Global Configuration Mode Commands
(T-threshold phspc)

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

This section includes the commands tacacs mode through threshold phspc-sm-entry-denial.

Command Modes
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).

- tacacs mode, page 5
- task facility acsmgr, page 6
- task facility insimgr, page 7
- task facility ipsecmgr, page 10
- task facility linkmgr, page 12
- task facility mmedemux, page 14
- task facility mmemgr, page 16
- task facility mmemgr max, page 18
- task facility mmemgr per-sesscard-count, page 20
- task facility sessmgr, page 22
- task resource cpu-memory-low, page 23
- tech-support test-commands password, page 24
• template-session-trace, page 26
• terminal, page 27
• threshold 10sec-cpu-utilization, page 29
• threshold aaa-acct-archive-queue-size, page 31
• threshold aaa-acct-archive-size, page 33
• threshold aaa-acct-failure, page 35
• threshold aaa-acct-failure-rate, page 37
• threshold aaa-auth-failure, page 39
• threshold aaa-auth-failure-rate, page 41
• threshold aaa-retry-rate, page 43
• threshold aaamgr-request-queue, page 45
• threshold asngw-auth-failure, page 47
• threshold asngw-handoff-denial, page 49
• threshold asngw-max-eap-retry, page 51
• threshold asngw-network-entry-denial, page 53
• threshold asngw-r6-invalid-nai, page 55
• threshold asngw-session-setup-timeout, page 57
• threshold asngw-session-timeout, page 59
• threshold asnpc-idle-mode-timeout, page 61
• threshold asnpc-im-entry-denial, page 63
• threshold asnpc-lu-denial, page 65
• threshold asnpc-session-setup-timeout, page 67
• threshold call-reject-no-resource, page 68
• threshold call-setup, page 70
• threshold call-setup-failure, page 72
• threshold card-temperature-near-power-off-limit, page 74
• threshold cdr-file-space, page 75
• threshold contfilt-block, page 77
• threshold contfilt-rating, page 79
• threshold cpu-available-memory, page 81
• threshold cpu-load, page 83
• threshold cpu-memory-usage, page 85
• threshold cpu-orbs-crit, page 87
• threshold cpu-orbs-warn, page 89
• threshold cpu-session-throughput, page 91
• threshold cpu-utilization, page 93
• threshold dcca-bad-answers, page 95
• threshold dcca-protocol-error, page 97
• threshold dcca-rating-failed, page 99
• threshold dcca-unknown-rating-group, page 101
• threshold diameter diameter-retry-rate, page 103
• threshold dns-learnt-ip-max-entries, page 105
• threshold dns-learnt-ipv4-max-entries, page 107
• threshold dns-learnt-ipv6-max-entries, page 109
• threshold dns-lookup-failure, page 111
• threshold edr-file-space, page 113
• threshold edr-udr-dropped flow control, page 115
• threshold egtpc-s2b-setup-fail-rate, page 117
• threshold egtpc-s5-setup-fail-rate, page 119
• threshold epdg-current-sessions, page 121
• threshold fng-current-active-sessions, page 123
• threshold fng-current-sessions, page 125
• threshold fw-deny-rule, page 127
• threshold fw-dos-attack, page 129
• threshold fw-drop-packet, page 131
• threshold fw-no-rule, page 133
• threshold license remaining-sessions, page 135
• threshold mgmt-cpu-memory-usage, page 137
• threshold mgmt-cpu-utilization, page 139
• threshold mme-attach-failure, page 141
• threshold mme-auth-failure, page 143
• threshold model, page 145
• threshold monitoring, page 147
• threshold nat-pkt-drop, page 154
• threshold nat-port-chunks-usage, page 156
• threshold npu-utilization, page 158
- threshold packets-filtered-dropped, page 160
- threshold packets-forwarded-to-cpu, page 162
- threshold pdg-current-active-sessions, page 164
- threshold pdg-current-sessions, page 165
- threshold pdif-current-active-sessions, page 166
- threshold pdif-current-sessions, page 167
- threshold per-service-asngw-sessions, page 168
- threshold per-service-ggsn-sessions, page 170
- threshold per-service-gprs-pdp-sessions, page 172
- threshold per-service-gprs-sessions, page 174
- threshold per-service-ha-sessions, page 176
- threshold per-service-Ins-sessions, page 178
- threshold per-service-pdg-sessions, page 180
- threshold per-service-pdsn-sessions, page 182
- threshold per-service-samog-sessions, page 184
- threshold per-service-sgsn-pdp-sessions, page 186
- threshold per-service-sgsn-sessions, page 188
- threshold phsgw-auth-failure, page 190
- threshold phsgw-eapol-auth-failure, page 192
- threshold phsgw-handoff-denial, page 194
- threshold phsgw-max-eap-retry, page 196
- threshold phsgw-max-eapol-retry, page 198
- threshold phsgw-network-entry-denial, page 200
- threshold phsgw-session-setup-timeout, page 202
- threshold phsgw-session-timeout, page 204
- threshold phspc-session-setup-timeout, page 206
- threshold phspc-sleep-mode-timeout, page 208
- threshold phspc-sm-entry-denial, page 210
**tacacs mode**

Enters the TACACS+ (Terminal Access Controller Access Control System+) configuration mode. Use this mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol.

**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**
tacacs mode

**Usage Guidelines**
Enter TACACS Configuration Mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol. For additional information, see the *TACACS+ Configuration Mode Commands* chapter.

**Examples**
Use the following command to enter TACACS mode:
```
tacacs mode
```
task facility acsmgr

This command configures ACSMgr task settings.

Product
ACS

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
  task facility acsmgr start | aggressive | normal |
  no task facility acsmgr start

  no
  Disables the configured ACSMgr setting.

  aggressive
  Specifies to start the maximum possible ACSMgr tasks.

  normal
  Configures the resource subsystem to start/stop ACSMgr tasks on an as-needed basis.

Usage Guidelines
This command provides option for the resource subsystem to start maximum possible ACSMgr tasks based on the license configured and the available system configuration.

Examples
The following command starts the maximum possible ACSMgr tasks:
  task facility acsmgr start aggressive
task facility imsimgr

This command is used to configure the IMSI Manager parameters.

**Product**
SGSN
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**

task facility imsimgr { avoid-sessmgr-broadcast { cpu_threshold percentage_value } | max <integer_value> | required-sessmgr no_sess_mgrs | sessmgr-sessions-threshold high-watermark <high_value> low-watermark <low_value> }

no task facility imsimgr [ avoid-sessmgr-broadcast | required-sessmgr ]

default task facility imsimgr sessmgr-sessions-threshold

no

Disables the selected parameter's functionality in the configuration.

default

This prefix is only used with the ** sessmgr-sessions-threshold** parameter. By default, the threshold levels are set to the maximum allowed sessions per Session Manager based on the card type. Both high and low watermarks are set to "100%" by default to ensure backward compatibility.

**avoid-sessmgr-broadcast**

This keyword configures the IMSIMgr to avoid or disable broadcast requests to all SessMgrs when the IMSIMgr finds a particular IMSI is unknown. With this keyword, broadcasting can be disabled 'on the fly' if CPU usage is too high due to a large number of broadcast messages.

By default, broadcasting is enabled.
**max integer_value**

This keyword defines the number of IMSI managers spawned for the system. This keyword is supported only on ASR5500 and VPC-DI platforms. A maximum of "4" IMSI Managers can be configured for release prior to 21.0.

---

**Important**

**max** is a boot-time configuration setting. It should be added in the configuration file before any SGSN/MME related configuration is created or any IMSI Manager is started. Run-time (dynamic) configuration of this parameter is stored but not effective until after the next reboot. Any attempt at dynamic configuration of this parameter results in a display of the following error message:

New config requires system restart to be effective. Please save config and restart.

---

**cpu_threshold percentage_value**

The keyword "cpu_threshold" specifies the CPU value of the IMSI Manager in percentage. The "percentage_value" is a percentage integer from 50 up to 70%. The default value is 50%.

---

**required-sessmgr**

SGSN only.

This keyword configures the required number of Session Manager instances at the IMSI Manager. By default, this parameter is disabled to ensure backward compatibility.

no_sess_mgrs: The number of required Session Managers can be an integer value from "1" through "384".

---

**sessmgr-sessions-threshold**

This option is used to configure the threshold high and low watermarks, in terms of percentage, for the sessions per Session Manager. The actual session limits are derived based on the card type.

**high-watermark high_value**: The high-watermark value can be a percentage value from "70" through "100". The default percentage value is "100".

**low-watermark low_value**: The low-watermark value can be a percentage value from "50" through "100". The default percentage value is "100".

---

**Usage Guidelines**

**For the MME:**

Typically, the **avoid-sessmgr-broadcast** and **sessmgr-sessions-threshold** keywords are available for configuration but not used.

**For the SGSN:**

This command configures the number of Session Manager instances required at the IMSI Manager before forwarding any calls from the Gb Manager or Link Manager, as well, it configures the high watermark and low watermark threshold levels per Session Manager.

If the required number of Session Managers are configured through this command, once the Link Manager or Gb Manager comes up, it sends a query to the IMSI Manager to verify if the IMSI Manager has learnt the configured number of Session Manager instances. IMSI Manager readiness status is determined based on the number of Session Manager instances present in the list maintained. Once the IMSI Manager has completed learning about all the required number Session Manager instances, it informs the Link Manager and Gb Manager. Runtime enabling and modification of Session Manager instance is disabled except disabling this...
configuration. Disabling of this configuration does not affect the call forwarding to the IMSI Manager as the default behavior is to always forward the calls to the IMSI Manager. This configuration is used to avoid the session imbalance across Session Manager instances due to call forwarding to the same Session Manager instance during or after re-load, if the IMSI Manager has learnt only few Session Manager instances. By default, this feature is disabled and Gb Manager or Link Manager start forwarding calls immediately during or after re-load to the IMSI Manager which in turn forwards the request to the available Session Manager instances. It is recommended to have this configuration before re-load. This option is available only under a SGSN license.

The high and low watermark limits allow the IMSI Manager to decide and select the Session Manager for processing new calls and eliminate the chances of it receiving a "call reject" in instances where the Session Manager has reached its maximum allowed session limits and the IMSI Manager is not aware of the same. The IMSI Manager converts the high and low watermark percentage to the maximum session allowed for the configured percentage based on the card type. It uses the calculated session values for both high and low watermark to decide and select the Session Manager for processing new calls. Once the Session Manager active session count reaches the calculated high watermark sessions the IMSI Manager stops forwarding the new calls to the Session Manager until the active session count becomes less than the calculated low watermark value. This option is available only under SGSN and MME licenses.

**Examples**

Use the following command to configure the required session manager count to be learnt by IMSI Manager for processing new calls to "28":

```
task facility imsimgr required-sessmgr 28
```

Use the following command to configure the threshold for the sessions per Session Manager:

```
 task facility imsimgr avoid-sessmgr-broadcast 95 low-watermark 85
```

The following command is used to disable all IMSI Manager Broadcasts:

```
 task facility imsimgr avoid-sessmgr-broadcast
```

The following command is used to disable broadcast after the IMSI Manager CPU reaches 60%:

```
 task facility imsimgr avoid-sessmgr-broadcast cpu_threshold 60
```

The following command enables broadcasting by default but once the CPU reaches a threshold of 50% the broadcast is disabled:

```
no task facility imsimgr avoid-sessmgr-broadcast
```
**task facility ipsecmgr**

Configures IPSec manager settings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
c

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**
```
task facility ipsecmgr { ikev1 { task-count { increased | normal } } | task-count { increased | normal } }
```

**ikev1 { task-count { increased | normal } }**

Default: **normal**

Adjusts the IPSec manager task count to support EHA for IKEv1. See **task-count** below.

**task-count { increased | normal }**

Default: **normal**

Adjusts the IPSec manager task count to support EHA.

- **increased**: Starts additional IPSec manager tasks operating on the packet processing cards. In increased mode, they run on all but demux packet processing cards. Also, all the IPSec managers start at the same time when an active non-demux card is detected and IPSec is configured.

- **normal**: Uses the standard algorithm for allocating memory for IPSec manager tasks. In normal mode, IPSec managers do not run on session packet processing cards.

---

**Caution**

If **task-count** is set to **normal** and session recovery is enabled, IPSec manager tasks are not allowed to start on most packet processing cards. Because the resources are not reserved, IPSec managers in normal mode only run on demux packet processing cards.

**Usage Guidelines**

Sets IPSec manager parameters for all IPSec managers in the system.
Examples

Use the following command to set the IPSec manager task count to increased mode:

```
task facility ipsecmgr task-count increased
```
**task facility linkmgr**

This command controls the maximum number of Link Managers that can be configured for an SGSN.

**Product**

SGSN

**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**

- `task facility linkmgr max max_linkmgrs`
- `default task facility linkmgr max`

- `default`
  
  Resets the value to 4.

- `max max_linkmgrs`
  
  Sets the maximum number of LinkMgrs configurable for the SGSN.

  `max_linkmgrs` is an integer from 1 to 4. With Release 15.0, the range is from 1 to 12.

**Note**

It is recommended to restrict the number of Link Managers for PSC2 to a maximum of "4" due to memory and hardware limitations.

**Usage Guidelines**

By default, 4 LinkMgrs will be started in the system when an SGSN service configuration is present. Use this command to change the maximum number of LinkMgrs to be started in the system.

**Important**

If a change to the default is needed, this command must be used before configuring any SGSN service-related configuration, including SS7 Routing Domain and SCCP Network configurations.

The number of LinkMgrs configurable impacts the following SS7 routing domain components:
• The number of Application Server Process (ASP) instances that can be configured (maximum of 12).
• The number of peer-servers that can be configured across all SS7RDs (maximum of 512).
• The number of peer-servers that can be configured per SS7RD (maximum of 256).
• The number of Peer-Server Process (PSP) instances that can be configured per SS7 Peer (maximum of 12).

**Important** This command cannot be set dynamically. If the LinkMgr count is modified dynamically, the system must be rebooted for the change to take effect.

**Examples**

Change the maximum number of LinkMgrs that can be configured for an SGSN from 4 to 8:

```
(task facility linkmgr max 8)
```
task facility mmedemux

Configures wait-time and percentage parameters related to the MMEDEMUX. The MMEDEMUX distributes the incoming traffic to the associated MMEMGRs based on the percentage value and wait-time configured in this command. The command has an option to configure a rate limit for incoming S1 SCTP connections in MME per chassis.

**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**

```plaintext
task facility mmedemux { mmemgr-startup-percentage percent_value | mmemgr-startup-wait-time wait_time | s1-sctp rate-limit value }
default task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time
do task facility mmedemux { mmemgr-startup-percentage mmemgr-startup-wait-time | s1-sctp rate-limit}
```

Either of these command filters disables the operator defined configuration and replaces the configuration with default values.

**mmemgr-startup-percentage percent_value**
The percentage parameter allows the operator to configure the percentage of MMEMGRs to be associated with the MMEDEMUX.

*percent_value* must be an integer from 1 to 100. Default is 90%.

**mmemgr-startup-wait-time wait_time**
This parameter enables the operator to configure the time (in seconds) that the MMEDEMUX waits for MMEMGRs to start before processing incoming traffic.

*wait_time* must be an integer from 300 to 3600. Default is 600 (10 minutes).
**s1-sctp rate-limit value**

The keyword **s1-sctp** identifies the MME SCTP interface type. The keyword **rate-limit** is used to configure the rate limit for incoming S1 SCTP connections from eNodeB. The value of the rate limit that can be configured is an integer from 1 up to 65535. Once the rate of incoming S1 SCTP connections exceed the configured value, the SCTP cookie echo packets are dropped by the MME. The SCTP connection with eNodeB is eventually be established after retries/retransmission by the eNodeB. The statistics of the dropped S1 SCTP packets are collected and displayed as part of MME Demux subsystem statistics. By default rate limiting is not imposed on incoming SCTP connections at the MME. Configuring the rate limit is an optional configuration, to prevent overload of MME from surge/burst of S1 SCTP connections from eNodeBs.

**Usage Guidelines**

This command gives operators some control over the MMEDEMUX system. It allows operators to configure the percentage of MMEMGRs to be associated with the MMEDEMUX. It also assigns the waiting time before processing the incoming traffic. Incoming traffic is distributed to the MMEMGRs based on a combination of the configured values of the two parameters.

By default, the MME waits for ten minutes to check if 90% of the MMEMGRs have started.

**Examples**

The following configures the MMEDEMUX to distribute incoming traffic after a minimum of 5 minutes after the MME starts and as soon as 75% of the MMEMGRs are up and running:

```
task facility mmedemux mmemgr-startup-percentage 75 mmemgr-startup-wait-time 5
```

The following CLI configures rate-limit of 100 S1 SCTP connections per second for a chassis:

```
task facility mmedemux s1-sctp rate-limit 100
```
task facility mmemgr

This command scales up or down the number of MMEMgrs per PSC3/DPC/SF-VM.

Important

This command is deprecated from release 19.2 onwards. It was introduced in release 18.0 and is valid until release 19.0. When an operator using this configuration command upgrades to release 19.2, this CLI is mapped to a new CLI command task facility mmemgr per-sesscard-count count.

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

task facility mmemgr per-sesscard-density { high | normal }
default task facility mmemgr per-sesscard-density

default

Resets the task facility mmemgr to normal density per session card/VM.

per-sesscard-density { high | normal }

Important

This is a boot-time configuration and should be added in the configuration file before any MME service related configuration is created or any MME Manager is started. Run-time (dynamic) configuration should be saved and will take effect only after reboot.

This keyword sets the maximum number (density) of MMEmgrs per session card. The two options are:

• high for High Density, which allows for eNB scaling and provides for a lower number of session cards. Currently, a maximum of 2 MMEmgrs per active session card.

• normal for Normal Density, the default model, which supports a max of 1 MMEmgr per active session card.
This CLI command is deprecated as it does not allow the operator to configure the required number of MME managers per session card. This command only allows two predefined modes of either "high" or "normal" density.

New commands are introduced to provide more flexibility to the operator to configure required number of MME managers per session card and to configure the desired number of MME managers per chassis.

**Usage Guidelines**

It is expected that this command will develop further to take advantage of higher capacity (e.g., the ASR5500) and next generation (e.g., the VPC-DI) platforms.

**Examples**

Use a command similar to the following to set a maximum of 2 MMEmgrs:

```
task facility mmemgr per-sesscard-density high
```
task facility mmemgr max

This command is used to configure desired number of MME managers per chassis.

Product

SGSN

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

task facility mmemgr max value
default task facility mmemgr max
default

This CLI is not configured by default. The keyword default resets the number of MME managers per chassis to the default values. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>48</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>1</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>24</td>
</tr>
</tbody>
</table>
The keyword **max** is used to set the maximum number of MME managers per chassis. Listed below is the maximum number of MME managers allowed per chassis based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per chassis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000</td>
<td>12</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>24</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>48</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>VPC-DI or SCALE LARGE/MEDIUM</td>
<td>48</td>
</tr>
<tr>
<td><strong>Note</strong> For release prior to 20.0, the default value was 24.</td>
<td></td>
</tr>
<tr>
<td>ASR5700</td>
<td>24</td>
</tr>
</tbody>
</table>

The maximum **value** is an integer with range 1 up to 36.

**Usage Guidelines**

This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload.

The maximum number of MME managers that can be configured per chassis varies based on the platform. However, the upper limit of MME managers per chassis is set to 36.

**Examples**

Listed below is an example where 5 MME managers are configured per chassis on an ASR5500 platform with DPC2 card:

**task facility mmemgr max 5**

Listed below is an example where default number of MME managers configured per chassis on an ASR5500 platform with DPC card:

**default task facility mmemgr max**
task facility mmemgr per-sesscard-count

This command is introduced to configure the desired number of MME managers per session card.

**Product**
SGSN
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**

```
task facility mmemgr per-sesscard-count count
default task facility mmemgr per-sesscard-count
```

default

The keyword `default` resets the number MME managers per session card to the default number of MME managers per session card/VM. By default this CLI is not configured. When this CLI is not configured default number of MME managers per session card will be selected based on platform and card type. Listed below are the default values:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Default number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>4</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>8</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>1</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>1</td>
</tr>
</tbody>
</table>
per-sesscard-count

This keyword is used to configure the desired number of mmemgrs to be started on each session card.

Listed below is the maximum number of MME managers allowed per session card based on the platform/VM and card type:

<table>
<thead>
<tr>
<th>Platform/VM and card type</th>
<th>Maximum number of MME managers per session card</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR5000 PSC/PSC2/PSC3</td>
<td>2</td>
</tr>
<tr>
<td>ASR 5500 DPC</td>
<td>6</td>
</tr>
<tr>
<td>ASR 5500 DPC2</td>
<td>8</td>
</tr>
<tr>
<td>SSI MEDIUM/LARGE</td>
<td>2</td>
</tr>
<tr>
<td>SSI FORGE/SMALL</td>
<td>1</td>
</tr>
<tr>
<td>SCALE LARGE/MEDIUM</td>
<td>2</td>
</tr>
<tr>
<td>ASR 5700</td>
<td>1</td>
</tr>
</tbody>
</table>

count

Is an integer value from 1 up to 6 .

Usage Guidelines

The maximum number of MME managers that can be configured per session card varies based on the platform/VM and card type. However, the upper limit of MME managers that can be configured per session card is set to 6 . This configuration change will be effective only after a chassis reload. The operator must save the configuration changes prior to a reload. The system issues appropriate warnings to the operator to indicate that configuration changes must be saved and the changes will be effective only after a chassis reload. This command is not specific to any platform or card type. It is applicable and available to all platforms and card types.

Examples

Listed below is an example where 3 MME managers are configured per session card on an ASR5500 platform with DPC2 card:

```
task facility mmemgr per-sesscard-count 3
```

Listed below is an example where default number of MME managers configured per session card on an ASR5500 platform with DPC card:

```
default task facility mmemgr per-sesscard-count
```
**task facility sessmgr**

Configures system information which is accessible via SNMP.

**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**

```
task { facility sessmgr start { aggressive | normal }
```

- `facility sessmgr start { aggressive | normal }`
  - Default: Normal
  - Specifies the facility options for the session manager.
  - **aggressive**: specifies the maximum number of session manager processes are started immediately.

**Caution**
The `task facility sessmgr start aggressive` command should only be used if the system will reach capacity (for the existing configuration) during the first few minutes of service.

**Caution**
This command must only be executed last during configuration (or appended to the end of the configuration file) to ensure the availability of memory resources to contexts and services.

**Usage Guidelines**
Set the session manager start policy to aggressive on heavily utilized systems to avoid undue delays in processing subscriber sessions.

**Examples**

- `task facility sessmgr start aggressive`
- `task facility sessmgr start normal`
**task resource cpu-memory-low**

Configures the system action for SNMP trap generation and logging whenever CPU memory.

**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**

```
task resource cpu-memory-low { kill | warn } }
```

{ kill | warn }

Default: kill

Sets the action for the Resource Manager to take when the amount of free memory on a CPU falls below 12MB. An SNMP TRAP and CORBA notification are generated and the event is logged.

Once the free memory threshold is crossed, The Resource Manager examines all tasks on that cpu and finds the most over limit task and kills it. If there are no over limit tasks nothing happens. Resource Manager takes preference on killing a non-sessmgr task over a sessmgr task.

**Usage Guidelines**

Set the CPU memory low action to only log CPU low memory events.

**Examples**

```
task resource cpu-memory-low warn
```
**tech-support test-commands password**

Configures the password that protects access to the **cli test-commands** mode in the Exec mode and Global Configuration mode. This command is only visible to a user logged in as a Security Administrator.

**Product**
All

**Privilege**
Security Administrator

**Caution**
The cli test-commands are for use by or under the supervision of Cisco TAC.

**Command Modes**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
tech-support test-commands [encrypted] password new_password [ old-password old_password ]
no tech-support test-commands password [ old-password old_password ]
```

**no**
Disables the use of a test-commands password. All subsequent attempts to execute **cli test-commands** in Exec or Global Configuration modes will fail.

Default: no password, access disabled

**[encrypted]**
If this optional keyword is specified, the **new_password** is interpreted as an encrypted string containing the password value. If the encrypted keyword is not specified, then **new_password** is interpreted as the actual plain text value. In the output of **show configuration** and **save configuration** commands, only the encrypted option of this command syntax appears.

**new_password**
Specifies the password to be used when executing the **cli test-commands** command in Exec or Global Configuration modes. For a plain text password, **new_password** is an alphanumeric string of 1 through 64 characters. For an encrypted password, **new_password** is an alphanumeric string of 1 through 524 characters.
If a password is not entered via this command, the `cli test-commands` command remains disabled in the Exec and Global Configuration modes.

Default: no password, access disabled

---

**Important**

An SNMP trap is generated when an administrator enters or edits a password via this command (starTechSupportPasswordChanged). Refer to the SNMP MIB Reference for additional information.

---

**old-password old_password**

If the `new_password` replaces an existing password, you must enter the old password for the change to be accepted.

Entering `old-password old_password` allows you to replace the existing password without being prompted to enter the old password. If you incorrectly enter the old password or do not enter the old password, an error message appears: "Failure: Must enter matching old tech-support password to replace existing password".

---

**Usage Guidelines**

Sets the password required to execute the `cli test-commands` command in the Exec and Global Configuration mode.

The `show configuration` and `save configuration` commands will never output this value in plain text.

`new_password` is the password you wish to configure. It has either never been previously set or is different from a previously configured password. It is an alphanumeric string of 1 to 64 characters.

If the new password replaces an existing password, you must enter the old password for the change to be accepted.

If the old password is not entered or does not match the existing configured value, the following error message appears: "tech-support password is already configured". A prompt then appears to accept entry of the old password: "Enter old tech-support password:"

If `tech-support test-commands password new_password old-password old_password` is included in a script, the password will be changed as long as `old_password` is valid.

---

**Important**

Access to the `cli test-commands` command also requires that an administrator enables the Global Configuration mode `cli hidden` command.

---

**Examples**

The following command sets the password for `cli test-commands` to `testCommander`.

`tech-support test-commands password testCommander`
template-session-trace

This command configures a template used for Session Tracing and Cell Traffic Tracing.

**Product**
- GGSN
- HNBGW
- MME
- P-GW
- SAEGW
- S-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**

```
template-session-trace network-element { ggsn | hnbgw | mme | pgw | saegw | sgw } template-name
```

```
template_name
```

Specifies the name of the template used for tracing as an alphanumeric string of 1 through 64 characters.

**Usage Guidelines**

Operators have the option of creating a template using the `template-session-trace` command for Session Tracing and Cell Traffic Tracing in the configuration mode for the MME.

Session traces executed in the Exec mode will use this template. Once created, the template can be associated with different subscribers to trace the interfaces configured in the template.

**Examples**

The following configuration shows a template configuration for the Home NodeB network element:

```
template-session-trace network-element hnbgw template-name cell-trace
```
terminal

Configures the Console port on the ASR 5000 SPIO card. This command is not supported on the ASR 5500.

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
terminal | carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware { off | on } | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } |

carrierdetect { off | on }
Specifies whether or not the console port is to use Data Carrier Detect (DCD) when connecting to a terminal.
Default: off
off: Do not use DCD.
on: Use DCD.

databits { 7 | 8 }
Specifies the number of data bits used to transmit and receive characters.
Default: 8
7: Use 7 databits to transmit and receive characters.
8: Use 8 databits to transmit and receive characters.

flowcontrol { hardware { off | on } | none }
Specifies how the flow of data is controlled between the SPIO and a terminal.
Default: none
hardware: Enables or disables the use of hardware-based flow control
off: Disables the use of Ready to Send (RTS) and Clear to Send (CTS).
on: Enables the use of Ready to Send (RTS) and Clear to Send (CTS).
**terminal**

none: Disables the use of DCD, RTS and CTS.

parity { even | none | odd }

Specifies the type of error checking used on the port.

Default: none

- **even** - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
- **none** - Disables error checking.
- **odd** - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed { 115200 | 19200 | 38400 | 57600 | 9600 }

Specifies the flow of data in bits per second between the console port and terminal.

Default: 9600

stopbits { 1 | 2 }

Specifies the number of stop bits between each transmitted character.

Default: 1

- **1**: Use one stop bit between each transmitted character.
- **2**: Use two stop bits between each transmitted character.

**Usage Guidelines**

Sets the ASR 5000 SPIO Console port parameters for communication with the terminal device.

**Examples**

The following command sets the SPIO Console port. The terminal must support these values.

```
terminal carrierdetect off databits 7 flowcontrol hardware on parity even speed 115200 stopbits 1
```
threshold 10sec-cpu-utilization

Configures alarm or alert thresholds that measure a 10-second average of CPU utilization. Its polling interval can be set down to 30 seconds.

**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 10sec-cpu-utilization percent | clear percent |

- **percent**
  Default: 0
  Configures Specifies the high threshold for 10-second average cpu-utilization. If the monitored CPU utilization is greater than or equal to the specified percentage an alert is sent. Regardless of the length of the polling interval, only one sample at the end of the polling interval is tested.

- **clear percent**
  Default: 0:
  This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

**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 set a threshold that sends an alert when CPU utilization over a 10-second average exceeds the limit set.

Alerts or alarms are triggered for 10-second sample of CPU utilization based on the following rules:
- **Enter condition**: 10-second average percentage of CPU utilization is greater than or equal to the high threshold.
- **Clear condition**: 10-second average percentage of CPU 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.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command generates an alert when the 10-second average CPU utilization reaches 45 percent:

```
threshold 10sec-cpu-utilization 45
```
threshold aaa-acct-archive-queue-size

Configures AAA accounting archive, alarm or alert thresholds based on the maximum values of session manager and ACS manager archive queue size.

**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 aaa-acct-archive-queue-size1 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size1 percent [ clear percent ]
threshold aaa-acct-archive-queue-size2 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size2 percent [ clear percent ]
threshold aaa-acct-archive-queue-size3 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size3 percent [ clear percent ]
```

**percent**
Configures Specifies the high threshold for monitoring the accounting message archive queue length. If the queue length is greater than or equal to the specified percentage an alarm is sent.
Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%

**clear percent**
This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.
Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%
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

In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive queue size thresholds generate alerts or alarms based on the queue length of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting message archive queue size thresholds based on the following rules:

- **Enter condition**: Actual number of archived messages is greater than or equal to the high threshold.
- **Clear condition**: Actual number of archived messages 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.

### Examples

The following command generates an alarm when 70% of the AAA accounting message archive buffer is filled, and clears the alarm when the buffer size is reduced to 30%:

```
threshold aaa-acct-archive-queue-size1 70 clear 30
```
**threshold aaa-acct-archive-size**

Configures accounting message archive size, alarm or alert thresholds.

**Product**
PDSN
GGSN
HA
ASN-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 aaa-acct-archive-size high_thresh [ clear low_thresh ]
default threshold aaa-acct-archive-size
```

**high_thresh**

Default: 1

Specifies the high threshold number of archived accounting messages that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 1044000.

**clear low_thresh**

Default: 1

Specifies the low threshold number of archived accounting messages that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 1044000.

**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.
In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive size thresholds generate alerts or alarms based on the number of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition**: Actual number of archived messages that is greater than or equal to the high threshold.
- **Clear condition**: Actual number of archived messages that 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.

The following command configures a high threshold count of 250 AAA accounting archived messages and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold aaa-acct-archive-size 250 clear 100
```
threshold aaa-acct-failure

Configures accounting failure, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-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 aaa-acct-failure high_thresh | clear low_thresh |
default threshold aaa-acct-failure
```

**high_thresh**

Default: 0

Specifies the high threshold number of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

 Specifies the low threshold number of accounting failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 10000000. 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

Accounting failure thresholds generate alerts or alarms based on the number of failed AAA accounting message requests that occur during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failures based on the following rules:

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

Examples

The following command configures a high threshold count of 100 AAA accounting failures and low threshold of 25 for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure 100 clear 25
```
threshold aaa-acct-failure-rate

Configures accounting failure rate, alarm or alert thresholds for the system.

Product

- PDSN
- GGSN
- HA
- ASN-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 aaa-acct-failure-rate high_thresh [ clear low_thresh ]
default threshold aaa-acct-failure-rate

high_thresh

Default: 1
Specifies the high threshold percent of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 and 100.

clear low_thresh

Default: 1
Specifies the low threshold percent of accounting failures that maintains a previously generated alarm condition. If the percentage of 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.

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.
Accounting failure rate thresholds generate alerts or alarms based on the percentage of AAA accounting message requests that failed during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

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

- **Enter condition**: Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual failure percentage 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.

The following command configures a AAA accounting failure rate high threshold percentage of 30 and a low threshold percentage of 10 for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure-rate 30 clear 10
```
threshold aaa-auth-failure

Configures authentication failure, alarm or alert thresholds for the system.

<table>
<thead>
<tr>
<th>Product</th>
<th>PDSN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GGSN</td>
</tr>
<tr>
<td></td>
<td>HA</td>
</tr>
<tr>
<td></td>
<td>ASN-GW</td>
</tr>
</tbody>
</table>

| Privilege   | Security Administrator, Administrator |

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Exec &gt; Global Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

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

| Syntax Description | threshold aaa-auth-failure high_thresh | clear low_thresh | default threshold aaa-auth-failure |

**high_thresh**

Default: 0

Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 10000000. 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

Authentication failure thresholds generate alerts or alarms based on the number of failed AAA authentication message requests that occur during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with.

Alerts or alarms are triggered for authentication failures based on the following rules:

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

Examples

The following command configures a high threshold count of 100 AAA authentication failures for a system using the Alert thresholding model:

`threshold aaa-auth-failure 100`
threshold aaa-auth-failure-rate

Configures authentication failure rate, alarm or alert thresholds for the system.

Product
PDSN
GGSN
HA
ASN-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 aaa-auth-failure-rate high_thresh [ clear low_thresh ]
default threshold aaa-auth-failure-rate
```

high_thresh
Default: 5
Specifies the high threshold percent of authentication failures 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.

clear
Allows the configuration of Specifies the low threshold.

low_thresh
Default: 5
Specifies the low threshold percent of authentication failures that maintains a previously generated alarm condition. If the percentage of 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.
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**

Authentication failure rate thresholds generate alerts or alarms based on the percentage of AAA authentication message requests that failed during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with.

Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual failure percentage 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.

**Examples**

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```
threshold aaa-auth-failure-rate 30
```
threshold aaa-retry-rate

Configures AAA retry rate, alarm or alert thresholds for the system.

**Product**
- PDSN
- GGSN
- HA
- ASN-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 aaa-retry-rate high_thresh [ clear low_thresh ]
default threshold aaa-retry-rate
```

*high_thresh*

Default: 5

Specifies the high threshold percent of AAA request message retries 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.

*clear low_thresh*

Default: 5

Specifies the low threshold percent of AAA request message retries that maintains a previously generated alarm condition. If the percentage of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thresh* is an integer from 0 through 100.

**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**

AAA request message retry rate thresholds generate alerts or alarms based on the percentage of request messages (both authentication and accounting) that were retried during the specified polling interval. The percentage is based on a message count taken for all AAA authentication and accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for request message retries based on the following rules:

- **Enter condition:** Actual retry percentage is greater than or equal to the high threshold.
- **Clear condition:** Actual retry percentage 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.

**Examples**

The following command configures a AAA message retry rate high threshold percentage of 25 and a low threshold percentage of 10 for a system using the Alarm thresholding model:

```
threshold aaa-retry-rate 25 clear 10
```
threshold aaamgr-request-queue

Configures the AAA Manager internal request queue, alarm or alert thresholds.

**Product**
- PDSN
- GGSN
- HA
- ASN-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 aaamgr-request-queue high_thresh [ clear low_thresh ]
default threshold aaamgr-request-queue
```

**high_thresh**

Default: 0

Specifies the high threshold number of AAA Manager Requests that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 1 through 100.

**clear**

Allows the configuration of Specifies the low threshold.

**low_thresh**

Default: 5

Specifies the low threshold number of AAA Manager Requests that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm is generated. low_thresh is an integer from 0 through 100.
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**

AAA Manager Request thresholds generate alerts or alarms based on the number of AAA Manager Requests for an AAA manager process during the specified polling interval.

Alerts or alarms are triggered for AAA Manager Requests based on the following rules:

- **Enter condition**: Actual number of AAA Manager Requests per AAA manager is greater than or equal to the high threshold.

- **Clear condition**: Actual number of AAA Manager Requests per AAA manager process is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm is not 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.

**Examples**

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```
threshold aaamgr-request-queue 30
```
**threshold asngw-auth-failure**

Configures authentication failure, alarm or alert thresholds for the ASN-GW system.

**Product**
ASN-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 asngw-auth-failure high_thresh | clear low_thresh |
default threshold asngw-auth-failure
```

**high_thresh**
Default: 0
Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. 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 configure threshold limits to generate alerts or alarms based on the number of failed ASN-GW authentication message requests that occur during the specified polling interval. Authentication
requests are counted for all ASN Gateway authentication servers with which the system is configured to communicate.

Alerts or alarms are triggered for authentication failures based on the following rules:

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

**Examples**

The following command configures a high threshold count of 100 authentication failures for an ASN-GW using the Alert thresholding model:

```
threshold asngw-auth-failure 100
```
threshold asngw-handoff-denial

Configures alarm or alert thresholds for hand-off denials within the ASN-GW service.

**Product**
ASN-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 asngw-handoff-denial high_thresh [ clear low_thresh ]
default threshold asngw-handoff-denial
```

- **high_thresh**
  Default: 0
  Specifies the high threshold number of hand-off denials that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  `high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of hand-off denials that maintains a previously generated alarm condition. If the number of hand-off denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  `low_thresh` is an integer from 0 through 10000000. 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 set threshold limits to generate alerts or alarms based on the number of denied hand-off that occurred during the specified polling interval. Hand-off denial messages are counted for all ASN Gateways that the system is configured to communicate with.

Alerts or alarms are triggered for hand-off denials based on the following rules:

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

Examples

The following command configures a high threshold count of 100 hand-off denials using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```
threshold asngw-max-eap-retry

Configures alarm or alert thresholds for maximum retries for Extensible Authentication Protocol (EAP) authentication within an ASN-GW service.

**Product**
ASN-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**

\[ threshold asngw-max-eap-retry \]
  
  \[ high_thresh \]
  
  \[ clear low_thresh \]

\[ default \]

\[ threshold asngw-max-eap-retry \]

\[ high_thresh \]

Default: 0

Specifies the high threshold number of retries for EAP authentication that must be met or exceeded within the polling interval to generate an alert or alarm.

\[ high_thresh \] is an integer from 0 through 10000000. A value of 0 disables the threshold.

\[ clear low_thresh \]

Default: 0

Specifies the low threshold number of retries for EAP authentication that maintains a previously generated alarm condition. If the number of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated.

\[ low_thresh \] is an integer from 0 through 10000000. 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 set threshold limits to generate alerts or alarms based on the number of retries for EAP authentication that occur during the specified polling interval.

Alerts or alarms are triggered for maximum number of retries for EAP authentication based on the following rules:

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

Examples

The following command configures a high threshold count of 100 alerts or alarms generated on maximum number of retries for EAP authentication for an ASN Gateway using the Alert thresholding model:

`threshold asngw-max-eap-retry 100`
**threshold asngw-network-entry-denial**

Configures alarm or alert thresholds for denials of network entry to an MS within the ASN-GW service.

**Product**

ASN-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 asngw-network-entry-denial high_thresh [ clear low_thresh ]
default threshold asngw-network-entry-denial
```

**high_thresh**

Default: 0

Specifies the high threshold number of denial of network entry to an MS that must be met or exceeded within
the polling interval to generate an alert or alarm.

**clear low_thresh**

Default: 0

Specifies the low threshold number of denial of network entry to an MS that maintains a previously generated
alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear
alarm will be generated.

**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 set threshold limits to generate alerts or alarms based on the number of network entry denials that occurred during the specified polling interval. Network denial messages are counted for an MS with which the system is configured to communicate.

Alerts or alarms are triggered for network entry denials based on the following rules:

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

Examples

The following command configures a high threshold count of 100 network entry denials for an MS using the Alert thresholding model:

```
threshold asngw-network-entry-denial 100
```
**threshold asngw-r6-invalid-nai**

Configures alarm or alert thresholds for invalid Network Access Identifier (NAI) occurrences in R6 messages.

<table>
<thead>
<tr>
<th><strong>Product</strong></th>
<th>ASN-GW</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Privilege</strong></td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td><strong>Command Modes</strong></td>
<td>Exec &gt; Global Configuration, configure</td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold asngw-r6-invalid-nai high_thresh [ clear low_thresh ]
default threshold asngw-r6-invalid-nai
```

**high_thresh**

Default: 0

Specifies the high threshold number of invalid NAIs in R6 messages that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of invalid NAIs in R6 messages that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. 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 set threshold limits to generate alerts or alarms based on the number of invalid NAIs in R6 messages that occurred during the specified polling interval. Invalid NAIs are counted for an MS that the system is configured to communicate with or per system for all R6 messages.

Alerts or alarms are triggered for invalid NAIs based on the following rules:

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

Examples

The following command configures a high threshold count of 100 invalid NAIs in R6 messages using the Alert thresholding model:

```
threshold asngw-r6-invalid-nai 100
```
**threshold asngw-session-setup-timeout**

Configures alarm or alert thresholds for session setup timeouts in an ASN-GW service.

**Product**
ASN-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 asngw-session-setup-timeout high_thresh [ clear low_thresh ]
default threshold asngw-session-setup-timeout
```

**high_thresh**

Default: 0

Specifies the high threshold number of timeouts during session setup that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of timeouts during session setup that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. 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 set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.
Alerts or alarms are triggered for session setup timeouts based on the following rules:

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

**Examples**

The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```
threshold asngw-session-setup-timeout 100
```
threshold asngw-session-timeout

Configures alarm or alert thresholds for session timeouts in an ASN-GW service.

Product
ASN-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 asngw-session-timeout high_thresh | clear low_thresh |
default threshold asngw-session-timeout

high_thresh
Default: 0
Specifies the high threshold number of timeouts during session that must be met or exceeded within the polling interval to generate an alert or alarm.

low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 10000000. 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 set threshold limits to generate alerts or alarms based on the number of timeouts during a session that occurred during the specified polling interval.
Alerts or alarms are triggered for session timeouts based on the following rules:

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

**Examples**

The following command configures a high threshold count of 100 timeouts during a session using the Alert thresholding model:

```
threshold asngw-session-timeout 100
```
threshold asnpc-idle-mode-timeout

Configures alarm or alert thresholds for ASNPC Instant Messenger idle mode timeouts.

Product
ASN-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 asnpc-idle-mode-timeout high_thresh | clear low_thresh |

high_thresh
Default: 0
Specifies the high threshold number of ASNPC idle mode timeouts that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of ASNPC idle mode timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 10000000. 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
Set the maximum number of idle mode timeouts allowed in the ASNPC service.

Alerts or alarms are triggered for session timeouts based on the following rules:
- **Enter condition**: Actual number of timeouts is greater than or equal to the high threshold.
- **Clear condition**: Actual number of timeouts 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.

**Examples**

The following command configures the high threshold for ASNPC idle mode timeouts at 10000:

```
threshold asnpc-idle-mode-timeout 10000
```
threshold asnpc-im-entry-denial

Configures the ASNPC Instant Messenger (IM) entry denial, alarm or alert thresholds.

**Product**
ASN-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 asnpc-im-entry-denial high_thresh [ clear low_thresh ]`

- `high_thresh`
  
  Default: 0
  
  Specifies the high threshold number of IM entry denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  `high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

- `clear low_thresh`
  
  Default: 0
  
  Specifies the low threshold number of IM entry denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` is an integer from 0 through 10000000. 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**
Set the maximum number of IM session denials allowed in the ASNPC service.

Alerts or alarms are triggered for session timeouts based on the following rules:
• **Enter condition**: Actual number of failures is greater than or equal to the high threshold.

• **Clear condition**: Actual number of 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.

**Examples**

The following command configures the high threshold for IM session counts at 10000:

```
threshold asnpc-im-entry-denial 10000
```
threshold asnpc-llu-denial

Configures the alarm or alert thresholds for Location Update (LU) denials.

**Product**
ASN-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 asnpc-llu-denial high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of LU denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of LU denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 10000000. 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**

Set the maximum number of Location Update denials allowed in the ASNPC service.
Examples

The following command configures high threshold of 10000 LU denials:

```
threshold asnpc-lu-denial 10000
```
threshold asnpc-session-setup-timeout

Configures alarm or alert thresholds for ASNPC session setup timeouts in an ASN-GW service.

**Product**
ASN-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 asnpc-session-setup-timeout value
default threshold asnpc-session-setup-timeout
```

`value`

`value` is an integer from 1 through 1000000.

**Usage Guidelines**

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.

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.

**Examples**
The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```
threshold asnpc-session-setup-timeout 100
```
threshold call-reject-no-resource

Configures alarm or alert thresholds on the system for calls rejected due to insufficient resources.

**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 call-reject-no-resource high_thresh | clear low_thresh |

**high_thresh**

Default: 0

Specifies the high threshold number of no-resource call rejects issued by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

The number is an integer from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of no-resource call rejects issued by the system that maintains a previously generated alarm condition. If the number of rejections falls beneath the low threshold within the polling interval, a clear alarm will be generated.

The number is an integer from 0 through 100000. 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**

No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (memory and/or session licenses) during the specified polling interval.
Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

- **Enter condition:** Actual number of calls rejected due to no resources is greater than or equal to the high threshold.
- **Clear condition:** Actual number of calls rejected due to no resources 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.

**Examples**

The following command configures a high threshold count for the number of calls rejected by the system due to insufficient or no resources to 100 and allow threshold of 40 for a system using the Alarm thresholding model:

```
threshold call-reject-no-resource 100 clear 40
```
threshold call-setup

Configures call setup, alarm or alert thresholds for the system.

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 call-setup high_thresh [ clear low_thresh ]

**high_thresh**
Default: 0
Specifies the high threshold number of calls setup 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 100000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of calls setup by the system that maintains a previously generated alarm condition. If the number of setups falls beneath the low threshold within the polling interval, a clear alarm will be generated.
(low_thresh) is an integer from 0 through 100000. 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**
Call setup thresholds generate alerts or alarms based on the total number of calls setup by the system during the specified polling interval.
Alerts or alarms are triggered for call setups based on the following rules:

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

**Examples**

The following command configures a high threshold count of 100 calls setup for a system using the Alert thresholding model:

```
threshold call-setup 100
```
threshold call-setup-failure

Configures call setup failure, alarm or alert thresholds for the system.

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 call-setup-failure high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of call 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 100000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of call 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 100000. 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

Call setup failure thresholds generate alerts or alarms based on the total number of call setup failures experienced by the system during the specified polling interval.
Alerts or alarms are triggered for call setup failures 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.

### Examples

The following command configures a high threshold count of 100 call setup failures and a low threshold of 80 for a system using the Alarm thresholding model:

```
threshold call-setup-failure 100 clear 80
```
**threshold card-temperature-near-power-off-limit**

Configures alarm or alert thresholds for triggering and clearing high card temperature alarms.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```plaintext
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
threshold card-temperature-near-power-off-limit high_temp [ clear low_temp ]
```

- **high_thresh**
  Default: 0
  Specifies the high card temperature (in degrees Celsius) 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 card temperature (in degrees Celsius) before a high temperature alarm is cleared.
  
  *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**

Set the high and low temperatures in degrees Celsius that generate and clear alarms.

**Examples**

The following command configures sets the high and low temperatures to 40 and 35 degrees:

```
threshold card-temperature-near-power-off-limit 40 clear 35
```
threshold cdr-file-space

Configures, alarm or alert thresholds for monitoring the percentage of total file space allocated for Charging Data Records (CDRs) used during the polling interval.

Product

ACS

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 cdr-file-space high_thresh [ clear low_thresh ]

default threshold cdr-file-space

default

Configures this command with the default threshold settings.

high_thresh

Specifies the high threshold for percentage of total allocated CDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

high_thresh is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Default: 90

clear low_thresh

Specifies the low threshold for percentage of total allocated CDR file space used that maintains a previously generated alarm condition. If the space usage falls below Specifies the low threshold within the polling interval, a clear alarm is generated.

low_thresh is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0
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 Specifies the low threshold.

**Usage Guidelines**

CDR file space usage generate alerts or alarms based on the percentage of total allocated CDR file space used during the polling interval.

Alerts or alarms are triggered for CDR file space usage session based on the following rules:

- **Enter condition**: Actual percentage of allocated CDR file space usage is greater than or equal to the specified percentage of total CDR file space.
- **Clear condition**: Actual CDR file space used is less than the specified clear percentage of total allocated CDR file space usage.

If a trigger condition exists at the end of 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.

**Examples**

The following command configures a threshold of 65 percent of total allocated CDR file space usage and a clear threshold of 35 percent:

```
threshold cdr-file-space 65 clear 35
```
threshold contfilt-block

Configures, alarm or alert thresholds for Content Filtering rating operations blocked during a polling interval at which the threshold are raised or cleared.

**Product**
CF

**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 contfilt-block high_thresh_value [ clear low_thresh_value ]
default threshold contfilt-block
```

**default**
Configures this command with the default threshold settings.

**high_thresh**
Specifies the high threshold for number of rating operations blocked for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**
Specifies the low threshold for the total number of rating operations blocked for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below specifies the low threshold within the polling interval, a clear alarm is generated.

*low_thresh* is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

Default: 0

**Usage Guidelines**
Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations blocked for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-block` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65000 rating operations blocked and a clear threshold of 35000 operations:

```
threshold contfilt-block 65000 clear 35000
```
**threshold contfilt-rating**

Configures, alarm or alert thresholds for Content Filtering rating operations performed during a polling interval at which the threshold are raised or cleared.

**Product**  
CF

**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 contfilt-rating high_thresh_value | clear low_thresh_value | default threshold contfilt-rating  
default
```

*default*  
Configures this command with the default threshold settings.

*high_thresh*  
Specifies the high threshold for number of rating operations performed for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.  
`high_thresh` is measured in numbers of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

*clear low_thresh*  
Specifies the low threshold for the total number of rating operations performed for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below specifies the low threshold within the polling interval, a clear alarm is generated.  
`low_thresh` is measured in number of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.  
Default: 0

**Usage Guidelines**  
Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations performed for a content filtering service during the polling interval.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll contfilt-rating` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Examples**

The following command configures a threshold of 65000 percent of total rating operations performed and a clear threshold of 35000 percent:

```
threshold contfilt-rating 65000 clear 35000
```
threshold cpu-available-memory

Configures alarm or alert thresholds for available CPU memory in the system.

**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 cpu-available-memory low_thresh [ clear ] high_thresh ]`

`low_thresh`

Default: 32
Specifies the low threshold amount of CPU memory that must be met or exceeded at the polling time to generate an alert or alarm.
`low_thresh` is measured in megabytes (MB) and is an integer from 0 through 2048.

`clear high_thresh`

Default: 32
Specifies the high threshold amount of CPU memory that maintains a previously generated alarm condition. If the memory amount rises above the high threshold within the polling interval, a clear alarm will be generated.
`high_thresh` is measured in megabytes (MB) and is an integer from 0 through 2048.

**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 low threshold.

**Usage Guidelines**

CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each packet processing card CPU at the polling time. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for available CPU memory based on the following rules:

- **Enter condition**: Average measured amount of memory/CPU for the last 5 minutes is less than or equal to the low threshold.
- **Clear condition**: Average measured amount of memory/CPU for the last 5 minutes is greater than the high 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.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a low threshold count of 50 MB CPU memory available and a high threshold of 112 MB for a system using the Alarm thresholding model:

```
threshold cpu-available-memory 50 clear 112
```
threshold cpu-load

Configures alarm or alert thresholds for monitoring packet processing card CPU loads using a 5-minute average measurement. The threshold is enabled by enabling CPU resource monitoring.

**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 cpu-load high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  If the monitored CPU load is greater than or equal to the specified number an alert is sent. *high_thresh* must be an integer from 0 through 15.

- **clear low_thresh**
  
  Default: 0
  
  This is a low watermark value that sets the alarm clearing threshold value. If not present it is taken from the first value. *low_thresh* must be an integer from 0 through 15.

---

**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 Specifies the low threshold.

**Usage Guidelines**

Use this command to set an alert when the card's CPU load is equal to or greater than the number specified. Alerts or alarms are triggered for CPU load based on the following rules:

- **Enter condition**: Actual CPU load is greater than or equal to the high threshold.
- **Clear condition**: Actual CPU load 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.

**Important**

This command is not supported on all platforms.

**Examples**

To set an alert when the packet processing card CPU load is over 10 and set an alert clear when the CPU load drops down equal or less than 7, enter the following command;

```
threshold cpu-load 10 clear 7
```
threshold cpu-memory-usage

Configures, alarm or alert thresholds for monitoring the percentage of total CPU memory used during the polling interval.

**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 cpu-memory-usage high_thresh | clear low_thresh |
```

**high_thresh**
Default: 0

Specifies the high threshold for percentage of total memory used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

`high_thresh` is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0

Specifies the low threshold for percentage of total CPU memory used that maintains a previously generated alarm condition. If the memory usage falls below the low threshold within the polling interval, a clear alarm is generated.

`low_thresh` is measured as a percentage of total CPU memory used and is an integer from 0 and 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 Specifies the low threshold.
Usage Guidelines

CPU memory usage generate alerts or alarms based on the percentage of total CPU memory used during the polling interval.

Alerts or alarms are triggered for CPU memory usage session based on the following rules:

• **Enter condition:** Actual percentage of CPU memory usage is greater than or equal to the specified percentage of total CPU memory.

• **Clear condition:** Actual CPU memory usage is less than the specified clear percentage of total CPU memory usage.

If a trigger condition exists at the end of 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.

Examples

The following command configures a threshold of 65 percent of total packet processing card CPU memory usage and a clear threshold of 35 percent:

`threshold cpu-memory-usage 65 clear 35`
threshold cpu-orbs-crit

Configures thresholds for generating critical-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

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 cpu-orbs-crit high_thresh [ clear low_thresh ] [ default ] threshold cpu-orbs-crit

default

Restores this parameter to its default setting.

high_thresh

Default: 60

Specifies the high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a critical-level alert or alarm.

high_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

clear low_thresh

Default: 60

Specifies the low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to Specifies the low threshold at the time of polling, a clear alarm will be generated.

low_thresh is measured in percentage of total CPU utilization and 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 Specifies the low threshold.

Usage Guidelines

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling. Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

• Enter condition: Actual CPU usage percentage is greater than the high threshold.
• Clear condition: Actual CPU usage percentage is less than or equal to the low threshold.

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

Examples

The following command configures a critical-level alarm threshold of 35 percent of CPU utilization by the ORBS task and a clear threshold of 30 percent:

threshold cpu-orbs-crit 35 clear 30
**threshold cpu-orbs-warn**

Configures thresholds for generating warning-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

**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 cpu-orbs-warn high_thresh [ clear low_thresh ]
[ default ] threshold cpu-orbs-warn

default
```

Restores this parameter to its default setting.

```
high_thresh
```

Default: 50

Specifies the high threshold percent of CPU utilization by the ORBS software task that must be exceeded as measured at the time of polling to generate a warning-level alert or alarm.

`high_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

```
clear low_thresh
```

Default: 50

Specifies the low threshold percent of CPU utilization by the ORBS software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to specifies the low threshold at the time of polling, a clear alarm will be generated.

`low_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.
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 Specifies the low threshold.

**Usage Guidelines**

Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling. Warning-level alerts or alarms are triggered for CPU usage by the ORBS software task based on the following rules:

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

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

**Examples**

The following command configures a warning-level alarm threshold of 25 percent of CPU utilization by the ORBS task and a clear threshold of 20 percent:

```
threshold cpu-orbs-warn 25 clear 20
```
threshold cpu-session-throughput

Configures alarm or alert thresholds for CPU session throughput within the system.

**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 cpu-session-throughput high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold session throughput that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold session thereof about that maintains a previously generated alarm condition. If the throughput falls below Specifies the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. 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

CPU session throughput thresholds generate alerts or alarms based on total throughput for all Session Manager tasks running on each packet processing card CPU during the polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for CPU session throughput based on the following rules:

- **Enter condition**: Actual CPU session throughput is greater than or equal to the high threshold.
- **Clear condition**: Actual CPU session throughput 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.

Important

This command is not supported on all platforms.

Examples

The following command configures a high threshold count of 900 Kbps session throughput and a low threshold of 500 KBps for a system using the Alarm thresholding model:

```
threshold cpu-session-throughput 900 clear 500
```
threshold cpu-utilization

Configures alarm or alert thresholds for CPU utilization within the system.

**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 cpu-utilization high_thresh [ clear low_thresh ]
```

**`high_thresh`**

Default: 85

Specifies the high threshold CPU 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.

**`clear low_thresh`**

Default: 85

Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 100.

---

**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**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each packet processing card CPU during the specified polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.
Alerts or alarms are triggered for CPU utilization based on the following rules:

- **Enter condition**: Average measured CPU utilization for the last 5 minutes
- **Clear condition**: Average measured CPU utilization for the last 5 minutes 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.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a high threshold CPU utilization percentage of 90 for a system using the Alert thresholding model:

```
threshold cpu-utilization 90
```
**threshold dcca-bad-answers**

Configures alarm or alert thresholds for invalid or bad responses to the system from Diameter servers.

**Product**
ACS

**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 dcca-bad-answers high_thresh [ clear low_thresh ]
default threshold dcca-bad-answers
```

**default**

Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**

Default: 0

Specifies the high threshold number of invalid messages or responses 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.

**clear low_thresh**

Default: 0

Specifies the low threshold number of invalid messages/responses that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000.

**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

In the event that the system receives invalid message or response from Diameter server `dcca-bad-answers` is generated.

DCCA bad answer messages size threshold generates alerts or alarms based on the number of invalid response or messages received during the specified polling interval.

Alerts or alarms are triggered for DCCA bad answers based on the following rules:

- **Enter condition**: Actual number of DCCA bad answer messages is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA bad answer messages 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.

Examples

The following command configures a high threshold count of 250 DCCA bad answer messages and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-bad-answers 250 clear 100
```
threshold dcca-protocol-error

Configures alarm or alert thresholds for Diameter Credit Control Application (DCCA) protocol errors from the Diameter server.

**Product**
ACS

**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 dcca-protocol-error high_thresh [ clear low_thresh ]
default threshold dcca-protocol-error
```

default
Disables the threshold for configured alarm and sets the high_thres and low_thres values to 0.

**high_thres**
Default: 0

Specifies the high threshold number of protocol error received from Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thres is an integer from 0 through 1000000.

**clear low_thres**
Default: 0

Specifies the low threshold number of protocol error received from Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thres is an integer from 0 through 1000000.
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.

**Important**

**Usage Guidelines**

In the event that the system receives the protocol errors from Diameter server, `dcca-protocol-error` is generated. DCCA protocol error threshold generates alerts or alarms based on the number of protocol error messages received from Diameter server during the specified polling interval.

Alerts or alarms are triggered for DCCA protocol error based on the following rules:

- **Enter condition**: Actual number of DCCA protocol error is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA protocol errors 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.

**Examples**

The following command configures a high threshold count of 250 protocol errors and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-protocol-error 250 clear 100
```
### threshold dcca-rating-failed

Configures Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject, alarm or alert thresholds.

**Product**

ACS

**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 dcca-rating-failed high_thresh | clear low_thresh 
default threshold dcca-rating-failed
```

- **default**
  
  Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server 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.

- **clear low_thresh**
  
  Default: 0
  
  Specifies the low threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` is an integer from 0 through 1000000.
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**

In the event that the Diameter server rejects the system request for a block of credits due to invalid Rating Group, defined as content-id, `dcca-rating-failed` message is generated.

Rating Group failed threshold generates alerts or alarms based on the number of requests rejected from Diameter server during the specified polling interval.

Alerts or alarms are triggered for Rating Group failed based on the following rules:

- **Enter condition**: Actual number of DCCA Rating Group failed is greater than or equal to the high threshold.
- **Clear condition**: Actual number of DCCA Rating Group failed 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.

**Examples**

The following command configures a high threshold count of 250 requests rejected and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-rating-failed 250 clear 100
```
threshold dcca-unknown-rating-group

Configures alarm or alert thresholds for the unknown Diameter Credit Control Application (DCCA) Rating Group (content-id) messages returned by Diameter servers.

**Product**

ACS

**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 dcca-unknown-rating-group **high_thresh** | **clear low_thresh** |

default threshold dcca-unknown-rating-group

default

Disables the threshold for configured alarm and sets the **high_thresh** and **low_thresh** values to 0.

**high_thresh**

Default: 0

Specifies the high threshold number of unknown Rating Group (content-id) messages sent by the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

**low_thresh** is an integer from 0 through 1000000.

**clear low_thresh**

Default: 0

Specifies the low threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

**low_thresh** is an integer from 0 through 1000000.
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**

In the event that the Diameter server sends invalid Rating Groups, `content-ids` to the system, `dcca-unk-rating-group` message is generated.

Unknown Rating Group threshold generates alerts or alarms based on the number of unknown Rating Groups received by the system from Diameter server during the specified polling interval.

Alerts or alarms are triggered for unknown rating groups based on the following rules:

- **Enter condition**: Actual number of unknown rating groups is greater than or equal to the high threshold.
- **Clear condition**: Actual number of unknown rating groups 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.

**Examples**

The following command configures a high threshold count of 250 unknown rating groups and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-unknown-rating-group 250 clear 100
```
threshold diameter diameter-retry-rate

Configures Diameter Retry Rate, alarm or alert thresholds based on the percentage of Diameter requests that were retried during the polling interval.

Product
ACS

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 diameter diameter-retry-rate high_thresh [ clear low_thresh ]
default threshold diameter diameter-retry-rate

default

Configures this command with the default threshold settings.

Default: 0—disabled

high_thresh

Specifies the high threshold. If, within the polling interval, the percentage of Diameter requests retried equals or exceeds high_thresh an alert or alarm is generated.

high_thresh is an integer from 0 through 100.

Default: 0

clear low_thresh

Specifies the low threshold. If, within the polling interval, the percentage of Diameter requests retried falls below low_thresh, a clear alarm is generated.

low_threshold is an integer from 0 through 100.

Default: 0
This value is applicable for the Alarm mode, and ignored for the Alert mode. In addition, if this value is not configured for the Alarm mode, the system assumes it is identical to the high threshold.

**Usage Guidelines**

Diameter Retry Rate threshold generates alerts or alarms based on the percentage of Diameter requests that were retried during the specified polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Percentage of Diameter requests retried is greater than or equal to the high threshold.
- **Clear condition:** Percentage of Diameter requests retried 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.

**Examples**

The following command configures a high threshold of 75 percent, and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold diameter diameter-retry-rate 75 clear 50
```
threshold dns-learnt-ip-max-entries

Configures alarm or alert thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature.

Important
In 16.0 and later releases, this command has been deprecated and replaced by the threshold dns-learnt-ipv4-max-entries and threshold dns-learnt-ipv6-max-entries commands to configure alarm or alert thresholds for the percentage of total DNS-learnt IPv4 entries and total DNS-learnt IPv6 entries respectively.

Product
ACS

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 dns-learnt-ip-max-entries high_thresh [ clear low_thresh ]
default threshold dns-learnt-ip-max-entries

default
Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

high_thresh
Default: 90 percent
Specifies the high threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.
When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.
When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.
high_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**clear low_thresh**

Default: 90 percent

Specifies the low threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries goes below the low threshold within the polling interval, a clear alarm is generated.

When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated.

When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.

low_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

---

**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 low threshold.

---

**Usage Guidelines**

Use this command to configure thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature. Note that this threshold applies to both IPv4 and IPv6 DNS entries.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IP entries is greater than or equal to the specified percentage of total DNS-learnt IP entries.

- **Clear condition**: Actual of total DNS-learnt IP entries is less than the specified clear percentage of total DNS-learnt IP entries.

If a trigger condition exists at the end of 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.

**Examples**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS-learnt IP entries:

```
threshold dns-learnt-ip-max-entries 65 clear 35
```
threshold dns-learnt-ipv4-max-entries

Configures alarm or alert thresholds for the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature.

**Product**
ACS

**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 dns-learnt-ipv4-max-entries high_thresh [ clear low_thresh ]
```

**high_thresh**

Specifies the high threshold for percentage of total DNS-learnt IPv4 entries. When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.

`high_thresh` is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

Default: 90 percent

**clear low_thresh**

Specifies the low threshold for percentage of total DNS-learnt IPv4 entries. When the percentage of total DNS-learnt IPv4 entries goes below the low threshold within the polling interval, a clear alarm is generated.

When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated.

`low_thresh` is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

Default: 90 percent
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 low threshold.

**Usage Guidelines**

Use this command to configure thresholds for the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IPv4 entries is greater than or equal to the specified percentage of total DNS-learnt IPv4 entries.

- **Clear condition**: Actual percentage of total DNS-learnt IPv4 entries is less than the specified clear percentage of total DNS-learnt IPv4 entries.

If a trigger condition exists at the end of 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.

**Examples**

The following command configures a high threshold of 60 percent and a clear threshold of 30 percent for total DNS-learnt IPv4 entries:

```
threshold dns-learnt-ipv4-max-entries 60 clear 30
```
**threshold dns-learnt-ipv6-max-entries**

Configures alarm or alert thresholds for the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature.

**Product**
ACS

**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 dns-learnt-ipv6-max-entries high_thresh | clear low_thresh`

- **high_thresh**
  Specifies the high threshold for percentage of total DNS-learnt IPv6 entries. When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.
  
  When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.
  
  `high_thresh` is an integer value from 0 through 100. When configured to 0 the threshold is disabled.
  
  Default: 90 percent

- **clear low_thresh**
  Specifies the low threshold for percentage of total DNS-learnt IPv6 entries. When the percentage of total DNS-learnt IPv6 entries goes below the low threshold within the polling interval, a clear alarm is generated.
  
  When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.
  
  `low_thresh` is an integer value from 0 through 100. When configured to 0 the threshold is disabled.
  
  Default: 90 percent
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 low threshold.

Usage Guidelines

Use this command to configure thresholds for the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS-learnt IPv6 entries is greater than or equal to the specified percentage of total DNS-learnt IPv6 entries.
- **Clear condition**: Actual percentage of total DNS-learnt IPv6 entries is less than the specified clear percentage of total DNS-learnt IPv6 entries.

If a trigger condition exists at the end of 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.

Examples

The following command configures a high threshold of 75 percent and a clear threshold of 45 percent for total DNS-learnt IPv6 entries:

```
threshold dns-learnt-ipv6-max-entries 75 clear 45
```
threshold dns-lookup-failure

Configures alarm or alert thresholds based on the percentage of total DNS lookup failures.

Product
ACS

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 dns-lookup-failure

default
Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

high_thresh
Default: 90 percent
Specifies the high threshold for percentage of total DNS lookup failures. When the percentage of total failures meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

high_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

clear low_thresh
Default: 90 percent
Specifies the low threshold for percentage of total DNS lookup failures. When the percentage of total failures goes below the low threshold within the polling interval, a clear alarm is generated.

low_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

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 low threshold.
**Usage Guidelines**

Use this command to configure thresholds for the percentage of total DNS lookup failures. Note that this threshold applies to both IPv4 and IPv6 DNS entries.

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Actual percentage of total DNS lookup failures is greater than or equal to the specified percentage of total DNS lookup failures.

- **Clear condition**: Actual of total DNS lookup failures is less than the specified clear percentage of total DNS lookup failures.

If a trigger condition exists at the end of 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.

**Examples**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS lookup failures:

```
threshold dns-lookup-failure 65 clear 35
```
threshold edr-file-space

Configures alarm or alert thresholds for monitoring the percentage of total file space allocated for Event Data Records (EDRs) used during the polling interval.

**Product**
ACS

**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**

```
[ default ] threshold edr-file-space high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 90

Specifies the high threshold for percentage of total allocated EDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

`high_thresh` is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold for percentage of total allocated EDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated.

`low_thresh` is measured in percentage of total allocated EDR file space used and 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 low threshold.
**Usage Guidelines**

EDR file space usage generate alerts or alarms based on the percentage of total allocated EDR file space used during the polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated EDR file space usage is greater than or equal to the specified percentage of total EDR file space.

- **Clear condition:** Actual EDR file space used is less than the specified clear percentage of total allocated EDR file space usage.

If a trigger condition exists at the end of 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.

**Examples**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total allocated EDR file space usage:

`threshold edr-file-space 65 clear 35`
threshold edr-udr-dropped flow control

Configures alarm or alert thresholds to monitor the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control.

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 edr-udr-dropped-flow-control high_thresh [ clear low_thresh ]
default threshold edr-udr-dropped-flow-control

default

Configures this command with the default threshold settings.
Default: High threshold: 90; Low threshold: 10

high_thresh

Specifies the high threshold for total number of EDRs + UDRs dropped due to flow control, which must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh must be an integer from 0 through 100000.

A value of 0 disables the threshold.
Default: 90

clear low_thresh

Specifies the low threshold for total number of EDRs + UDRs dropped that maintains a previously generated alarm condition. If the total number of EDRs + UDRs dropped falls below

low_thresh must be an integer from 0 through 100000 that must be lower than high_thresh.

A value of 0 disables the threshold.
Default: 10
Usage Guidelines
Use this command to configure thresholds to monitor the total number of EDRs + UDRs discarded due to flow control. Alerts or alarms are generated based on the total number of EDRs + UDRs dropped during polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual number of EDRs + UDRs dropped greater than or equal to the specified number of EDRs + UDRs dropped.
- **Clear condition:** Actual number of EDR + UDRs dropped is less than the specified clear number of EDRs + UDRs dropped.

If a trigger condition exists at the end of 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.

Examples
The following command configures a high threshold of 90 and a clear threshold of 45 to monitor EDRs + UDRs dropped due to flow control:

```
threshold edr-udr-dropped-flow-control 90 clear 45
```
threshold egtpc-s2b-setup-fail-rate

Configures the eGTP-C S2b setup fail rate threshold.

**Product**
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**
```
threshold egtpc-s2b-setup-fail-rate high_thresh [ clear low_thresh ]
default threshold egtpc-s2b-setup-fail-rate
```

default

Configures this command with the default threshold settings and disables the threshold.

```
high_thresh
```

Default: 0

Specifies the high threshold number of eGTP-C S2b call setup failures that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold.

```
clear low_thresh
```

Default: 0

Specifies the low threshold number of eGTP-C S2b call setup failures that maintain a previously generated alarm condition. If the number of call setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` must be an integer from 0 through 100 that must be lower than `high_thresh`. 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

P-GW will use the formula below for detecting Create Session Response failure rate. This failure rate is calculated based on statistics collected during a configured polling interval. The calculated failure rate is then validated against the configured threshold. Based on threshold and actual failure rate calculation, alarm will be generated or cleared.

The failure rate is the percentage of failures as determined by this formula: 1 - (Create Session Response Accept / Create Session Request).

Alerts or alarms are triggered for eGTP-C S2b setup fail rates based on the following rules:

- **Enter condition:** Actual number of S2b setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of S2b setup failures is less than the low threshold.

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

Refer to the `threshold poll egtpc-s2b-setup-fail-rate interval` command to configure the polling interval and the `threshold monitoring call-setup` command to enable monitoring for this threshold.

Examples

The following command configures a high threshold of 10 and a clear threshold of 5 to monitor call setup failure for an S2b interface:

```
threshold egtpc-s2b-setup-fail-rate 10 clear 5
```
**threshold egtpc-s5-setup-fail-rate**

Configures the eGTP-C S5 setup fail rate threshold.

**Product**
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**

```
threshold egtpc-s5-setup-fail-rate high_thresh [ clear low_thresh ]
```

**default threshold egtpc-s5-setup-fail-rate**

**default**

Configures this command with the default threshold settings and disables the threshold.

**high_thresh**

Default: 0

Specifies the high threshold number of call setup failures that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

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

*low_thresh* must be an integer from 0 through 100 that must be lower than *high_thresh*. 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

P-GW will use the formula below for detecting Create Session Response failure rate. This failure rate is calculated based on statistics collected during a configured polling interval. This calculated failure rate is then validated against the configured threshold. Based on threshold and actual failure rate calculation, alarm will be generated or cleared.

The failure rate is the percentage of failures as determined by this formula: 1 - (Create Session Response Accept / Create Session Request).

Alerts or alarms are triggered for eGTP-C S5 setup fail rates based on the following rules:

- **Enter condition**: Actual number of S5 setup failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of S5 setup failures is less than the low threshold.

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

Refer to the `threshold poll egtpc-s5-setup-fail-rate interval` command to configure the polling interval and the `threshold monitoring call-setup` command to enable monitoring for this threshold.

Examples

The following command configures a high threshold of 10 and a clear threshold of 5 to monitor call setup failure for an S5 interface:

```
threshold egtpc-s5-setup-fail-rate 10 clear 5
```
threshold epdg-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Evolved Packet Date Gateway (ePDG) sessions.

**Product**
ePDG

**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 epdg-current-sessions
default threshold epdg-current-sessions
default
```

*default*

Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

```
high_thresh
```

Default: 0

Specifies the high threshold number of the total number of ePDG subscriber 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 1000000.

```
clear low_thresh
```

Default: 0

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

`low_thresh` is an integer from 0 through 1000000.
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**

Sets the upper and power thresholds for the total number of ePDG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

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

- **Clear condition**: Actual number of ePDG 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.

**Examples**

The following command configures sets the upper threshold of ePDG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold epdg-current-sessions 100000 clear 90000
```
**threshold fng-current-active-sessions**

Configures alarm or alert thresholds for the number of subscribers currently active Femto Network Gateway (FNG) sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

**Syntax Description**
```
[ default ] threshold fng-current-active-sessions

default
Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

high_thresh
Default: 0
Specifies the high threshold number of the total number of active FNG subscriber 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 1000000.

clear low_thresh
Default: 0
Specifies the low threshold number of the total number of active FNG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.
```

**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**

Sets the upper and power thresholds for the total number of active FNG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

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

- **Clear condition**: Actual number of active FNG 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.

**Examples**

The following command configures sets the upper threshold of active FNG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold fng-current-active-sessions 100000 clear 90000
```
threshold fng-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Femto Network Gateway (FNG) sessions, including inactive sessions.

**Product**
FNG

**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 fng-current-sessions`
- `default threshold fng-current-sessions`

  **default**

  Configures this command with the default threshold settings.
  Default: High threshold: 90; Low threshold: 10

  **high_thresh**

  Default: 0

  Specifies the high threshold number of the total number of FNG subscriber 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 1000000.

  **clear low_thresh**

  Default: 0

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

  `low_thresh` is an integer from 0 through 1000000.
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**

Sets the upper and power thresholds for the total number of FNG subscriber sessions that will generate and clear alerts or alarms.

Alerts or alarms are triggered based on the following rules:

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

**Examples**

The following command configures sets the upper threshold of FNG subscriber sessions at 200000 and the lower threshold at 190000:

```
threshold fng-current-sessions 200000 clear 190000
```
## threshold fw-deny-rule

Configures alarm or alert thresholds for the Stateful Firewall Deny Rule.

### Product
PSF

### 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 fw-deny-rule high_thresh | clear low_thresh |
default threshold fw-deny-rule
```

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the Stateful Firewall Deny-Rule threshold value, which if met or exceeded generates an alert or alarm.

- `high_thresh` must be an integer from 0 through 1000000.
- Default: 0

**clear low_thresh**

Specifies the Stateful Firewall Deny-Rule alarm clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

- `low_thresh` must be an integer from 0 through 1000000.
- Default: 0
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 low threshold.

**Usage Guidelines**

When the number of Deny-Rule instances exceeds a given value, an alarm or alert is raised; it is cleared when the number of Deny-Rule instances falls below a value within 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.

**Examples**

The following command configures a Stateful Firewall Deny Rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:

```
threshold fw-deny-rule 1000 clear 900
```
**threshold fw-dos-attack**

Configures alarm or alert thresholds for Stateful Firewall Denial-of-Service (DoS) attacks.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold fw-dos-attack high_thresh [ clear low_thresh ]
default threshold fw-dos-attack
```

default
Configures this command with the default threshold settings.
Default: 0—disabled

`high_thresh`

Specifies the Stateful Firewall DoS attacks threshold value, which if met or exceeded generates an alert or alarm.

`high_thresh` must be an integer from 0 through 1000000.

Default: 0

`clear low_thresh`

Specifies the Stateful Firewall DoS attacks clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be an integer from 0 through 1000000.

Default: 0
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 low threshold.

**Usage Guidelines**

When the number of DoS attacks exceed a given value, a threshold is raised and it is cleared when the number of DoS attacks fall below a value within 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.

**Examples**

The following command configures a Stateful Firewall DoS attacks high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

```
threshold fw-dos-attack 1000 clear 100
```
threshold fw-drop-packet

Configures alarm or alert thresholds for Stateful Firewall dropped packets.

**Product**

PSF

**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 fw-drop-packet high_thresh [ clear low_thresh ]

default threshold fw-drop-packet`

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the Stateful Firewall dropped packets threshold value, which if met or exceeded generates an alert or alarm.

`high_thresh` must be an integer from 0 through 1000000.

Default: 0

**clear low_thresh**

Specifies the Stateful Firewall dropped packets clear threshold value. If, in the same polling interval, the threshold falls below `low_thresh` a clear alarm is generated.

`low_thresh` must be an integer from 0 through 1000000.

Default: 0
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 low threshold.

**Usage Guidelines**

When the number of dropped packets exceed a given value, a threshold is raised and it is cleared when the number of dropped packets fall below a value within 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.

**Examples**

The following command configures a Stateful Firewall dropped packets high threshold of 1000 and a low threshold of 900 for a system using the Alarm thresholding model:

```
threshold fw-drop-packet 1000 clear 900
```
threshold fw-no-rule

Configures alarm or alert thresholds for Stateful Firewall no rule occurrences.

**Product**

PSF

**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 fw-no-rule high_thresh [ clear low_thresh ]
default threshold fw-no-rule
```

default

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the Stateful Firewall no rules threshold value, which if met or exceeded generates an alert or alarm.

Default: 0

**clear low_thresh**

Specifies the Stateful Firewall no rules clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.

Default: 0

---

**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 low threshold.
Usage Guidelines

When the number of no rule occurrences exceeds a given value, a threshold is raised and it is cleared when the number of no rules fall below a value within 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.

Examples

The following command configures a Stateful Firewall no rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:

```
threshold fw-no-rule 1000 clear 900
```
threshold license remaining-sessions

Configures alarm or alert thresholds for the percentage of session license utilization by the system.

**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**

```
[ no ] threshold license remaining-sessions low_thresh clear high_thresh
```

`no low_thresh`

Disables threshold session license utilization alerts or alarms.

`remaining-sessions low_thresh`

Default: 10

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

`low_thresh` is an integer from 0 through 100.

`clear high_thresh`

Default: 10

Specifies the high threshold session license utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated.

`high_thresh` is an integer from 0 through 100.

**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 `Specifies the low threshold`. 
**Usage Guidelines**

Session license utilization thresholds generate alerts or alarms based on the utilization percentage of all session capacity licenses during the specified polling interval.

The system uses session capacity license to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses. Although, a single threshold is configured for all session types, alerts or alarms can be generated for each type.

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

- **Enter condition**: Actual session license utilization percentage per session type is greater than or equal to the low threshold.
- **Clear condition**: Actual session license utilization percentage per session type is greater than the high 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.

**Examples**

The following command configures a session license low threshold percentage of 10 and a high threshold of 35 for a system using the Alarm thresholding model:

```
threshold license remaining-sessions 10 clear 35
```
**threshold mgmt-cpu-memory-usage**

Configures alarm or alert thresholds for the percentage of CPU memory usage on management cards.

**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 mgmt-cpu-memory-usage high_thresh [ clear low_thresh ]

**high_thresh**

Default: 0

Specifies the high threshold percent of CPU memory usage that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

Specifies the low threshold percent of CPU memory usage that maintains a previously generated alarm condition. If the percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is measured in percentage of total memory used and can be configured to 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**

CPU memory usage thresholds generate alerts or alarms based on memory usage for the SPC, SMC, or MIO CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby SPCs, SMCs, or MIOs allowing for alerts or alarms to be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU memory usage based on the following rules:

- **Enter condition**: Actual CPU memory usage is greater than or equal to the high threshold
- **Clear condition**: Actual CPU memory usage 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.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a threshold of 65 percent of total SPC, SMC, or MIO CPU memory usage and a clear threshold of 35 percent:

```
threshold mgmt-cpu-memory-usage 65 clear 35
```
**threshold mgmt-cpu-utilization**

Configures alarm or alert thresholds for the percentage of CPU utilization on management cards.

**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 mgmt-cpu-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

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

**clear low_thresh**

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

**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**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each SPC, SMC, or MIOCPU during the specified polling interval. Although, a single threshold is configured for both SPC, SMC, or MIO CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU utilization based on the following rules:
**Enter condition**: Average measured CPU utilization for the last 5 minutes is greater than or equal to the high threshold.

**Clear condition**: Average measured CPU utilization for the last 5 minutes 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.

---

**Important**

This command is not supported on all platforms.

---

**Examples**

The following command configures a high threshold SPC, SMC, or MIO CPU utilization percentage of 90 for a system using the Alert thresholding model:

`threshold mgmt-cpu-utilization 90`
**threshold mme-attach-failure**

Configures alarm or alert thresholds for the total number of MME Attach Failure messages 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-attach-failure high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0 (Disabled)

Specifies the high threshold number of total MME Attach Failure messages across all services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0 (Disabled)

Specifies the low threshold number of total MME Attach Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages 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 through 100000. 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 Attach Failure message 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 Attach Failure message based on the following rules:

- **Enter condition**: Actual total number of MME Attach Failure messages is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of MME Attach Failure messages 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 mme-attach-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

Examples

The following command configures the limit of MME Attach Failure high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold mme-attach-failure 10000
```
**threshold mme-auth-failure**

Configures alarm or alert thresholds for the total number of MME Auth Failure messages across all the MME services.

**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-auth-failure high_thresh \[ clear low_thresh \]
```

**high_thresh**
Default: 0 (Disabled)

Specifies the high threshold number of total MME Auth Failure messages across all MMM services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

**clear low_thresh**

Default: 0 (Disabled)

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

**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 Auth Failure message 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 Auth Failure message based on the following rules:

- **Enter condition**: Actual total number of MME Auth Failure messages is greater than or equal to the high threshold.

- **Clear condition**: Actual total number of MME Auth Failure messages 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 mme-auth-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

Examples

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

```
threshold mme-auth-failure 10000
```
threshold model

Configures the thresholding model, alarm or alert, for the system to use.

**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 model { alarm | alert }

- **alarm**
  
  Selects the alarm thresholding model as described in the Usage section for this command.

- **alert**
  
  Selects the alert thresholding model as described in the Usage section for this command.

**Usage Guidelines**

The system supports the following thresholding models:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded the high threshold.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated and/or sent at the end of the polling interval.

  The alarm is cleared at the end of the first interval where the measured value is below the low threshold.
In the example shown in the figure below, this model generates an alarm during period 2 when the count exceeds the high threshold. A second alarm is generated in period 6 when the count falls beneath low threshold. The second alarm indicates a "clear" condition.

**Figure 1: Thresholding Model Example**

![Thresholding Model Example Diagram](image)

- HT = High Threshold
- LT = Low Threshold

**Important**

For certain values the alert or alarm serves to warn of low quantities (such as, memory, session licenses, etc.). In these cases, the low threshold is the condition that must be met or exceeded within the polling interval to generate the alert or alarm. When the high threshold is exceeded during an interval, the low quantity condition is cleared.

Refer to the **threshold monitoring** command for additional information on thresholding.

**Examples**

The following command configures the system to support the Alarm thresholding model:

```
threshold model alarm
```
threshold monitoring

Enables threshold monitoring for the selected value.

**Product**
All

**Privilege**
Administrator

**Command Modes**
Exec > Global Configuration

```configure
Entering the above command sequence results in the following prompt:

[local] host_name(config)#
```

**Syntax Description**

```
| no | default | threshold monitoring { aaa-acct-archive-queue | aaa-acct-archive-size | aaa-acct-failure
| aaaa-auth-failure | aaaa-retry-rate | aamgr-request-queue | asngw | call-setup | content-filtering |
cpu-resource | cpu-session-throughput | diameter | disconnect-reason | ecs | epdg-service | fa-service |
firewall | fw-and-nat | ha-service | henbgw-service | hnbkg-service | hsgw-service | ipsec | license |
lma-service | mme-service | npu-resource | packets-filtered-dropped | packets-forwarded-to-cpu | pdg-service | pdif-service | pdsn-service | pgw-service | phsgw | phspc | route-service | saegw-service |
sess-flow-count | sgw-service | subscriber | system | tpo }
```

**no**
Disables threshold monitoring for the specified value.

**default**
Sets or restores the default value assigned to the specified parameter.

**aaa-acct-archive-queue**
Enables threshold monitoring for the AAA accounting archive message queue size.
Refer to the `threshold aaa-acct-archive-queue-size` command for additional information on these values.

**aaa-acct-archive-size**
Enables threshold monitoring for the size of the AAA accounting record archive.

**aaa-acct-failure**
Enables threshold monitoring for AAA accounting failures and AAA accounting failure rate values.
Refer to the `threshold aaa-acct-failure` and `threshold aaa-acct-failure-rate` commands for additional information on these values.

**aaa-auth-failure**
Enables threshold monitoring for AAA authentication failures and AAA authentication failure rate values.

Refer to the `threshold aaa-auth-failure` and `threshold aaa-auth-failure-rate` commands for additional information on these values.

**aaa-retry-rate**
Enables threshold monitoring for the AAA retry rate value.

Refer to the `threshold aaa-retry-rate` command for additional information on this value.

**aaamgr-request-queue**
Enables threshold monitoring for AAA Manager Requests for each AAA manager process. Refer to the `threshold aaamgr-request-queue` command for additional information on these values.

**asngw**
Enables the threshold monitoring for ASN-GW services.

**call-setup**
Enables threshold monitoring for the call setup, call setup failures, and no-resource rejected call values.

Refer to the `threshold call-setup`, `threshold call-setup-failure`, `threshold egtpc-s2b-setup-fail-rate`, `threshold egtpc-s5-setup-fail-rate`, `threshold ppp-setup-fail-rate`, `threshold rp-setup-fail-rate`, and `threshold call-reject-no-resource` commands for additional information on these values.

**cpu-resource**
Enables threshold monitoring for CPU thresholds.


**cpu-session-throughput**
Enables threshold monitoring for the CPU session throughput value.

Refer to the `threshold cpu-session-throughput` command for additional information on this value.

**content-filtering**
Enables threshold monitoring for the Content Filtering in-line service.

**diameter**
Enables threshold monitoring for Diameter.
disconnect-reason
 Enables disconnect-reason related thresholds.

ecs
 Enables threshold monitoring for the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

epdg-service
 Enables threshold monitoring for Evolved Packet Data Gateway (ePDG) service.
 Refer to the threshold epdg-current-sessions command for additional information on this value.

fa-service
 Enables threshold monitoring for Registration Reply errors for each FA service.
 Refer to the threshold reg-reply-error FA Service Configuration Mode command for additional information on this value.

firewall
 Enables threshold monitoring for the Stateful Firewall in-line service.
 Default: Disabled
 Refer to the threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop-packet, and threshold fw-no-rule commands for additional information on this value.

Important
 Stateful Firewall thresholds can only be enabled if the Stateful Firewall license is present.

fw-and-nat
 Enables threshold monitoring for the Firewall and NAT in-line service.
 Default: Disabled
 Refer to the threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop-packet, threshold fw-no-rule, threshold nat-pkt-drop, and threshold nat-port-chunks-usage commands for additional information on this value.

ha-service
 Enables threshold monitoring for Registration Reply errors, re-registration reply errors, deregistration reply errors, and average calls setup per second for each HA service and average calls setup per second at the context level.
 Refer to the threshold init-rrq-rcvd-rate, threshold reg-reply-error, threshold rereg-reply-error, and threshold dereg-reply-error HA Service Configuration Mode commands and the threshold ha-service init-rrq-rcvd-rate Context Configuration mode command for additional information on this value.
henbgw-service

Important: In Release 20.0, HeNBGW is not supported. This command must not be used in Release 20.0. For more information, contact your Cisco account representative.

Enables threshold monitoring for HeNB-GW service.

Important: This keyword is required to activate the threshold alarm/alert for HeNB-GW service to use threshold <henbgw-paging-messages>, threshold total-henbgw-henb-sessions, and threshold total-henbgw-ue-sessions commands for threshold values.

hnbgw-service

Important: In Release 20.0, HNBGW is not supported. This command must not be used in Release 20.0. For more information, contact your Cisco account representative.

Enables threshold monitoring for HNBGW sessions including Iu-CS and Iu-PS sessions for HNBGW services on a system at the system level.

Important: This keyword is required to activate the threshold alarm/alert for HNBGW service to use threshold total-hnbgw-hnb-sessions, threshold total-hnbgw-iu-sessions, and threshold total-hnbgw-ue-sessions command for threshold values.

hsgw-service

Enables threshold monitoring for HSGW services.
Refer to the threshold total-hsgw-sessions for more information on HSGW thresholds.

ipsec

Enables monitoring of IPSec thresholds.
Refer to the HA-Service Configuration Mode chapter of the Command Line Interface Reference for information on the IPSec thresholds.

license

Enables threshold monitoring for the session license value.
Refer to the threshold license command for additional information on this value.

lma-service

Enables threshold monitoring for LMA services.
Refer to the threshold total-lma-sessions command for more information on LMA thresholds.
mme-service
Default: Disabled.
Enables threshold monitoring for the MME services.
Refer to the threshold total-mme-sessions command for additional information on this value.

npu-resource
Enables threshold monitoring for the Network Processor Unit (NPU) resources, including NPU utilization.
Refer to the threshold npu-utilization command for additional information on this value.

packets-filtered-dropped
Enables threshold monitoring for the filtered/dropped packet value.
Refer to the threshold packets-filtered-dropped command for additional information on this value.

packets-forwarded-to-cpu
Enables threshold monitoring for the forwarded packet value.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pdg-service
Enables threshold monitoring for PDG service.
Threshold monitoring for PDG service is disabled by default.

pdif-service
Enables threshold monitoring for PDIF service.

pdsn-service
Enables threshold monitoring for average calls setup per second for contexts and for PDSN services, A11 Request.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pgw-service
Enables threshold monitoring for P-GW services.
Refer to the threshold total-pgw-sessions for more information on P-GW thresholds.

route-service
Enables threshold monitoring for BGP/VRF route services.
Refer to the ip maximum-routes command in Context configuration mode and threshold route-service bgp-routes in this mode for more information on route thresholds.

saegw-service
Enables threshold monitoring for SAEGW services.
Refer to the threshold total-saegw-sessions for more information on SAEGW thresholds.
sess-flow-count
Enables threshold monitoring for Session Flow Count.
Default: 90%
Refer to the threshold sess-flow-count for more information on Session Flow Count Thresholds

sgw-service
Enables threshold monitoring for S-GW services.
Refer to the threshold total-sgw-sessions for more information on S-GW thresholds.

subscriber
Enables threshold monitoring for the subscriber and session values.
Refer to the threshold subscriber active, threshold subscriber total, threshold total-ggsn-sessions, threshold total-gprs-sessions, threshold total-ha-sessions, threshold total-lns-sessions, threshold total-pdsn-sessions, threshold total-pgw-sessions, threshold total-sgw-sessions, threshold per-service-ggsn-sessions, threshold per-service-ha-sessions, threshold per-service-lns-sessions, and threshold per-service-pdsn-sessions commands for additional information on these values.

system
Enables system (chassis) thresholds monitoring.

Important
The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

Usage Guidelines
Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

• **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

• **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
• **Alarm System:** High threshold alarms generated within the specified polling interval are considered "outstanding" until a the condition no longer exists and/or a condition clear alarm is generated. "Outstanding" alarms are reported to through the system's alarm subsystem and are viewable through the CLI. The following table indicates the reporting mechanisms supported by each of the above models.

**Table 1: ASR 5000 Thresholding Reporting Mechanisms by Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Table 2: ASR 5500 Thresholding Reporting Mechanisms by Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

In addition to the values that can be enabled by this command, the system supports the enabling of threshold monitoring for IP pool address availability (refer to the `ip pool` and threshold commands in this reference) and port utilization (refer to the threshold commands in this chapter).

**Examples**

The following command enables thresholding for subscriber totals:

```
threshold monitoring subscriber
```

---

*This page is from the Command Line Interface Reference, Commands G - H, StarOS Release 20.*
threshold nat-pkt-drop

Configures alarm or alert thresholds for the percentage of Network Address Translation (NAT) packet drops.

**Product**

NAT

**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 nat-pkt-drop high_thresh [ clear low_thresh ]
default threshold nat-pkt-drop

default
```

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

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

`high_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**clear low_thresh**

Specifies the low NAT packet drop percentage threshold that must be met within the polling interval for a clear alarm to be generated.

`low_thresh` must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the `high_thresh` will be the high and low threshold setting.

Default: 0

**Usage Guidelines**

Use this command to configure the NAT packet drop threshold settings.
Examples

The following command sets the NAT packet drop threshold settings to a high of 55% and a low of 15%:

```
threshold nat-pkt-drop 55 clear 15
```
threshold nat-port-chunks-usage

Confirms alarm or alert thresholds for the percentage of Network Address Translation (NAT) port chunk utilization.

<table>
<thead>
<tr>
<th>Important</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command is only available in 8.3 and later releases.</td>
</tr>
</tbody>
</table>

**Product**

NAT

**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 nat-port-chunks-usage high_thresh [ clear low_thresh ]
default threshold nat-port-chunks-usage
```

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the high NAT-port-chunks-usage percentage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**clear low_thresh**

Specifies the low nat-port-chunks-usage percentage threshold that must be met within the polling interval for a clear alarm to be generated.

*low_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the high_thresh will be the high and low threshold setting.
Default: 0

Usage Guidelines
Use this command to configure the NAT port chunk utilization threshold settings.

Examples
The following command sets the NAT port chunk utilization threshold settings to a high of 75% and a low of 15%:
threshold nat-port-chunks-usage 75 clear 15
threshold npu-utilization

Configures alarm or alert thresholds for the percentage of network processing unit (NPU) 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 npu-utilization high_thresh clear low_thresh
```

default

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

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

*high_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**clear low_thresh**

Specifies the low percentage threshold for NPU utilization that must be met within the polling interval for a clear alarm to be generated.

*low_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the *high_thresh* will be the high and low threshold setting.

Default: 0

**Usage Guidelines**

Use this command to configure the NPU utilization threshold settings.
Examples

The following command sets the NPU utilization threshold settings to a high of 90% and a low of 75%:

```
threshold npu-utilization 90 clear 75
```
threshold packets-filtered-dropped

Configures alarm or alert thresholds for filtered or dropped packets within the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-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 packets-filtered-dropped high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of filtered/dropped packets experienced by the system resulting from access control list (ACL) rules that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.
Usage Guidelines
Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of ACL rules during the specified polling interval.

Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets is greater than or equal to the high threshold.
- **Clear condition:** Actual number of filtered/dropped packets 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. In addition, refer to information on ACLs in this reference.

Examples
The following command configures a filtered/dropped packet high threshold count of 150000 for a system using the Alert thresholding model:

```
threshold packets-filtered-dropped 150000
```
threshold packets-forwarded-to-cpu

Configures alarm or alert thresholds for packets forwarded to active system CPUs in the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-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 packets-forwarded-to-cpu *high_thresh* [ clear *low_thresh* ]

*high_thresh*
Default: 0
Specifies the high threshold number of packets forwarded to CPUs that must be met or exceeded within the polling interval to generate an alert or alarm.
*high_thresh* is an integer from 0 through 1000000000. A value of 0 disables the threshold.

*clear low_thresh*
Default: 0
Specifies the low threshold number of packets forwarded to CPUs that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
*low_thresh* is an integer from 0 through 1000000000. A value of 0 disables the threshold.
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**

Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

**Important**

Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

- **Enter condition:** Actual number of forwarded packets is greater than or equal to the high threshold
- **Clear condition:** Actual number of forwarded packets 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.

**Examples**

The following command configures a forwarded packet high threshold count of 100000 for a system using the Alert thresholding model:

```
threshold packets-forwarded-to-cpu 100000
```
threshold pdg-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions.

**Product**
PDG/TTG

**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**

```plaintext
threshold pdg-current-active-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Configures the total number of active PDG sessions to be monitored on a chassis. `high_thresh` is an integer from 0 through 1000000.
There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**
Clears the number of sessions being monitored using the `high_thresh` variable defined above.
`low_thresh` is an integer from 0 through 1000000.

**Usage Guidelines**
Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of active PDG sessions for an entire chassis.

**Examples**
The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDG sessions on a chassis:

```
threshold pdg-current-active-sessions 300000 clear 100000
```
threshold pdg-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

**Product**
PDG/TTG

**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 pdg-current-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Configures the total number of PDG sessions on a chassis, both active and inactive. *high_thresh* is any integer from 0 through 1000000.

There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**
Clears any number of sessions being monitored using the *high_thresh* variable defined above.

*low_thresh* is any integer from 0 through 1000000.

**Usage Guidelines**
Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of PDG sessions, both active and inactive, for an entire chassis.

**Examples**
The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDG sessions on a chassis:

```
threshold pdg-current-sessions 300000 clear 100000
```
threshold pdif-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Interworking Function (PDIF) sessions.

**Product**
PDIF

**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 pdif-current-active sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Configures the total number of active PDIF sessions to be monitored on a chassis. `high_thresh` is any integer from 0 through 1000000.

There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**

Clears the specified number of sessions being monitored using the `high_thresh` variable defined above. `low_thresh` is any integer from 0 through 1000000.

**Usage Guidelines**

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of active PDIF sessions for an entire chassis.

**Examples**

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDIF sessions on a chassis:

```
threshold pdif-current-active-sessions 300000 clear 100000
```
threshold pdif-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

**Product**
PDIF

**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 pdif-current-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Configures the total number of PDIF sessions on a chassis, both active and inactive. `high_thresh` is an integer from 0 through 1000000.

There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**
Clears the specified number of sessions being monitored using the `high_thresh` variable defined above. `low_thresh` is an integer from 0 through 1000000.

**Usage Guidelines**
Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of PDIF sessions, both active and inactive, for an entire chassis.

**Examples**
The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDIF sessions on a chassis:

`threshold pdif-current-sessions 300000 clear 100000`
threshold per-service-asngw-sessions

Configures alarm or alert thresholds for the number of sessions per ASN-GW service in the system.

**Product**
ASN-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 per-service-asngw-sessions high_thresh [ clear low_thresh ]
```

`high_thresh`

Default: 0

Specifies the high threshold number of PDP contexts for any one ASN-GW service 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 PDP contexts for any one ASN-GW service 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 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 number of PDP contexts for any ASN-GW service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any ASN-GW service is greater than or equal to the high threshold
- **Clear condition:** Actual 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.

### Examples

The following command configures a high threshold count of 10000 subscriber attaches per ANS-GW service for the Alert thresholding model:

```
threshold per-service-asngw-sessions 10000
```
threshold per-service-ggsn-sessions

Configures alarm or alert thresholds for the number of PDP contexts per GGSN service 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 per-service-ggsn-sessions high_thresh [ clear low_thresh ]

**high_thresh**

Default: 0

Specifies the high threshold number of PDP contexts for any one GGSN service 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 PDP contexts for any one GGSN service 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 number of PDP contexts for any GGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GGSN service is greater than or equal to the high threshold
- **Clear condition:** Actual 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.

**Examples**

The following command configures a high threshold count of 10000 subscriber attaches per GGSN service for the Alert thresholding model:

```
threshold per-service-ggsn-sessions 10000
```
threshold per-service-gprs-pdp-sessions

Configures alarm or alert thresholds for the number of 2G-activated PDP contexts per GPRS service.

Product

SGSN

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 per-service-gprs-pdp-sessions high_thresh | clear low_thresh

high_thresh

Default: 0

Specifies the high threshold number of 2G-activated PDP contexts for any one GPRS service. This number 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 2G-activated PDP contexts for any one GPRS service. This number or higher maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, then 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 number of 2G-activated PDP contexts for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GPRS service is greater than or equal to the high threshold.
- **Clear condition:** Actual 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.

**Examples**

The following command configures a high threshold count of 10000 2G-activated PDP contexts per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-gprs-sessions

Configures alarm or alert thresholds for the number of 2G-attached subscribers per GPRS service.

**Product**
SGSN

**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 per-service-gprs-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of 2G-attached subscribers for any one GPRS service. This threshold number must be met or exceeded within the polling interval to generate an alert or alarm.

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

**clear low_thresh**

Default: 0

Specifies the low threshold number of 2G-attached subscribers for any one GPRS service. The number of subscribers must remain above this threshold in order to maintain a previously generated alarm condition. If the number of 2G subscribers falls beneath the low threshold within the polling interval, then 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 number of 2G-attached subscribers for any GPRS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 2G-attached subscribers for any GPRS service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of 2G-attached subscribers 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.

**Examples**

The following command configures a high threshold count of 10000 2G-attaches per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-ha-sessions

Configures alarm or alert thresholds for the number of HA sessions per Home Agent (HA) service 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 per-service-ha-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of HA sessions for any one HA service 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 any one HA service 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 number of HA sessions for any HA service 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 number of HA sessions for any HA service is greater than or equal to the high threshold.
- **Clear condition**: Actual 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.

**Examples**

The following command configures a HA session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-ha-sessions 10000
```
threshold per-service-lns-sessions

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

**Product**

- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**

Security Administrator, Administrator

**Command Modes**

Exec > Global Configuration

```markdown
configure
```

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```
threshold per-service-lns-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of LNS sessions for any one LNS service 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 LNS sessions for any one LNS service 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 through 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 number of LNS sessions for any LNS service in the system is equal to or greater than the set limit.

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

- **Enter condition**: Actual number of LNS sessions for any LNS service is greater than or equal to the high threshold.
- **Clear condition**: Actual 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.

Examples

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

`threshold per-service-lns-sessions 10000`
threshold per-service-pdg-sessions

Configures alarm or alert thresholds for the number of Packet Data Gateway (PDG) sessions per PDG service in the system.

**Product**
PDG/TTG

**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 per-service-pdg-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of PDG sessions for any one PDG service 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

Specifies the low threshold number of PDG sessions for any one PDG service that maintains a previously generated alarm condition. If the number of PDG sessions 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**

Monitor and set alarms or alerts when the number of PDG sessions for any PDG service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition**: Actual number of PDG sessions for any PDG service is greater than or equal to the high threshold.

- **Clear condition**: Actual 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.

**Examples**

The following command configures a PDG session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-pdg-sessions 10000```

Threshold per-service-pdsn-sessions

Configures alarm or alert thresholds for the number of Packet Data Serving Node (PDSN) sessions per PDSN service 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 per-service-pdsn-sessions high_thresh | clear low_thresh`

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of PDSN sessions for any one PDSN service 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 PDSN sessions for any one PDSN service 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 through 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 number of PDSN sessions for any PDSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition**: Actual number of PDSN sessions for any PDSN service is greater than or equal to the high threshold.

- **Clear condition**: Actual 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.

**Examples**

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

```
threshold per-service-pdsn-sessions 10000
```
threshold per-service-samog-sessions

Configures alarm or alert thresholds for the number of S2a Mobility over GTP (SaMOG) sessions per SaMOG service in the system.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Command Modes**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

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

**Syntax Description**

```plaintext
threshold per-service-samog-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of SaMOG sessions for any one SaMOG service that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 4,000,000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of SaMOG sessions for any one SaMOG service that maintains a previously generated alarm condition. If the number of SaMOG sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 through 4,000,000. 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 number of SaMOG sessions for any SaMOG service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SaMOG sessions based on the following rules:

- **Enter condition:** Actual number of SaMOG sessions for any SaMOG service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of SaMOG 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 for this value.

### Examples

The following command configures a SaMOG session per service high threshold count of 15000 for a system using the Alert thresholding model:

```
threshold per-service-samog-sessions 15000
```
threshold per-service-sgsn-pdp-sessions

Configures alarm or alert thresholds for the number of 3G-activated PDP contexts per SGSN service on the system.

Product
SGSN

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 per-service-sgsn-pdp-sessions high_thresh | clear low_thresh |

high_thresh
Default: 0
Specifies the high threshold number of 3G-activated PDP contexts for any one SGSN service. This number 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 3G-activated PDP contexts for any one SGSN service. This number or higher maintains a previously generated alarm condition. If the number of 3G-activated PDP contexts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2400000. 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 number of 3G-activated PDP contexts for any SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 3G-activated PDP contexts for any SGSN service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of 3G-activated 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.

**Examples**

The following command configures a high threshold count of 10000 3G-activated PDP contexts per SGSN service for the system's Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold per-service-sgsn-sessions

Configures alarm or alert thresholds for the number of 3G-attached subscribers per SGSN service in the system.

**Product**
SGSN

**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 per-service-sgsn-sessions high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

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

**clear low_thresh**

Default: 0

Specifies the low threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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 number of 3G-attached subscribers for any one SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 3G-attached subscribers for any single SGSN service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of 3G-attached subscribers for any single SGSN service 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.

### Examples

The following command configures a high threshold count of 10000 3G-attached subscribers per SGSN service for a system using the Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold phsgw-auth-failure

Configures alarm or alert thresholds for the number of authentication failures in Personal Handyphone Service Gateway (PHSGW) service.

**Product**

PHSGW

**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 phsgw-auth-failure high_thresh [ clear low_thresh ]`

* `high_thresh`

  Default: 0

  Specifies the high threshold number for PHSGW authentication failures in any one PHSGW service. This number 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_thres`

  Default: 0

  Specifies the low threshold number of PHSGW authentication failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

  `low_thres` 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**

Set the monitoring and clearing thresholds for PHSGW authentication failures.
Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual number of PHSGW authentication failures in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of PHSGW authentication failures in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW authentication failures:

```
threshold phsgw-auth-failure 100000 clear 50000
```
threshold phsgw-eapol-auth-failure

Configures alarm or alert thresholds for authentication failures for a PHSGW service using Extensible Authentication Protocol Over LAN (EAPOL).

Product

PHSGW

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 phsgw-eapol-auth-failure [high_thresh | clear low_thresh]

    high_thresh
    Default: 0
    Specifies the high threshold number for PHSGW EAPOL failures in any one PHSGW service. This number 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
    Specifies the low threshold number of PHSGW EAPOL failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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

Set the monitoring and clearing thresholds for PHSGW EAPOL failures.
Alerts or alarms are triggered for EAPOL failures based on the following rules:

- **Enter condition:** Actual number of PHSGW EAPOL failures in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAPOL failures in any one PHSGW service 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.

### Examples

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL failures:

```
threshold phsgw-eapol-auth-failure 100000 clear 50000
```
# threshold phsgw-handoff-denial

Configures alarm or alert thresholds for handoff denials in PHSGW.

**Product**

PHSGW

**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 phsgw-handoff-denial high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of handoff denials for any one PHSGW service. This number 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
  
  Specifies the low threshold number of handoff denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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**

Set the monitoring and clearing thresholds for PHSGW handoff denials.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSGW handoff denials in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW handoff denials in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW handoff denials:

```
threshold phsgw-handoff-denial 100000 clear 50000
```
threshold phsgw-max-eap-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol (EAP) retries in PHSGW.

**Product**  
PHSGW

**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 phsgw-max-eap-retry high_thresh [ clear low_thresh ]
```

*high_thresh*

Default: 0  
Specifies the high threshold number of EAP retries for any one PHSGW service. This number 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  
Specifies the low threshold number of EAP retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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**  
Set the monitoring and clearing thresholds for PHSGW EAP retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW EAP retries in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAP retries in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAP retries:

```
threshold phsgw-max-eap-retry 100000 clear 50000
```
threshold phsgw-max-eapol-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol over LAN (EAPOL) retries in PHSGW.

**Product**

PHSGW

**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 phsgw-max-eapol-retry high_thresh [ clear low_thresh ]`

`high_thresh`

Default: 0

Specifies the high threshold number of EAPOL retries for any one PHSGW service. This number 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

Specifies the low threshold number of EAPOL retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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**

Set the monitoring and clearing thresholds for PHSGW EAPOL retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW EAPOL retries in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAPOL retries in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL retries:

```
threshold phsgw-max-eapol-retry 100000 clear 50000
```
threshold phsgw-network-entry-denial

Configures, alarm or alert thresholds for the number of network entry denials in PHSGW.

**Product**

PHSGW

**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 phsgw-max-network-entry-denial high_thresh | clear low_thresh |

*high_thresh*

Default: 0

Specifies the high threshold number of network entry denials for any one PHSGW service. This number 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

Specifies the low threshold number of network entry denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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.

---

**Usage Guidelines**

Set the monitoring and clearing thresholds for PHSGW network entry denials.

Alerts or alarms are triggered for handoff denials based on the following rules:

---

**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.
• **Enter condition:** Actual number of PHSGW network entry denials in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW network entry denials in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW network entry denials:

```
threshold phsgw-network-entry-denial 100000 clear 50000
```
**threshold phsgw-session-setup-timeout**

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out during setup.

**Product**

PHSGW

**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 phsgw-session-setup-timeout high_thresh | clear low_thresh
```

**high_thresh**

Default: 0

Specifies the high threshold number of session setup timeouts for any one PHSGW service. This number 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

Specifies the low threshold number of session setup timeouts for any one PHSGW service. This number must be met to maintain a previously generated alarm condition. If the number of subscribers 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**

Set the monitoring and clearing thresholds for PHSGW session setup timeouts.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSGW session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW session setup timeouts in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of `100000` and a clearing threshold of `50000` for PHSGW session setup timeouts:

```plaintext
threshold phsgw-session-setup-timeout 100000 clear 50000
```
threshold phsgw-session-timeout

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out.

**Product**
PHSGW

**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 phsgw-session-timeout **high_thresh** [ **clear** **low_thresh** ]

**high_thresh**

Default: 0

Specifies the high threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

**low_thresh**

Default: 0

Specifies the low threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

**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**

Set the monitoring and clearing thresholds for PHSGW session timeouts.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSGW session timeouts in any one PHSGW service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSGW session timeouts in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW session timeouts:

```
threshold phsgw-session-timeout 100000 clear 50000
```
threshold phspc-session-setup-timeout

Configures alarm or alert thresholds for the number of Personal Handyphone System - Personal Computer (PHSPC) sessions that timed out during setup.

**Product**

PHSGW

**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 phspc-session-setup-timeout high_thresh \[ clear low_thresh \]
```

**high_thresh**

Default: 0

Specifies the high threshold number of session setup timeouts for any one PHSPC service. This number 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

Specifies the low threshold number of session setup timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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**

Set the monitoring and clearing thresholds for PHSPC session setup timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC session setup timeouts:

```
threshold phspsc-session-setup-timeout 100000 clear 50000
```
threshold phspc-sleep-mode-timeout

Configures alarm or alert thresholds for the number of PHSPC sessions that timed out when the personal computer went into sleep mode.

Product  PHSGW

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 phspc-sleep-mode-timeout high_thresh | clear low_thresh |

  high_thresh
  Default: 0
  Specifies the high threshold number of sleep mode timeouts for any one PHSPC service. This number 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
  Specifies the low threshold number of sleep mode timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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  Set the monitoring and clearing thresholds for PHSPC sleep mode timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC sleep mode timeouts in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSPC sleep mode timeouts in any one PHSGW service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC sleep mode timeouts:

`threshold phspc-sleep-mode-timeout 100000 clear 50000`
threshold phspc-sm-entry-denial

Configures alarm or alert thresholds for the number of denied PHSPC short message (SM) sessions.

Product

PHSGW

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 phspc-sm-entry-denial \[high\_thresh \[ clear low\_thresh \]

high\_thresh

Default: 0

Specifies the high threshold number of SM entry denials for any one PHSPC service. This number 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

Specifies the low threshold number of SM entry denials for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers 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

Set the monitoring and clearing thresholds for PHSPC SM entry denials.

Alerts or alarms are triggered for handoff denials based on the following rules:
• **Enter condition:** Actual number of PHSPC SM entry denials in any one PHSPC service is greater than or equal to the high threshold.

• **Clear condition:** Actual number of PHSPC SM entry denials in any one PHSPC service 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.

**Examples**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC SM entry denials:

```
threshold phsgw-sm-entry-denial 100000 clear 50000
```
threshold phspc-sm-entry-denial