Global Configuration Mode Commands (threshold ppp - wsg-lookup)

The Global Configuration Mode is used to configure basic system-wide parameters.

Command Modes

This section includes the commands **threshold ppp-setup-fail-rate** through **wsg-lookup**.

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

threshold ppp-setup-fail-rate

Configures alarm or alert thresholds for the percentage of point-to-point protocol (PPP) setup failures.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold ppp-setup-fail-rate *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold rate percentage for PPP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold rate percentage for PPP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

PPP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of PPP setup failures divided by the total number of PPP sessions initiated.

Alerts or alarms are triggered for PPP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a PPP setup failure rate high percentage threshold of *50* percent and a clear threshold of *45* percent:

```
threshold ppp-setup-fail-rate 50 clear 45
```

threshold route-service bgp-routes

Configures alarm or alert thresholds for the percentage of BGP routes.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **threshold route-service bgp-routes** *high_thresh* **[clear** *low_thresh* **]**

bgp-routes

Specifies the threshold for percentage of maximum bgp routes per context. It is an integer from 0 through 100.

- *high_thresh*

  Specifies the high threshold rate percentage for maximum BGP routes per context that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

- **clear** *low_thresh*

  Specifies the low threshold rate percentage for BGP routes per context that maintains a previously generated alarm condition. If the number of BPG routes falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

For more information on the maximum route value per context, refer to *Engineering Rules* in the *System Administration Guide*.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to configure a threshold in percentage of maximum BGP routes allowed. If the percentage of the number of BGP routes in a context reaches *high_thresh*, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a **Threshold_Clear** notification is generated when the percentage of the number of BGP routes in a context goes below *low_thresh*. The maximum number of BGP routes is also sent by BGP task when getting the statistics.

Alerts or alarms are triggered for BGP routes based on the following rules:

- **Enter condition:** Actual number of BGP routes is greater than the high threshold.
- **Clear condition:** Actual number BGP routes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures system for high threshold for **bgp-routes** of *50* percent and a clear threshold of *45* percent:

```
threshold route-service bgp-routes 50 clear 45
```

threshold route-service vrf-framed-routes

Configures alarm or alert thresholds for the percentage of VRF framed routes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold route-service vrf-framed-routes *high_thresh* **[clear** *low_thresh* **] [context** *context_name* **vrf** *vrf_name* **]**

vrf-framed-routes

Specifies the threshold for percentage of VRF framed routes per VRF. It is an integer from 0 through 100.

- *high_thresh*

  Specifies the high threshold rate percentage for VRF framed routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 100. A value of 0 disables the threshold. The default value is 0.

- **clear** *low_thresh*

  Configures the alarm clear threshold. It is an integer from 0 through 100. The default value is 0.

- **context** *context_name*

  Configures the context to apply **vrf-framed-routes** threshold.

- **vrf** *vrf_name*

  Configures the VRF to apply **vrf-framed-routes** threshold.

For more information on the maximum route value per context, refer to *Engineering Rules* in the *System Administration Guide*.

Important

When the root level version of the **threshold route-service** command is issued without **context** and **vrf** information, the framed routes threshold value is configured for every VRF in the system. When the vrf-framed-routes command is issued for a specific context and VRF name, then the threshold value is configured only for that context and VRF. Any previously configured root level or VRF specific threshold value will be overwritten. The threshold values are set as a percentage of the ip maximum routes for the VRF. If ip maximum routes for a VRF is not configured, the default value is the maximum routes per context. If the threshold values in the above CLI command is set to 0, then the respective threshold configuration is removed.

Usage Guidelines

Use this command to configure a threshold in percentage of the maximum VRF framed routes. If the percentage of the number VRF framed routes reaches *high_thresh*, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a **Threshold_Clear** notification is generated when the percentage of the number of VRF framed routes s in a context goes below *low_thresh*.

Alerts or alarms are triggered for VRF framed routes based on the following rules:

- **Enter condition:** Actual number of VRF framed routes is greater than the high threshold.
- **Clear condition:** Actual number of VRF framed routes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures system for high threshold for **vrf-framed-routes** of *70* percent with a clear threshold of *40* percent for all the VRFs in the system:

```
threshold route-service vrf-framed-routes 70 clear 40
```

The following command configures system for high threshold for **vrf-framed-routes** of *30* percent with a clear threshold of *20* percent for a context *egress1* and vrf *vrf1*:

```
threshold route-service vrf-framed-routes 30 clear 20 context egress1 vrf
 vrf1
```

threshold route-service vrf-total-routes

Configures alarm or alert thresholds for the count of VRF total routes.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold route-service vrf-total-routes *high_thresh* **[clear** *low_thresh* **] [context** *context_name* **vrf** *vrf_name* **]**

vrf-total-routes

Specifies the number of VRF total routes threshold value per VRF. It is an integer from 0 through 65536.

- *high_thresh*

  Specifies the high threshold count of total routes per VRF that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 65536. A value of 0 disables the threshold. The default value is 0.

- **clear** *low_thresh*

  Configures the alarms clear threshold. It is an integer from 0 through 65536. The default is 0.

- **context** *context_name*

  Configures the context to apply **vrf-total-routes** threshold.

- **vrf** *vrf_name*

  Configures the VRF to apply **vrf-total-routes** threshold.

For more information on the maximum route value per context, refer to *Engineering Rules* in the *System Administration Guide*.

Important When the root level version of the **threshold-route-service** command is issued without **context** and **vrf** information, the total routes threshold value is configured for every VRF in the system. When the **vrf-total-routes** command is issued for a specific context and VRF name, the threshold value is configured only for that context and VRF. Any previously configured root level or VRF specific threshold value will be overwritten. The threshold values are set as the total count of the routes in the VRF which includes pool routes, interface routes, static routes, dynamic routes and framed routes. If the threshold values in the above CLI command is set to 0, then the respective threshold configuration is removed.

Usage Guidelines

Use this command to configure a threshold in number of the VRF total routes. If the count of VRF total routes in a context reaches *high_thresh*, a notification is generated. Optionally, if the threshold subsystem is configured in 'alarm' mode, a **Threshold_Clear** notification is generated when count of VRF total routes in a context goes below *low_thresh*.

Alerts or alarms are triggered VRF total routes based on the following rules:

- **Enter condition:** Actual number of VRF total routes is greater than the high threshold.
- **Clear condition:** Actual number of VRF total routes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures system for high threshold for **vrf-total-routes** of *3000* with a clear threshold of *2800* for all the VRFs in the system

```
threshold route-service vrf-total-routes 3000 clear 2800
```

The following command configures system for high threshold for **vrf-total-routes** of *1500* with a clear threshold of *800* for a context *egress1* and vrf *vrf1*:

```
threshold route-service vrf-total-routes 1500 clear 800 context egress1
vrf vrf1
```

threshold rp-setup-fail-rate

Configures alarm or alert thresholds for the percentage of RAN PDSN (RP) setup failures.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold rp-setup-fail-rate *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold rate percentage for RP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold rate percentage for RP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

RP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of Registration Request Messages rejected divided by the total number of Registration Request Messages received.

Alerts or alarms are triggered for RP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a RP setup failure rate high threshold of *50* percent and a clear threshold of *45* percent:

```
threshold rp-setup-fail-rate 50 clear 45
```

threshold sess-flow-count

Configures alarm or alert thresholds for the percentage of session manager flow count.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold sess-flow-count *flow_count_thresh* **[clear** *clear_thresh* **]**

flow_count_percent

Default: 90

Specifies the high threshold rate percentage for session manager flow count to generate an alert or alarm.

flow_count_thresh is an integer from 1 through 100.

clear *clear_thresh*

Specifies the low threshold rate percentage for session manager flow count. If the number of session manager flow count falls beneath the low threshold, a clear alarm will be generated.

clear_thresh is an integer from 1 through 100. The value chosen for the *clear_thresh* must always be lesser than the *flow_count_thresh*.

Usage Guidelines

Use this command to configure thresholds for monitoring the session flow count.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a session flow count high threshold of *50* percent and a clear threshold of *45* percent:

```
threshold sess-flow-count 50 clear 45
```

threshold storage-utilization

Configures alarm or alert thresholds for the percentage of management card flash memory utilization.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold storage-utilization *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 90

Specifies the high threshold storage utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 90

Specifies the low threshold storage utilization percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Flash memory utilization thresholds generate alerts or alarms based on the utilization percentage of storage available to the system.

Alerts or alarms are triggered for storage utilization based on the following rules:

- **Enter condition:** Actual percentage storage utilization is greater than or equal to the high threshold.
- **Clear condition:** Actual percentage storage utilization is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold for storage utilization percentage of *85* for a system using the Alert thresholding model:

```
threshold storage-utilization 85
```

threshold subscriber active

Configures alarm or alert thresholds for the number of active subscribers in the system.

Product

PDSN

GGSN

SGSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold subscriber active *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of active subscriber sessions facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of active subscriber sessions facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Active subscriber thresholds generate alerts or alarms based on the total number of active subscriber sessions facilitated by the system during the specified polling interval.

Alerts or alarms are triggered for active subscriber totals based on the following rules:

- **Enter condition:** Actual total number of active subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of active subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures an active subscriber high threshold count of *150000* and a low threshold of *100000* for a system using the Alarm thresholding model:

```
threshold subscriber active 150000 clear 100000
```

threshold subscriber total

Configures alarm or alert thresholds for the total number of active and inactive subscribers in the system.

Product

PDSN

GGSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold subscriber total *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of subscriber sessions (active and dormant) facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of subscriber sessions (active and dormant) facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Total subscriber thresholds generate alerts or alarms based on the total number of subscriber sessions (active and dormant) facilitated by the system during the specified polling interval.

Alerts or alarms are triggered for subscriber totals based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures an active subscriber high threshold count of *450000* and a low threshold of *250000* for a system using the Alarm thresholding model:

```
threshold subscriber total 450000 clear 250000
```

threshold system-capacity

Configures alarm or alert thresholds based on the percentage of current system capacity.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold system *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 90

Specifies the high threshold system capacity percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear *low_thresh*

Default: 90

Specifies the low threshold system capacity percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Flash memory utilization thresholds generate alerts or alarms based on the system utilization.

Alerts or alarms are triggered for system capacity based on the following rules:

- **Enter condition:** Actual percentage of system capacity is greater than or equal to the high threshold.
- **Clear condition:** Actual percentage of system capacity is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a high threshold for system capacity percentage of *95* for a system using the Alert thresholding model:

```
threshold system-capacity 95
```

threshold total-asngw-sessions

Configures alarm or alert thresholds for the total number of ASN-GW sessions across all the services in the system.

Product

ANS-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-asngw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold number of total ASN-GW sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold number of total ASN-GW sessions that maintains a previously generated alarm condition. If the number of ASN-GW sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important

This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of ASN-GW sessions across all the services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of ASN-GW sessions based on the following rules:

- **Enter condition:** Actual total number of ASN-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of ASN-GW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total ASN-GW session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-asngw-sessions 10000
```

threshold total-ggsn-sessions

Configures alarm or alert thresholds for the total number of GGSN sessions across all the services in the system.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-ggsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold number of total GGSN sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold number of total GGSN sessions that maintains a previously generated alarm condition. If the number of GGSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of GGSN sessions across all the services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of GGSN sessions based on the following rules:

- **Enter condition:** Actual total number of GGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total GGSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-ggsn-sessions 10000
```

threshold total-gprs-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts per GPRS sessions in the system.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-gprs-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total PDP contexts per GPRS session for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total PDP contexts per GPRS session for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of PDP Contexts is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of PDP contexts per GPRS session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-gprs-pdp-sessions 10000
```

threshold total-gprs-sessions

Configures alarm or alert thresholds for the total number of GPRS sessions in the system.

Product SGSN

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **threshold total-gprs-sessions** *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total GPRS sessions for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total GPRS sessions for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of GPRS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GPRS sessions is less than the low threshol.d

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of GPRS sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-gprs-sessions 10000
```

threshold total-ha-sessions

Configures alarm or alert thresholds for the total number of Home Agent (HA) sessions across all services in the system.

Product HA

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-ha-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of HA sessions for all HA services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of HA sessions for all HA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of HA sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition:** Actual total number of HA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of HA sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-ha-sessions 10000
```

threshold total-hnbgw-hnb-sessions

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Configures alarm or alert thresholds for the total number of Home NodeB (HNB) sessions across all the HNB Gateway (HNB-GW) services in the system.

Product

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-hnbgw-hnb-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all services on a system that maintains a previously generated alarm condition. If the number of HNB-HNB-GW sessions in a system falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to monitor and set alarms or alerts when the total number of HNB-HNB-GW sessions on IuH interface across all HNB-GW services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of HNB-HNB-GW sessions on IuH interface based on the following rules:

- **Enter condition:** Actual total number of HNB-HNB-GW sessions on IuH interface is greater than the high threshold.
- **Clear condition:** Actual total number of HNB-HNB-GW sessions on IuH interfaces is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll total-hnbgw-hnb-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshTotalHNBGWHnbSess** command in this mode.

Example

The following command configures the total number of HNB-GW-HNB sessions on IuH interfaces to a high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-hnb-sessions 10000
```

threshold total-hnbgw-iu-sessions

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Configures alarm or alert thresholds for the total number of subscriber sessions towards the Core Networks (CN) across all HNBGW services over Iu interfaces (Iu-CS/Iu-PS interface) on a system.

Product

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-hnbgw-iu-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold for the total number of subscriber sessions towards CN across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold for the total number of subscriber sessions towards CN across all services on a system that maintains a previously generated alarm condition. If the number of subscriber sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to monitor and set alarms or alerts when the total number of subscriber sessions towards CN across all HNB-GW services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of subscriber sessions towards CN across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is greater than the high threshold.
- **Clear condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll total-hnbgw-iu-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshTotalHNBGWIuSess** command in this mode.

Example

The following command configures the total number of subscriber sessions towards CN across all HNB-GW services to a high threshold count of *30000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-iu-sessions 30000
```

threshold total-hnbgw-ue-sessions

Important In Release 20 and later, HNBGW is not supported. This command must not be used for HNBGW in Release 20 and later. For more information, contact your Cisco account representative.

Configures alarm or alert thresholds for the total number of UEs connected to an HNB-GW service across all the HNB-GW services in the system.

Product

HNBGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-hnbgw-ue-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold for the total number of UEs connected across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold for the total number of UEs connected to HNB-GW service across all HNB-GW services that maintains a previously generated alarm condition. If the number of UE sessions across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to monitor and set alarms or alerts when the total number of UEs connected to HNB-GW service across all HNB-GW services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of UEs connected across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is greater than the high threshold.
- **Clear condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll total-hnbgw-ue-sessions** command to configure the polling interval and the **threshold monitoring hnbgw-service** command to enable thresholding for this value.

Important To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshTotalHNBGWUeSess** command in this mode.

Example

The following command configures the total number of UEs connected to HNB-GW service across all HNB-GW services to a high threshold count of *40000* for a system using the Alert thresholding model:

```
threshold total-hnbgw-ue-sessions 40000
```

threshold total-hsgw-sessions

Configures alarm or alert thresholds for the total number of HRPD Serving Gateway (HSGW) sessions across all services in the system.

Product HSGW

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **threshold total-hsgw-sessions** *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold for the number of HSGW sessions for all HSGW services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold for the number of HSGW sessions for all HSGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2500000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of HSGW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for HSGW sessions based on the following rules:

- **Enter condition:** Actual total number of HSGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HSGW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of HSGW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-hsgw-sessions 500000
```

threshold total-lma-sessions

Configures alarm or alert thresholds for the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

Product

P-GW

SAEGW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-lma-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of LMA sessions for all LMA services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 1500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of LMA sessions for all LMA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1500000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of LMA sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for LMA sessions based on the following rules:

- **Enter condition:** Actual total number of LMA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LMA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of LMA sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-lma-sessions 500000
```

threshold total-lns-sessions

Configures alarm or alert thresholds for the total number of L2TP Network Server (LNS) sessions in the system.

Product

PDSN

GGSN

HA

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-lns-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total LNS sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total LNS sessions that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of LNS sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of LNS sessions based on the following rules:

- **Enter condition:** Actual total number of LNS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LNS sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total LNS session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-lns-sessions 10000
```

threshold total-mme-sessions

Configures alarm or alert thresholds for the total number of Mobility Management Entity (MME) sessions across all the MME services in the system.

Product

MME

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-mme-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0 (Disabled)

Specifies the high threshold number of total MME sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0 (Disabled)

Specifies the low threshold number of total MME sessions that maintains a previously generated alarm condition. If the number of MME sessions, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2500000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Use this command to monitor and set alarms or alerts when the total number of MME sessions across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME sessions based on the following rules:

- **Enter condition:** Actual total number of MME sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll total-mme-sessions** command to configure the polling interval and the **threshold monitoring mme-service** command to enable thresholding for this value.

Example

The following command configures a total MME session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-mme-sessions 10000
```

threshold total-pdsn-sessions

Configures alarm or alert thresholds for the total number of Packet Data Serving Node (PDSN) sessions in the system.

Product

PDSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-pdsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total PDSN sessions that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total PDSN sessions that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2500000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines Monitor and set alarms or alerts when the total number of PDSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of PDSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total PDSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-pdsn-sessions 10000
```

threshold total-pgw-sessions

Configures alarm or alert thresholds for the total number of Packet Data Network Gateway (P-GW) sessions across all services in the system.

Product P-GW

SAEGW

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **threshold total-pgw-sessions** *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of P-GW sessions for all P-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 3000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of P-GW sessions for all P-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of P-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for P-GW sessions based on the following rules:

- **Enter condition:** Actual total number of P-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of P-GW sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of P-GW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-pgw-sessions 500000
```

threshold total-saegw-sessions

Configures alarm or alert thresholds for the total number of System Architecture Evolution Gateway (SAEGW) sessions across all services in the system.

Product SAEGW

Privilege Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-saegw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of SAEGW sessions for all SAEGW services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 3000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of SAEGW sessions for all SAEGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of SAEGW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SAEGW sessions based on the following rules:

- **Enter condition:** Actual total number of SAEGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SAEGW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of SAEGW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-saegw-sessions 500000
```

threshold total-sgsn-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts for all Serving GPRS Support Node (SGSN) sessions in the system.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-sgsn-pdp-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total PDP contexts per SGSN session for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 4000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total PDP contexts per SGSN session for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

Important

This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDP contexts is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of PDP contexts per SGSN session high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-sgsn-pdp-sessions 10000
```

threshold total-sgsn-sessions

Configures alarm or alert thresholds for the total number of SGSN sessions in the system.

Product

SGSN

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-sgsn-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of total SGSN sessions for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of total SGSN sessions for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important

This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of SGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of SGSN sessions high threshold count of *10000* for a system using the Alert thresholding model:

```
threshold total-sgsn-sessions 10000
```

threshold total-sgw-sessions

Configures alarm or alert thresholds for the total number of Serving Gateway (S-GW) sessions across all services in the system.

Product

S-GW

Privilege

Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

threshold total-sgw-sessions *high_thresh* **[clear** *low_thresh* **]**

high_thresh

Default: 0

Specifies the high threshold number of S-GW sessions for all S-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 3000000. A value of 0 disables the threshold.

clear *low_thresh*

Default: 0

Specifies the low threshold number of S-GW sessions for all S-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage Guidelines

Monitor and set alarms or alerts when the total number of S-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for S-GW sessions based on the following rules:

- **Enter condition:** Actual total number of S-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of S-GW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

Example

The following command configures a total number of S-GW sessions high threshold count of *500000* for a system using the Alert thresholding model:

```
threshold total-sgw-sessions 500000
```

throttling-override-policy

Creates a GTP-C Throttling Override Policy. Entering this command creates a Throttling Override Policy mode. Use this mode to configure the Throttling Override Policy that can be used at the GGSN/P-GW nodes to selectively bypass throttling for a configured message type or for the configured APN.

Product

GGSN

P-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description **throttling-override-policy** *throttling-override-policy_name*

throttling-override-policy

Creates a GTP-C throttling overrride policy.

throttling-override-policy_name is a throttling overrride policy name for the policy that can be used at the GGSN/P-GW nodes.

Usage Guidelines Enter this command mode to configure the Throttling Override Policy that can be used at the GGSN/P-GW nodes to selectively bypass throttling for a configured message type or for the configured APN.

Example

Use the following command to enter throttling-override-policy mode:

throttling-override-policy *throttling-override-policy_name*

timestamps

Enables or disables the generation of a timestamp in response to each commands entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects all future CLI sessions. Use the **timestamps** command in the Exec Mode to change the behavior for the current CLI session only.

Product All

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

Syntax Description

timestamps
no timestamps

no

Disables generation of timestamps for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

Usage Guidelines Enable the timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

Example

The following commands enable and disable timestamps for each CLI command:

timestamps

no timestamps

traffic shape

Configures the maximum buffer limit for sessmgr and subscribers for use during traffic shaping.

Product

GGSN

P-GW

SAEGW

Important Traffic Shaping is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

Privilege

Administrator, Security Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

traffic shape max-buffer-size sessmgr *MBs* **subscriber** *MBs*
default traffic shape max-buffer-size

default

Returns sessmgr and subscriber settings to their default values.

Default setting for the sessmgr is 10MB. Default setting for the subscriber is 1MB.

traffic

Allows configuration for data traffic.

shape

Allows configuration for traffic shaping.

max-buffer-size

Allows configuration of the maximum buffer size for the session manager and subscriber.

sessmgr

Specifies the maximum buffer limit for the session manager for use during traffic shaping.

Valid entries are from 1 to 100 MB.

The default is 10 MB.

The sessmgr value should be greater than the subscriber value.

Caution Standard size buffers (500, 2k, and 10k bytes) are used for buffering packets to avoid memory fragmentation. As a result, there may be additional memory overhead in the memory used for buffering. The buffer limit in the above configuration refers to actual effective bytes used to store packets. Use caution to use appropriate buffer limits, so that the system does not significantly affect the overall Session Manager memory requirement for sessions.

subscriber

Specifies the maximum buffer limit for subscriber use during traffic shaping.

Valid entries are from 1 to 100 MB.

The default is 1 MB.

The **subscriber** value should be less than the **sessmgr** value.

Note

Usage Guidelines Use this command to set the maximum memory buffer limit for session manager and subscriber use during traffic shaping.

Traffic shaping and policing must first be configured in *APN Configuration Mode* using the **apn-ambr** command before the **traffic shape** command can be used.

Example

The following example configures the maximum buffer size for the sessmgr at 20 MB, and configures the maximum buffer size for subscriber at 2 MB:

```
traffic shape max-buffer-size sessmgr 20 subscriber 2
```

transaction-rate bucket-interval

Enables operators to set the time interval used for gathering transaction rate Session Events per Second and N/w Initiated Setup/Teardown Events per Second key performance indicator (KPI) information.

Product ePDG

P-GW

SAE-GW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

transaction-rate bucket-interval*time-interval*
default transaction-rate bucket-interval

transaction-rate bucket-interval *time_interval*

Where **bucket-interval** is the time interval, in minutes, used for gathering transaction rate statistics. This setting must be an integer from 1 to 20 minutes. The default value is 2 minutes. If no entry is made for the **bucket-interval**, then the default value of 2 minutes is used.

default

Returns the bucket-interval setting to the default value of 2 minutes.

Usage Guidelines

Session Events Per Second (SEPS) KPIs measure the signaling load on the P-GW/ePDG. Network initiated setup/tear down KPIs are available to measure the event rate for VoLTE call setup and tear down. Together, these measurements assist operators in performing network dimensioning/planning for the P-GW/SAE-GW/ePDG node.

The P-GW/SAE-GW/ePDG contains 8 buckets for transaction rate statistics collection for both session events per second KPIs and N/w Initiated Setup/Tear down Events per Second KPIs. The buckets are based on a configurable bucket interval that is from 1 to 20 minutes in length. During the configured time interval, an average is computed and stored for the entire bucket interval.

After the first 8 bucket intervals have elapsed and statistics collected, the P-GW continues sequentially through the 8 bucket intervals and eventually overwrites the original 8 bucket-intervals with more recent data. In short, the 8 bucket intervals provide a running average for the last eight bucket-intervals for which KPIs have been computed. While the bucket-interval statistics are eventually overwritten with new values, all statistic totals are added to the historical statistics, which are not overwritten.

To keep the number of buckets carrying new data across 2 consecutive bulk statistics sampling intervals as constant, use the following recommended configuration:

- Configure the bucket-interval so that the bulk statistic sampling interval is an integer (from 1 to 8) multiple of the configured bucket-interval. This new integer multiple reflects the number of buckets with new information in a given sampling interval. For example:
  - If the bulk statistic sampling interval is 15, then the configured bucket interval should be 3 so that the bucket interval is an integer multiple (3*5=15) of the sampling interval. In this case, 5 indicates the number of buckets with new information in a given sampling interval.
  - Similarly, when the bulk statistic sampling interval is 16, then the bucket interval could be 2 (so that 2*8=16). In this example 8 is the number of buckets with new information in a given sampling interval.
- The transaction rates statistics are lost if the sessmgr/demuxmgr restarts. Also the cumulative statistics accumulated to that point are also lost.
- If the sessmgr/demuxmgr restarts in the middle of a bucket interval, the transaction rates stats collected to that point are lost.

To view transaction rate KPI information, use the **show transaction-rate pgw-service** command in *Exec Mode*.

Example

Use the following command to set the bucket-interval for SEPS and network initiated setup/tear down KPIs to 3 minutes:

```
transaction-rate bucket-interval 3
```

transaction-rate nw-initiated-setup-teardown-events qci

Enables operators to set the Quality of Class Identifier (QCI) value for use in tracking Network Initiated Setup/Tear down Events per Second key performance indicator (KPI) information.

Product

ePDG

P-GW

SAE-GW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

transaction-rate nw-initiated-setup-teardown-events qci [all | *qci_value*]
default transaction-rate nw-initiated-setup-teardown-events qci[all | *qci_value*]
no transaction-rate nw-initiated-setup-teardown-events qci[all | *qci_value*]

transaction-rate nw-initiated-setup-teardown-events qci *qci_value*

Specifies the Quality of Service Class Identifier (QCI) value for which nw-initiated-setup-teardown-events will be tracked. QCI values of 1-9, 65, 66, 69, 70, 80, 82, 83 and 128 - 254 are supported. A maximum of 4 unique QCI settings can be configured. The default is for network-initiated setup/teardown events to be supported for all supported QCI values.

QCI values 65 and 66 are available for guaranteed bit rate (GBR) network initiated QCI values only.

QCI values 69 and 70 are available for non-GBR network initiated QCI values only.

all : Specifies all the Quality of Service Class Identifier (QCI) values for which nw-initiated-setup-teardown-events will be tracked.

default

Returns the setting to its default value. The default is for network-initiated setup/teardown events to be tracked for all supported QCI values.

no

Disables the collection of network-initiated setup/teardown events for the specified QCI value.

Usage Guidelines

Network initiated setup/tear down KPIs are available to measure the event rate for VoLTE call setup and tear down. These KPIs assist operators in performing network dimensioning/planning for the P-GW/ePDG node.

The P-GW/ePDG contains 8 buckets for transaction rate statistics collection for N/w Initiated Setup/Tear down Events per Second KPIs. The buckets are based on a configurable bucket interval that is from 1 to 20 minutes in length. During the configured time interval, an average is computed and stored for the entire bucket interval. Refer to the description of the **transaction-rate bucket-interval** command in Global Configuration Mode Commands chapter for details on configuring the bucket interval.

The transaction rates statistics are lost when the sessmgr/demux restarts.

Existing transaction-rate configuration settings can be viewed by using the **show configuration** command in Exec Mode.

To view network-initiated setup/tear down event statistics, use the **show transaction-rate pgw-service** command in Exec Mode.

To clear the transaction-rate statistics, use the **clear transaction-rate pgw-service** command in Exec Mode.

Example

Use the following command to set QCI value for network-initiated setup/tear down event KPIs to 3:

```
transaction-rate nw-initiated-setup-teardown-events qci 3
```

unexpected-scenario session drop-call

Configures behavior when an unexpected call processing scenario is encountered. Enabling this command sets call clearing logic that replaces the automatic generation of asserts and core dumps for an initial assert.

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
unexpected-scenario session drop-call [ disable-core ]
```

```
default unexpected-scenario session drop-call
```

default

Disables call clearing logic for a graceful assert. This results in automatic core dump generation for unexpected scenarios resulting in control and data outage for the task instance until the core is fully generated.

[disable-core]

This option disables the automatic generation of core dumps when a call is dropped for a specific session.

Usage Guidelines

Use this command to enable call clearing logic that will minimize the automatic generation of asserts and core dumps during a specific call processing session that may lead to data outage and session manager recovery.

The call clearing logic is only applied to the first assert generated during a call processing session. When that assert occurs, a zero-second timer lets the current stack unwind to avoid reentrancy issues. The call is then dropped from all interfaces. This is considered to be a graceful assert.

A core dump is generated along with any application supplied debug info. The line number and file index of the ASSERT appears in the call-line; the current call-line is marked as being in "assert_hit" scenario.

With the **disable-core** option set, a core dump is not generated following a graceful assert.

An assert generated after a graceful assert for the same unexpected scenario will cause the call to be dropped and trigger an automatic core dump. Depending on the length of time required to generate the associated core dump, a session manager recovery may be initiated. This is a highly unlikely possibility.

Important The graceful assert call clearing logic can only be applied to call processing events, such as VoLTE. It cannot be used for ICSR-SRP scenarios.

Example

The following command enables call clearing logic for graceful asserts of initial call processing failures:

```
unexpected-scenario session drop-call disable-core
```

wait cards timeout

Configures the active CF to pause the application of configuration to other cards/VMs during bootup until the specified timeout period expires (VPC-DI only).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
wait cards timeout seconds
no wait cards timeout
```

no

Removes the timeout (timeout = 0 seconds); SF cards do not wait to apply the configuration to other cards.

timeout *seconds*

timeout

Wait for the specified number of seconds before applying the configuration. The wait is terminated early when/if the cards specified in the **wait cards mask** *cards* | **actives** *cards* command become operational. Otherwise the wait is terminated when the timeout period expires.

seconds : An integer from 0 through 3600. Default: 300 seconds.

Usage Guidelines

Use this command to set the time in seconds to pause the application of configuration by the CF to the SFs until all specified cards are operational or the timeout period expires (whichever criteria is met first). The pause occurs immediately following local management context creation and ntp/snmp configuration.

This prevents a scenario where SFs come online late following chassis load/reload and the configuration pertaining to those SFs is not applied (and thereby lost).

During the wait period, information messages are reported on the console every 30 seconds.

Example

The following example command instructs the system to wait up to 120 seconds before applying the configuration to the SF cards:

```
wait cards timeout 120
```

wait cards

Configures the active CF to pause the application of configuration to other cards/VMs during bootup until the specified cards are operational (VPC-DI only).

Product

All

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

```
wait cards [ mask bitmask-value | actives active-count ]
no wait cards
```

no

Returns this setting to the default behavior where CF does not wait to apply the configuration to other cards.

mask *bitmask-value*

mask

Specifies a bitmask of specific cards to wait to reach terminal operational state before applying the configuration.

bitmask-value : A bitmask value specifying the specific cards; cards 3 through 7 would be entered as **3-7**, cards 4 and 8 is entered as **4,8**, and cards 3 through 10, 12 through 14, 16 and 19 would be entered as **3-10,12-14,16,19**.

actives *active-count*

actives

Specifies the number of cards to wait to become active before applying the configuration.

active-count : An integer value from 3 through 48.

Usage Guidelines

Use this command to define the specific cards, or number of cards, which must become active before the CF applies the configuration to the other cards in the system. The pause occurs immediately following local management context creation and ntp/snmp configuration.

The values for the keywords in this command are automatically generated by the system each time a **save configuration** command is issued.

As a result, the **mask** and **actives** keywords described below are concealed commands. These commands should only be used in specific instances where these settings must be manually applied.

In Release 21.3.3-21.5, the command **wait card active** *active-count* **standby** *standby-count* **timeout** *timeout-value* was used to control this Boot Configuration Pause functionality. In Release 21.6 and higher, this command has been deprecated. If this command exists in the configuration file, the system will honor the **timeout** *timeout-value* command, and **active** *active-count* **standby** *standby-count* keywords of the deprecated command.

Example

The following example command instructs the system to wait for cards 2-10 to become active and at least 12 cards become active overall:

```
wait cards mask 2-10 actives 12
```

The following example command instructs the system to wait for cards 2-10 to become active or at least 8 cards to become active:

```
wait cards mask 2-10 actives 8
```

The following example command instructs the system to wait for at least 8 cards to become active:

```
wait cards actives 8
```

wsg-lookup

Enters the WSG lookup priority list configuration mode for site-to-site tunnels.

Product

WSG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax Description

wsg-lookup

Usage Guidelines

Use this command to enter the WSG lookup priority list configuration mode for site-to-site tunnels.

Examples

The following command enters the SG lookup priority configuration mode:

wsg-lookup