Cisco ASR 5000 Series Thresholding Configuration Guide

Version 10.0

Last Updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22967-01

Cisco ASR 5000 Series Thresholding Configuration Guide

CONTENTS

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
Thresholding Overview

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.

The following thresholding models are supported by the system:

- **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 then generated and/or sent at the end of the polling interval.

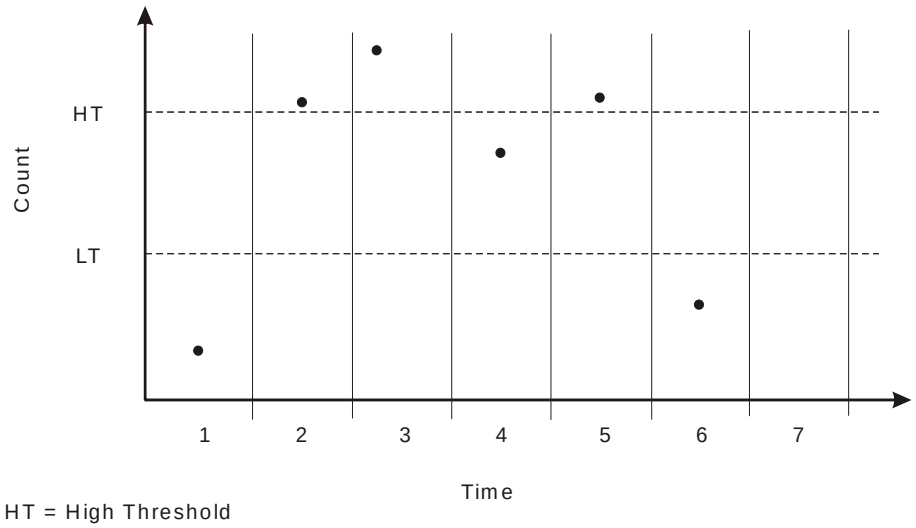
  In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded HT.

- **Alarm:** Both high and low thresholds 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 then 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 in the figure below, this model generates an alarm during period 2 when the count exceeds HT. A second alarm is generated in period 6 when the count falls beneath LT. The second alarm indicates a “clear” condition.

Figure 1. Example of Thresholding Model



HT = High Threshold
LT = Low Threshold

Important: Note that for certain values, the alert or alarm serves to warn of low quantities (i.e. 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. Once the high threshold is exceeded during an interval, the low quantity condition is cleared.

Thresholding functionality on the system can be configured to monitor the following values:

- AAA:
  - Archive size
  - Number of authentication failures
  - Authentication failure rate
  - Number of accounting failures
  - Accounting failure rate
  - Retry rate
  - AAA Manager request queue usage
- ASN GW Service:
  - Number of ASN GW Authentication failures
  - Number of ASN GW hand-off denials
  - Maximum number of EAP retries
  - Number of network entry denials
  - Number of Network Access Identifier (NAI) in R6 message
  - ASN GW timeout duration during session setup
  - ASN GW session timeout duration
- FA Service registration reply errors

- HA Service:
  - Call setup rate
  - Registration Reply, Re-registration Reply, and De-registration Reply errors
- PDSN Service:
  - Call setup rate
  - A11 Messages failed and discarded
  - PPP send packets discarded
- Call setup:
  - Number of calls setup
  - Number of call setup failures
  - RP setup failure rate
  - PPP setup failure rate
  - Number of calls rejected due to no processing resources being available
- MME Service
  - Number of MME Authentication failures
  - Number of MME Session Attachment failures
  - Number of MME sessions
- PAC/PSC CPU resource availability:
  - 10 second sample utilization
  - Percent utilization
  - Available memory
  - Load
  - Memory usage
  - Session throughput
- SPC/SMC CPU resource availability:
  - Memory usage
  - Percent utilization
  - ORBS software task utilization
- IP address pool utilization
- Licensed session utilization
- Packet processing:
  - Number of packets filtered/dropped
  - Number of packets forwarded to CPU
- Per-service session count
- Port utilization:
  - High activity
  - Transmit utilization

    - Receive utilization
- Subscriber number:
    - Total number
    - Number active
- Total session count
- SPC/SMC CompactFlash memory utilization

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.

  Refer to the System Administration Guide for additional information on system logging functionality.
- **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 system's CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 1. Thresholding Reporting Mechanisms by Model

Model	SNMP Traps	Logs	Alarm System
Alert	X	X	
Alarm	X	X	X

Chapter 2
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##################################################################################

Displaying Global
AAA-configuration errors
##################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices.This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

`save configuration` *`tftp://config_server/init_config.cfg`*

Chapter 3
AAA Thresholds

Threshold monitoring can be enabled for the AAA-related values described in the following table.

Value	Description	To configure, go to section:
Archive size	Enables the generation of alerts or alarms based on the number of AAA (RADIUS and/or GTPP) accounting messages archived during the polling interval.	AAA Accounting Message Archive Size Thresholds
Accounting Failures	Enables the generation of alerts or alarms based on the number of failed AAA accounting requests that occur during the polling interval.	AAA Accounting Failure Thresholds
Accounting Failure Rate	Enables the generation of alerts or alarms based on the percentage of AAA accounting requests that failed during the polling interval.	AAA Accounting Failure Rate Thresholds
Authentication Failures	Enables the generation of alerts or alarms based on the number of failed AAA authentication requests that occur during the polling interval.	AAA Authentication Failure Thresholds
Authentication Failure Rate	Enables the generation of alerts or alarms based on the percentage of AAA authentication requests that failed during the polling interval.	AAA Authentication Failure Rate Thresholds
Retry Rate	Enables the generation of alerts or alarms based on the percentage of AAA requests (both accounting and authentication) that were re-tried during the polling interval.	AAA Request Message Retry Rate Thresholds
AAA Manager Request Queue Usage	Enables the generation of alarms or alerts when the AAA Manager request queue usage reaches a specified percentage level.	AAA Manager Request Queue Threshold

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

AAA Accounting Message Archive Size Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of archived messages < 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.

Configuring AAA Accounting Message Archive Size Threshold

Use the following example to configure the accounting message archive size threshold:

```
configure
   threshold aaa-acct-archive-size <high_thresh> [ clear <low_thresh> ]
   threshold poll aaa-acct-archive-size interval <time>
   threshold monitoring aaa-acct-archive-size
   end
```

AAA Accounting Failure Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of failures < 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.

Configuring AAA Accounting Failure Threshold

Use the following example to configure AAA accounting failure threshold:

```
config
    threshold aaa-acct-failure <high_thresh> [ clear <low_thresh> ]
    threshold poll aaa-acct-failure interval <time>
    threshold monitoring aaa-acct-failure
    end
```

AAA Accounting Failure Rate Thresholds

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 number of failures > or = High Threshold
- **Clear condition:** Actual number of failures < 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.

Configuring AAA Accounting Failure Rate Threshold

Use the following example to configure AAA accounting failure rate threshold:

```
configuration
    threshold aaa-acct-failure-rate <high_thresh> [ clear <low_thresh> ]
    threshold poll aaa-acct-failure-rate interval <time>
    threshold monitoring aaa-acct-failure
    end
```

AAA Authentication Failure Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of failures < 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.

Configuring AAA Authentication Failure Threshold

Use the following example to configure AAA authentication failure threshold:

```
configuration
    threshold aaa-auth-failure <high_thresh> [ clear <low_thresh> ]
    threshold poll aaa-auth-failure interval <time>
    threshold monitoring aaa-auth-failure
    end
```

AAA Authentication Failure Rate Thresholds

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 failure rates based on the following rules:

- **Enter condition:** Actual failure percentage > or = High Threshold
- **Clear condition:** Actual failure percentage < 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.

Configuring AAA Authentication Failure Rate Threshold

Use the following example for configuring AAA authentication failure rate threshold:

```
configure
    threshold aaa-auth-failure-rate <high_thresh> [ clear <low_thresh> ]
    threshold poll aaa-auth-failure-rate interval <time>
    threshold monitoring aaa-auth-failure
    end
```

AAA Request Message Retry Rate Thresholds

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 failure percentage > or = High Threshold
- **Clear condition:** Actual failure percentage < 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.

Configuring AAA Authentication Failure Rate Threshold

Use the following example for configuring AAA request message retriy rate threshold:

```
configure
    threshold aaa-retry-rate <high_thresh> [ clear <low_thresh> ]
    threshold poll aaa-retry-rate interval <time>
    threshold monitoring aaa-retry-rate
    end
```

AAA Manager Request Queue Threshold

The AAA Manager request queue threshold generates an alert or alarm based on the usage percentage of the AAA Manager request queue during the specified polling interval. The percentage is based on the total number of pending requests for the AAA Manager and the total size allowed for the queue. This is polled for each AAA Manager process.

Alerts or alarms are triggered for the AAA Manager request queue threshold based on the following rules:

- **Enter condition:** Actual AAA Manager request queue percentage used > or = High Threshold
- **Clear condition:** Actual AAA Manager request queue percentage used < 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.

Configuring AAA Manager Request Queue Threshold

Use the following example for configuring AAA Manager request queue threshold.

```
configure
    threshold aaamgr-request-queue <high_thresh> [ clear <low_thresh> ]
    threshold poll aaamgr-request-queue interval <time>
    threshold monitoring aaamgr-request-queue
    end
```

Chapter 4
ASN GW Service Thresholds

ASN GW Service thresholds generate alerts or alarms for the average number of calls setup. A threshold can be configured to report this information on entire system for ASN GW service. Thresholds can also be configured for session registration response failures, discarded interface registration requests, discarded network entry registration acknowledgments for ASN GW services.

Alerts or alarms are triggered for these ASN GW thresholds based on the following rules:

- **Enter condition:** When the actual average of call setups or actual number of failures or discards passes, or is equal to, the configured Threshold value an alert or alarm is set.
- **Clear condition:** When the actual average of call setups or actual number of failures or discards passes below the Threshold value the alert or alarm is cleared.

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

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

System-Level ASN GW Service Thresholds

The system-level thresholds for ASN GW Service-Level can be configured to monitor thresholds for subscriber network entry, authentication, session registration response failures, discarded registration requests, session timeout, and hand-off denials for individual ASN GW services.

Following thresholds can be configured for the ASN GW service-level:

- Number of ASN GW Authentication failures
- Number of ASN GW hand-off denials
- Maximum number of EAP retries
- Number of network entry denials
- Number of Network Access Identifier (NAI) in R6 message
- ASN GW timeout duration during session setup
- ASN GW session timeout duration

Configuring System-level ASN GW Service Thresholds

Use the following example to configure and enable these thresholds:

```
configuration
   threshold asngw-auth-failure <high_thresh> [clear <low_thresh>]
   threshold asngw-handoff-denial <high_thresh> [clear <low_thresh>]
   threshold asngw-max-eap-retry <high_thresh> [clear <low_thresh>]
   threshold asngw-network-entry-denial <high_thresh> [clear
   <low_thresh>]
   threshold asngw-r6-invalid-nai <high_thresh> [clear <low_thresh>]
   threshold asngw-session-setup-timeout <high_thresh> [clear
   <low_thresh>]
   threshold asngw-session-timeout <high_thresh> [clear <low_thresh>]
   threshold poll asngw-auth-failure interval <time>
   threshold poll asngw-handoff-denial interval <time>
   threshold poll asngw-max-eap-retry interval <time>
   threshold poll asngw-network-entry-denial interval <time>
   threshold poll asngw-r6-invalid-nai interval <time>
```

```
threshold poll asngw-session-setup-timeout interval <time>
threshold poll asngw-session-timeout interval <time>
threshold monitoring asngw
end
```

Chapter 5
Call Setup Thresholds

Threshold monitoring can be enabled for the call setup values described in the following table.

Value	Description	To configure, go to section:
Number of calls setup	Enables the generation of alerts or alarms based on the number of calls setup by the system during the polling interval.	Call Setup Thresholds
Number of call setup failures	Enables the generation of alerts or alarms based on the number of call setup failures experienced by the system during the polling interval.	Call Setup Failure Thresholds
RP setup failure rate	Enables the generation of alerts or alarms based on the rate at which RP failures are experienced by the system during the polling interval.	RP Setup Failure Rate Thresholds
PPP setup failure rate	Enables the generation of alerts or alarms based on the rate at which PPP failures are experienced by the system during the polling interval.	PPP Setup Failure Rate Thresholds
Number of calls rejected due to no processing resources being available	Enables the generation of alerts or alarms based on the number of calls rejected by the system due to insufficient resources (memory and/or session licenses) during the polling interval.	No Resource Call Reject Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Call Setup Thresholds

Threshold monitoring can be enabled for the call setup values described in the following table.

Value	Description	To configure, go to section:
Number of calls setup	Enables the generation of alerts or alarms based on the number of calls setup by the system during the polling interval.	Call Setup Thresholds
Number of call setup failures	Enables the generation of alerts or alarms based on the number of call setup failures experienced by the system during the polling interval.	Call Setup Failure Thresholds
RP setup failure rate	Enables the generation of alerts or alarms based on the rate at which RP failures are experienced by the system during the polling interval.	RP Setup Failure Rate Thresholds
PPP setup failure rate	Enables the generation of alerts or alarms based on the rate at which PPP failures are experienced by the system during the polling interval.	PPP Setup Failure Rate Thresholds
Number of calls rejected due to no processing resources being available	Enables the generation of alerts or alarms based on the number of calls rejected by the system due to insufficient resources (memory and/or session licenses) during the polling interval.	No Resource Call Reject Thresholds

Configuring Call Setup Thresholds

Use the following example to configure call setup thresholds:

```
configure
   threshold call-setup <high_thresh> [ clear <low_thresh> ]
   threshold poll call-setup interval <time>
   threshold monitoring call-setup
   end
```

Call Setup Failure Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of call setup failures < 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.

Configuring Call Setup Failure Thresholds

Use the following example for configuring call setup failure thresholding:

```
configure
   threshold call-setup-failure <high_thresh> [ clear <low_thresh> ]
   threshold poll call-setup-failure interval <time>
   threshold monitoring call-setup
   end
```

RP Setup Failure Rate Thresholds

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

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

- **Enter condition:** Actual number of call setup failures > or = High Threshold
- **Clear condition:** Actual number of call setup failures < 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.

Configuring RP Setup Failure Rate Thresholds

Use the following example for configuring RP setup failure rate thresholding:

```
configure
   threshold rp-setup-fail-rate <high_thresh> [ clear <low_thresh> ]
   threshold poll rp-setup-fail-rate interval <time>
   threshold monitoring call-setup
   end
```

PPP Setup Failure Rate Thresholds

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

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

- **Enter condition:** Actual number of call setup failures > or = High Threshold
- **Clear condition:** Actual number of call setup failures < 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.

Configuring PPP Setup Failure Rate Thresholds

Use the following example for configuring PPP setup failure rate thresholding:

```
configure
   threshold ppp-setup-fail-rate <high_thresh> [ clear <low_thresh> ]
   threshold poll ppp-setup-fail-rate interval <time>
   threshold monitoring call-setup
   end
```

No Resource Call Reject Thresholds

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 (CPU, memory, etc.) 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 > or = High Threshold
- **Clear condition:** Actual number of calls rejected due to no resources < 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.

Configuring No Resource Call Reject Thresholds

Use the following example for configuring no resource call reject thresholding:

```
configure
   threshold call-reject-no-resource <high_thresh> [ clear <low_thresh> ]
   threshold poll call-reject-no-resource interval <time>
   threshold monitoring call-setup
   end
```

Chapter 6
Content Filtering Thresholds

Thresholds generate alerts or alarms based on either the total number of Content Filtering calls setup by the system during the specified polling interval, or on the number of currently active calls only.

Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups > or = High Threshold
- **Clear condition:** Actual number of call setups < 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.

Default value is 0, which means there will be no monitoring.

The polling interval is in seconds and it is an integer between 30 and 60000. Entries will be rounded up to the nearest 30 seconds.

Configuring Content Filtering Thresholds

This section describes how to enable and configure Content Filtering thresholds.

Enabling Thresholds

To enable thresholds use the following configuration:

```
configure
   threshold monitoring content-filtering
   end
```

Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

```
configure
   threshold poll contfilt-block interval <interval>
   threshold poll contfilt-rating interval <interval>
   end
```

Configuring Thresholds Limits

To configure threshold limits use the following configuration:

```
configure
   threshold contfilt-block <high_thresh> [ clear <low_thresh> ]
   threshold contfilt-rating <high_thresh> [ clear <low_thresh> ]
   end
```

Saving Your Configuration

When you configure thresholds, they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 7
CPU Resource Thresholds

Threshold monitoring can be enabled for the CPU resource values described in the following table.

Value	Description	To configure, go to section:
10 second average of total processing card CPU utilization	Enables the generation of alerts or alarms based on a 10 second average of processing card CPU utilization.	10-second Average of Total Processing Card CPU Utilization Thresholds
Processing card CPU available memory	Enables the generation of alerts or alarms based on the amount of available memory for each processing card CPU during the polling interval.	Processing Card CPU Available Memory Thresholds
Processing card CPU load	Enables the generation of alerts or alarms based on processing card CPU load using a 5 minute average measurement.	Processing Card CPU Load Thresholds
Processing card CPU memory usage	Enables the generation of alerts or alarms based on the percentage of total processing card CPU memory used during the polling interval.	Processing Card CPU Memory Usage Thresholds
Processing card CPU session throughput	Enables the generation of alerts or alarms based on the total throughput for all Session Manager tasks running on each processing card CPU during the polling interval.	Processing Card CPU Session Throughput Thresholds s
Processing card CPU utilization	Enables the generation of alerts or alarms based on the utilization percentage for each processing card CPU during the polling interval.	Processing Card CPU Utilization Thresholds
System management card CPU memory usage	Enables the generation of alerts or alarms based on the percentage of total system management card CPU memory used during the polling interval.	System Management Card CPU Memory Usage Thresholds
System management card CPU utilization	Enables the generation of alerts or alarms based on the utilization percentage for each active system management card CPU during the polling interval.	System Management Card CPU Utilization Thresholds
ORBS task CPU utilization warning	Enables the generation of warning-level alerts or alarms based on the percentage CPU resources utilized by the Object Request Broker (ORB) software task.	ORBS Software Task CPU Usage Warning-Level Thresholds
ORBS task CPU utilization critical	Enables the generation of critical-level alerts or alarms based on the percentage CPU resources utilized by the Object Request Broker (ORB) software task.	ORBS Software Task CPU Usage Critical-Level Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

10-second Average of Total Processing Card CPU Utilization Thresholds

10-second average of total CPU utilization thresholds generate alerts or alarms based on a 10 second average of cpu utilization for all processing card CPUs during the specified polling interval.

Alerts or alarms are triggered for 10-second average of total CPU utilization based on the following rules:

- **Enter condition:** Average measured amount of total CPU utilization for the last 10 seconds > or = High Threshold
- **Clear condition:** Average measured amount of total CPU utilization for the last 10 seconds < 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.

Configuring 10-second Average of Processing Card CPU Thresholds

Use the following example for configuring 10-second average of total CPU utilization thresholding.

```
configure
   threshold 10sec-cpu-utilization <high_thresh> [ clear <low_thresh> ]
   threshold poll 10sec-cpu-utilization interval <time>
   threshold monitoring cpu-resource
   end
```

Processing Card CPU Available Memory Thresholds

CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each processing card CPU during the specified polling interval. Although, a single threshold is configured for all processing card CPUs, separate alerts or alarms can be generated for each CPU. Both active and standby processing card CPUs are monitored.

Alerts or alarms are triggered for available processing card CPU memory based on the following rules:

- **Enter condition:** Average measured amount of memory/CPU for last 5 minutes = or < Low Threshold
- **Clear condition:** Average measured amount of memory/CPU for last 5 minutes > 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.

Configuring Processing Card CPU Available Memory Thresholds

Use the following example for configuring processing card CPU available memory thresholding.

```
configure
   threshold cpu-available-memory <low_thresh> [ clear <high_thresh> ]
   threshold poll cpu-available-memory interval <time>
   threshold monitoring cpu-resource
   end
```

Processing Card CPU Load Thresholds

CPU load thresholds generate alerts or alarms based on a five-minute average of processing card CPU load during the polling interval. Although, a single threshold is configured for all processing card CPUs, separate alerts or alarms can be generated for each CPU.

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

- **Enter condition:** 5 minute average CPU load > or = High Threshold
- **Clear condition:** 5 minute average CPU load < 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.

Configuring Processing Card CPU Load Thresholds

Use the following example for configuring processing card CPU load thresholding.

```
configure
   threshold cpu-load <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-load interval <time>
   threshold monitoring cpu-resource
   end
```

Processing Card CPU Memory Usage Thresholds

CPU memory usage thresholds generate alerts or alarms based on memory usage for each processing card CPU during the polling interval. Although, a single threshold is configured for all processing card CPUs, separate alerts or alarms can be generated for each CPU.

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

- **Enter condition:** Actual CPU memory usage > or = High Threshold
- **Clear condition:** Actual CPU memory usage < 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.

Configuring Processing Card CPU Memory Usage Thresholds

Use the following example for configuring processing card CPU memory usage thresholding.

```
configure
   threshold cpu-memory-usage <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-memory-usage interval <time>
   threshold monitoring cpu-resource
   end
```

Processing Card CPU Session Throughput Thresholds

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

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

- **Enter condition:** Actual CPU session throughput > or = High Threshold
- **Clear condition:** Actual CPU session throughput < 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.

Configuring Processing Card CPU Session Throughput Thresholds

Use the following example for configuring processing card CPU session throughput thresholding.

```
configure
   threshold cpu-session-throughput <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-session-throughput interval <time>
   threshold monitoring cpu-session-throughput
   end
```

Processing Card CPU Utilization Thresholds

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

Alerts or alarms are triggered for processing card CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for last 5 minutes > or = High Threshold
- **Clear condition:** Average measured CPU utilization for last 5 minutes < 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.

Configuring Processing Card CPU Utilization Thresholds

Use the following example for configuring processing card CPU utilization thresholding.

```
configure
   threshold cpu-utilization <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-utilization interval <time>
   threshold monitoring cpu-resource
   end
```

System Management Card CPU Memory Usage Thresholds

CPU memory usage thresholds generate alerts or alarms based on memory usage for the system management card CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby system management cards allowing for alerts or alarms to be generated for each CPU.

Alerts or alarms are triggered for system management card CPU memory usage based on the following rules:

- **Enter condition:** Actual CPU memory usage > or = High Threshold
- **Clear condition:** Actual CPU memory usage < 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.

Configuring System Management Card CPU Memory Usage Thresholds

Use the following example for configuring system management card CPU memory usage thresholding.

```
configure
   threshold mgmt-cpu-memory-usage <high_thresh> [ clear <low_thresh> ]
   threshold poll mgmt-cpu-memory-usage interval <time>
   threshold monitoring cpu-resource
   end
```

System Management Card CPU Utilization Thresholds

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

Alerts or alarms are triggered for system management card CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for last 5 minutes > or = High Threshold
- **Clear condition:** Average measured CPU utilization for last 5 minutes < 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.

Configuring System Management Card CPU Utilization Thresholds

Use the following example for configuring system management card CPU utilization thresholding.

```
configure
   threshold mgmt-cpu-utilization <high_thresh> [ clear <low_thresh> ]
   threshold poll mgmt-cpu-utilization interval <time>
   threshold monitoring cpu-resource
   end
```

ORBS Software Task CPU Usage Warning-Level Thresholds

Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of system management 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 > High Threshold
- **Clear condition:** Actual CPU usage percentage = or < Low Threshold

Configuring ORBS Software Task CPU Usage Warning-Level Thresholds

Use the following example for configuring warning-level ORB software task CPU usage thresholding.

```
configure
   threshold cpu-orbs-warn <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-orbs-warn interval <time>
   threshold monitoring cpu-resource
   end
```

ORBS Software Task CPU Usage Critical-Level Thresholds

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of system management 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 > High Threshold
- **Clear condition:** Actual CPU usage percentage = or < Low Threshold

Configuring ORBS Software Task CPU Usage Critical-Level Thresholds

Use the following example for configuring critical-level ORB software task CPU usage thresholding.

```
configure
   threshold cpu-orbs-crit <high_thresh> [ clear <low_thresh> ]
   threshold poll cpu-orbs-crit interval <time>
   threshold monitoring cpu-resource
   end
```

Chapter 8
Diameter Thresholds

Threshold monitoring can be enabled for the Diameter-related values described in the following table.

Threshold	Description	To configure, go to section:
DCCA Bad Answers	Enables generation of alerts or alarms based on the number of times DIAMETER-BAD-ANSWER code is sent to the Diameter server during a polling interval.	DCCA Bad Answers Threshold
DCCA Protocol Errors	Enables generation of alerts or alarms based on the number protocol error messages received from the Diameter server during a polling interval.	DCCA Protocol Errors Threshold
DCCA Rating Failure	Enables generation of alerts or alarms based on the number of times the Diameter server rejected requests for a block of credits, due to the Rating Group (content-id) being invalid during a polling interval.	DCCA Rating Failure Threshold
DCCA Unknown Rating Group	Enables generation of alerts or alarms based on the number of times the block of credits returned by the Diameter server is rejected due to the Rating Group being unknown during a polling interval.	DCCA Unknown Rating Group Threshold
Diameter Retry Rate	Enables generation of alerts or alarms based on the percentage of Diameter requests that were re-tried during a polling interval.	Diameter Retry Rate Threshold

Configuring Diameter Thresholds

This section describes how to enable and configure Diameter thresholds.

DCCA Bad Answers Threshold

DCCA Bad Answers threshold generates alerts or alarms based on the number of times DIAMETER-BAD-ANSWER code is sent to the Diameter server during the polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition** : Actual number of times DIAMETER-BAD-ANSWER code sent > or = High Threshold
- **Clear condition** : Actual number of times DIAMETER-BAD-ANSWER code sent < 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.

Configuring DCCA Bad Answers Threshold

To configure the DCCA Bad Answers threshold use the following configuration:

```
configure
   threshold dcca-bad-answers <high_thresh> [ clear <low_thresh> ]
   threshold poll dcca-bad-answers interval <seconds>
   threshold monitoring ecs
   end
```

DCCA Protocol Errors Threshold

DCCA Protocol Errors threshold generates alerts or alarms based on the number protocol error messages received from the Diameter server during the polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition** : Actual number of protocol error messages received > or = High Threshold
- **Clear condition** : Actual number of protocol error messages received < 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.

Configuring DCCA Protocol Errors Threshold

To configure the DCCA Protocol Errors threshold use the following configuration:

```
configure
   threshold dcca-protocol-error <high_thresh> [ clear <low_thresh> ]
   threshold poll dcca-protocol-error interval <seconds>
   threshold monitoring ecs
   end
```

DCCA Rating Failure Threshold

DCCA Rating Failure threshold generates alerts or alarms based on the number of times the Diameter server rejected requests for a block of credits, due to the Rating Group (content-id) being invalid during the polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition** : Actual number of rating failures > or = High Threshold
- **Clear condition** : Actual number of rating failures < 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.

Configuring DCCA Rating Failure Threshold

To configure the DCCA Rating Failure threshold use the following configuration:

```
configure
   threshold dcca-rating-failed <high_thresh> [ clear <low_thresh> ]
   threshold poll dcca-rating-failed interval <seconds>
   threshold monitoring ecs
   end
```

DCCA Unknown Rating Group Threshold

DCCA Unknown Rating Group threshold generates alerts or alarms based on the number of times the block of credits returned by the Diameter server is rejected due to the Rating Group being unknown during the polling interval.

Alerts or alarms are triggered based on the following rules:

- **Enter condition** : Actual number of "unknown rating group" failures > or = High Threshold
- **Clear condition** : Actual number of "unknown rating group" < 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.

Configuring DCCA Unknown Rating Group Threshold

To configure the DCCA Unknown Rating Group threshold use the following configuration:

```
configure
   threshold dcca-unknown-rating-group <high_thresh> [ clear <low_thresh> ]
   threshold poll dcca-unknown-rating-group interval <seconds>
   threshold monitoring ecs
   end
```

Diameter Retry Rate Threshold

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

Alerts or alarms are triggered based on the following rules:

- **Enter condition**: Percentage of Diameter requests retried > or = High Threshold
- **Clear condition**: Percentage of Diameter requests retried < 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.

Configuring Diameter Retry Rate Threshold

To configure the Diameter Retry Rate threshold use the following configuration:

```
configure
```

```
threshold diameter diameter-retry-rate <high_thresh> [ clear <low_thresh> ]
threshold poll diameter-retry-rate interval <seconds>
threshold monitoring diameter
end
```

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 9
FA Service Thresholds

An FA Service threshold generates alerts or alarms for registration reply errors for individual FA services.

Alerts or alarms are triggered for the FA threshold based on the following rules:

- **Enter condition:** Actual number of errors > or = High Thresholds
- **Clear condition:** Actual number of errors < 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.

Configuring FA Service Thresholds

Use the following example to configure the threshold, set the polling interval for the threshold and enable monitoring of the threshold.

```
configure
   context <context_name>
      fa-service <name>
         threshold reg-reply-error <high_thresh> [ clear <low_thresh> ]
         exit
      exit
   threshold poll fa-reg-reply-error interval <time>
   threshold monitoring fa-service
   end
```

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Saving Your Configuration* chapter.

Chapter 10
HA Service Thresholds

HA Service thresholds generate alerts or alarms for the average number of calls setup. A threshold can be configured to report this information for an entire context or for an individual HA service. Thresholds can also be configured for registration reply, re-registration reply and de-registration reply errors for individual HA services.

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

- **Enter condition:** Actual average of call setups or actual number of errors > or = High Threshold
- **Clear condition:** Actual average of call setups or actual number of errors < 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.

The following table describes the possible methods for configuring HA Service thresholds:

Method	Description	To configure, go to section:
Context-Level	This threshold keeps track of the average number of call setups for all HA services in a context. When the actual average of call setups per polling period meets or exceeds the set high threshold an alert or alarm is set.	Context-Level HA Service Thresholds
HA Service-Level	HA services send and receive registration messages. The thresholds in the HA Service-Level can be configured to monitor thresholds for registration reply, re-registration reply, and de-registration reply errors.	HA Service-Level HA Service Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Saving Your Configuration* chapter.

Context-Level HA Service Thresholds

There is only one HA service threshold that can be configured, the average number of call setups for all HA services in a context.

Configuring Context-Level HA Service Thresholds

Use the following example to configure the threshold, set the polling interval for the threshold and enable monitoring of the threshold:

```
configuration
   context <context_name>
      threshold ha-service-init-rrq-rcvd-rate <high_thresh> [ clear
<low_thresh> ]
      exit
   threshold poll <threshold_name> interval <time>
   threshold monitoring ha-service
   threshold monitoring ip-sec
   end
```

HA Service-Level HA Service Thresholds

There are 10 thresholds that can be configured for the HA service-level:

- Total De-registration Reply Errors
- Average Calls Setup Per Second
- Total IPSec Call Requests Rejected
- Percentage of IPSec IKE Failures
- Total IPSec IKE Failures
- Total IPSec IKE Requests
- Total IPSec Tunnels Established
- Total IPSec tunnels Setup
- Total Registration Reply Errors
- Total Re-registration Reply Errors

Configuring HA Service-Level HA Service Thresholds

Use the following example to configure the HA service-level thresholds:

```
configure
   context <context_name>
      ha-service <name>
         threshold { dereg-reply-error | init-rrq-rcvd-rate | ipsec-call-req-rej
| ipsec-ike-failrate | ipsec-ike-failures | ipsec-ike-requests | ipsec-tunnels-
established | ipsec-tunnels-setup | reg-reply-error | rereg-reply-error }
         exit
      exit
   threshold poll ha-init-rrq-rcvd-rate interval <time>
   threshold poll reg-reply-error interval <time>
   threshold poll rereg-reply-error interval <time>
   threshold poll dereg-reply-error interval <time>
   threshold monitoring ha-service
   end
```

Chapter 11
IP Pool Utilization Thresholds

When IP address pools are configured on the system, they can be assigned to a group. All configured public IP address pools that were not assigned to a group are treated as belonging to the same group (automatically named "Public IP Pools"). Individually configured static or private pools are each treated as their own group.

IP address pool thresholds can be configured for all IP pools or pool groups configured within a system context or for individual pools or groups. These thresholds generate alerts or alarms based on calculations pertaining to percent-available for pool groups and percent-free, percent-on-hold, percent-released, and percent-used for individual pools.

Alerts or alarms are triggered for IP address pool utilization based on the following rules:

- **Enter condition:** When the actual IP address utilization percentage passes, or is equal to, the configured Threshold value an alert or alarm is set.
- **Clear condition:** When the actual IP address utilization percentage passes the Threshold value the alert or alarm is cleared.

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

The following table describes the possible methods for configuring IP pool utilization thresholds:

Method	Description	To configure, go to section:
Context-level	IP Pool Group: A single percent available threshold can be configured for all IP pool groups within a given context. The threshold is based on an aggregate measurement of available IP addresses for all IP pools within each group. **NOTE:** Separate alerts or alarms are generated for each group that experiences an event.	Context-Level IP Pool and Group Thresholds
	IP Pool: The following thresholds can be configured for all IP address pools configured within a given system context: • Percent-free; • Percent-hold; • Percent-release; • Percent-used. **NOTE:** Separate alerts or alarms are generated for each pool that experiences an event.	Context-Level IP Pool and Group Thresholds

Method	Description	To configure, go to section:
IP address pool-level	The following thresholds can be configured for each IP address pool: • Percent-available for the group that the IP pool belongs to; • Percent-free; • Percent-hold; • Percent-release; and • Percent-used. Thresholds configured for individual pools take precedence over the context-level threshold that would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are configured with different group-available thresholds, the system uses the pool configuration that has the Enter condition that would be encountered first for the entire group.	IP Address Pool-Level Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Context-Level IP Pool and Group Thresholds

This section provides instructions for configuring a single IP address pool utilization threshold for all pools within the context. These become the default settings for all pool existing or created in this context. See IP Address Pool-Level Thresholds for setting thresholds for individual IP pools.

Important: These instructions assume that IP address pools have been previously configured.

Configuring Context-Level IP Pool and Group Thresholds

Use the following example to configure the context-level IP Pool and group thresholds:

```
configure

   threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-pool-release | ip-pool-used } interval <time>

      context <context_name>

      threshold available-ip-pool-group <low_thresh> [ clear <high_thresh> ]

      threshold ip-pool-free <low_thresh> [ clear <high_thresh> ]

      threshold ip-pool-hold <high_thresh> [ clear <low_thresh> ]

      threshold ip-pool-release <high_thresh> [ clear <low_thresh> ]

      threshold ip-pool-used <high_thresh> [ clear <low_thresh> ]

      threshold monitoring available-ip-pool-group

      end
```

IP Address Pool-Level Thresholds

This section provides instructions for configuring a single IP address pool utilization threshold for all pool groups within the context.

Important: The IP pool-level threshold settings configured with the **ip pool** *pool_name* **alert-threshold** command take precedence over the context level IP pool threshold configuration commands.

Important: These instructions also assume that IP address pools have been previously configured.

If the group-available threshold is set for individual IP pools that are a part of an IP pool group, the IP pool with the threshold that is encountered first sets the threshold for the entire group.

For example; assume there is a group named *IPGroup1*, and there are three IP pools in that group; *PoolA*, *PoolB*, and *PoolC*. Also assume that, at the IP address-pool level, the three pools have the group-available threshold set as follows:

- PoolA:
  - Enter condition (low threshold) set to 40 percent
  - Clear condition (high threshold) set to 60 percent
- PoolB:
  - Enter condition (low threshold) set to 30 percent
  - Clear condition (high threshold) set to 70 percent
- PoolC:
  - Enter condition (low threshold) set to 20 percent
  - Clear condition (high threshold) set to 50 percent

In this case, the Enter condition for the percentage of IP pool addresses available from the group that is encountered first is the low threshold setting for PoolA. So both the low and high threshold settings for PoolA are used for the whole group.

Configuring IP Address Pool-Level Thresholds

```
configure

   threshold poll { available-ip-pool-group | ip-pool-free | ip-pool-hold | ip-
pool-release | ip-pool-used } interval <time>

      context  <context_name>

      ip pool name alert-threshold group-available <low_thresh> [ clear
<high_thresh> ]
```

```
      ip pool name alert-threshold pool-free <low_thresh> [ clear  <high_thresh>
]

      ip pool name alert-threshold pool-hold <high_thresh> [ clear <low_thresh>
]

      ip pool name alert-threshold pool-release <high_thresh> [ clear
<low_thresh>]

      ip pool name alert-threshold pool-used <high_thresh> [ clear <low_thresh>
]

      exit

   threshold monitoring available-ip-pool-group

   end
```

Chapter 12
MME Service Thresholds

MME Service thresholds generate alerts or alarms for the average number of calls setup. A threshold can be configured to report this information on entire system for MME service. Thresholds can also be configured for session registration response failures, discarded interface registration requests, discarded network entry registration acknowledgments for MME services.

Alerts or alarms are triggered for these MME thresholds based on the following rules:

- **Enter condition:** When the actual average of call setups or actual number of failures or discards passes, or is equal to, the configured Threshold value an alert or alarm is set.
- **Clear condition:** When the actual average of call setups or actual number of failures or discards passes below the Threshold value the alert or alarm is cleared.

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

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

System-Level MME Service Thresholds

The system-level thresholds for MME Service-Level can be configured to monitor thresholds for MME authentication, session registration response failures, discarded registration requests for individual or all MME services.

Following thresholds can be configured for the MME service-level:

- Number of MME authentication failures
- Number of MME session registration failures

Configuring System-level MME Service Thresholds

Use the following example to configure and enable these thresholds:

```
configuration
   threshold mme-auth-failure <high_thresh> [ clear <low_thresh>]
   threshold mme-attach-failure <high_thresh> [ clear <low_thresh> ]
   threshold total-mme-sessions <high_thresh> [ clear <low_thresh>]
   threshold poll mme-auth-failure interval <dur>
   threshold poll mme-attach-failure interval <dur>
   threshold poll total-mme-session interval <dur>
   threshold monitoring mme-service
   end
```

Chapter 13
Network Address Translation Thresholds

Thresholds generate alerts or alarms based on either the total number of Network Address Translation (NAT) calls setup by the system during the specified polling interval, or on the number of currently active calls only.

Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups > or = High Threshold
- **Clear condition:** Actual number of call setups < 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.

Default value is 0, which means there will be no monitoring.

The polling interval is in seconds and it is an integer between 30 and 60000. Entries will be rounded up to the nearest 30 seconds.

Configuring NAT Thresholds

This section describes how to enable and configure NAT thresholds.

Enabling Thresholds

To enable thresholds use the following configuration:

```
configure
   threshold monitoring firewall
   context  <context_name>
      threshold monitoring available-ip-pool-group
      end
```

Notes:

The **threshold monitoring available-ip-pool-group** command is required only if you are configuring IP pool thresholds. It is not required if you are only configuring NAT port-chunks usage threshold or many-to-one NAT.

Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

```
configure
   threshold poll ip-pool-used interval <interval>
   threshold poll nat-port-chunks-usage interval <interval>
   end
```

Notes:

The **threshold poll nat-port-chunks-usage interval** command is only applicable to many-to-one NAT.

Configuring Thresholds Limits

To configure threshold limits use the following configuration:

```
configure
   context<context_name>
      threshold ip-pool-free <high_thresh> [ clear <low_thresh> ]
      ip-pool-hold <high_thresh> [ clear <low_thresh> ]
      ip-pool-release <high_thresh> [ clear <low_thresh> ]
      ip-pool-used <high_thresh> [ clear <low_thresh> ]
      exit
   threshold nat-port-chunks-usage <high_thresh> clear <low_thresh>
   end
```

Notes:

- Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in the context
- Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in, and will take priority, i.e. will override the context-wide configuration mentioned above.

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 14
Packet Processing Thresholds

Threshold monitoring can be enabled for the packet processing values described in the following table.

Value	Description	To configure, go to section:
Packets filtered/dropped	Enables the generation of alerts or alarms based on the total number of packets that were filtered or dropped based on ACL rules during the polling interval.	FilteredDropped Packet Thresholds
Packets forwarded	Enables the generation of alerts or alarms based on the total number of packets that were forwarded to the CPU during the polling interval.	Forwarded Packet Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Filtered/Dropped Packet Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of filtered/dropped packets < 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.

Important: These instructions assume that ACLs have been previously configured.

Configuring Filtered/Dropped Packet Thresholds

Use the following example to configure the filtered/dropped packet thresholds:

```
configure
   threshold packets-filtered-dropped <high_thresh> [ clear <low_thresh>]
   threshold poll packets-filtered-dropped interval <time>
   threshold monitoring packets-filtered-dropped
   end
```

Forwarded Packet Thresholds

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 > or = High Threshold
- **Clear condition:** Actual number of forwarded packets < 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.

Configuring Forwarded Packet Thresholds

Use the following example to configure the forwarded packet thresholds:

```
configure
   threshold packets-forwarded-to-cpu <high_thresh> [ clear <low_thresh> ]
   threshold poll packets-forwarded-to-cpu interval <time>
   threshold monitoring packets-forwarded-to-cpu
   end
```

Chapter 15
PDG/TTG Thresholds

Thresholds generate alerts or alarms based on either the total number of PDG/TTG calls set up by the system during the specified polling interval, or on the number of currently active calls only.

Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups > High Threshold
- **Clear condition:** Actual number of call setups < 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.

Default value is 0, which means there will be no monitoring.

The polling interval is in seconds and it is an integer between 30 and 60000. Entries will be rounded up to the nearest 30 seconds.

Configuring PDG/TTG Thresholds

Use the following configuration example to enable, disable and configure PDG/TTG threshold monitoring.

```
configure
   [ no | default ] threshold monitoring pdg-service
   [ default ] threshold pdg-current-sessions <high_thresh> [ clear <low_thresh>
]
   [ default ] threshold poll pdg-current-sessions interval <time>
   [ default ] threshold pdg-active-sessions <high_thresh> [ clear  <low_thresh>
]
   [ default ] threshold poll pdg-active-sessions interval <time>
   end
```

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter of this guide.

Chapter 16
PDIF Thresholds

Thresholds generate alerts or alarms based on either the total number of PDIF calls setup by the system during the specified polling interval, or on the number of currently active calls only.

Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups > or = High Threshold
- **Clear condition:** Actual number of call setups < 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.

Default value is 0, which means there will be no monitoring.

The polling interval is in seconds and it is an integer between 30 and 60000. Entries will be rounded up to the nearest 30 seconds.

Configuring PDIF Thresholds

Use the following configuration example to enable, disable and configure PDIF threshold monitoring.

```
configure

   [ no ] threshold monitoring pdif

   threshold pdif-current-sessions high_thresh [ clear <low_thresh> ]

   threshold pdif-current-active-sessions [ <high_thresh> clear <low_thresh> ]

   default threshold { pdif-current-sessions | pdif-current-active-sessions }

   threshold poll { pdif-current-sessions | pdif-current-active-sessions }
interval <time>

   default threshold poll { pdif-current-sessions | pdif-current-active-sessions
}

   end
```

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 17
PDSN Service Thresholds

PDSN Service thresholds generate alerts or alarms for the average number of calls setup. A threshold can be configured to report this information for an entire context or for an individual PDSN service. Thresholds can also be configured for A11 registration response failures, discarded A11 registration requests, discarded A11 registration acknowledgments, and discarded PPP send packets for individual PDSN services.

Alerts or alarms are triggered for these PDSN thresholds based on the following rules:

- **Enter condition:** When the actual average of call setups or actual number of failures or discards passes, or is equal to, the configured Threshold value an alert or alarm is set.
- **Clear condition:** When the actual average of call setups or actual number of failures or discards passes below the Threshold value the alert or alarm is cleared.

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

The following table describes the possible methods for configuring PDSN Service thresholds:

Method	Description	To configure, go to section:
Context-Level	This threshold keeps track of the average number of call setups for all PDSN services in a context. When the actual average of call setups per polling period meets or exceeds the set high threshold an alert or alarm is set.	Context-Level PDSN Service Thresholds
PDSN Service-Level	PDSN services send and receive A11 registration messages and PPP packets. The thresholds in the PDSN Service-Level can be configured to monitor thresholds for A11 registration response failures, discarded A11 registration requests, discarded A11 registration acknowledgments, and discarded PPP send packets for individual PDSN services.	PDSN Service-Level PDSN Service Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Context-Level PDSN Service Thresholds

This threshold keeps track of the average number of call setups for all PDSN services in a context. When the actual average of call setups per polling period meets or exceeds the set high threshold an alert or alarm is set.

Configuring Context-Level PDSN Service Thresholds

Use the following example to configure the threshold for monitoring the average number of calls setup per second for the context, set the polling interval for the threshold and enable monitoring of the threshold.

```
configure
   context <context_name>
      threshold pdsn-service init-rrq-rcvd-rate <high_thresh> [ clear
<low_thresh>]
      exit
   threshold poll pdsn-init-rrq-rcvd-rate interval <time>
   threshold monitoring pdsn-service
   end
```

PDSN Service-Level PDSN Service Thresholds

PDSN services send and receive A11 registration messages and PPP packets. The thresholds in the PDSN Service-Level can be configured to monitor thresholds for A11 registration response failures, discarded A11 registration requests, discarded A11 registration acknowledgments, and discarded PPP send packets for individual PDSN services.

There are five thresholds that can be configured for the PDSN service-level:

- Average Calls Setup Per Second
- Total A11 Registration Response Failures
- Total A11 Registration Request Messages Discarded
- Total A11 Registration Acknowledgement Messages Discarded
- Total Packets PPP Protocol Processing Layer Discarded on Transmit

Configuring PDSN Service-Level PDSN Service Thresholds

Use the following example to configure and enable these thresholds:

```
configuration
   context  <context_name>
      pdsn-service <name>
         threshold init-rrq-rcvd-rate <high_thresh> [ clear <low_thresh>]
         threshold a11-rrp-failure <high_thresh> [ clear <low_thresh>]
         threshold a11-rrq-msg-discard <high_thresh> [ clear
<low_thresh>]
         threshold a11-rac-msg-discard <high_thresh> [ clear
<low_thresh>]
         threshold all-ppp-send-discard <high_thresh> [ clear
<low_thresh>]
         exit
      exit
   threshold poll pdsn-init-rrq-rcvd-rate interval <time>
   threshold poll a11-rrp-failure interval <time>
   threshold poll a11-rrq-msg-discard interval <time>
   threshold poll a11-rac-msg-discard interval <time>
```

```
threshold poll a11-ppp-send-discard interval <time>
threshold monitoring pdsn-service
end
```

Chapter 18
Per-service Session Thresholds

Threshold monitoring can be enabled for the per-service session counts described in the following table.

Value	Description	To configure, go to section:
PDSN Services	Enables the generation of alerts or alarms based on the number of sessions (active and dormant) facilitated by any PDSN service counted during the polling interval.	Per-PDSN Service Thresholds
HA Services	Enables the generation of alerts or alarms based on the number of sessions (active and dormant) facilitated by any HA service counted during the polling interval.	Per-HA Service Thresholds
GGSN Services	Enables the generation of alerts or alarms based on the number of PDP contexts (active and dormant) facilitated by any GGSN service counted during the polling interval.	Per-GGSN Service Thresholds
LNS Services	Enables the generation of alerts or alarms based on the number of sessions facilitated by any LNS service counted during the polling interval.	Per-LNS Service Thresholds
GPRS Services	Enables the generation of alerts or alarms based on the number of GPRS sessions or the number of r GPRS PDP contexts (active and dormant) facilitated by any GPRS service counted during the polling interval.	Per-GPRS Service Thresholds Per-GPRS Service PDP Contexts Thresholds
SGSN Services	Enables the generation of alerts or alarms based on the number of SGSN sessions or the number of SGSN PDP contexts (active and dormant) facilitated by any SGSN service counted during the polling interval.	Per-SGSN Service Thresholds Per-SGSN Service PDP Contexts Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Per-PDSN Service Thresholds

Per-PDSN service thresholds generate alerts or alarms based on the total number of sessions facilitated by any PDSN service configured on the system during the specified polling interval.

Alerts or alarms are triggered for sessions per-PDSN service based on the following rules:

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

This section provides instructions for configuring per-PDSN service thresholding. These instructions assume that you are at the prompt for the Global Configuration mode:

Configuring Per-PDSN Service Thresholds

Use the following example to configure the per-PDSN service thresholds:

```
configure
   threshold per-service-pdsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-pdsn-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-HA Service Thresholds

Per-HA service thresholds generate alerts or alarms based on the total number of sessions facilitated by any HA service configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Per-HA Service Thresholds

Configure the per-HA service thresholds by entering the following command:

```
configure
   threshold per-service-ha-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-ha-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-GGSN Service Thresholds

Per-GGSN service thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by any GGSN service configured on the system during the specified polling interval.

Alerts or alarms are triggered for sessions per-GGSN service based on the following rules:

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Per-GGSN Service Thresholds

Use the following example to configure the per-GGSN service thresholds:

```
configure
   threshold per-service-ggsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-ggsn-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-LNS Service Thresholds

Per-LNS service thresholds generate alerts or alarms based on the total number of sessions facilitated by any LNS service configured on the system during the specified polling interval.

Alerts or alarms are triggered for sessions per-LNS service based on the following rules:

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Per-LNS Service Thresholds

Use the following example to configure the per-LNS service thresholds:

```
configure
   threshold per-service-lns-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-lns-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-GPRS Service Thresholds

Per-GPRS service thresholds generate alerts or alarms based on the total number of attached subscribers facilitated by any GPRS service configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of attached subscribers > or = High Threshold
- **Clear condition:** Actual total number of attached subscribers < 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.

Configuring Per-GGSN Service Thresholds

Use the following example to configure the per-GGSN service thresholds:

```
configure
   threshold per-service-ggsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-ggsn-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-GPRS Service PDP Contexts Thresholds

Per-GPRS service PDP context thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by any GPRS service session configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Per-GPRS Service PDP Contexts Thresholds

Use the following example to configure the per-GPRS service PDP contexts thresholds:

```
configure
   threshold per-service-gprs-pdp-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-gprs-pdp sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-SGSN Service Thresholds

Per-SGSN service thresholds generate alerts or alarms based on the total number of attached subscribers facilitated by any SGSN service configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of attached subscribers > or = High Threshold
- **Clear condition:** Actual total number of attached subscribers < 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.

Configuring Per-SGSN Service Thresholds

Use the following example to configure the per-SGSN service thresholds:

```
configure
   threshold per-service-sgsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll per-service-sgsn-sessions interval <time>
   threshold monitoring subscriber
   end
```

Per-SGSN Service PDP Contexts Thresholds

Per-SGSN service PDP context thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by any SGSN service session configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Per-SGSN Service PDP Contexts Thresholds

Use the following example to configure the per-SGSN service PDP contexts thresholds:

```
configure
   threshold per-service-sgsn-pdp-sessions <high_thresh> [ clear<low_thresh> ]
   threshold poll per-service-sgsn-pdp sessions interval <time>
   threshold monitoring subscriber
   end
```

Chapter 19
Port Utilization Thresholds

Threshold monitoring can be enabled for the port utilization values described in the following table.

Value	Description	To configure, go to section:
Receive port utilization	Enables the generation of alerts or alarms based on the port utilization percentage for data received during the polling interval.	Receive Port Utilization Thresholds
Transmit port utilization	Enables the generation of alerts or alarms based on the port utilization percentage for data transmitted during the polling interval.	Transmit Port Utilization Thresholds
High port activity	Enables the generation of alerts or alarms based on the overall port utilization percentage during the polling interval.	High Port Activity Thresholds

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive **or** transmit utilization threshold be configured.

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Receive Port Utilization Thresholds

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

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

- **Enter condition:** Actual percent utilization of a port for received data > or = High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < 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.

Configuring Receive Port Utilization Thresholds

Use the following example to configure the polling interval over which to measure receive port utilization

```
configure
   threshold poll port-rx-utilization interval <seconds>
   port  <port-type> <slot#/port#>
      threshold rx-utilization <high_thresh_%> [ clear <low_thresh_%> ]
      threshold monitoring
      end
```

Transmit Port Utilization Thresholds

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

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

- **Enter condition:** Actual percent utilization of a port for transmit data > or = High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data < 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.

Configuring Transmit Port Utilization Thresholds

Use the following example to configure the polling interval over which to measure transmit port utilization:

```
configure
   threshold poll port-tx-utilization interval <seconds>
   port <port-type> <slot#/port#>
      threshold tx-utilization <high_thresh_%> [ clear <low_thresh_%> ]
      threshold monitoring
      end
```

High Port Activity Thresholds

High port activity thresholds generate alerts or alarms based on the peak utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis.

Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent peak utilization of a port > or = High Threshold
- **Clear condition:** Actual percent peak utilization of a port < 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.

Configuring High Port Activity Thresholds

Use the following example to configure the polling interval over which to measure for high port activity:

```
configure
   threshold poll port-high-activity interval <time>
   port  <port-type>  <slot#/port#>
      threshold high-activity <high_thresh_%> [ clear  <low_thresh_%> ]
      threshold monitoring
      end
```

Chapter 20
Session License Utilization Thresholds

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 licenses to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses (i.e. Simple IP, Mobile IP, L2TP, etc.). 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 < Low Threshold
- **Clear condition:** Actual session license utilization percentage per session type > 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.

Configuring Session License Utilization Thresholds

Use the following example to configure the thresholds for session license utilization:

```
configure

   threshold license-remaining-sessions <low_thresh> [ clear
   <high_thresh> ]

   threshold poll license-remaining-sessions interval <time>

   threshold monitoring license

   end
```

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 21
Stateful Firewall Thresholds

Thresholds generate alerts or alarms based on either the total number of Stateful Firewall calls setup by the system during the specified polling interval, or on the number of currently active calls only.

Alerts or alarms are triggered for call setups based on the following rules:

- **Enter condition:** Actual number of call setups > or = High Threshold
- **Clear condition:** Actual number of call setups < 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.

Default value is 0, which means there will be no monitoring.

The polling interval is in seconds and it is an integer between 30 and 60000. Entries will be rounded up to the nearest 30 seconds.

Configuring Stateful Firewall Thresholds

This section describes how to enable and configure Stateful Firewall thresholds.

Enabling Thresholds

To enable thresholds use the following configuration:

```
configure
   threshold monitoring firewall
   end
```

Configuring Threshold Polling Intervals

To configure threshold poll interval use the following configuration:

```
configure
   threshold poll fw-deny-rule interval <interval>
   threshold poll fw-dos-attack interval <interval>
   threshold poll fw-drop-packet interval <interval>
   threshold poll fw-no-rule interval <interval>
   end
```

Configuring Thresholds Limits

To configure threshold limits use the following configuration:

```
configure
   threshold fw-deny-rule <high_thresh> [ clear <low_thresh> ]
   threshold fw-dos-attack <high_thresh> [ clear <low_thresh> ]
   threshold fw-drop-packet <high_thresh> [ clear <low_thresh> ]
```

threshold fw-no-rule *<high_thresh>* [**clear** *<low_thresh>*]

end

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 22
Subscriber Thresholds

Threshold monitoring can be enabled for the subscriber values described in the following table.

Value	Description	To configure, go to section:
Total subscribers	Enables the generation of alerts or alarms based on the total number subscriber sessions (active and dormant) counted during the polling interval.	Total Subscriber Thresholds
Active subscribers	Enables the generation of alerts or alarms based on the total number of subscribers with active sessions counted during the polling interval.	Active Subscriber Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Total Subscriber Thresholds

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

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

- **Enter condition:** Actual total number of subscriber sessions > or = High Threshold
- **Clear condition:** Actual total number of subscriber sessions < 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.

This section provides instructions for configuring total subscriber thresholding. These instructions assume that you are at the prompt for the Global Configuration mode:

Configuring Total Subscriber Thresholds

Use the following example to configure the total subscriber thresholds:

```
configure
   threshold subscriber total <high_thresh> [ clear  <low_thresh> ]
   threshold poll total-subscriber interval <time>
   threshold monitoring subscriber
   end
```

Active Subscriber Thresholds

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

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

- **Enter condition:** Actual total number of active subscriber sessions > or = High Threshold
- **Clear condition:** Actual total number of active subscriber sessions < 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.

This section provides instructions for configuring active subscriber thresholding. These instructions assume that you are at the prompt for the Global Configuration mode:

Configuring Active Subscriber Thresholds

Use the following example to configure the active subscriber thresholds:

```
configure
   threshold subscriber active <high_thresh> [ clear  <low_thresh> ]
   threshold poll active-subscriber interval <time>
   threshold monitoring subscriber
   end
```

Chapter 23
System Management Card CompactFlash Memory Thresholds

System management card CompactFlash memory utilization thresholds generate alerts or alarms based on the percentage of memory used for the CompactFlash during the polling interval. A single threshold enables memory utilization monitoring for both the active and standby system management cards allowing for alerts or alarms to be generated for each CompactFlash.

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

- **Enter condition:** Actual percentage memory utilization > or = High Threshold
- **Clear condition:** Actual percentage memory utilization < 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.

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Chapter 24
Total Session Thresholds

Threshold monitoring can be enabled for the total session counts described in the following table.

Value	Description	To configure, go to section:
PDSN Services	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all PDSN services counted during the polling interval.	Total PDSN Session Thresholds
GGSN Services	Enables the generation of alerts or alarms based on the total number of PDP contexts (active and dormant) facilitated by all GGSN services counted during the polling interval.	Total GGSN Session Thresholds
GPRS Services	Enables the generation of alerts or alarms based on the total number of GPRS sessions or the total number of PDP sessions facilitated by the GPRS services counted during the polling interval.	Total GPRS Session Thresholds Total GPRS PDP Contexts Thresholds
HA Services	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all HA services counted during the polling interval.	Total HA Session Thresholds
HSGW Service	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all HSGW services counted during the polling interval.	Total HSGW Session Thresholds
LMA Service	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all LMA services counted during the polling interval.	Total LMA Session Thresholds
LNS Services	Enables the generation of alerts or alarms based on the total number of sessions facilitated by all LNS services counted during the polling interval.	Total LNS Session Thresholds
MME Service	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all P-GW services counted during the polling interval.	Ref - Total MME Session Thresholds
P-GW Service	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all P-GW services counted during the polling interval.	Total P-GW Session Thresholds
SGSN Services	Enables the generation of alerts or alarms based on the total number of SGSN sessions or the total number of PDP sessions facilitated by the SGSN services counted during the polling interval.	Total SGSN Session Thresholds Total SGSN PDP Contexts Thresholds
S-GW Service	Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all S-GW services counted during the polling interval.	Total S-GW Session Thresholds

Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration as described in the *Verifying and Saving Your Configuration* chapter.

Total PDSN Session Thresholds

Total PDSN session thresholds generate alerts or alarms based on the total number of sessions facilitated by any PDSN service configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total PDSN Session Thresholds

Use the following example to configure the total PDSN session thresholds:

```
configure
   threshold total-pdsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-pdsn-sessions interval <time>
   threshold monitoring pdsn-service
   end
```

Total GGSN Session Thresholds

Total GGSN session thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by all GGSN services configured on the system during the specified polling interval.

Alerts or alarms are triggered for the total of all GGSN PDP contexts based on the following rules:

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Total GGSN Session Thresholds

Use the following example to configure the per-GGSN service thresholds:

```
configure
   threshold total-ggsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-ggsn-sessions interval <time>
   threshold monitoring ggsn-service
   end
```

Total GPRS Session Thresholds

Total GPRS session thresholds generate alerts or alarms based on the total number of attached subscribers facilitated by all GPRS services configured on the system during the specified polling interval.

Alerts or alarms are triggered for the total of all subscribers attached to the GPRS based on the following rules:

- **Enter condition:** Actual total number of attached subscribers > or = High Threshold
- **Clear condition:** Actual total number of attached subscribers < 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.

Configuring Total GPRS Session Thresholds

Use the following example to configure the per-SGSN service thresholds:

```
configure
   threshold total-gprs-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-gprs-sessions interval <time>
   threshold monitoring gprs-service
   end
```

Total GPRS PDP Contexts Thresholds

Total GPRS PDP contexts thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by all GPRS services configured on the system during the specified polling interval.

Alerts or alarms are triggered for the total of all GPRS PDP contexts based on the following rules:

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Total GPRS PDP Context Thresholds

Use the following example to configure the per-GPRS service thresholds:

```
configure
   threshold total-gprs-pdp-sessions <high_thresh> [ clear <low_thresh>]
   threshold poll total-gprs-pdp-sessions interval <time>
   threshold monitoring gprs-service
   end
```

Total HA Session Thresholds

Total HA session thresholds generate alerts or alarms based on the total number of sessions facilitated by all HA services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total HA Session Thresholds

Use the following example to configure the total HA session thresholds:

```
configure
   threshold total-ha-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-ha-sessions interval <time>
   threshold monitoring ha-service
   end
```

Total HSGW Session Thresholds

Total HSGW session thresholds generate alerts or alarms based on the total number of sessions facilitated by all HSGW services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total HSGW Session Thresholds

Use the following example to configure the total HSGW session thresholds:

```
configure
   threshold total-hsgw-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-hsgw-sessions interval <time>
   threshold monitoring hsgw-service
   end
```

Total LMA Session Thresholds

Total LMA session thresholds generate alerts or alarms based on the total number of sessions facilitated by all HSGW services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total LMA Session Thresholds

Use the following example to configure the total LMA session thresholds:

```
configure
   threshold total-lma-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-lma-sessions interval <time>
   threshold monitoring lma-service
   end
```

Total LNS Session Thresholds

Total LNS session thresholds generate alerts or alarms based on the total number of sessions facilitated by all LNS services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total LNS Session Thresholds

Use the following example to configure the total LNS session thresholds:

```
configure
   threshold total-lns-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-lns-sessions interval <time>
   threshold monitoring lns-service
   end
```

Total MME Session Thresholds

Total MME session thresholds generate alerts or alarms based on the total number of sessions facilitated by all MME services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total MME Session Thresholds

Use the following example to configure the total P-GW session thresholds:

```
configure
   threshold total-mme-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-mmr-sessions interval <time>
   threshold monitoring mme-service
   end
```

Total P-GW Session Thresholds

Total P-GW session thresholds generate alerts or alarms based on the total number of sessions facilitated by all P-GW services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total P-GW Session Thresholds

Use the following example to configure the total P-GW session thresholds:

```
configure
   threshold total-pgw-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-pgw-sessions interval <time>
   threshold monitoring pgw-service
   end
```

Total SGSN Session Thresholds

Total SGSN session thresholds generate alerts or alarms based on the total number of attached subscribers facilitated by all SGSN services configured on the system during the specified polling interval.

Alerts or alarms are triggered for the total of all subscribers attached to the SGSN based on the following rules:

- **Enter condition:** Actual total number of attached subscribers > or = High Threshold
- **Clear condition:** Actual total number of attached subscribers < 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.

Configuring Total SGSN Session Thresholds

Use the following example to configure the per-SGSN service thresholds:

```
configure
   threshold total-sgsn-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-sgsn-sessions interval <time>
   threshold monitoring sgsn-service
   end
```

Total SGSN PDP Contexts Thresholds

Total SGSN PDP contexts thresholds generate alerts or alarms based on the total number of PDP contexts facilitated by all SGSN services configured on the system during the specified polling interval.

Alerts or alarms are triggered for the total of all SGSN PDP contexts based on the following rules:

- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < 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.

Configuring Total SGSN PDP Context Thresholds

Use the following example to configure the per-SGSN service thresholds:

```
configure
   threshold total-sgsn-pdp-sessions <high_thresh> [ clear <low_thresh>]
   threshold poll total-sgsn-pdp-sessions interval <time>
   threshold monitoring sgsn-service
   end
```

Total S-GW Session Thresholds

Total S-GW session thresholds generate alerts or alarms based on the total number of sessions facilitated by all S-GW services configured on the system during the specified polling interval.

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

- **Enter condition:** Actual total number of sessions > or = High Threshold
- **Clear condition:** Actual total number of sessions < 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.

Configuring Total S-GW Session Thresholds

Use the following example to configure the total S-GW session thresholds:

```
configure
   threshold total-sgw-sessions <high_thresh> [ clear <low_thresh> ]
   threshold poll total-sgw-sessions interval <time>
   threshold monitoring sgw-service
   end
```