

Congestion Action Profile Configuration Mode Commands

The Congestion Policy Configuration Mode is used to create and manage the action profiles to be associated with congestion control policies supporting MME configurations on the system.

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

- ddn, on page 1
- drop, on page 2
- end, on page 4
- exclude-emergency-events, on page 5
- exclude-voice-events, on page 5
- exit, on page 6
- none, on page 6
- reject, on page 8
- report-overload, on page 10

ddn

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

ddn sgw-throttling throttle-factor *throttle_factor_value* **delay** *delay_time*
no ddn sgw-throttling

no

Removes the DDN Throttling configuration towards SGW.

ddn

The **ddn** keyword configures the action to be taken for all DDN requests. The operator can reject DDN requests based on ARP or LAPI values or both. Also, there is an option provided to reject all DDN requests without using ARP/LAPI values.

sgw-throttling

Enables DDN throttling towards SGW.

throttle-factor

Specifies the total number of DDN requests to be processed. The number of DDN requests is indicated as a percentage value from 1 to 100.

delay

Specifies the total time for throttling in seconds. The delay value ranges from 2 to 1116000 seconds.

Usage Guidelines

Configures DDN Throttling towards SGW based on the configured throttling factor and throttling delay.

Example

The following example shows DDN throttling with a throttling factor of 30 percent and a throtlling delay of 100 seconds.

```
ddn sgw-throttling throttle-factor 30 delay  100
```

drop

Specifies that incoming packets containing new session requests be dropped when a congestion control threshold has been reached.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > **lte-policy** > **congestion-action-profile** *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

```
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 ]
```

addn-brr-requests

Drops packets containing UE initiated bearer resource requests.

This keyword option will be available only if a valid license is installed.

addn-pdn-connects

Drops packets containing additional PDN context connections.

This keyword option will be available only if a valid license is installed.

brr-ctxt-mod-requests

Drops packets containing Bearer Context Modification requests.

This keyword option will be available only if a valid license is installed.

combined-attaches

Drops packets containing combined Attach requests.

handovers

Drops packets containing handover attempts.

ps-attaches

Drops packets containing packet switched Attach requests.

s1-setups

Drops packets containing S1 setup attempts.

This keyword option will be available only if a valid license is installed.

service-request

Drops packets containing all service requests.

This keyword option will be available only if a valid license is installed.

tau-request

Drops packets containing all Tracking Area Update requests.

[lapi] [apn-based]

These keyword options are available only if a valid license is installed.

When a congestion action profile is configured with the **drop <call-event> lapi** option, only requests with Low Access Priority Indication (LAPI) will be dropped for those call-events during congestion. However, if the call-event is configured without the **lapi** option, all LAPI and non-LAPI requests will be dropped.

If the congestion action profile is configured with the **drop <call-event> apn-based** option, only the requests for those APNs configured for congestion control in the Operator Policy will be dropped for those call-events during congestion. However, if the call-event is configured without the **apn-based** option, all requests will be dropped. Refer to the **apn network-identifier** command in the *Operator Policy Configuration Mode* chapter to enable congestion control for a specific APN.

If the congestion action profile is configured with both the **lapi** and **apn-based** options, the call-event will be dropped only if both conditions are matched.

Usage Guidelines

Creates a congestion action profile that drops packets containing a specified request when a threshold is reached.

Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

Example

The following command drops packets containing Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
drop tau-request
```

The following command drops Additional PDN Context connetion requests when a congestion threshold has been reached. Only those APNs specified for APN-based congestion in the Operator Policy configuration mode will be dropped. Note that APN-based congestion control functionality supports APN remapping via the APN Remap Table Configuration Mode. The APN to which it is remapped will be checked for the congestion-control configuration.

```
drop addn-pdn-connects apn-based
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines

Use this command to return to the Exec mode.

exclude-emergency-events

Excludes emergency events when a congestion control threshold is reached. Emergency events continue to be processed when the threshold has been exceeded.

Product

ePDG

MME

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

`[no] exclude-emergency-events`

no

Removes the specified option from the system.

Usage Guidelines

Create a congestion action profile that allows emergency events to be processed when a congestion threshold has been reached.

When exclude-emergency is configured, congestion actions will not be applied for the following messages for emergency attached UEs:

- tau-request
- service-request
- handovers

When exclude-emergency is configured and addn-pdn-requests are configured for reject or drop actions, the reject or drop action on addn-pdn-requests for emergency PDN will not be applied.

Example

The following command allows emergency events to be processed:

`exclude-emergency-events`

exclude-voice-events

Excludes voice calls when a congestion control threshold is reached. Voice calls continue to be processed when the threshold has been exceeded.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

`[local]`*`host_name`*`(congestion-action-profile)#`

Syntax Description

`[no] exclude-voice-events`

`no`

Removes the specified option from the system.

Usage Guidelines

Create a congestion action profile that allows voice calls to be processed when a congestion threshold has been reached.

Example

The following command allows voice calls to be processed:

`exclude-voice-events`

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

`exit`

Usage Guidelines

Use this command to return to the parent configuration mode.

none

Specifies that no congestion control action be taken on an incoming request when a congestion control threshold has been reached.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

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

addn-brr-requests

No congestion control action is taken for additional bearer requests when a congestion threshold is reached.

addn-pdn-connects

No congestion control action is taken for additional PDN context connections when a congestion threshold is reached.

brr-ctxt-mod-requests

No congestion control action is taken for Bearer Resource Context Modification Requests when a congestion threshold is reached.

combined-attaches

No congestion control action is taken for combined Attach requests when a congestion threshold is reached.

handovers

No congestion control action is taken for handover attempts when a congestion threshold is reached.

ps-attaches

No congestion control action is taken for packet switched Attach requests when a congestion threshold is reached.

s1-setups

No congestion control action is taken for S1 setup attempts when a congestion threshold is reached.

service-request

No congestion control action is taken for service requests when a congestion threshold is reached.

tau-request

No congestion control action is taken for Tracking Area Update requests when a congestion threshold is reached.

Usage Guidelines

Specifies that no congestion control action be taken for the specified request when a threshold is reached. For all of the above requests, 'none' is the default action; requests are processed normally even when a congestion threshold has been reached.

Example

The following command configures the congestion action profile to take no Congeston Control action for Tracking Area Update (TAU) requests when a congestion threshold is reached, so TAU procedure proceeds normally:

```
none tau-request
```

reject

Processes a specified request when a congestion control threshold has been reached and responds with a reject message.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

```
reject { addn-brr-requests | addn-pdn-connects |  brr-ctxt-mod-requests
| combined-attaches | ddn [ arp-watermark arpwatermark_value [ cause cause_value
 ] | cause cause_value | lapi [ cause cause_value ] ] | handovers | ps-attaches
 | s1-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 } | service-request
 | tau-request }[ lapi ] [ apn-based ]
none ddn [ lapi | arp-watermark ]
```

addn-brr-requests

Rejects UE initiated bearer resource requests.

This keyword option will be available only if a valid license is installed.

addn-pdn-connects

Rejects additional PDN context connections.

This keyword option will be available only if a valid license is installed.

brr-ctxt-mod-requests

Rejects packets containing Bearer Context Modification requests.

This keyword option will be available only if a valid license is installed.

combined-attaches

Rejects combined Attach requests.

ddn [arp-watermark | cause | lapi]

The **ddn** keyword configures the action to be taken for all DDN requests. The operator can reject DDN requests based on ARP or LAPI values or both. Also, there is an option provided to reject all DDN requests without using ARP/LAPI values.

The **arp-watermark** keyword specifies that DDN reject is applicable for ARP values greater than or equal to the ARP specified. The ARP value ranges from 1 through 15.

The **cause** keyword rejects DDN with the specified cause value. The valid cause value ranges from 1 through 255. The default value is 90 with the display message "Unable to page ue".

The **lapi** keyword for DDN specifies that DDN rejection is applicable for UEs with LAPI.

This keyword option will be available only if a valid license is installed.

none

Disables DDN configuration.

handovers

Rejects handover attempts.

ps-attaches

Rejects packet switched Attach requests.

s1-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 }

Rejects S1 setup attempts with an eNodeB after 1, 2, 10, 20, 50 or 60 seconds.

This keyword option will be available only if a valid license is installed.

service-request

Rejects all service requests.

This keyword option will be available only if a valid license is installed.

tau-request

Rejects all Tracking Area Update requests.

[lapi] [apn-based]

These keyword options are available only if a valid license is installed.

When a congestion action profile is configured with the **reject <call-event> lapi** option, only requests with Low Access Priority Indication (LAPI) will be rejected for those call-events during congestion. However, if the call-event is configured without the **lapi** option, all LAPI and non-LAPI requests will be rejected.

If the congestion action profile is configured with the **reject <call-event> apn-based** option, only the requests for those APNs configured for congestion control in the Operator Policy will be rejected for those call-events

during congestion. However, if the call-event is configured without the **apn-based** option, all requests will be rejected. Refer to the **apn network-identifier** command in the *Operator Policy Configuration Mode* chapter to enable congestion control for a specific APN.

If the congestion action profile is configured with both the **lapi** and **apn-based** options, the call-event will be rejected only if both conditions are matched.

Usage Guidelines

Creates a congestion action profile that rejects a specified request when a congestion threshold is reached.

Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

Example

The following command rejects Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
reject tau-request
```

The following command rejects Additional PDN Context connetion requests when a congestion threshold has been reached. Only those APNs specified for APN-based congestion in the Operator Policy configuration mode will be rejected. Note that APN-based congestion control functionality supports APN remapping via the APN Remap Table Configuration Mode. The APN to which it is remapped will be checked for the congestion-control configuration.

```
reject addn-pdn-connects apn-based
```

report-overload

Enables the MME to report overload conditions to eNodeBs to alleviate congestion scenarios.

Product

MME

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

Syntax Description

```
report-overload { permit-emergency-sessions-and-mobile-terminated-services
 | permit-high-priority-sessions-and-mobile-terminated-services |
reject-delay-tolerant-access | reject-new-sessions |
reject-non-emergency-sessions } enodeb-percentage percent
[no] report-overload
```

no

Removes the 'report-overload' action from this congestion action profile.

permit-emergency-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only emergency sessions are allowed to access the MME during the overload period.

permit-high-priority-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only high-priority sessions and mobile-terminated services are allowed to access the MME during the overload period.

reject-delay-tolerant-access

Specifies in the overload message to the eNodeB that delay-tolerant access destined for the MME will be rejected during the overload period.

reject-new-sessions

Specifies in the overload message to the eNodeB that all new connection requests destined for the MME will be rejected during the overload period.

reject-non-emergency-sessions

Specifies in the overload message to the eNodeB that all non-emergency sessions will be rejected during the overload period.

enobeb-percentage *percentage*

Configures the percentage of known eNodeBs that will receive the overload report.

percentage must be an integer from 1 through 100.

Usage Guidelines

Configures the MME to invoke the S1 overload procedure (using the S1AP OVERLOAD START message) to report overload conditions to the specified proportion of eNodeBs to which this MME has an S1 interface connection. The MME selects the eNodeBs at random, such that two overloaded MMEs in the same pool do not send overload messages to the same eNodeBs. When the MME has recovered and can increase its load, the it sends an OVERLOAD STOP message to the eNodeBs.



Important The 'report-overload' option must be configured before the threshold is exceeded in order for the action to take place.

Example

The following command configures the MME to report an overload condition to 50% of all known eNodeBs and to request the eNodeBs to reject all non-emergency sessions to this MME until the overload condition is cleared:

```
report-overload reject-non-emergency-sessions enodeb-percentage 50
```