Konfigurieren des Überlastungskontrollmechanismus auf dem ASR 5X00

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Überlastungskontrollmechanismus auf dem Cisco Aggregated Services Router (ASR) der Serie 5x00 konfiguriert wird. Die in diesem Dokument beschriebene Überlastungskontrollfunktion wird hauptsächlich auf die Netzwerkfunktionen des Serving General Packet Radio Service (GPRS) Support Node (SGSN) und der Mobility Management Entity (MME) angewendet.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Übersicht über die Überlastungskontrolle

Manchmal kann im Netzwerk eine übermäßige Last beobachtet werden, die zu Lizenzverletzungen, hoher CPU-Auslastung, hoher Port-Auslastung oder hoher Speichernutzung führen kann. Dies kann zu Leistungseinbußen auf dem Knoten führen, der sich unter starker Auslastung befindet. Diese Bedingungen sind jedoch in der Regel temporär und werden schnell behoben. Die Überlastungskontrolle dient dazu, die Identifizierung solcher Bedingungen zu erleichtern und die Richtlinien anzuwenden, die die Situation berücksichtigen, wenn diese hohen Belastungsbedingungen fortbestehen oder eine große Anzahl dieser Bedingungen gegeben ist.

In diesem Abschnitt wird der Überlastungskontrollmechanismus im SGSN und im MME gemäß dem 3rd Generation Partnership Project (3GPP) beschrieben.

MME/SGSN-Überlastungskontrolle

Die MME bietet einen Überlastungskontrollmechanismus auf NAS-Ebene (Non-Access Startum), der auf der Kontrolle von Access Point Name (APN) oder General NAS-Level Mobility Management (MM) basiert.

Die APN-basierten Überlastungssteuerungsmechanismen können die Evolved Packet System (EPS) Session Management (ESM)- und EPS Mobility Management (EMM)-Signalisierung verarbeiten, die mit der Benutzerausrüstung (UE) verknüpft ist, die über ein bestimmtes APN und ein bestimmtes UE verfügt. Das Netzwerk sollte diese Überlastungskontrollfunktion unterstützen. Die MME erkennt die dem APN zugeordnete Überlastungskontrolle auf NAS-Ebene und startet und stoppt die APN-basierte Überlastungskontrolle gemäß den folgenden Kriterien:

- Maximale Anzahl aktiver EPS-Träger pro APN
- Maximale Anzahl von EPS-Trägeraktivierungen pro APN
- Ein oder mehrere Packet Data Network (PDN) Gateways (PGWs) auf einem APN sind nicht erreichbar oder weisen auf eine Überlastung der MME hin
- Die maximale Anzahl von MM-Signalisierungsanfragen ist den Geräten mit dem Abonnement für eine bestimmte APN zugeordnet.
- Netzwerkverwaltungseinstellungen

  Hinweis: Die MME sollte keine Überlastungskontrolle für Zugang mit hoher Priorität und Notdienste anwenden. Allgemeine MM-Steuerung auf NAS-Ebene kann verwendet werden, um Signalisierungsanforderungen auf NAS-Ebene MM unter einem allgemeinen Überlastungszustand abzulehnen.

APN-basierte Sitzungsmanagement-Überlastungskontrolle

Die APN-basierte Sitzungsmanagement-Überlastungssteuerung kann aufgrund einer Überlastungssituation, durch OAM oder durch Neustart/Wiederherstellung eines PGW auf dem MME aktiviert werden. Die MME kann ESM-Anfragen von der UE ablehnen, die in die Anforderungen für PDN-Verbindungen, Träger-Ressourcenzuweisung oder Träger-Ressourcenmodifizierung einbezogen werden können. Die MME kann auch die aktuelle PDN-Verbindung bei Überlastungen deaktivieren und einen Sitzungs-Back-off-Timer an die UE senden. Wenn dieser Timer enthalten ist, sollte die *Reaktivierungsanfrage* nicht aktiviert werden.

Die MME kann während einer Überlastung den Sitzungsverwaltungs-(SM-)Sicherungs-Timer für ein bestimmtes UE und APN speichern und nachfolgende SM-Nachrichten von der UE, die für dieses APN vorgesehen sind, sofort ablehnen, bis der Zeitgeber abgelaufen ist. Dies ist für UEs erforderlich, die den SM-Back-Off-Timer nicht unterstützen (für UE-Versionen vor Version 10). Die MME löscht diesen Timer zunächst, wenn sie eine SM-Nachricht an die UE senden möchte, für die der Timer bereits ausgeführt wird.

Während der Ausführung des Timers kann die EU folgende Aktionen durchführen:

- Wenn das APN in der abgelehnten EPS SM-Anforderungsnachricht bereitgestellt wird oder

der SM-Sicherungs-Timer im NAS empfangen wird, um die EPS-Trägerkontextanforderungsnachricht zu deaktivieren, sollte die UE kein SM-Verfahren für die überlastete APN initiieren.

- Wenn in der abgelehnten EPS SM-Anforderungsnachricht kein APN angegeben ist, darf die UE keine SM-Anfragen ohne APN initiieren.
- Durch diese Änderungen wird der Zeitgeber für die Backoff-Verarbeitung nicht angehalten:

  Zelle

  Verfolgungsbereich (TA)

  Public Land Mobile Network (PLAMN)

  RAT (Radio Access Technology)

- Die EU darf die SM-Verfahren für Zugriffsdienste mit hoher Priorität und Notdienste auch dann initiieren, wenn der SM-Sicherungs-Timer ausgeführt wird.
- Wenn die UE eine vom Netzwerk initiierte EPS SM-Anforderungsmeldung für das überlastete APN empfängt, während der SM-Sicherungs-Timer ausgeführt wird, beendet die UE den mit diesem APN verknüpften SM-Sicherungs-Timer und antwortet auf die MME.
- Wenn die UE mit der Erlaubnis konfiguriert ist, eine niedrige Zugriffspriorität zu überschreiben, und der SM-Backoff-Timer aufgrund einer Ablehnungsmeldung ausgeführt wird, die als Antwort auf eine Anfrage mit niedriger Zugriffspriorität empfangen wird, können die oberen Schichten in der EU die Einleitung von SM-Prozeduren ohne niedrige Zugriffspriorität anfordern.
- Der UE kann das PDN-Trennungsverfahren initiieren, löscht jedoch nicht den zugehörigen SM-Sicherungs-Timer.
- Der Backoff-Timer verhindert nicht die Datenübertragung durch den UE oder die Initiierung von Serviceanfragen zur Aktivierung des Benutzerebenen-Trägergeräts zum überlasteten APN.

APN-basierte MM-Überlastungskontrolle

Ähnlich wie bei den SM-Prozeduren verfügt die MME auch über einen MM-Sicherungs-Timer und kann die Anfügeprozedur ablehnen. Die MME sollte die Abonnenten-Daten noch eine Zeit lang aufbewahren, nachdem sie das Attach-Verfahren zurückgewiesen hat, sodass die Ablehnung nachfolgender Anfragen für denselben Teilnehmer ohne Interaktion mit dem HSS abgeschlossen werden kann.

Während der Back-off-Timer ausgeführt wird, sollte die UE keine NAS-Anforderung für das MM-Verfahren initiieren, mit Ausnahme des Zugriffs mit hoher Priorität oder von Notdiensten. Die EU kann jedoch Datenverfolgungsbereichsaktualisierungen (Tracking Area Updates, TAUs)

durchführen, wenn sie sich bereits im *verbundenen* Modus befindet.

Die MME sollte einen Back-Off-Timer auswählen, sodass nicht alle UE denselben Wert für diesen Timer haben sollten, und die UEs sollten verzögerte Anfragen gleichzeitig initiieren. Wenn der Mobility Back-off-Timer empfangen wird, ist das UE-Verhalten nicht APN-spezifisch.

Allgemeine Überlastungskontrolle auf NAS-Ebene

Die allgemeine Überlastungskontrolle auf NAS-Ebene ist bei allgemeinen Überlastungsbedingungen hilfreich. Er funktioniert ähnlich wie die APN-basierte Überlastungssteuerung und hat ein ähnliches Konzept für den Back-Off-Timer. Wenn der Back-Off-Timer ausgeführt wird, kann die EU Abfindungsanfragen, Anfragen mit hoher Priorität und TAUs (im *Connected* Mode) initiieren.

Der Back-off-Timer wird auch dann ausgeführt, wenn die UE vom Netzwerk getrennt wurden. Die MME sollte den Back-Off-Timer beenden, wenn die MME die UE, für die der Back-Off-Timer bereits ausgeführt wird, aufrufen möchte, und die UE sollte den Back-Off-Timer beenden, nachdem sie die Paging-Anfrage von der MME erhalten hat, und die Service-Anfrage initiieren.

Der MM-Sicherungs-Timer hat keine Auswirkungen auf die Zellen-/RAT- und PLMN-Änderung. Die TA-Änderung beendet diesen Timer nicht. Dieser Timer wird beendet, wenn eine neue PLMN ausgewählt wird, die nicht der PLMN entspricht.

Wenn die EU einen Übergabebefehl erhält, sollte sie unabhängig vom Status des Zeitgebers weitergeben.

Wenn die MME die TAU-Anforderung oder die Service-Anfrage mit einem MM-Sicherungs-Timer zurückweist, der größer ist als die Summe des UE-Zeitgebers für regelmäßige TAU und des Timers für implizite Detach, sollte die MME den erreichbaren Zeitgeber für Mobilgeräte und/oder den Timer für implizite Detach so anpassen, dass die MME die UE beim Ausführen des MM-Sicherungs-Timers nicht implizit trennt.

> **Hinweis**: Die Überlastungskontrolle des SGSN funktioniert auch auf ähnliche Weise wie die der MME. Weitere Einzelheiten zum SGSN-Überlastungskontrollmechanismus finden Sie unter 3GPP TS 23.060 und unter 3GPP TS 23.401 für weitere Informationen zum MME-Überlastungskontrollmechanismus.

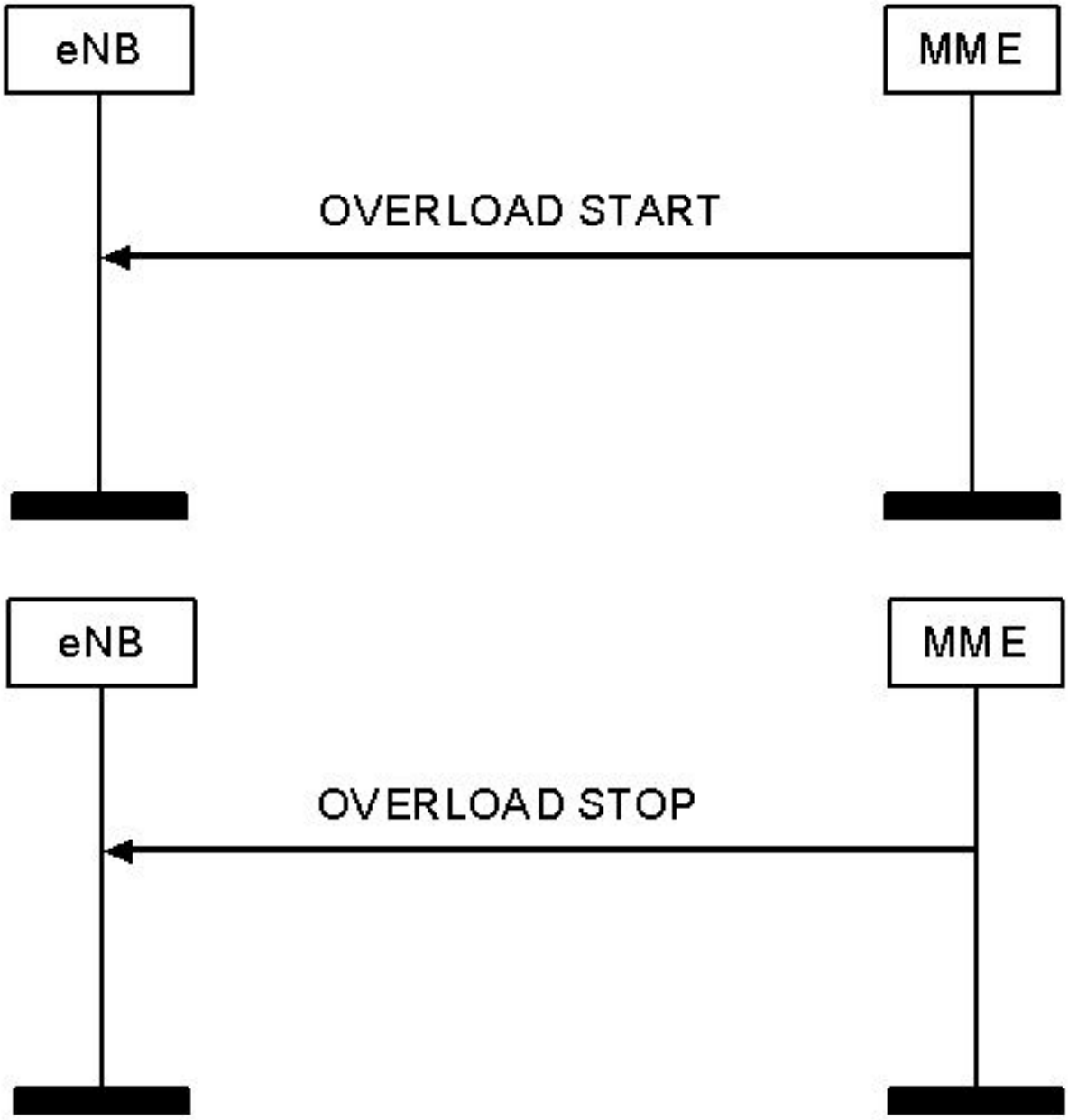
Reduzierung der Überlastung durch MME auf S1-MME-Schnittstelle

Die MME kann eine *Overload Start*-Nachricht an den E-NodeB (eNB) senden, um die Signalisierungslast zu reduzieren. Bei diesem Verfahren wird eine nicht mit UE verknüpfte Signalisierung verwendet. Das Overload Action Information Element (IE) verfügt über einen Overload Response IE in der Overload Start-Nachricht, die Informationen über Ablehnungskriterien enthält, und der eNB ergreift entsprechende Maßnahmen.

> **Tipp**: Weitere Informationen finden Sie in den 3GPP Technical Specifications (TS) 36.413.

Um das Ende der Überlastungssituation anzuzeigen, sendet die MME eine Overload Stopp-

Meldung an eNB:



Hinweis: Das SGSN verfügt ebenfalls über einen ähnlichen Mechanismus zur Signalreduktion, der in 3GPP TS 25.413 erwähnt wird.

PGW-Kontrolle der Überlastung

Der PGW kann eine PDN-Verbindung in Überlastungsszenarien ablehnen. Das PGW kann eine Überlastungsbedingung erkennen und die Überlastungssteuerung anhand folgender Kriterien starten oder beenden:

- Die maximale Anzahl aktiver Träger pro APN
- Die maximale Anzahl an Trägeraktivierungen pro APN

Das PGW kann für einen bestimmten APN einen PGW-Back-Off-Timer für die MME angeben, und die MME sollte die PDN-Verbindungsanforderungen für diesen APN während dieses Zeitraums

ablehnen. Die MME kann in diesem Zeitraum statt der Ablehnung einen anderen PGW auswählen, es sei denn, es besteht bereits eine aktuelle PDN-Verbindung mit demselben APN für diesen UE-Zeitraum.

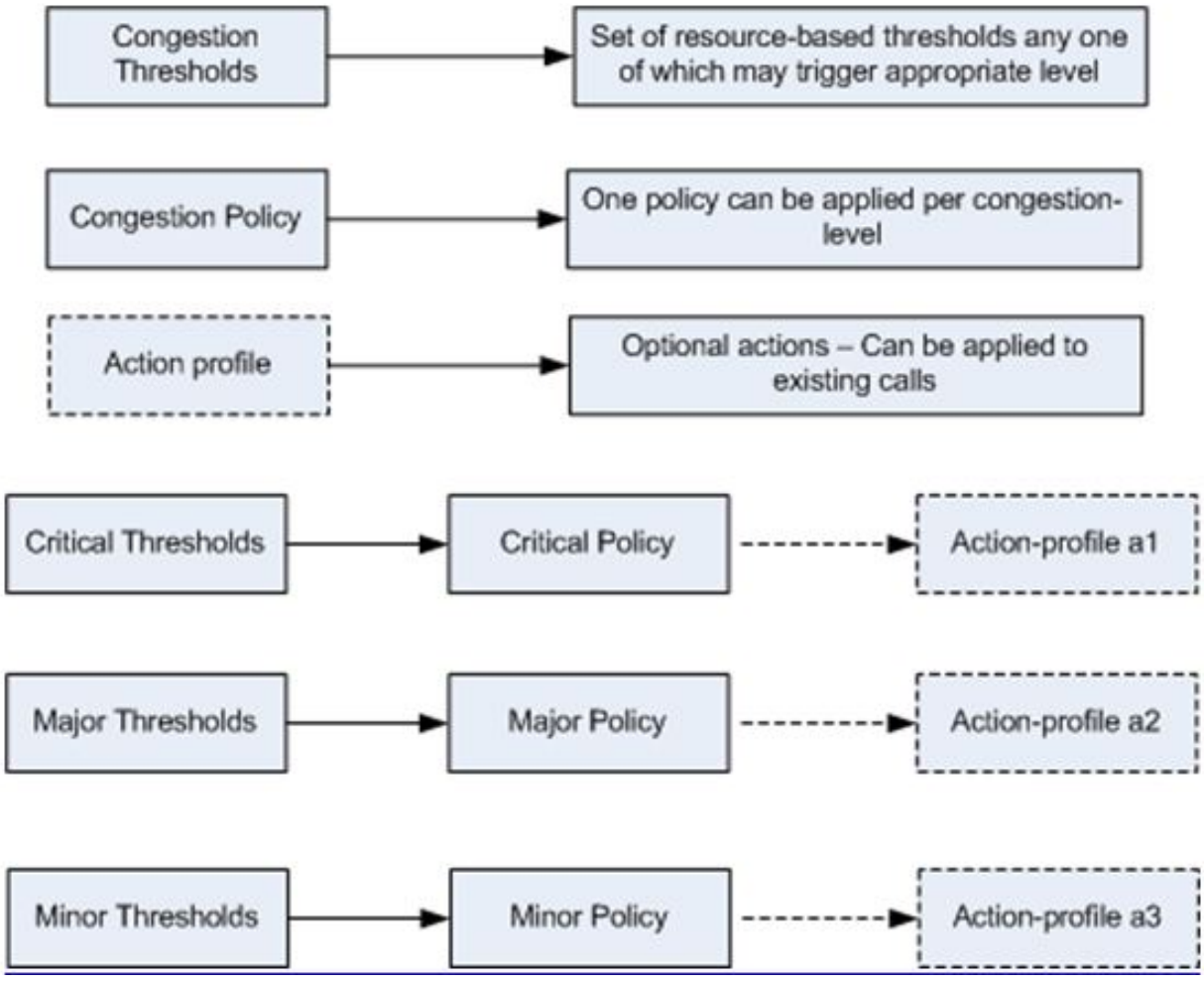
> **Hinweis**: Der GGSN-Überlastungssteuerungsmechanismus ähnelt dem auf dem PGW, der in 3GPP TS 23.060 erwähnt wird. Der PGW-Überlastungssteuerungsmechanismus wird im 3GPP TS 23.401 erwähnt.

Überlastungsverwaltung auf dem ASR 5x00

Die Überlastungskontrolle basiert auf der Konfiguration der folgenden zusätzlichen Funktionen:

- Anruftrennung bei Überlastung
- Grenzwerte für Überlastungskontrolle
- Richtlinien für Service-Überlastung

Hier ein Beispiel:



Anruftrennung bei Überlastung

Mit dieser Funktion kann das System die Richtlinie für die Trennung passiver Anrufe (Chassis-weit) während einer Überlastungssituation aktivieren oder deaktivieren. Außerdem können Sie die Richtlinie für die Überlastungsverteilung optimieren.

Grenzwerte für Überlastungsbedingungen

Es können verschiedene Grenzwerte für die Überlastungskontrolle festgelegt werden, die die Bedingungen vorgeben, unter denen die Überlastungskontrolle aktiviert werden soll. Außerdem werden die Grenzwerte für die Definition des Systemzustands festgelegt, der überlastet oder gelöscht wird. Wenn diese Schwellenwerte erreicht werden, wird nicht nur ein Simple Network Management Protocol (SNMP)-Trap (Überlastung) generiert, sondern auch eine Überlastungsrichtlinie aufgerufen.

Eine Schwellenwerttoleranz wird verwendet, um den Prozentsatz unter dem konfigurierten Grenzwert festzulegen, der erreicht werden muss, bevor eine Bedingung als gelöscht gilt und ein SNMP-Trap (CongestionClear) ausgelöst wird.

Richtlinien für Service-Überlastungen

Die Richtlinien für Überlastungsdienste sind für jeden Service konfigurierbar, z. B. Packet Data Serving Node (PDSN), Gateway GPRS Support Node (GGSN) und Serving GPRS Support Node (SGSN). Diese Richtlinien bestimmen die Art und Weise, wie die Services reagieren, wenn eine Überlastung im System aufgrund einer Überlastungsschwellenwertüberschreitung festgestellt wird.

Konfigurieren

In diesem Abschnitt werden die Konfigurationen beschrieben, die erforderlich sind, um die Überlastungskontrolle zu aktivieren und die grundlegende Optimierung der Überlastungskontrolle zu ermöglichen.

Überlastungskontrolle aktivieren

Die Überlastungskontrolle ist im Chassis standardmäßig deaktiviert. Geben Sie den Befehl **Congestion-control** im *globalen Konfigurationsmodus ein*, um Folgendes zu aktivieren:

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

Überlastungskontrolle Trennung

Die Überlastungsverwaltung aktiviert oder deaktiviert die Richtlinie zum Trennen der Verbindung der passiven Anrufe im Chassis während einer Überlastungssituation. Dies ist standardmäßig deaktiviert. Sie ermöglicht die Trennung der passiven Anrufe in Phasen und Iterationen vom Chassis, bis die Überlastungssteuerung beseitigt ist. Der Grenzwert für die *Lizenzauslastung* und die *Nutzung* pro *Service* kann zusammen mit dem Schwellenwert konfiguriert werden.

Wenn der Grenzwert beispielsweise mit einem Wert von 90 % und einer Toleranz von 5 %

konfiguriert ist, beendet das System die passive Anruftrennung, wenn die Anzahl der Anrufe unter 85 % der insgesamt zulässigen Anrufe für diesen Dienst fällt.

Die folgende CLI-Syntax kann verwendet werden, um die Überlastungskontrolle zu aktivieren, die immer im *globalen Konfigurationsmodus* konfiguriert wird:

```
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> } ]
```

Hier einige Hinweise zu dieser Syntax:

- Iterationen pro Phase: Dieser Parameter definiert die Anzahl der Anrufe, die während der festgelegten Anzahl von Sekunden getrennt werden sollen. Dieser Wert kann zwischen zwei und acht liegen.

- Prozent: Dieser Parameter gibt den Prozentsatz der Anrufe an, die während einer Überlastungssituation schrittweise getrennt werden sollen. Dieser Wert kann zwischen 0 und 100 liegen, wobei fünf als Standardwert verwendet werden.

- Grenzwert: Dieser Parameter definiert die Schwellenwerte für die Lizenz und die maximale Sitzungsauslastung. Sie ermöglicht auch eine Definition des Toleranzwerts.

  Lizenznutzung: Dieser Parameter gibt den Grenzwert für den Prozentsatz der Lizenzauslastung bei Überlastungen an. Bei einem Trigger wird die Verbindung der passiven Anrufe getrennt. Dieser Wert liegt zwischen einhundert und 80 als Standardwert.

  Max. Nutzung von Sitzungen pro Service: Gibt den Prozentsatz der max. Sitzungen pro Servicenutzungsschwellenwert an. Wenn der festgelegte Wert überschritten wird, trennt das System die passiven Anrufe. Dieser Wert liegt zwischen einhundert und 80 als Standardwert.

  Toleranz: Dieser Wert definiert den Prozentsatz der Anrufe, die das System unter den definierten Werten für die *Lizenzauslastung* und *die maximale Nutzung pro Sitzung* trennt. Dieser Wert liegt zwischen 1 und 25, der Standardwert beträgt zehn. Eine klare Trap-Meldung wird nur gesendet, wenn die Auslastung unter die festgelegten Toleranzwerte fällt.

Konfiguration der Richtlinie zur Überlastungskontrolle

Sie können die Richtlinie zur Überlastungskontrolle auf Dienstbasis konfigurieren. Die Richtlinie kann dazu führen, dass das System bei neuen Sitzungen Aktionen wie "Drop", "none", "Redirect" und "Ablehnen" durchführt, wenn eine der festgelegten Grenzwerte für die Überlastungskontrolle überschritten wird, wodurch die Überlastungskontrolle aktiviert wird.

Diese Konfiguration ermöglicht eine präzisere Definition der Richtlinie zur Überlastungskontrolle für den MME- und SGSN-Service und die Konfiguration verschiedener Phasen der Überlastungskontrolle, z. B. kritisch, schwerwiegend und gering (zusammen mit der Zuordnung von Aktionsprofilen).

Richtlinie zur Überlastungskontrolle

Die CLI-Syntax der Richtlinie zur Konfiguration der Überlastungskontrolle (mit Ausnahme von MME-Diensten) lautet wie folgt:

```
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 |
pdsnclosedrp-service | pgw-service | phsgw-service | phspc-service | saegw-service
| sgsn-service | sgw-service | wsg-service } action { drop | none | redirect |
reject }
```

Hier einige Hinweise zu dieser Syntax:

- **Servicetyp**: Dieser Parameter definiert den Dienstnamen, für den die Richtlinie zur Überlastungskontrolle definiert wird. Die Dienste, die für diesen CLI-Befehl gelten, werden in der oben erwähnten CLI-Syntax angegeben.

- **Aktion**: Dieser Parameter definiert die Aktion, die beim Überschreiten des Grenzwerts für die Überlastungskontrolle für den angegebenen Dienst zu ergreifen ist. Diese vier Aktionsarten können konfiguriert werden:

  Löschen: Diese Aktion veranlasst das System, die neuen Sitzungsanfragen zu verwerfen. Es wird keine Ablehnungs-/Fehlerantwort gesendet.

  Ablehnen: Diese Aktion veranlasst die Ablehnung der neuen Sitzungsanfragen. Eine Ablehnungsantwort wird gesendet. Diese Option gilt nicht für den IPSG-Service.

  Keine: Diese Option wird verwendet, wenn Sie das System so konfigurieren möchten, dass keine Maßnahmen ergriffen werden.

  Umleitung: Diese Aktion veranlasst die Umleitung der neuen Sitzungsanfragen an ein anderes Gerät. Dies gilt nur für die Services CSCF, HSGW, HA und PDSN. Die IP-Adresse des alternativen Geräts sollte mit dem Befehl **Policy Overload Redirect** (Umleitung **der Richtlinienüberladung)** konfiguriert werden.

Policy Overload Redirect

Dies sollte konfiguriert werden, wenn eine Umleitungsaktion für den Service Call Session Control Function (CSCF), HRPD Serving Gateway (HSGW), Home Agent (HA) oder PDSN konfiguriert wird.

- Dieser Befehl ist in der Konfiguration der CSCF-Richtlinienregeln für den CSCF-Dienst konfiguriert.

- Für den HSGW Service, den HA-Service und den PDSN-Service ist dieser Befehl in den entsprechenden Dienstkonfigurationen konfiguriert.

Überlastungskontrollrichtlinie für MME-Dienst

Vor Version 14.0 kann die Richtlinie zur Überlastungskontrolle für den MME-Dienst ähnlich wie die im vorherigen Abschnitt erwähnte CLI-Syntax definiert werden, jedoch mit einigen zusätzlichen Optionen. Die CLI-Syntax lautet wie folgt:

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

Neben dem Drop, none und Ablehnen von Aktionen hat der MME-Dienst auch die Möglichkeit, Überlastungsbedingungen für die eNodeBs zu melden. Die MME ruft das S1-Überlastungsverfahren mit der Meldung *S1AP Overload Start* auf, um einen Überlastungszustand an den angegebenen Anteil von eNodeBs zu melden, an den die MME über eine S1-Schnittstellenverbindung verfügt. Die MME wählt die eNodeBs zufällig aus. Zwei überladene MMEs im selben Pool senden keine Überlastungsmeldungen an dieselben eNodeBs. Wenn die MME wiederhergestellt ist und ihre Last erhöhen kann, sendet sie eine *S1AP*-Meldung zum *Überladen*. Darüber hinaus können diese Aktionen ausgeführt werden, wenn eine Berichtsüberlastungsaktion konfiguriert wird:

- Zulassen-Notfall-Sitzungen: Diese Aktion erlaubt nur Notsitzungen auf der MME während einer Überlastungszeit.
- Neue Sitzungen ablehnen: Diese Aktion bewirkt eine Ablehnung aller neuen Sitzungen, die während einer Überlastungssituation in Richtung MME eingehen.
- Ablehnen von Sitzungen, die nicht in Notfällen stattfinden: Diese Aktion bewirkt, dass alle Sitzungen, die keine Notfälle verursachen, während einer Überlastungszeit auf der MME abgelehnt werden.
- Enodeb-Prozentsatz: Durch diese Aktion wird der Prozentsatz der bekannten eNodeBs konfiguriert, die den Überlastungsbericht erhalten. Der Prozentsatz kann zwischen 1 und 100 liegen.

In den Versionen 14.0 und höher kann der MME-Dienst drei verschiedene Richtlinien und zugeordnete Aktionsprofile aufweisen. Die CLI-Syntax lautet wie folgt:

```
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> }
```

Es gibt drei Richtlinientypen, die in Version 14.0 und höher für die MME konfiguriert werden können:

- Kritisch: Dadurch wird der kritische Grenzwert für die Überlastungskontrolle für den MME-Dienst definiert.
- Wichtig: Dadurch wird der größte Grenzwert für die Überlastungskontrolle für den MME-Dienst definiert.
- Geringfügig: Dies definiert den geringen Grenzwert für die Überlastungskontrolle für den MME-Dienst.

  Hinweis: Der Aktionsprofil-Parameter definiert das Aktionsprofil, das dem zuvor erwähnten Richtlinientyp (Minor, Major, Critical) zugeordnet ist.

MME Congestion Control Policy-Aktionsprofil

Das Aktionsprofil für die MME-Überlastungskontrollrichtlinie kann unter der *aktuellen Richtlinie* konfiguriert werden. Die CLI-Syntax lautet wie folgt:

```
configure > lte-policy

congestion-action-profile <profile_name>
```

In den folgenden Abschnitten werden die verfügbaren Aktionen beschrieben, die im Überlastungsprofil konfiguriert werden können.

Löschen

Diese Aktion verursacht einen Rückgang der neuen Sitzungsanforderungen, wenn der Grenzwert für die Überlastungskontrolle erreicht wird. Die CLI-Syntax lautet wie folgt:

```
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 ]
```

Sie ermöglicht eine präzisere Kontrolle der Art der Anforderungen/Anrufereignisse, die verworfen werden sollen. Details hierzu:

- Addn-brr-Request: Dadurch werden Pakete verworfen, die durch UE initiierte Träger-Ressourcenanforderungen enthalten. Dies ist ein lizenziertes Schlüsselwort.
- Addn-connect: Dadurch werden Pakete mit zusätzlichen PDN-Kontextverbindungen verworfen. Dies ist ein lizenziertes Schlüsselwort.
- Brr-ctxt-mod-Requests: Dadurch werden Pakete mit Anforderungen zur Änderung des Trägerkontexts verworfen. Dies ist ein lizenziertes Schlüsselwort.
- Kombinierte Anhänge: Dadurch werden Pakete mit kombinierten Attach-Anforderungen verworfen.
- Handovers: Dadurch werden Pakete mit Übergabeversuchen verworfen.
- PS-Anhänge: Dadurch werden Pakete verworfen, die paketvermittelte Attach-Anfragen enthalten.
- S1-Einrichtungen: Dadurch werden Pakete mit S1-Setup-Versuchen verworfen. Dies ist ein lizenziertes Schlüsselwort.
- Service-Anfragen: Dadurch werden Pakete mit allen Serviceanfragen verworfen. Dies ist ein lizenziertes Schlüsselwort.
- Tau-Anfragen: Dadurch werden Pakete verworfen, die alle Aktualisierungsanforderungen für den Verfolgungsbereich enthalten.

Diese beiden Optionen können auch mit dem zuvor erwähnten Anrufereignistyp konfiguriert werden (beide Optionen sind lizenzgesteuert):

- **Lapi**: Dies bedeutet, dass Anfragen mit LAPI (Low Access Priority Indication) für die Anrufereignisse verworfen werden. Andernfalls werden sowohl LAPI- als auch Nicht-LAPI-Ereignisse verworfen. Die CLI-Syntax lautet wie folgt:

  drop

- **API-basiert**: Dies bedeutet, dass Anforderungen für die Access Point Names (APNs), die für die Überlastungskontrolle in der Operatorrichtlinie konfiguriert sind, verworfen werden. Die CLI-Syntax lautet wie folgt:

  drop

  Hinweis: Der Befehl **APN network-identifier** in der Operatorrichtlinie wird verwendet, um die Überlastungskontrolle für eine APN zu konfigurieren.

  Hinweis: Wenn das Überlastungsprofil mit LAPI- und APN-basierten Optionen konfiguriert ist, werden Anrufereignisse nur verworfen, wenn beide Bedingungen übereinstimmen.

Ausnahmeereignisse ausschließen

So können die Notrufe auch dann bearbeitet werden, wenn der Schwellenwert überschritten wurde. Die CLI-Syntax lautet wie folgt:

exclude-emergency-events

Wenn diese konfiguriert ist, werden diese Meldungen in den als Notfallalarm gekennzeichneten UEs nicht durch die Überlastungsaktion zurückgewiesen und verworfen:

- TAU-Anfragen
- Serviceanfragen
- Handover
- ADDN-PDN-Anfragen

Sprachereignisse ausschließen

Dadurch können Sprachanrufe auch dann verarbeitet werden, wenn der Schwellenwert überschritten wurde. Die CLI-Syntax lautet wie folgt:

exclude-voice-events

Keine

Dies gibt an, dass bei eingehenden Anforderungen keine Maßnahmen zur Überlastungskontrolle ergriffen werden sollten, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde. Die CLI-Syntax lautet wie folgt:

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

Im Folgenden sind die Details der Anrufereignisse aufgeführt, die für diese Aktion konfiguriert werden können (*keine* ist die Standardaktion für alle diese Anrufereignisse):

- Addn-brr-Request: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete durchgeführt wird, die durch UE initiierte Träger-Ressourcenanforderungen enthalten.
- Addn-connect: Dies führt dazu, dass keine Überlastungskontrollaktion für zusätzliche PDN-Kontexverbindungen (Packet Data Network) abgeschlossen wird.
- Brr-ctxt-mod-Requests: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete abgeschlossen wird, die Änderungen am Trägerkontext enthalten.
- Kombinierte Anhänge: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete ausgeführt wird, die kombinierte Attach-Anfragen enthalten.
- Handovers: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete mit Übergabeverfahren durchgeführt wird.
- PS-Anhänge: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete ausgeführt wird, die Paket-Switched Attach-Anforderungen enthalten.
- S1-Einrichtungen: Dies führt dazu, dass für Pakete mit S1-Setup-Versuchen keine Überlastungskontrollaktion durchgeführt wird. Dies ist ein lizenziertes Schlüsselwort.
- Service-Anfragen: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete ausgeführt wird, die alle Serviceanforderungen enthalten. Dies ist ein lizenziertes Schlüsselwort.
- Tau-Anfragen: Dies führt dazu, dass keine Überlastungskontrollaktion für Pakete ausgeführt wird, die alle Aktualisierungsanforderungen für den Verfolgungsbereich enthalten.

Ablehnen

Dies bewirkt, dass eingehende Anfragen abgelehnt werden und eine *Ablehnungsmeldung* gesendet wird, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde. Die CLI-Syntax lautet wie folgt:

```
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 ]
```

Im Folgenden sind die Details der Anrufereignisse aufgeführt, die mit der *Ablehnungsaktion*

konfiguriert werden können:

- **Addn-brr-Request**: Dadurch werden Pakete mit von UE initiierten Trägerressourcenanforderungen abgelehnt. Dies ist ein lizenziertes Schlüsselwort.
- **Addn-connect**: Dadurch werden Pakete mit zusätzlichen PDN-Kontextverbindungen zurückgewiesen. Dies ist ein lizenziertes Schlüsselwort.
- **Brr-ctxt-mod-Requests**: Dadurch werden Pakete mit Anforderungen zur Änderung des Trägerkontexts zurückgewiesen. Dies ist ein lizenziertes Schlüsselwort.
- **Kombinierte Anhänge**: Dadurch werden Pakete mit kombinierten Attach-Anforderungen zurückgewiesen.
- **Handovers**: Dadurch werden Pakete mit Übergabeversuchen zurückgewiesen.
- **PS-Anhänge**: Dadurch werden Pakete mit paketvermittelten Attach-Anforderungen zurückgewiesen.
- **S1-Einrichtung Time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 }** : Dadurch werden Pakete mit S1-Einrichtungsversuchen nach 1, 2, 10, 20, 50 oder 60 Sekunden zurückgewiesen. Dies ist ein lizenziertes Schlüsselwort.
- **Service-Anfragen**: Dadurch werden Pakete mit allen Serviceanfragen zurückgewiesen. Dies ist ein lizenziertes Schlüsselwort.
- **Tau-Anfragen**: Dadurch werden Pakete mit allen Aktualisierungsanforderungen für den Verfolgungsbereich zurückgewiesen.

Diese beiden Optionen können auch mit dem zuvor erwähnten Anrufereignistyp konfiguriert werden (beide Optionen sind lizenzgesteuert):

- **Lapi**: Dies bedeutet, dass Anforderungen mit LAPI für die Anrufereignisse abgelehnt werden. Andernfalls werden sowohl LAPI- als auch Nicht-LAPI-Ereignisse abgelehnt. Die CLI-Syntax lautet wie folgt:

  ```
  reject
  ```

- **API-basiert**: Dies bedeutet, dass Anforderungen für die APNs, die für die Überlastungskontrolle in der Operatorrichtlinie konfiguriert sind, abgelehnt werden. Die CLI-Syntax lautet wie folgt:

  ```
  reject
  ```

Hinweis: Der Befehl **APN network-identifier** in der Operatorrichtlinie wird verwendet, um die Überlastungskontrolle für eine APN zu konfigurieren.

Hinweis: Wenn das Aktionsprofil für Überlastungen mit LAPI- und APN-basierten Optionen konfiguriert ist, werden die Anrufereignisse nur abgelehnt, wenn beide Bedingungen übereinstimmen.

Berichtsüberlastung

Dadurch kann die MME Überlastungsbedingungen an die eNodeBs melden, um Überlastungsszenarien zu entschärfen. Die MME ruft das S1-Überlastungsverfahren mit der Meldung *S1AP Overload Start* auf, um die Überlastungsbedingung an den angegebenen Anteil von eNodeBs zu melden, an die die MME eine S1-Schnittstellenverbindung hat.

Die MME wählt die eNodeBs zufällig aus. Zwei überladene MMEs im selben Pool senden keine Überlastungsmeldungen an dieselben eNodeBs. Wenn die MME wiederhergestellt ist und ihre Last erhöhen kann, sendet sie eine *S1AP-Überlastungs-Stopp*-Nachricht. Die CLI-Syntax lautet wie folgt:

```
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
```

Die folgenden Optionen können mit dieser Aktion konfiguriert werden:

- **Zulassen-Notruf-Sitzungen und Mobile-Terminated-Services**: In der Überlastungsmeldung an eNodeB wird angegeben, dass während der Überlastungszeit nur Notsitzungen auf die MME zugreifen dürfen.
- **Zulassen-Sitzungen mit hoher Priorität und Mobile-terminierte Dienste**: Dies gibt in der Überlastungsmeldung für eNodeB an, dass während der Überlastungszeit nur Sitzungen mit hoher Priorität und mobile beendet Dienste auf die MME zugreifen dürfen.
- **Ablehnungs-toleranter Zugriff**: Dies legt in der Überlastungsmeldung für eNodeB fest, dass verzögerungstoleranter Zugriff für MME während der Überlastungszeit abgelehnt werden soll.
- **Ablehnen-Neu-Sitzungen**: Dies gibt in der Überlastungsmeldung für eNodeB an, dass alle neuen Verbindungsanforderungen, die für die MME bestimmt sind, während der Überlastungszeit abgelehnt werden sollen.
- **Nicht-Notfall-Sitzungen ablehnen**: Dies gibt in der Überlastungsmeldung an eNodeB an, dass alle Sitzungen, die keine Notfälle sind, während der Überlastungszeit abgelehnt werden sollen.
- **enobeb-Prozentsatz**: Dadurch wird der Prozentsatz der bekannten eNodeBs konfiguriert, die einen Überlastungsbericht erhalten.

Richtlinie zur Überlastungskontrolle für SGSN mit Version 17.0 und höher

In den Versionen 17.0 und höher benötigte das SGSN außerdem eine Richtlinie zur Überlastungskontrolle, die der Richtlinie für MME ähnelte. Das SGSN kann über drei Aktionen zur Überlastungskontrolle verfügen, und jede Aktion ist einem Aktionsprofil zugeordnet. Die CLI-Syntax lautet wie folgt:

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

Diese drei *Richtlinientypen* können in Version 14.0 und höher für die MME konfiguriert werden:

- Kritisch: Dadurch wird der kritische Grenzwert für die Überlastungskontrolle für den MME-Dienst definiert.
- Wichtig: Dadurch wird der größte Grenzwert für die Überlastungskontrolle für den MME-Dienst definiert.
- Geringfügig: Dies definiert den geringen Grenzwert für die Überlastungskontrolle für den MME-Dienst.

  Hinweis: Der Aktionsprofilparameter definiert das Aktionsprofil, das dem *Richtlinientyp* zugeordnet ist (Minor, Major oder Critical).

Richtlinienaktionsprofil für SGSN-Überlastungskontrolle

Das Aktionsprofil der SGSN-Richtlinie zur Überlastungskontrolle wird im *sgsn-global*-Konfigurationsmodus konfiguriert. Sie definiert die auszuführende Aktion für diese Arten von Anruf-/Nachrichtenereignissen, wenn im SGSN-Knoten ein Grenzwert für die Überlastungskontrolle erreicht wurde:

- Aktive Anrufe
- Neue Anrufe
- SM-Nachrichten

Die Syntax für die Konfiguration des Aktionsprofils für die SGSN-Überlastungssteuerung lautet wie folgt:

```
configure > sgsn-global > congestion-control

congestion-action-profile <action_profile_name>
```

In den folgenden Abschnitten werden die verschiedenen Richtlinien beschrieben, die im SGSN-Überlastungsprofil konfiguriert werden können.

Aktive Anrufrichtlinie

Dieser Parameter gibt das Verwerfen oder Ablehnen von aktiven Anrufnachrichten an, wenn während eines aktiven Anrufs eine Überlastung auftritt. Ein Drop oder Ablehnen aktiver Anrufe kann nur als LAPI für die Nachricht definiert werden. Die CLI-Syntax lautet wie folgt:

```
active-call-policy { rau | service-req } { drop | reject } [ low-priority-ind-ue ]
```
Hier einige Hinweise zu dieser Syntax:

- **Nachrichtentyp/Anrufereignis**: Diese Meldungstypen oder Anrufereignisse können für eine aktive Anrufrichtlinie definiert werden:

  RAU: Dies definiert die RAU-Meldung (Routing Area Update), die vom SGSN empfangen wird.

  Serviceanforderungen: Damit wird die SR-Nachricht definiert, die vom SGSN empfangen wird.

- **Aktionen**: Dies definiert die Aktionen, die beim Empfang der zuvor erwähnten Nachrichten beim aktiven Anruf beim Erreichen des Grenzwerts für die Überlastungskontrolle durch das SGSN zu ergreifen sind.

  Löschen: Dadurch wird der SGSN angewiesen, die definierte Nachricht zu verwerfen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

  Ablehnen: Dadurch wird der SGSN angewiesen, die definierte Nachricht abzulehnen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.**Hinweis**: Drop-and-Ablehnungs-Aktionen können für LAPI weiter verfeinert werden. Das **Low-Priority-ind-ue-**Schlüsselwort wird mit einer Drop/Ablehnen-Aktion verwendet.
- **Verwendung mit niedriger Priorität:** Dadurch wird der SGSN angewiesen, die definierte Nachricht nur dann abzulehnen/zu löschen, wenn eine Nachricht von der EU einen LAPI enthält, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

Richtlinie für neue Anrufe

Diese Eigenschaft gibt das Verwerfen oder Ablehnen neuer Anrufnachrichten an, wenn eine Überlastung auftritt. Die Drop- oder Ablehnungs-Aktionen für neue Anrufe (Attach Request oder new inter SGSN RAU) können auf LAPI- oder APN-basiert oder auf beidem optimiert werden. Die CLI-Syntax lautet wie folgt:

```
new-call-policy { drop | reject } [ apn-based ] [ low-priority-ind-ue ]
```
Hier einige Hinweise zu dieser Syntax:

- **Nachrichtentyp/Anrufereignis**: Wenn eine neue Anrufrichtlinie definiert wird, wird sie für alle *Attach Requests* oder *Inter-SGSN RAUs* übernommen. Aus diesem Grund ist in diesem CLI-Befehl kein Meldungs-/Anruferereignistyp erforderlich.

- **Aktionen**: Dies definiert die auszuführenden Aktionen, wenn der SGSN die zuvor genannten Nachrichten während der aktiven Anrufe empfängt, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

  Löschen: Dadurch wird der SGSN angewiesen, die neuen Anrufnachrichten zu löschen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

  Ablehnen: Dadurch wird der SGSN angewiesen, die neuen Anrufnachrichten abzulehnen,

wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.**Hinweis**: Die Drop-and-Ablehnungs-Aktionen können für LAPI und APN weiter verfeinert werden. Die **Low-Priority-ind-** und **apn-basierten** Schlüsselwörter werden für die Drop-/Ablehnungsaktionen verwendet.
- **Verwendung mit niedriger Priorität**: Dadurch wird der SGSN angewiesen, die definierte Nachricht nur dann abzulehnen/zu löschen, wenn eine Nachricht von der EU einen LAPI enthält, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

- **apn-basiert**: Dadurch wird der SGSN angewiesen, die neuen Anrufnachrichten basierend auf dem APN abzulehnen/zu verwerfen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde. Dies tritt nur auf, wenn eine APN unter der Operatorrichtlinie mit Überlastungskontrolle konfiguriert wird.**Hinweis**: Wenn das Aktionsprofil für Überlastungen mit LAPI- und APN-basierten Optionen konfiguriert ist, werden neue Anrufereignisse nur abgelehnt, wenn beide Bedingungen übereinstimmen.

SM-Nachrichten

Dadurch wird die Richtlinie für die SM-Nachrichten definiert, z. B. *aktive* oder *geänderte* Anforderungen. Die Antwort des SGSN kann nur *zurückgewiesen* werden, und diese kann auf LAPI- oder APN-basierte Werte oder beides verfeinert werden. Die CLI-Syntax lautet wie folgt:

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

Hier einige Hinweise zu dieser Syntax:

- **Nachrichtentyp/Anrufereignis**: Wenn die SM-Nachrichtenrichtlinie definiert ist, wird sie auf alle *Aktivierungs-* oder *Modifizierungsanforderungen* angewendet. Aus diesem Grund ist in diesem CLI-Befehl der Meldungs-/Anrufereignistyp erforderlich.

- **Aktionen**: Dies definiert die auszuführenden Aktionen, wenn der SGSN die zuvor erwähnte Nachricht empfängt und der Grenzwert für die Überlastungskontrolle erreicht wurde. Die *Ablehnungsaktion* weist den SGSN an, die SM-Nachrichten abzulehnen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.**Hinweis**: Die Ablehnungsaktionen können für LAPI und APN weiter verfeinert werden. Die **Low-Priority-ID-**und **apn-basierten** Schlüsselwörter werden für die Drop-/Ablehnungsaktionen verwendet.
- **Verwendung mit niedriger Priorität**: Dies weist den SGSN an, die SM-Nachricht nur dann abzulehnen, wenn die Nachricht von der UE einen LAPI enthält, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde.

- **apn-basiert**: Dies weist den SGSN an, die SM-Nachrichten basierend auf dem APN abzulehnen, wenn der Grenzwert für die Überlastungskontrolle erreicht wurde. Dies tritt nur auf, wenn die APN unter der Operatorrichtlinie mit Überlastungskontrolle konfiguriert wird.**Hinweis**: Wenn das Aktionsprofil für Überlastungen mit LAPI- und APN-basierten Optionen konfiguriert ist, werden die neuen Anrufereignisse nur abgelehnt, wenn beide Bedingungen übereinstimmen.

Grenzwert für Überlastungskontrolle

Der Grenzwert für die Überlastungskontrolle definiert die Schwellenwerte für die verschiedenen Parameter, die bei Überschreiten des Schwellenwerts die Überlastungskontrolle aufrufen können. Die CLI-Syntax lautet wie folgt:

```
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> }
```

Nachfolgend sind die verschiedenen Parameter aufgeführt, die mit Schwellenwerten konfiguriert werden können und bei Erreichen des Grenzwerts eine Überlastungskontrolle auslösen können:

- Lizenznutzung: Dieser Parameter definiert die prozentuale Nutzung der lizenzierten Kapazität, gemessen in Intervallen von zehn Sekunden. Dieser Wert wird als Prozentsatz formatiert und kann zwischen 0 und 100 liegen (der Standardwert ist 100).

- maximale Nutzung pro Sitzung: Dieser Parameter definiert die prozentuale Nutzung der maximal zulässigen Sitzungen pro Dienst, gemessen in Echtzeit. Dieser Schwellenwert basiert auf der maximalen Anzahl von Sitzungen oder dem PDP-Kontext, der für einen bestimmten Dienst konfiguriert ist. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80.

- Message-Queue-Nutzung: Dieser Parameter definiert die prozentuale Auslastung der Aufgabenmeldungswarteschlange für die DEMUX Manager-Software, gemessen in Intervallen von zehn Sekunden. Diese Warteschlange kann 10.000 Nachrichten speichern. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80.

- Message-queue-wait-time: Dieser Parameter legt die maximale Zeit (in Sekunden) fest, die eine Nachricht in der Warteschlange verbleiben kann, gemessen anhand der Paketzeitstempel. Dieser Wert liegt zwischen einer und 30 Sekunden mit einem Standardwert von fünf Sekunden.

- Port-rx-Nutzung: Dieser Parameter definiert die durchschnittliche prozentuale Nutzung der Port-Ressourcen für alle Ports nach empfangenen Daten, gemessen in Intervallen von fünf Minuten. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80. Dieser Schwellenwert-Parameter kann mit dem Befehl no deaktiviert werden.

- portspezifisch: Dieser Parameter definiert die Port-spezifischen Schwellenwerte. Wenn ein einzelner Port-spezifischer Grenzwert erreicht wird, wird die Überlastungskontrolle systemweit angewendet. Dies ist standardmäßig für jede bestimmte Portnummer oder für alle Ports deaktiviert, für die das All-Schlüsselwort verwendet werden kann. Dieser Parameter verfügt über zwei Unteroptionen, die definiert werden können:

  rx-Nutzung: Der Standardwert für diese Option ist 80 %. Es misst die durchschnittliche Auslastung der Port-Ressourcen für den jeweiligen Port nach empfangenen Daten, gemessen in Intervallen von fünf Minuten. Die Werte liegen zwischen 0 und 100.

  tx-Nutzung: Der Standardwert für diese Option ist 80 %. Es misst die durchschnittliche prozentuale Nutzung der Port-Ressourcen für den jeweiligen Port anhand der übertragenen

Daten, gemessen in Intervallen von fünf Minuten. Der Wert liegt zwischen 1 und 100.

- **Port-tx-Nutzung**: Dieser Parameter definiert die durchschnittliche prozentuale Nutzung der Port-Ressourcen für alle Ports nach übertragenen Daten, gemessen in Intervallen von fünf Minuten. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80. Dieser Schwellenwert kann über die **no**-Version dieses Befehls deaktiviert werden.

- **Service-Control-CPU-Nutzung**: Dieser Parameter definiert die durchschnittliche prozentuale Auslastung von CPUs, auf denen eine DEMUX Manager-Softwareinstanz ausgeführt wird, wie in Intervallen von zehn Sekunden gemessen. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80.

- **System-CPU-Nutzung**: Dieser Parameter definiert die durchschnittliche prozentuale Auslastung aller für das System verfügbaren PSC/PSC2-CPUs, gemessen in Intervallen von zehn Sekunden. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80. Diese Option kann deaktiviert werden, wenn **kein** CLI-Befehl **zur Überlastungskontrolle erforderlich ist**.

- **Systemspeichernutzung**: Dieser Parameter definiert die durchschnittliche prozentuale Auslastung für den gesamten dem System zur Verfügung stehenden CPU-Speicher, gemessen in Intervallen von zehn Sekunden. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 80.

- **Toleranz**: Dieser Parameter definiert den Prozentsatz unter einem konfigurierten Grenzwert, der den Punkt vorgibt, an dem die Bedingung gelöscht wird. Dieser Wert liegt zwischen 0 und 100, bei einem Standardwert von 10. Wenn z. B. der Grenzwert mit einem Wert von 90 konfiguriert und die Überlastungskontrolle ausgelöst wird, wird der Trigger mit 80 gelöscht, wenn der Standardwert von zehn für die Toleranz definiert ist.

Grenzwerte für die Überlastungskontrolle für MME und SGSN

In diesem Abschnitt wird die Konfiguration des Schwellenwerts für MME und SGSN definiert, wenn drei verschiedene Auslöser zusammen mit den Profilen für die Überlastungssteuerung definiert werden.

Diese Informationen gelten für MME-Versionen 14.0 und höher und SGSN-Versionen 17.0 und höher. Dies sind die drei verschiedenen Auslösestufen, die für MME und SGSN verfügbar sind und zusätzlich mit den Richtlinien zur Überlastungskontrolle verknüpft sind, die übereinstimmen:

- **Kritisch**: Diese Triggerebene definiert die kritischen Schwellenwerte für verschiedene Parameter. Der Wert dieser Auslöseschwelle sollte der größte unter allen drei Schwellenwerten sein. Die kritischen Schwellenwerte umfassen vorkonfigurierte Standardwerte.

- **Wichtig**: Diese Triggerebene definiert die wichtigsten Schwellenwerte für verschiedene Trigger. Die Werte dieses Triggergrads sollten größer als der kleine Grenzwert und kleiner als der kritische Wert sein. Der Standardwert ist 0.

- **Geringfügig**: Diese Triggerebene definiert die unteren Schwellenwerte für verschiedene Trigger. Die Werte dieses Triggers sollten mindestens unter allen drei Schwellenwerten liegen. Der Standardwert ist 0.

Die drei Schwellenwerte können für alle im vorherigen Abschnitt erwähnten Parameter/Trigger definiert werden. Die folgende CLI-Syntax dient zur Definition der Schwellenwerte für die verschiedenen Parameter:

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

> **Hinweis**: Die kritischen Schwellenwerte für die verschiedenen Parameter (mit Ausnahme der **Lizenzauslastung**) verwenden dieselben Standardwerte wie die im vorherigen Abschnitt beschriebenen. Der Standardwert für den **Lizenzauslastungsparameter** für das kritische Profil beträgt *80 %*.

Überprüfen

Verwenden Sie die in diesem Abschnitt beschriebenen Informationen, um die Konfiguration der Überlastungskontrolle zu überprüfen.

Überprüfung der Konfiguration der Überlastungskontrolle

Geben Sie die **Konfiguration für die Show Congestion-control ein. | mehr** CLI-Befehl, um die Konfiguration der Überlastungssteuerung zu überprüfen. Die folgenden Abschnitte enthalten Beispielausgaben für die verschiedenen Phasen der Überlastungskontrolle.

Überlastungskontrolle vor der Aktivierung

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

Überlastungskontrolle nach Aktivierung

```
[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
............
```

Überlastungskontrolle nach der Overload Disconnect-Aktivierung

```
[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

 ............
```

Überlastungskontrolle nach Aktivierung anderer Richtlinien als SGSN und MME

Durch die Konfiguration der **Richtlinie für die Überlastungskontrolle <service-name> action <action>** ändert sich der Wert des Abschnitts **für die Überlastungskontrollrichtlinie** entsprechend der Konfiguration. Im Folgenden finden Sie ein Beispiel für die Konfiguration eines **Action-Drop** für den **ggsn-Service**:

```
[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
 closedrp-service: none
.............
```

Grenzwerte für Überlastungskontrolle bei Haupt- und Nebenprofilen

In diesem Abschnitt wird die Überprüfung der Grenzwertkonfiguration für die Überlastungskontrolle für die Haupt- und Nebenprofile beschrieben. Das kritische Profil verfügt bereits über einige Standardwerte, die nach Bedarf geändert werden können. Es müssen jedoch die Haupt- und die untergeordneten Schwellenwerte konfiguriert werden. Diese drei Profile können später zusammen mit einer Richtlinie zur Überlastungskontrolle verwendet werden.

```
[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
............
```

Richtlinienaktivierung der Überlastungskontrolle für SGSN

Verwenden Sie diese Informationen, um die Aktivierung der Richtlinie für die Überlastungskontrolle für das SGSN zu überprüfen:

```
[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
 lns-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
...........
```

Aktivierung der Richtlinie für die Überlastungskontrolle für MME

Verwenden Sie diese Informationen, um die Aktivierung der Richtlinie für die Überlastungskontrolle für MME zu überprüfen:

```
[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-setups
[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-setups 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-setups
[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
 closedrp-service: none
 lns-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
............
```

Statistiken zur Überlastungskontrolle

Diese Befehle werden verwendet, um Statistiken und Status anzuzeigen, die sich auf die Überlastungskontrolle beziehen:

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 }]

Die Option **<manager>** kann folgende Werte aufweisen:

- **A11mgr**: Dies ist der PDSN-Service.
- **asngwmgr**: Dies ist der ASN-GW-Service (Access Service Network Gateway).
- **asnpcmgr**: Dies ist der ASN Paging Control (PC-LR)-Dienst.
- **Bindmux**: Dies ist der Bindmux Manager, der vom PCC-Dienst verwendet wird.

- **egtpinmgr**: Dies ist der Eingangs-DEMUX-Manager des Enhanced GPRS Tunneling Protocol (EGTP).
- **gtpcmgr**: Dies ist der GGSN-Service.
- **Hammer**: Dies gilt für die HA-Services.
- **hnbmgr**: Dies ist der Home Node B (HNB) Manager, der vom HNB-GW-Dienst verwendet wird.
- **imsimgr**: Dies ist der IMSI-Manager, der für das SGSN verwendet wird.
- **ipsecmgr**: Dies ist der IP Security (IPSec) Manager.
- **ipsgmgr**: Dies gilt für IP Service Gateway (IPSG)-Manager.
- **l2tpmgr**: Dies gilt für Layer 2 (L2) Tunneling Protocol (L2TP)-Manager.

Überlastungs-Steuerungs-Trigger für SGSN durch OAM-Intervention

Die **sgsn-Trigger-Überlastungsstufe { critical | Wichtigste | Der Befehl minor }** wird verwendet, um eine Überlastungskontrolle im SGSN manuell auszulösen. Der Befehl **sgsn clear-congestion** wird verwendet, um die Überlastung zu löschen, die durch den Befehl **sgsn trigger-congestion** initiiert wird.

Hier ein Beispiel für die Ausgabe:

```
[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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- 3GPP TS 23,401
- 3GPP TS 23.060
- 3GPP TS 25,413
- 3GPP TS 36,413
- Befehlszeilenschnittstellenreferenz, StarOS, Version 17
- Technischer Support und Dokumentation - Cisco Systems