ASR5x00 MME Overload Protection Features

Document ID: 119002

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

Jun 12, 2015

Contents

Introduction
MME Protection
Network Overload Protection: Attach Rate Throttling
Network Overload Protection: Paging Throttling
Sample Configuration
Network Overload Protection: DDN Throttling (Serving GateWay Functionality, Protects MME)
Network Overload Protection: EGTP Path Failure Throttling
Sample Configuration
Enhanced Congestion Control
Congestion Condition Thresholds
Thresholds and Tolerance Levels
Service Control CPU Thresholds
System CPU Thresholds
System Memory Thresholds
Related Information

Introduction

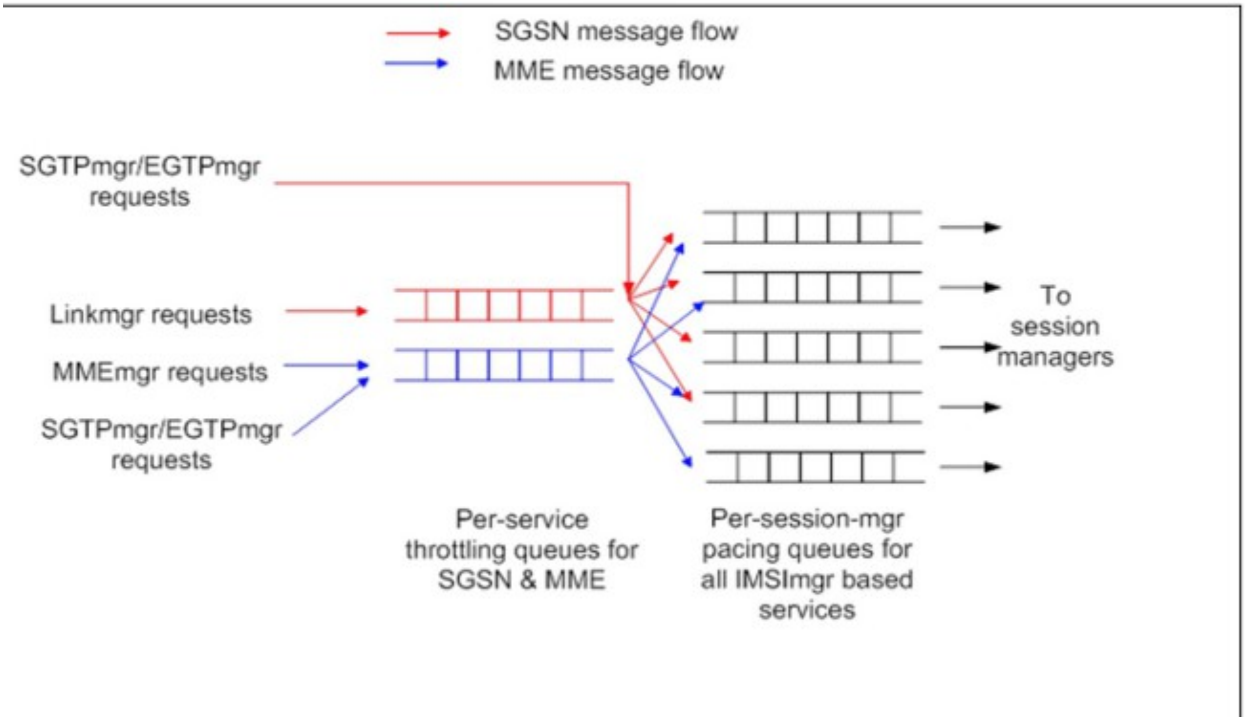
This document highlights the various Mobility Management Entity (MME) overload protection methods and features available on the Cisco Aggregation Services Router (ASR) 5000 Series. In the ASR 5000 Series, Cisco gives the customer various means to achieve control and this article explains the features and related CLI commands.

MME Protection

Network Overload Protection: Attach Rate Throttling

Attach Rate Throttling protects neighbor Network Elements such as Home Subscriber Server (HSS), Policy and Charging Rules Function (PCRF), and Online Charging Server (OCS), and internal MME resources such as imsimgr and sessmgr. Attach Rate Throttling processes the new calls that arrive to imsimgr, such at Attaches and Inter−MME/Serving GPRS Supporting Node (SGSN) Tracking Area Update (TAUs).

This picture shows the message flow for calls and throttling queues.



In order to protect MME (imsimgr and sessmgr onwards), the *throttling rate, queue wait time, and queue size time* should be defined. The *throttling rate* is dependent on the MME call model as the MME capacity is dependent on the call model.

For MME the throttling rate calculation is relatively simple, take the standard Call Events Per Second (CEPS) in the network plus tolerance. Also, you might need to consider the HSS database capacity also if HSS protection is needed.

Example

In busy hours, MME handles up to 170 to 200 calls per second (Attaches+ Inter TAU). In case of one site failure, up to 350 to 370 calls per second might arrive to one MME. Under this call rate, the MME utilization rises close to 80% and *400* calls per second is an optimal level to limit the throttling rate in order to avoid excessive signaling load inside the MME box.

The *queue wait time* by default is 5 seconds. It is optimal for CUSTOMER. The *queue size* by default is 2500. It is optimal for CUSTOMER.

The configuration command is as follows.

```
asr5k(config)#network-overload-protection mme-new-connections-per-second
 new_connections action attach { drop | reject-with-emm-cause
 { congestion | network-failure | no-suitable-cell-in-tracking-area}
 tau { drop | reject-with-emm-cause { congestion | network-failure
 | no-suitable-cells-in-tracking-area | no-sec-ctxt-in-nw} fwd-reloc
 { drop | reject} }{wait-time  <wait-time>} {queue-size <queue-size>}
```

new_connections
Defines the number of new MME connections to be accepted per second. Must be an integer from 50 to 5000. The default is 500.

action
Defines the action to be taken when the pacing queue becomes full. Whenever new connections are received at the MME, they are queued in the pacing queue and imsimgr processes messages from the queue at the

configured rate. When the queue overflows (due to high incoming rate), based on the "action" configured, packets are either dropped or rejected.

queue−size
Defines the maximum size of the pacing queue used for buffering the packets. Must be an integer from 250 to 25000. The default is 2500.

Sample Configuration

```
network−overload−protection mme−new−connections−per−second 400 action attach
  reject−with−emm−cause no−suitable−cell−in−tracking−area tau
 reject−with−emm−cause no−suitable−cell−in−tracking−area fwd−reloc drop
```

Now the call rate per second is set to 400 and the action is intelligent reject with cause #15 to make the User Equipment (UE) reconnect to different Radio Access Technologies (RATs). The wait time is set to the default (5 seconds) and the queue size is 2500.

Note: The action "reject" with EMM cause #15 "no−suitable−cell−in−tracking−area" is preferred as the calls rejected with #15 mostly will not rearrive to MME and will go to different RAT layers (3G, 2G). The action "Drop" for Serving Radio Network Subsystem (SRNS) relocation is for future use and will prevent a quick reattach to MME after rejection.

Network Overload Protection: Paging Throttling

Paging Throttling protects internal MME resources (mmemgr) as eNodeB/radio resources (if needed). This rate limit threshold shall be applicable to all the eNodeB that associates with MME for a given ASR 5000 chassis. S1 Paging requests to an eNodeB shall be rate limited at this threshold value. S1 Paging requests to an eNodeB that exceed this threshold shall be dropped.

For MME the throttling rate calculation is relatively simple, take the standard egress paging rate in the network plus the tolerance. (This is based purely on the design team's decision.)

Example

In busy hours, each MME handles up to 35000 paging messages per second. In case of one site failure, up to 70000 pages per second might go from one MME. Under this paging rate, the MME utilization (mmemgr) rises close to 80% and *70000 to 80000* pages per second would be an optimal level to limit the throttling rate in order to avoid excessive S1 signaling over mmemgr.

However, the rate is limited per average eNodeB. The average rate per eNodeB (in case of 6500 eNodeB) is *10* pages per second. However, the Tracking Areas (TAs) are not equal in the number of subscribers and various TA/member eNodeB are loaded with paging differently. In the case of two times the difference in TA size versus the average number of subscribers per TA, the rate per eNodeB would be *20*. In the case of 20 times the difference in the TA size versus the average number of subscribers per TA, the rate per eNodeB would be *200*. This means that the feature becomes most efficient in cases when TA (in number of subscribers) are evenly loaded.

Another action which should be taken in parallel is to activate the Intelligent Paging. Refer to the "TAI mgmt db and LTE Paging" section in the ASR 5000 MME Administration Guide.

The configuration command is as follows:

```
asr5000(config)# network−overload−protection mme−tx−msg−rate−control enb s1−paging
 <rate in messages per second>
```

- network−overload−protection identifies network overload protection
- mme−tx−msg−rate−control enb identifies MME message rate control per average eNodeB
- s1−paging identifies message rate control for S1 Paging
- <rate> specifies rate threshold in messages per second per eNodeB − range (1 to 65535)

Sample Configuration

```
network−overload−protection mme−tx−msg−rate−control enb s1−paging 200
```

Notes:
− The rate limit is the subject for further tuning, in a decreasing direction. The basis for tuning is the number of subscribers (number of paging) over TAs (TA−level statistics is required).

− The feature becomes most efficient in cases when TAs (in number of subscribers/paging per TA) are evenly loaded.

Network Overload Protection: DDN Throttling (Serving GateWay Functionality, Protects MME)

Downlink Data Notification (DDN) throttling is a feature to control the rate of DDN requests to MME from the Serving GateWay (SGW) side. It protects MME resources such as mmemgr and sessmgr against DDN (that is, ingress paging request) surges.

There are two parts to this feature, one for Rel−10 compliant MMEs and the other for Rel−10 non−compliant MMEs:

- For Rel−10 compliant MMEs, set the DDN Throttling Allocation and retention priority (ARP) watermark in SGW service in order to enable the feature.
- For Rel−10 non−compliant MMEs, some other parameters need to be set along with the ARP watermark (such as throttling factor, throttling time, stabilization time, poll interval, and so on) in SGW service.

When this feature is enabled on SGW, it sends an ARP watermark in the DDN Req to MME. In reply, MME sends Throttling Delay Unit, Throttling Delay Value, and Throttling Factor. The combination of Delay Value and Delay Unit calculates the Throttling Time. Upon receipt of these values, SGW drops DDN Req for particular ARP until the throttling timer expires.

For non Rel−10 compliant MMEs that use the local configuration, SGW throttles DDN Req with a particular ARP watermark.

Cisco ASR5x00 MME Releases 16 and 17 do not support automatic DDN Throttling, so it works as non−Rel 10 compliant in terms of DDN Throttling.

Note: DDN throttling provides further granularity on top of MME Paging Throttling on the ingress side (S11) rather than on the egress side (S1). Cisco *does not require* you to implement DDN throttling if Paging Throttling is configured, but it provides earlier overload detection and elimination.

Technical Specifications(TS) 23.401, reference for MME:

Throttling of DDN Requests

Under unusual circumstances (such as when the MME load exceeds an operator configured threshold), the MME might restrict the signalling load that its SGWs generate on it, if configured to do so.

The MME can reject DDN requests for low priority traffic for UEs in idle mode or to further offload the MME. The MME can request the SGWs to selectively reduce the number of DDN requests it sends for downlink low priority traffic received for UEs in idle mode in accordance with a throttling factor and for a throttling delay specified in the DDN Ack message.

The SGW determines whether a bearer is for low priority traffic or not on the basis of the bearer's ARP priority level and operator policy (that is, the operator's configuration in the SGW of the ARP priority levels to be considered as priority or non−priority traffic). The MME determines whether a DDN request is for low priority traffic or not on the basis of the ARP priority level that was received from the SGW and operator policy.

If Idle−state Signalling Reduction (ISR) is not active for the UE, during the throttling delay the SGW drops downlink packets received on all its low priority bearers for UEs known as not user plane connected (that is, the SGW context data indicates no downlink user plane Tunnel End Identifier (TEID)) served by that MME in proportion to the throttling factor, and sends a DDN message to the MME only for the non−throttled bearers.

If ISR is active for the UE during the throttling delay, the SGW does not send DDN to the MME and only sends the DDN to the SGSN. If both MME and SGSN request load reduction, the SGW drops downlink packets received on all its low priority bearers for UEs known as not user plane connected (that is, the SGW context data indicates no downlink user plane TEID) in proportion to the throttling factors.

The SGW resumes normal operations at the expiry of the throttling delay. The last received value of the throttling factor and throttling delay supersedes any previous values received from that MME. The reception of a throttling delay restarts the SGW timer associated with that MME.

For SGW versus MME, the throttling rate calculation is relatively simple. Take the maximum allowed *ingress* paging rate which is 1100 messages per second per MME box.

The configuration commands are as follows:

```
#configure

#context saegw−gtp

#sgw−service sgw−svc

#ddn throttle arp−watermark <arp_value> rate−limit <limit> time−factor <seconds>
 throttle−factor <percent> increment−factor <percent> poll−interval <second>
 throttle−time−sec <seconds> throttle−time−min <minutes> throttle−time−hour <hour>
 stab−time−sec <seconds> stab−time−min <minutes> stab−time−hour <hour>
```

throttle arp−watermark arp_value
If the ARP watermark is configured and if an MME/SGSN sends the throttling factor and delay in a DDN ACK message, all the DDNs which have an ARP value greater than the configured value will be throttled by the throttle factor for the specified delay.
arp_value is an integer from 1 through 15.

rate−limit limit
Configures the rate limit (use this and subsequent tokens to rate−limit only if the MME is a Non−Release 10 MME).
limit is an integer from 1 through 999999999.

time−factor seconds
Configures the time duration during which the SGW makes throttling decisions.
seconds is an integer from 1 to 300.

throttle−factor percent
Configures the DDN throttling factor. Enter the percentage of the DDN to be dropped upon detection of a DDN surge.
percent is an integer from 1 through 100.

increment−factor percent
Configures the DDN throttling increment factor. Enter the percentage by which the DDN throttling should be increased.
percent is an integer from 1 through 100.

poll−interval seconds
Configures the polling interval in DDN throttling.
seconds is an integer from 2 through 999999999.

throttle−time−sec seconds
Configures the DDN throttling time in seconds. Enter time period in seconds over which DDN are throttled at the SGW.
seconds is an integer from 0 through 59.

throttle−time−min minutes
Configures the DDN throttling time in minutes. Enter time period in minutes over which DDN are throttled at the SGW.
minutes is an integer from 0 through 59.

throttle−time−hour hour
Configures the DDN throttling time in hours. Enter time period in hours over which DDN are throttled at the SGW.
hour is an integer from 0 through 310.

stab−time−sec seconds
Configures the DDN throttling stabilization time in seconds. Enter a time period in seconds over which if the system is stabilized, throttling will be disabled.
seconds is an integer from 0 through 59.

stab−time−min minutes
Configures the DDN throttling stabilization time in minutes. Enter a time period in minutes over which if the system is stabilized, throttling will be disabled.
minutes is an integer from 0 through 59.

stab−time−hour hour
Configures the DDN throttling stabilization time in hours. Enter a time period in hours over which if the system is stabilized, throttling will be disabled.
hour is an integer from 0 through 310.

Sample Configuration

```
ddn throttle arp−watermark 1 rate−limit RATE time−factor 120 throttle−factor 50
 increment−factor 10 poll−interval 30 throttle−time−sec 0 throttle−time−min 1
 throttle−time−hour 0 stab−time−sec 0 stab−time−min 2 stab−time−hour 0
```

- 1100 pages/seconds is the maximum allowed ingress rate (including DDN)
- 1100 pages/seconds in case of a DDN surge corresponds to 1100 DDN/seconds
- Regions with 4xSGW per MME site > RATE = ***275*** DDN/second per SGW maximum allowed
- Regions with 3xSGW per MME site > RATE = ***366*** DDN/second per SGW maximum allowed
- Regions with 2xSGW per MME site > RATE = ***550*** DDN/second per SGW maximum allowed

- Regions with 1xSGW per MME site > RATE = ***1100*** DDN/second per SGW maximum allowed

Network Overload Protection: EGTP Path Failure Throttling

This feature protects MME resources (sessmgr, mmemgr) as well 4G resources against Enhanced GPRS Tunneling Protocol (EGTP) path failure surges in case of transmission failures in IP Backbone and IP BackHaul as well as side Network Element failures/restarts.The feature enables per sessmgr limiting of EGTP Path Failure events detected and defines further granularity to the subscriber management, on top of the S1 Paging Throttling. Dependent upon the split between Idle and Connected subscribers, the limits shall be set. It is very network specific and requires tuning in relation with the eUTRAN and UE status.

Example

Subscribers are split about 80:20 IDLE to CONNECTED. In the worst case, the EGTP PF for IDLE subscribers causes a surge of paging which might cause the mmemgr overload, the narrowest bottleneck in the chain. Such EGTP Paging Factor (PF) surge (for IDLE subscribers) first of all causes a paging surge and this surge hits the mmemgr bottleneck, so you need to protect mmemgr against this first. Thus the EGTP PF for IDLE might be considered as an unexpected ingress paging surge which is allowed to be maximum *1100* pages/second.

- The recommended throttling limit is *1000 msg*/second for IDLE subscribers.
- The number of CONNECTED subs is ~ 5 to 7 times less than IDLE.
- Paging surges do not happen with CONNECTED subscribers, so *2000 msg/sec* is recommended to be applied safely for CONNECTED subscribers.

Note: EGTP PF throttling provides further granularity on top of MME Paging Throttling on the ingress side (S11, Sv) rather than on the egress side (S1). Cisco *does not require* you to implement EGTP PF throttling if Paging Throttling is configured, but it provides earlier overload detection and elimination.

This configuration applies to an EGTP service that has an interface type "interface−mme".

The configuration command is as follows:

```
asr5000(config)# network−overload−protection mme−tx−msg−rate−control egtp−pathfail ecm−idle
 < rate in sessions per second > ecm−connected < rate in sessions per second >
```

- network−overload−protection identifies network overload protection
- mme−tx−msg−rate−control identifies MME message rate control
- egtp−pathfail identifies message rate control for EGTP Path Failure
- ecm−idle identifies rate for MME UE sessions in ECM−Idle mode
- ecm−connected identifies rate for MME UE sessions in ECM−Connected mode
- < rate in sessions per second> specifies rate threshold in sessions per second, the range is 1 to 5000

Sample Configuration

```
network−overload−protection mme−tx−msg−rate−control egtp−pathfail ecm−idle
 1000 ecm−connected 2000
```

Enhanced Congestion Control

Using the Enhanced Congestion Control functionality, the MME can signal to the eNodeBs to which it is connected in order to redirect traffic to other MMEs in the MME pool. This is accomplished with the S1 interface Overload Procedure (TS 36.300 and TS 36.413).

When overload control is configured and a congestion threshold is reached, the MME can be configured to send an S1AP interface Overload Start message to a percentage of the eNodeBs to which the MME is connected. In order to reflect the amount of load that the MME wishes to reduce, this percentage is configurable. In the Overload Response Information Element (IE) sent to the eNodeBs, the MME can request the eNodeB to reject or permit specific types of sessions, which include:

- reject non−emergency sessions
- reject new sessions
- permit emergency sessions
- permit high−priority sessions and mobile−terminated services
- reject delay−tolerant access

The congestion control feature allows you to set policies and thresholds and specify how the system reacts when faced with a heavy load condition. Congestion control monitors the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (for example, high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval might have an impact the system's ability to service subscriber sessions. Congestion control helps identify such conditions and invokes policies to address the situation.

Congestion Condition Thresholds

- System CPU usage
- System service CPU usage (Demux−Card CPU usage)
- System memory usage
- License usage
- Maximum sessions per service

Thresholds and Tolerance Levels

When you configure thresholds and tolerances for critical, major, and minor congestion levels, the threshold levels and tolerances should never overlap. Consider these example configurations, where the threshold levels do not overlap:

- Critical congestion triggers at 95% and clears at 90%
- Major congestion triggers at 90% and clears at 85%
- Minor congestion triggers at 85% and clears at 80%

Service Control CPU Thresholds

This threshold is calculated from the system's demux CPU. The threshold is calculated based on a five−minute average CPU usage.

The highest CPU usage value of two CPU cores of the demux CPU is considered. For example, if CPU core 0 has a five−minute CPU usage of 40% and CPU core 1 has a five−minute CPU usage of 80%, then CPU core 1 is considered for threshold calculation.

System CPU Thresholds

This threshold is calculated using the five−minute CPU usage average of all CPUs (except standby CPU and SMC CPU).

The highest CPU usage value of two CPU cores of all CPUs is considered.

System Memory Thresholds

This threshold is calculated with the five−minute memory usage average of all CPUs (except standby CPU and SMC CPU).

Configure a Congestion Action Profile

Congestion Action Profiles define a set of actions which can be executed after the corresponding threshold is crossed.

Associate a Congestion Action Profile with Congestion Control Policies

Each congestion control policy (critical, major, minor) must be associated with a congestion control profile.

Configure Overload Control

When an overload condition is detected on an MME, the system can be configured to report the condition to a specified percentage of eNodeBs and take the configured action on incoming sessions.

These overload actions are also available (in addition to reject−new−sessions):

- permit−emergency−sessions−and−mobile−terminated−services
- permit−high−priority−sessions−and−mobile−terminated−services
- reject−delay−tolerant−access
- reject−non−emergency−sessions

Sample Configuration Explanation

This enables the congestion control functionality:

```
congestion−control

This monitors the overall CPU Utilization including the sessmgr and demux mgrs

congestion−control threshold system−cpu−utilization critical 90

congestion−control threshold system−cpu−utilization major 85

congestion−control threshold system−cpu−utilization minor 80


Memory utilization thresholds:

congestion−control threshold system−memory−utilization critical 85

congestion−control threshold system−memory−utilization major 75

congestion−control threshold system−memory−utilization minor 70


CPU utilization on DEMUX card:

congestion−control threshold service−control−cpu−utilization critical 85

congestion−control threshold service−control−cpu−utilization major 75

congestion−control threshold service−control−cpu−utilization minor 70
```

```
Defining tolerance margins:

congestion−control threshold tolerance critical 5

congestion−control threshold tolerance major 5

congestion−control threshold tolerance minor 5
```

Define Congestion Action Profiles (Critical, Major, and Minor)

```
lte−policy

congestion−action−profile criticalCogestionProfile

   reject s1−setups time−to−wait 60

   drop handovers

   drop combined−attaches

   drop service−request

   drop addn−brr−requests

   drop addn−pdn−connects

   exclude−voice−events

   exclude−emergency−events

   report−overload permit−emergency−sessions−and−mobile−terminated−service enodeb−percentage 50

congestion−action−profile majorCogestionProfile

   report−overload permit−emergency−sessions−and−mobile−terminated−service enodeb−percentage 50

congestion−action−profile minorCogestionProfile

   report−overload permit−emergency−sessions−and−mobile−terminated−service enodeb−percentage 30

end
```

Apply Congestion Policies

```
configure

congestion−control policy critical mme−service action−profile criticalCogestionProfile

congestion−control policy major mme−service action−profile majorCogestionProfile

congestion−control policy minor mme−service action−profile minorCogestionProfile

end

.
```

Related Information

- ***Cisco ASR 5000 Mobility Management Entity Administration Guide***
- ***Technical Support & Documentation − Cisco Systems***