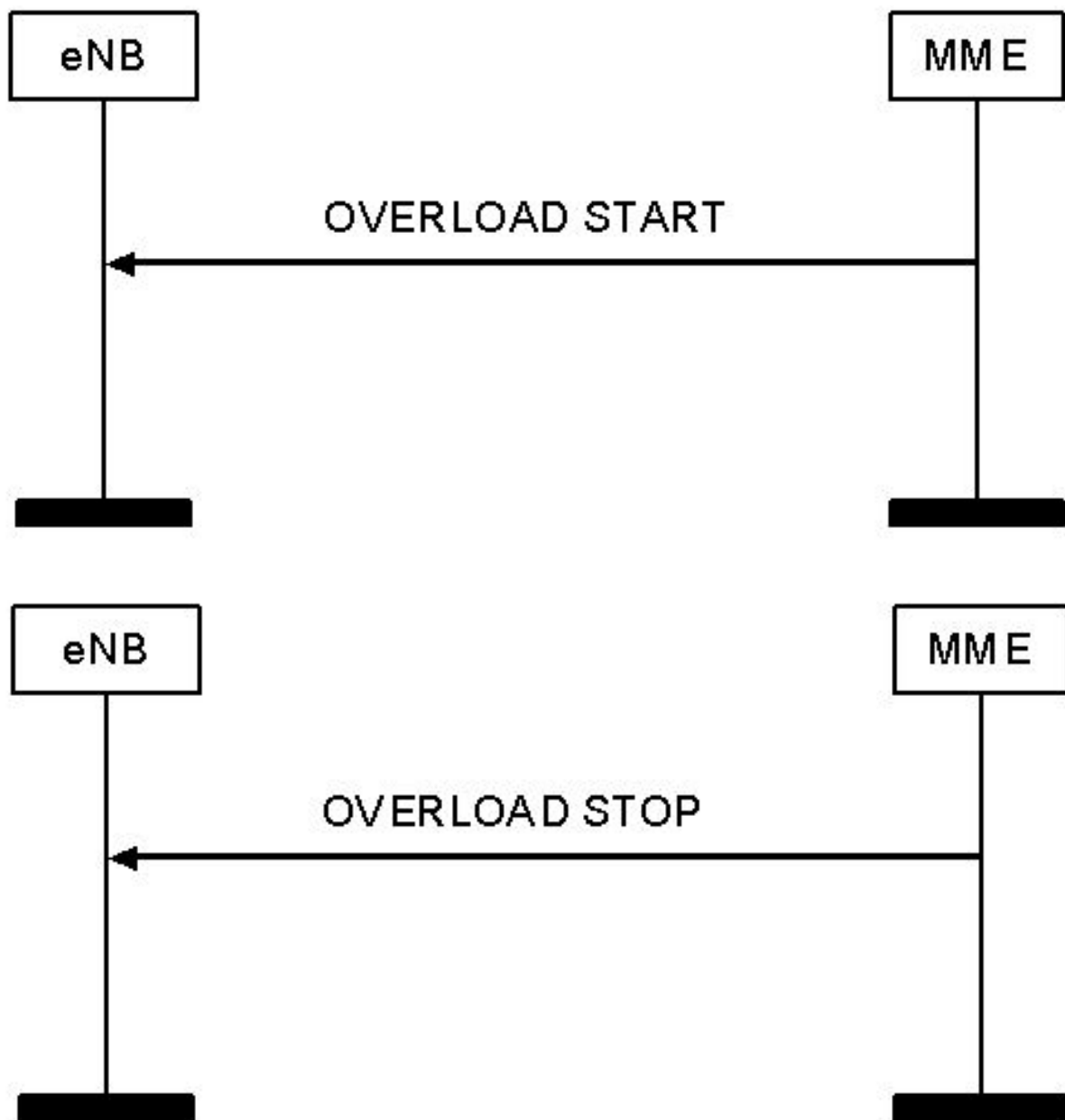
附註：SGSN擁塞控制的工作方式與MME類似。有關SGSN擁塞控制機制的詳細資訊，請參閱3GPP TS 23.060；有關MME擁塞控制機制的詳細資訊，請參閱3GPP TS 23.401。

S1-MME介面上的MME過載降低

MME可以向E-NodeB(eNB)傳送過載Start消息以減少信令負載。此過程使用非UE關聯的信令。過載操作資訊元素(IE)在過載開始消息中包含過載響應IE，該過載響應包含有關拒絕標準的資訊，並且eNB會相應地採取行動。

提示：有關詳細資訊，請參閱3GPP技術規範(TS)36.413。

為了指示過載情況的結束，MME向eNB傳送過載停止消息：



附註：SGSN還具有類似的信令減少機制，這在3GPP TS 25.413中提及。

過載的PGW控制

PGW可以在過載情況下拒絕PDN連線。PGW可以基於諸如以下的標準檢測過載狀況並啟動或停止過載控制：

- 每個APN的最大活動承載數
- 每個APN的最大承載啟用速率

PGW可以為特定APN指定對MME的PGW回退計時器，MME應拒絕該時間段內對該APN的PDN連線請求。MME可以選擇另一個PGW而不是在該時間段期間拒絕，除非已經存在到該UE的相同APN的當前PDN連線。

附註：GGSN擁塞控制機制與3GPP TS 23.060中提到的PGW擁塞控制機制類似，3GPP TS

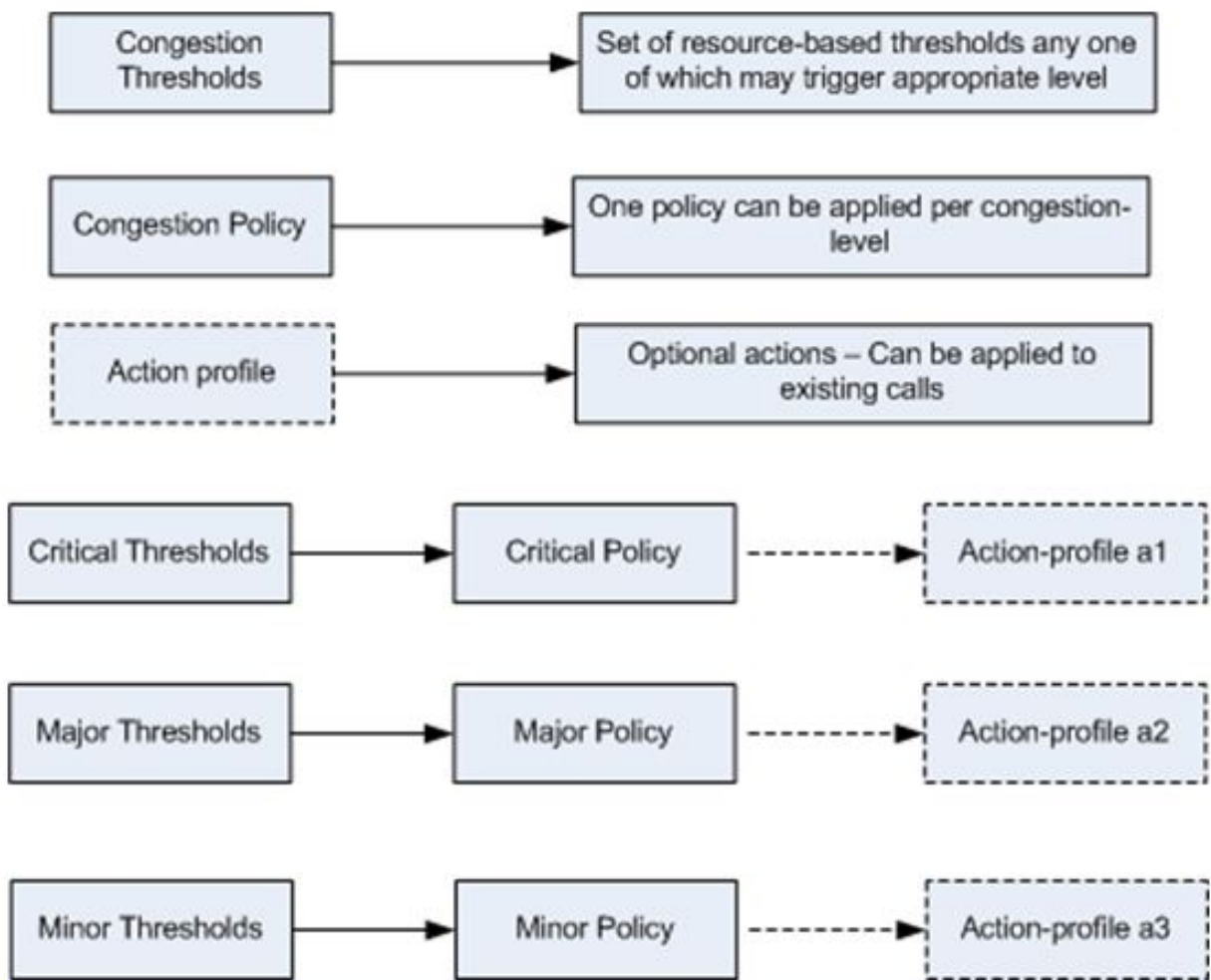
23.401中提到了PGW擁塞控制機制。

ASR 5x00上的擁塞控制操作

擁塞控制操作基於這些附加功能的配置：

- 過載時呼叫斷開
- 擁塞控制條件閾值
- 服務擁塞策略

以下是範例：



過載時呼叫斷開連線

此功能允許系統在過載情況下啟用或禁用被動呼叫（機箱範圍）斷開連線的策略。它還允許您微調過載斷開連線擁塞策略。

擁塞條件閾值

可以定義各種擁塞控制閾值，這些閾值規定了要啟用擁塞控制的條件。它還為擁塞或清除的系統狀態的定義建立限制。達到這些閾值後，不僅會生成簡單網路管理協定(SNMP)陷阱（擁塞），還會呼叫擁塞策略。

閾值容差用於指定在配置的閾值下必須達到的百分比，然後才考慮清除條件並觸發SNMP陷阱 (CongestionClear)。

服務擁塞策略

擁塞服務策略可針對每個服務進行設定，例如封包資料服務節點(PDSN)、閘道GPRS支援節點(GGSN)和服務GPRS支援節點(SGSN)。這些策略規定當系統檢測到因擁塞閾值漏洞導致擁塞時，服務響應的方式。

設定

本節介紹啟用擁塞控制和擁塞控制的基本調整所需的配置。

啟用擁塞控制

機箱上預設禁用擁塞控制。在全域組態模式下輸入`congestion-control`命令以啟用它：

```
[local]host_name(config)# congestion-control
```

擁塞控制過載斷開連線

擁塞控制過載斷開連線啟用或禁用在過載情況下斷開機箱範圍被動呼叫的策略。預設情況下禁用此功能。它允許分階段和重複從機箱斷開被動呼叫，直到清除擁塞控制。可以配置`license-utilization`和`max-sessions-per-service-utilization`的閾值以及閾值。

例如，如果閾值配置為at值為90%，容差為5%，則當該服務的呼叫數下降到總允許呼叫數的85%以下時，系統會停止被動呼叫斷開連線。

以下是可用於啟用擁塞控制過載斷開連線的CLI語法，該連線始終在全域性配置模式下配置：

```
congestion-control overload-disconnect
```

```
congestion-control overload-disconnect [ iterations-per-stage <integer> | percent  
<percentage_value> | threshold { license-utilization <percentage_value> |  
max-sessions-per-service-utilization <percentage_value> | tolerance <number> } ]
```

以下是關於此語法的一些註解：

- **每階段迭代:**此引數定義在定義的秒數內要斷開的呼叫數。此值的範圍為2到8。
- **百分比:**此引數指定在過載情況下分階段斷開的呼叫的百分比。此值的範圍為0到100，預設值是5。

- **閾值:**此引數定義許可證的閾值和最大會話利用率。它還允許定義公差值。

許可證利用率:這將為過載情況指定許可證利用率百分比閾值。在觸發的情況下，被動呼叫被斷開。此值的範圍介於1和100之間，預設值為80。

每個服務的最大會話利用率:這指定每個服務利用閾值的最大會話數百分比。一旦超過定義的值，系統就開始斷開被動呼叫。此值的範圍介於1和100之間，預設值為80。

容差:定義系統斷開的呼叫百分比低於為*license-utilization*和*max-sessions-per-service-utilization*設定的定義值。此值的範圍介於1和25之間，其中10為預設值。只有當利用率低於定義的容差值時，才會傳送清除陷阱消息。

擁塞控制策略配置

您可以基於每個服務配置擁塞控制策略。當超過任何已定義的擁塞控制閾值時，該策略可導致系統在新會話上執行丟棄、無、重定向和拒絕等操作，從而啟用擁塞控制。

此配置允許對MME和SGSN服務的擁塞控制策略進行更精細的定義，並允許配置不同的擁塞控制階段，如關鍵、主要和次要（以及操作配置檔案的關聯）。

擁塞控制策略

以下是擁塞控制策略配置CLI語法（MME服務除外）：

```
congestion-control policy { asngw-service | asnpc-service | cscf-service | fng-service  
| epdg-service | samog-service | ggsn-service | ha-service | hnbgw-service |  
hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service |  
pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service |  
pdsnclosedrps-service | pgw-service | phsgw-service | phspc-service | saegw-service  
| sgsn-service | sgw-service | wsg-service } action { drop | none | redirect |  
reject }
```

以下是關於此語法的一些註解：

- **服務型別:**此引數定義正在為其定義擁塞控制策略的服務名稱。適用於此CLI命令的服務在前面提到的CLI語法中指定。
- **Action:**此引數定義當超過指定服務的擁塞控制閾值時要採取的操作。可以配置以下四種型別的操作：

Drop:此操作將導致系統刪除新的會話請求。未傳送拒絕/失敗響應。

拒絕:此操作將導致拒絕新的會話請求。傳送拒絕響應。此選項不適用於IPSG服務。

無:如果要配置系統以便不執行任何操作，則使用此選項。

重定向:此操作會導致將新會話請求重定向到備用裝置。這僅適用於CSCF、HSGW、HA和PDSN服務。應使用*policy overload redirect*命令配置備用裝置的IP地址。

策略過載重定向

如果為呼叫會話控制功能(CSCF)、HRPD服務網關(HSGW)、主代理(HA)或PDSN服務配置了重定向操作，則應配置此功能。

- CSCF服務在CSCF策略規則配置下配置此命令。
- HSGW服務、HA服務和PDSN服務在相應的服務配置下配置了該命令。

MME服務的擁塞控制策略

在14.0版之前，MME服務的擁塞控制策略可以像前面部分提到的CLI語法那樣定義，但是有一些其他選項。以下是CLI語法：

```
congestion-control policy mme-service action { drop | none | reject | report-overload  
{ permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions }  
enodeb-percentage <percentage> }
```

除了drop、none和reject操作之外，MME服務還可以選擇報告eNodeB的過載條件。MME使用*S1AP Overload Start*消息呼叫S1過載過程，以便向MME具有S1介面連線的指定比例的eNodeB報告過載條件。MME隨機選擇eNodeB。同一池中的兩個過載的MME不會向同一個eNodeB傳送過載消息。當MME已恢復且可以增加其負載時，它傳送*S1AP過載停止*消息。此外，當配置報告過載操作時，可以完成以下操作：

- **Permit-emergency-sessions**:在過載期間，此操作僅允許MME上的緊急會話。
- **Reject-new-sessions**:在過載情況下，此操作將導致拒絕所有指向MME的新會話。
- **拒絕非緊急會話**:此操作將導致過載期間在MME上拒絕所有非緊急會話。
- **Enodeb-percentage**:此操作配置接收過載報告的已知eNodeB的百分比。百分比範圍可為1到100。

在版本14.0及更高版本中，MME服務可以具有三個不同的策略和相關聯的操作配置檔案。以下是CLI語法：

```
congestion-control policy { critical mme-service action-profile <action_profile_name> |  
major mme-service action-profile <action_profile_name> | minor mme-service  
action-profile <action_profile_name> }
```

在14.0及更新版本中，有三種原則型別可設定為MME：

- **重要**:這定義了MME服務的關鍵擁塞控制閾值。
- **主要**:這定義了MME服務的主要擁塞控制閾值。
- **輕微**:這定義了MME服務的次要擁塞控制閾值。

附註：action-profile 引數定義與前面提到的策略型別（次要、主要或關鍵）關聯的操作配置檔案。

MME擁塞控制策略操作配置檔案

MME擁塞控制策略操作配置檔案可在*lte-policy*下配置。以下是CLI語法：

```
configure > lte-policy
```

```
congestion-action-profile <profile_name>
```

接下來的幾節介紹了可在擁塞操作配置檔案下配置的可用操作。

drop

當達到擁塞控制閾值時，此操作會導致丟棄新會話請求。以下是CLI語法：

```
drop { addn-brr-requests | addn-pdn-connects | brr-ctxt-mod-requests |  
combined-attaches | handovers | ps-attaches | s1-setups | service-request |  
tau-request } [ lapi ] [ apn-based ]
```

它允許更精細地控制應丟棄的請求/呼叫事件的型別。詳情如下：

- **Addn-brr-request**:這將丟棄包含UE發起的承載資源請求的資料包。這是許可的關鍵字。
- **Addn-pdn-connect**:這將丟棄包含其他PDN上下文連線的資料包。這是許可的關鍵字。
- **Brr-ctxt-mod-requests**:這將丟棄包含載體上下文修改請求的資料包。這是許可的關鍵字。
- **組合連線**:這將丟棄包含組合連線請求的資料包。
- **切換**:這將丟棄包含切換嘗試的資料包。
- **Ps附件**:這將丟棄包含資料包交換連線請求的資料包。
- **S1設定**:這將丟棄包含S1設定嘗試的資料包。這是許可的關鍵字。
- **Service-requests**:這將丟棄包含所有服務請求的資料包。這是許可的關鍵字。
- **Tau-requests**:這將丟棄包含所有跟蹤區域更新請求的資料包。

這兩個選項也可以使用上述呼叫事件型別進行配置（這兩個選項均由許可證控制）：

- **Lapi**:這表示會針對通話事件丟棄具有低存取優先順序指示(LAPI)的請求；否則，LAPI和非LAPI事件將被丟棄。以下是CLI語法：

```
drop
```

- **基於APN**:這表示會丟棄為運營商策略中的擁塞控制配置的接入點名稱(APN)請求。以下是CLI語法：

```
drop
```

附註： 使用運營商策略中的 `apn network-identifier` 命令為 APN 配置擁塞控制。

附註： 如果擁塞操作配置檔案同時配置了基於 LAPI 和 APN 的選項，則只有在兩個條件都匹配的情況下才會丟棄呼叫事件。

排除緊急事件

這樣，即使已超過閾值，也可以處理緊急請求。以下是 CLI 語法：

`exclude-emergency-events`

配置此項後，在緊急連線的 UE 中，不對這些消息應用擁塞操作拒絕和丟棄：

- TAU 請求
- 服務請求
- 切換
- ADDN-PDN 請求

排除語音事件

這樣，即使已超出閾值，也可以處理語音呼叫。以下是 CLI 語法：

`exclude-voice-events`

無

這指定當達到擁塞控制閾值時，不應為入站請求執行擁塞控制操作。以下是 CLI 語法：

```
none { addn-brr-requests | addn-pdn-connects | combined-attaches | handovers |  
psattaches | s1-setups | service-request | tau-request }
```

以下是可以為此操作配置的呼叫事件的詳細資訊(*none*是所有這些呼叫事件的預設操作)：

- **Addn-brr-request:** 這會導致不為包含 UE 發起的承載資源請求的資料包完成擁塞控制操作。
- **Addn-pdn-connect:** 這會導致其他封包資料網路(PDN)內容連線沒有完成擁塞控制動作。
- **Brr-ctxt-mod-requests:** 這將導致不為包含承載上下文修改請求的資料包完成擁塞控制操作。
- **組合連線:** 這將導致不為包含組合連線請求的資料包完成擁塞控制操作。
- **切換:** 這會導致不為包含切換嘗試的資料包完成擁塞控制操作。
- **Ps 附件:** 這會導致不為包含封包交換連線請求的封包完成擁塞控制動作。

- **S1設定**:這將導致不為包含S1設定嘗試的資料包完成擁塞控制操作。這是許可的關鍵字。
- **Service-requests**:這會導致不為包含所有服務請求的資料包完成擁塞控制操作。這是許可的關鍵字。
- **Tau-requests**:這會導致不為包含所有跟蹤區域更新請求的資料包完成擁塞控制操作。

拒絕

這會導致在達到擁塞控制閾值時拒絕入站請求並傳送拒絕消息響應。以下是CLI語法：

```
reject { addn-brr-requests | addn-pdn-connects | brr-ctxt-mod-requests |
combined-attaches | handovers | ps-attaches | s1-setups time-to-wait
{ 1 | 10 | 2 | 20 | 50 | 60 } | service-request | tau-request }[ lapi ]
[ apn-based ]
```

以下是可以使用reject操作配置的呼叫事件的詳細資訊：

- **Addn-brr-request**:這將拒絕包含UE發起的承載資源請求的資料包。這是許可的關鍵字。
- **Addn-pdn-connect**:這將拒絕包含其他PDN內容連線的封包。這是許可的關鍵字。
- **Brr-ctxt-mod-requests**:這將拒絕包含載體上下文修改請求的資料包。這是許可的關鍵字。
- **組合連線**:這將拒絕包含組合連線請求的資料包。
- **切換**:這將拒絕包含切換嘗試的資料包。
- **Ps附件**:這將拒絕包含封包交換附加要求封包。
- **S1設定等待時間{ 1 } | 10 | 2 | 20 | 50 | 60 }**:這會拒絕在1、2、10、20、50或60秒後包含S1安裝嘗試的資料包。這是許可的關鍵字。
- **Service-requests**:這將拒絕包含所有服務請求的資料包。這是許可的關鍵字。
- **Tau-requests**:這將拒絕包含所有跟蹤區域更新請求的資料包。

這兩個選項也可以使用上述呼叫事件型別進行配置（這兩個選項均由許可證控制）：

- **Lapi**:這表示將拒絕具有LAPI的呼叫事件請求；否則，LAPI和非LAPI事件將被拒絕。以下是CLI語法：

```
reject
```

- **基於APN**:這表示為運營商策略中的擁塞控制配置的APN請求將被拒絕。以下是CLI語法：

```
reject
```

附註： 使用運營商策略中的 `apn network-identifier` 命令為 APN 配置擁塞控制。

附註： 如果擁塞操作配置檔案同時配置了基於 LAPI 和 APN 的選項，則只有在兩個條件都匹配的情況下才會拒絕呼叫事件。

報告過載

這使 MME 能夠向 eNodeB 報告過載狀況以緩解擁塞情況。MME 使用 *S1AP Overload Start* 消息呼叫 S1 過載過程，以便向 MME 具有 S1 介面連線的 eNodeB 的指定比例報告過載情況。

MME 隨機選擇 eNodeB。同一池中的兩個過載的 MME 不會向同一個 eNodeB 傳送過載消息。當 MME 已恢復且可以增加其負載時，它會傳送 *S1AP 過載停止* 消息。以下是 CLI 語法：

```
report-overload { permit-emergency-sessions-and-mobile-terminated-services |  
permit-highpriority-sessions-and-mobile-terminated-services |  
reject-delay-tolerant-access | reject-new-sessions |  
reject-non-emergency-sessions } enodeb-percentage
```

以下是可以使用此操作配置的選項：

- **permit-emergency-sessions-and-mobile-terminated-services:** 這指定在到 eNodeB 的過載消息中，在過載期間只允許緊急會話訪問 MME。
- **permit-high-priority-sessions-and-mobile-terminated-services:** 這在 eNodeB 的過載消息中指定，在過載期間只允許高優先順序會話和移動終止的服務訪問 MME。
- **reject-delay-tolerant-access:** 這指定在到 eNodeB 的過載消息中，在過載期間應拒絕目的地為 MME 的延遲容忍訪問。
- **reject-new-sessions:** 這指定在到 eNodeB 的過載消息中，在過載期間應拒絕所有發往 MME 的新連線請求。
- **reject-non-emergency-sessions:** 這指定在到 eNodeB 的過載消息中，在過載期間應拒絕所有非緊急會話。
- **enobeb-percentage:** 這將配置將接收過載報告的已知 eNodeB 的百分比。

17.0 及更新版本的 SGSN 擁塞控制策略

在版本 17.0 及更高版本中，SGSN 還需要類似於 MME 的擁塞控制策略。SGSN 可以有三個擁塞控制操作，每個操作都與一個操作配置檔案相關聯。以下是 CLI 語法：

```
congestion-control policy { critical | major | minor }  
sgsn-service action-profile <action_profile_name>
```

以下三種原則型別可在 14.0 及更新版本中設定為 MME：

- **重要:** 這定義了 MME 服務的關鍵擁塞控制閾值。

- **主要:**這定義了MME服務的主要擁塞控制閾值。
- **輕微:**這定義了MME服務的次要擁塞控制閾值。

附註： `action-profile` 引數定義與 `policy type` (次要、主要或關鍵) 關聯的操作配置檔案。

SGSN擁塞控制策略操作配置檔案

在 `sgsn-global` 配置模式下配置SGSN擁塞控制策略操作配置檔案。它定義當在SGSN節點中達到任何擁塞控制閾值時，針對這些型別的呼叫/消息事件要完成的操作：

- 活動呼叫
- 新呼叫
- SM消息

以下是配置SGSN擁塞控制策略操作配置檔案的語法：

```
configure > sgsn-global > congestion-control
congestion-action-profile <action_profile_name>
```

以下各節介紹可在SGSN擁塞操作配置檔案下配置各種策略。

活動呼叫策略

這指定在活動呼叫期間發生擁塞時，丟棄或拒絕任何活動呼叫消息。當前呼叫的丟棄或拒絕只能定義為消息的LAPI。以下是CLI語法：

```
active-call-policy { rau | service-req } { drop | reject } [ low-priority-ind-ue ]
```

以下是關於此語法的一些註解：

- **消息型別/呼叫事件:**可以為活動呼叫策略定義以下消息型別或呼叫事件：

RAU:這定義了SGSN接收的路由區域更新(RAU)消息。

Service-req:這定義SGSN接收的SR消息。

- **動作:**這定義了在達到擁塞控制閾值後，SGSN在活動呼叫期間收到上述消息時要採取的操作。

Drop:這指示SGSN在達到擁塞控制閾值時丟棄定義的消息。

拒絕:這指示SGSN在達到擁塞控制閾值時拒絕定義的消息。附註：可以進一步為LAPI改進丟棄和拒絕操作。`low-priority-ind-ue` 關鍵字用於丟棄/拒絕操作。

- **low-priority-ind-ue:**這指示SGSN僅在來自UE的消息包括LAPI時，在達到擁塞控制閾值時，拒絕/丟棄定義的消息。

新呼叫策略

這指定在發生擁塞時丟棄或拒絕任何新呼叫消息。新呼叫（連線請求或新的SGSN間RAU）的丟棄或拒絕操作可以細化為基於LAPI或APN，或兩者兼有。以下是CLI語法：

```
new-call-policy { drop | reject } [ apn-based ] [ low-priority-ind-ue ]
```

以下是關於此語法的一些註解：

- **消息型別/呼叫事件:**定義新的呼叫策略時，將針對所有*attach*請求或SGSN間RAU。因此，此CLI命令不需要消息/呼叫事件型別。
- **動作:**這定義了在達到擁塞控制閾值時，SGSN在活動呼叫期間收到上述消息時要完成的操作。

Drop:這指示SGSN在達到擁塞控制閾值時丟棄新呼叫消息。

拒絕:這指示SGSN在達到擁塞控制閾值時拒絕新的呼叫消息。**附註：**丟棄和拒絕操作可以進一步針對基於LAPI和APN進行最佳化。**low-priority-ind-ue**和**apn-based**關鍵字與drop/reject操作一起使用。

- **low-priority-ind-ue:**這指示SGSN僅在來自UE的消息包括LAPI時，在達到擁塞控制閾值時，拒絕/丟棄定義的消息。
- **基於apn的:**這指示SGSN在達到擁塞控制閾值時基於APN拒絕/丟棄新呼叫消息。僅當在運營商策略下配置了具有擁塞控制的APN時，才會發生這種情況。**附註：**如果擁塞操作配置檔案同時配置了基於LAPI和APN的選項，則只有在兩個條件都匹配時，新的呼叫事件才會被拒絕。

SM消息

這將定義SM消息的策略，例如*active*或*modification*請求。來自SGSN的響應只能為*reject*，並且它可以細化為基於LAPI或APN的響應，或者兩者兼有。以下是CLI語法：

```
sm-messages reject [ apn-based ] [ low-priority-ind-ue ]
```

以下是關於此語法的一些註解：

- **消息型別/呼叫事件:**定義SM消息策略後，該策略將應用於所有*activate*或*modification*請求。因此，此CLI命令中需要消息/呼叫事件型別。
- **動作:**這定義當SGSN收到上述消息並且達到擁塞控制閾值時要完成的操作。*reject*操作指示SGSN在達到擁塞控制閾值時拒絕SM消息。**附註：**針對基於LAPI和APN的拒絕操作可以進一步改進。**low-priority-ind-ue**和**apn-based**關鍵字與drop/reject操作一起使用。
- **low-priority-ind-ue:**這指示SGSN僅在達到擁塞控制閾值時來自UE的消息包括LAPI時才拒絕SM消息。
- **基於apn的:**這指示SGSN在達到擁塞控制閾值時基於APN拒絕SM消息。僅當在運營商策略下配置了具有擁塞控制的APN時，才會發生這種情況。**附註：**如果擁塞操作配置檔案同時配置了基於LAPI和APN的選項，則只有在兩個條件都匹配的情況下才會拒絕新的呼叫事件。

擁塞控制閾值

擁塞控制閾值定義了在超出閾值時可以呼叫擁塞控制的各種引數的閾值。以下是CLI語法：

```

congestion-control threshold { license-utilization percent |
max-sessions-per-service-utilization <percent> | message-queue-utilization <percent>
| message-queue-wait-time <time> | port-rx-utilization <percent> | port-specific
{ <slot/port> | all } [ tx-utilization <percent> ] [ rx-utilization <percent> ]
port-specific-rx-utilization critical | port-specific-tx-utilization critical |
port-tx-utilization <percent> | service-control-cpu-utilization

| system-cpu-utilization <percent> | system-memory-utilization <percent>
| tolerance <percent> }

```

以下是可以使用閾值進行配置，並在達到閾值時觸發擁塞控制的不同引數：

- **許可證利用率**:此引數定義許可容量的利用率百分比，以十秒為單位進行測量。此值的格式為百分比，範圍可以從零到100（預設值是100）。
- **max-sessions-per-service-utilization**:此引數定義每個服務所允許的最大會話的利用率百分比，以即時測量值。此閾值基於最大會話數或為特定服務配置的PDP上下文。此值的範圍介於0和100之間，預設值為80。
- **message-queue-utilization**:此引數定義DEMUX管理器軟體任務消息隊列的利用率百分比（以十秒為間隔）。此隊列能夠儲存10,000條消息。此值的範圍介於0和100之間，預設值為80。
- **message-queue-wait-time**:此引數定義消息可以保留在隊列中的最長時間（秒），由資料包時間戳度量。此值的範圍介於1到30秒之間，預設值為5秒。
- **port-rx-utilization**:此引數定義按接收的資料（以五分鐘為間隔）計算的所有埠的埠資源平均利用率百分比。此值的範圍介於0和100之間，預設值為80。可以使用no命令禁用此閾值引數。
- **埠特定**:此引數定義埠特定的閾值。當達到任何單個埠特定的閾值時，擁塞控制會在系統範圍內應用。每個特定連線埠號碼或可以使用all關鍵字的所有連線埠預設都會停用此選項。此引數有兩個可定義的子選項：
 - rx利用率**:此選項的預設值為80%。它按接收資料度量特定埠的埠資源平均利用率百分比，以五分鐘為間隔度量。這些值的範圍為0到100。
 - tx-utilization**:此選項的預設值為80%。它通過傳輸的資料測量特定埠的埠資源平均利用率百分比，以五分鐘為間隔測量。值範圍在1到100之間。
- **port-tx-utilization**:此引數定義按傳輸資料列出的所有埠的埠資源平均利用率百分比，以五分鐘為間隔進行測量。此值的範圍介於0和100之間，預設值為80。可以通過no版本的此命令禁用此閾值引數。
- **service-control-cpu-utilization**:此引數定義運行DEMUX管理器軟體任務例項的CPU的平均利用率百分比（以十秒為間隔）。此值的範圍介於0和100之間，預設值為80。
- **system-cpu-utilization**:此引數定義系統可用的所有PSC/PSC2 CPU的平均利用率百分比，以十秒為間隔測量。此值的範圍介於0和100之間，預設值為80。可以使用no congestion-control threshold system-cpu-utilization CLI命令禁用此值。
- **system-memory-utilization**:此引數定義系統可用的所有CPU記憶體的平均利用率百分比，以十

秒為單位進行測量。此值的範圍介於0和100之間，預設值為80。

- **容差:**此引數定義指定條件被清除的點的已配置閾值下的百分比。此值的範圍介於0和100之間，預設值為10。例如，如果閾值配置為90，並且觸發了擁塞控制，則如果定義了容差的預設值10，則在80處清除觸發器。

MME和SGSN的擁塞控制閾值

本節定義了三種不同觸發器和擁塞控制配置檔案時MME和SGSN的閾值配置。

此資訊適用於MME版本14.0及更高版本，以及SGSN版本17.0及更高版本。以下是MME和SGSN可用的三種不同級別的觸發器，它們進一步與相應的擁塞控制策略相關聯：

- **重要:**此觸發級別定義了不同引數的嚴重閾值。此觸發級別的值在所有三個閾值級別中應該是最大的。臨界閾值包括預配置的預設值。
- **主要:**此觸發器級別定義不同觸發器的主要閾值。此觸發級別的值應大於次閾值並小於嚴重閾值。預設值為零。
- **輕微:**此觸發器級別定義不同觸發器的次要閾值。此觸發器的值應至少位於所有三個閾值之間。預設值為零。

可為上一節中提到的所有引數/觸發器定義三個閾值。以下是用於定義不同引數閾值的CLI語法：

```
congestion-control threshold license-utilization { critical <percent> | major <percent> | minor <percent> }
```

```
congestion-control threshold max-sessions-per-service-utilization { critical <percent> | major <percent> | minor <percent> }
```

```
congestion-control threshold message-queue-utilization { critical <percent> | major <percent> | minor <percent> }
```

```
congestion-control threshold message-queue-wait-time { critical <time> | major <time> | minor <time> }
```

```
congestion-control threshold port-rx-utilization { critical | major | minor }
```

```
congestion-control threshold port-specific { [ tx-utilization { critical | major | minor } [ rx-utilization { critical | major | minor } ] | all { critical | major | minor } }
```

```
congestion-control threshold port-tx-utilization { critical <percent> | major <percent> | minor <percent> }
```

```
congestion-control threshold service-control-cpu-utilization { critical | major | minor }
```

```
congestion-control threshold system-cpu-utilization { critical <percent> | major <percent> | minor <percent> }
```

```
congestion-control threshold system-memory-utilization { critical | major | minor }
```

```
congestion-control threshold tolerance { critical <percent> | major
<percent> | minor <percent> }
```

附註：不同引數(`license-utilization`除外)的關鍵閾值使用的預設值與上一節中描述的相同。`license-utilization`引數將關鍵配置檔案的預設值設為80%。

驗證

使用本節中介紹的資訊驗證您的擁塞控制配置。

擁塞控制組態驗證

輸入`show congestion-control configuration` |更多CLI命令，以驗證擁塞控制的設定。以下各節提供了擁塞控制各個階段的示例命令輸出。

啟用前的擁塞控制

```
[local]st40-sim# show congestion-control configuration | more
Congestion-control: disabled
.....
```

啟用後的擁塞控制

```
[local]st40-sim# configure
[local]st40-sim(config)# congestion-control
[local]st40-sim(config)# end
[local]st40-sim# show congestion-control configuration | more
Congestion-control: enabled
.....
```

過載斷開連線啟用後的擁塞控制

```
[local]st40-sim# configure
[local]st40-sim(config)# congestion-control overload-disconnect
[local]st40-sim(config)# end
[local]st40-sim# show congestion-control configuration | more
Congestion-control: enabled
.....
```

Overload-disconnect: enabled

```
Overload-disconnect threshold parameters
license utilization:                80%
max-session-per-service utilization: 80%
tolerance:                          10%
session disconnect percent:         5%
iterations-per-stage:               8
.....
```

啟用除SGSN和MME以外的策略後的擁塞控制

`congestion-control policy <service-name> action <action>` 引數的配置根據配置更改 `congestion control policy` 部分的值。以下是 `ggsn-service` 的操作丟棄配置示例：

```
[local]st40-sim(config)# congestion-control policy ggsn-service action drop
[local]st40-sim(config)# end
[local]st40-sim# show congestion-control configuration | more
Congestion-control: enabled
.....

Congestion-control Policy
pdsn-service: none
hsgw-service: none
ha-service: none
ggsn-service: drop
closedrps-service: none
.....
```

主要和次要配置檔案的擁塞控制閾值

本節介紹主要和次要配置檔案的擁塞控制閾值配置驗證。關鍵配置檔案已具有一些預設值，可以根據需要進行更改，但需要配置主要和次要閾值。這三個配置檔案以後可以與擁塞控制策略一起使用。

o

```
[local]st40-sim# configure
[local]st40-sim(config)# congestion-control threshold license-utilization major 70
[local]st40-sim(config)# congestion-control threshold license-utilization minor 60
[local]st40-sim(config)# congestion-control threshold
max-sessions-per-service-utilization major 70
[local]st40-sim(config)# congestion-control threshold
max-sessions-per-service-utilization minor 60
[local]st40-sim(config)# congestion-control threshold mes
message-queue-utilization message-queue-wait-time
[local]st40-sim(config)# congestion-control threshold
message-queue-utilization major 70
[local]st40-sim(config)# congestion-control threshold
message-queue-utilization minor 60
[local]st40-sim(config)# congestion-control threshold message-queue-wait-time major 4
[local]st40-sim(config)# congestion-control threshold message-queue-wait-time minor 3
[local]st40-sim(config)# congestion-control threshold port-rx-utilization major 70
[local]st40-sim(config)# congestion-control threshold port-rx-utilization minor 60
[local]st40-sim(config)# congestion-control threshold port-tx-utilization major 70
[local]st40-sim(config)# congestion-control threshold port-tx-utilization minor 60
[local]st40-sim(config)# congestion-control threshold
service-control-cpu-utilization major 70
[local]st40-sim(config)# congestion-control threshold
service-control-cpu-utilization minor 60
[local]st40-sim(config)# congestion-control threshold syst
system-cpu-utilization system-memory-utilization
[local]st40-sim(config)# congestion-control threshold system-cpu-utilization major 70
[local]st40-sim(config)# congestion-control threshold system-cpu-utilization minor 60
[local]st40-sim(config)# congestion-control threshold
system-memory-utilization major 70
[local]st40-sim(config)# congestion-control threshold
system-memory-utilization minor 60
[local]st40-sim(config)# congestion-control threshold tolerance major 5
[local]st40-sim(config)# congestion-control threshold tolerance minor 2
```

```
[local]st40-sim(config)# end
[local]st40-sim# show congestion-control configuration | more
Congestion-control: enabled
```

Congestion-control Critical threshold parameters

```
system cpu utilization:          80%
service control cpu utilization: 80%
system memory utilization:       80%
message queue utilization:       80%
message queue wait time:        5 seconds
port rx utilization:             80%
port tx utilization:             80%
license utilization:             100%
max-session-per-service utilization: 80%
tolerance limit:                10%
```

Congestion-control Major threshold parameters

```
system cpu utilization:          70%
service control cpu utilization: 70%
system memory utilization:       70%
message queue utilization:       70%
message queue wait time:        4 seconds
port rx utilization:             70%
port tx utilization:             70%
license utilization:             70%
max-session-per-service utilization: 70%
tolerance limit:                5%
```

Congestion-control Minor threshold parameters

```
system cpu utilization:          60%
service control cpu utilization: 60%
system memory utilization:       60%
message queue utilization:       60%
message queue wait time:        3 seconds
port rx utilization:             60%
port tx utilization:             60%
license utilization:             60%
max-session-per-service utilization: 60%
tolerance limit:                2%
```

Overload-disconnect: enabled

Overload-disconnect threshold parameters

```
license utilization:          80%
max-session-per-service utilization: 80%
tolerance:                   10%
session disconnect percent:   5%
iterations-per-stage:        8
```

.....

針對SGSN的擁塞控制策略啟用

使用以下資訊驗證SGSN的擁塞控制策略啟用：

```
[local]st40-sim# configure
[local]st40-sim(config)# sgsn-global
[local]st40-sim(config-sgsn-global)# congestion-control
[local]st40-sim(config-congestion-ctrl)# end
[local]st40-sim# configure
[local]st40-sim(config)# congestion-control
[local]st40-sim(config)# end
```

```

[local]st40-sim# configure
[local]st40-sim(config)# sgsn-global
[local]st40-sim(config-sgsn-global)# congestion-control
[local]st40-sim(config-congestion-ctrl)# congestion-action-profile sgsn_critical
[local]st40-sim(config-cong-act-prof-sgsn_critical)# active-call-policy rau reject
[local]st40-sim(config-cong-act-prof-sgsn_critical)# active-call-policy
service-req reject
[local]st40-sim(config-cong-act-prof-sgsn_critical)# new-call-policy reject
[local]st40-sim(config-cong-act-prof-sgsn_critical)# sm-messages reject
[local]st40-sim(config-cong-act-prof-sgsn_critical)# exit
[local]st40-sim(config-congestion-ctrl)# congestion-action-profile sgsn_major
[local]st40-sim(config-cong-act-prof-sgsn_major)# active-call-policy rau drop
[local]st40-sim(config-cong-act-prof-sgsn_major)# active-call-policy
service-req drop
[local]st40-sim(config-cong-act-prof-sgsn_major)# new-call-policy drop
[local]st40-sim(config-cong-act-prof-sgsn_major)# sm-messages reject
low-priority-ind-ue
[local]st40-sim(config-cong-act-prof-sgsn_major)# exit
[local]st40-sim(config-congestion-ctrl)# congestion-action-profile sgsn_minor
[local]st40-sim(config-cong-act-prof-sgsn_minor)# exit
[local]st40-sim(config-congestion-ctrl)# exit
[local]st40-sim(config-sgsn-global)# exit
[local]st40-sim(config)# congestion-control policy critical sgsn-service
action-profile sgsn_critical
[local]st40-sim(config)# congestion-control policy major sgsn-service
action-profile sgsn_major
[local]st40-sim(config)# congestion-control policy minor sgsn-service
action-profile sgsn_minor
[local]st40-sim(config)#end

```

```

[local]st40-sim# show congestion-control configuration | more

```

```

Congestion-control: enabled

```

```

.....

```

```

pdsn-service: none
hsgw-service: none
ha-service: none
ggsn-service: drop
closedrp-service: none
lms-service: none
cscf-service: reject
pdif-service: none
wsg-service: none
pdg-service: none
epdg-service: none
fng-service: none

```

sgsn-service:

```

Critical Action-profile : sgsn_critical
Major Action-profile : sgsn_major
Minor Action-profile : sgsn_minor

```

```

.....

```

針對MME的擁塞控制策略啟用

使用以下資訊驗證為MME啟用的擁塞控制策略：

```

[local]st40-sim# configure
[local]st40-sim(config)# lte-policy
[local]st40-sim(lte-policy)# congestion-action-profile mme_critical
Are you sure? [Yes|No]: yes
[local]st40-sim(congestion-action-profile)# drop addn-brr-requests

```

```

[local]st40-sim(congestion-action-profile)# drop s1-setup
[local]st40-sim(congestion-action-profile)# exit
[local]st40-sim(lte-policy)# congestion-action-profile mme_major
Are you sure? [Yes|No]: yes
[local]st40-sim(congestion-action-profile)# reject addn-brr-requests
[local]st40-sim(congestion-action-profile)# reject s1-setup time-to-wait 20
[local]st40-sim(congestion-action-profile)# exit
[local]st40-sim(lte-policy)# congestion-action-profile mme_minor
Are you sure? [Yes|No]: yes
[local]st40-sim(congestion-action-profile)# none addn-brr-requests
[local]st40-sim(congestion-action-profile)# none s1-setup
[local]st40-sim(congestion-action-profile)# exit
[local]st40-sim(lte-policy)# exit
[local]st40-sim(config)# congestion-control policy critical mme-service
action-profile mme_critical
[local]st40-sim(config)# congestion-control policy major mme-service
action-profile mme_major
[local]st40-sim(config)# congestion-control policy minor mme-service
action-profile mme_minor
[local]st40-sim(config)# end

```

```

[local]st40-sim# show congestion-control configuration | more

```

```

Congestion-control: enabled

```

```

.....

```

```

pdsn-service: none
hsgw-service: none
ha-service: none
ggsn-service: drop
closedrps-service: none
lms-service: none
cscf-service: reject
pdif-service: none
wsg-service: none
pdg-service: none
epdg-service: none
fng-service: none
sgsn-service:
  Critical Action-profile : sgsn_critical
  Major Action-profile : sgsn_major
  Minor Action-profile : sgsn_minor
mme-service:
  Critical Action-profile : mme_critical
  Major Action-profile : mme_major
  Minor Action-profile : mme_minor

```

```

.....

```

擁塞控制統計資訊

以下命令用於檢視與擁塞控制相關的統計資訊和狀態：

```

show congestion-control { configuration | statistics { <manager> [ all | instance
<task_instance> ] } [ | { grep <grep_options> | more } ]

```

```

show congestion-control statistics mme { critical | full | major | minor } [ | {
grep <grep_options> | more } ]

```

<manager>選項可以具有以下值：

- **A11mgr**:這是PDSN服務。

- **asngwmgr**:這是接入服務網路網關(ASN-GW)服務。
- **asnpcmgr**:這是ASN尋呼控制(PC-LR)服務。
- **bindmux**:這是PCC服務使用的Bindmux管理器。
- **egtpinmgr**:這是增強型GPRS通道通訊協定(EGTP)輸入DEMUX管理員。
- **gtpcmgr**:這是GGSN服務。
- **hamgr**:這是用於HA服務。
- **hnbmgr**:這是HNB-GW服務使用的家庭節點B(HNB)管理器。
- **imsimgr**:這是用於SGSN的IMSI管理器。
- **ipsecmgr**:這是IP安全(IPSec)管理員。
- **ipsgmgr**:此清單適用於IP服務閘道(IPSG)管理員。
- **l2tpmgr**:此指令用於第2層(L2)通道通訊協定(L2TP)管理員。

OAM干預的SGSN擁塞控制觸發機制

sgsn trigger-congestion level { critical |主要 | minor }命令用於在SGSN中手動觸發擁塞控制。**sgsn clear-congestion**命令用於清除由**sgsn trigger-congestion**命令啟動的擁塞。

以下是輸出範例：

```
[local]st40-sim# sgsn trigger-congestion level critical
[local]st40-sim# show congestion-control statistics imsimgr all full | more
Current congestion status:                               Cleared
Current congestion Type  :                               None
Congestion applied:                                       0 times
Critical Congestion Control Resource Limits
system cpu use exceeded:                                  No
service cpu use exceeded:                                 No
system memory use exceeded:                              No
port rx use exceeded:                                    No
port tx use exceeded:                                    No
port specific rx use exceeded:                           No
port specific tx use exceeded:                           No
max sess use exceeded:                                   No
license use exceeded:                                    No
msg queue size use exceeded:                             No
msg queue wait time exceeded:                            No
license threshold exceeded:                              No
max sess threshold exceeded:                             No
Sessions disconnected due to overload disconnect:         0

Major Congestion Control Resource Limits
system cpu use exceeded:                                  No
service cpu use exceeded:                                 No
```

system memory use exceeded:	No
port rx use exceeded:	No
port tx use exceeded:	No
port specific rx use exceeded:	No
port specific tx use exceeded:	No
max sess use exceeded:	No
license use exceeded:	No
msg queue size use exceeded:	No
msg queue wait time exceeded:	No

Minor Congestion Control Resource Limits

system cpu use exceeded:	No
service cpu use exceeded:	No
system memory use exceeded:	No
port rx use exceeded:	No
port tx use exceeded:	No
port specific rx use exceeded:	No
port specific tx use exceeded:	No
max sess use exceeded:	No
license use exceeded:	No
msg queue size use exceeded:	No
msg queue wait time exceeded:	No

SGSN Congestion Control:

MM Congestion Level:	Critical
Congestion Resource:	None
SM Congestion Level:	Critical
O&M Congestion Level:	Critical

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [3GPP TS 23.401](#)
- [3GPP TS 23.060](#)
- [3GPP TS 25.413](#)
- [3GPP TS 36.413](#)
- [命令列介面參考, StarOS版本17](#)
- [技術支援與文件 - Cisco Systems](#)