



Cisco ASR 5000 Series Thresholding Configuration Guide

Version 12.2

Last Updated April 30, 2012

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-25552-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco ASR 5000 Series Thresholding Configuration Guide

© 2012 Cisco Systems, Inc. and/or its affiliated entities. All rights reserved.

CONTENTS

About this Guide	ix
Conventions Used	x
Contacting Customer Support	xii
Additional Information	xiii
Thresholding Overview	15
AAA Thresholds	19
Saving Your Configuration	20
AAA Accounting Message Archive Size Thresholds	21
Configuring AAA Accounting Message Archive Size Threshold	21
AAA Accounting Message Archive Queue Size Thresholds	22
Configuring AAA Accounting Message Archive Queue Size Threshold	22
AAA Accounting Failure Thresholds	23
Configuring AAA Accounting Failure Threshold	23
AAA Accounting Failure Rate Thresholds	24
Configuring AAA Accounting Failure Rate Threshold	24
AAA Authentication Failure Thresholds	25
Configuring AAA Authentication Failure Threshold	25
AAA Authentication Failure Rate Thresholds	26
Configuring AAA Authentication Failure Rate Threshold	26
AAA Request Message Retry Rate Thresholds	27
Configuring AAA Authentication Failure Rate Threshold	27
AAA Manager Request Queue Threshold	28
Configuring AAA Manager Request Queue Threshold	28
ASN GW Service Thresholds	29
Saving Your Configuration	30
System-Level ASN GW Service Thresholds	31
Configuring System-level ASN GW Service Thresholds	31
Call Setup Thresholds	33
Saving Your Configuration	34
Call Setup Thresholds	35
Configuring Call Setup Thresholds	35
Call Setup Failure Thresholds	36
Configuring Call Setup Failure Thresholds	36
RP Setup Failure Rate Thresholds	37
Configuring RP Setup Failure Rate Thresholds	37
PPP Setup Failure Rate Thresholds	38
Configuring PPP Setup Failure Rate Thresholds	38
No Resource Call Reject Thresholds	39
Configuring No Resource Call Reject Thresholds	39
Content Filtering Thresholds	41
Configuring Content Filtering Thresholds	42
Enabling Thresholds	42

Configuring Threshold Poll Interval	42
Configuring Threshold Limits	42
Saving Your Configuration	43
CPU Resource Thresholds	45
Saving Your Configuration	46
10-second Average of Total Processing Card CPU Utilization Thresholds	47
Configuring 10-second Average of Processing Card CPU Thresholds	47
Processing Card CPU Available Memory Thresholds	48
Configuring Processing Card CPU Available Memory Thresholds	48
Processing Card CPU Load Thresholds	49
Configuring Processing Card CPU Load Thresholds	49
Processing Card CPU Memory Usage Thresholds	50
Configuring Processing Card CPU Memory Usage Thresholds	50
Processing Card CPU Session Throughput Thresholds	51
Configuring Processing Card CPU Session Throughput Thresholds	51
Processing Card CPU Utilization Thresholds	52
Configuring Processing Card CPU Utilization Thresholds	52
System Management Card CPU Memory Usage Thresholds	53
Configuring System Management Card CPU Memory Usage Thresholds	53
System Management Card CPU Utilization Thresholds	54
Configuring System Management Card CPU Utilization Thresholds	54
ORBS Software Task CPU Usage Warning-Level Thresholds	55
Configuring ORBS Software Task CPU Usage Warning-Level Thresholds	55
ORBS Software Task CPU Usage Critical-Level Thresholds	56
Configuring ORBS Software Task CPU Usage Critical-Level Thresholds	56
CSCF Service Thresholds	57
Configuring CSCF Thresholds	58
Enabling CSCF Service Thresholds	58
Configuring CSCF Service Thresholds	58
Configuring Threshold Poll Intervals	59
Saving Your Configuration	61
Diameter Thresholds	63
Configuring Diameter Thresholds	64
DCCA Bad Answers Threshold	64
Configuring DCCA Bad Answers Threshold	64
DCCA Protocol Errors Threshold	64
Configuring DCCA Protocol Errors Threshold	64
DCCA Rating Failure Threshold	65
Configuring DCCA Rating Failure Threshold	65
DCCA Unknown Rating Group Threshold	65
Configuring DCCA Unknown Rating Group Threshold	65
Diameter Retry Rate Threshold	66
Configuring Diameter Retry Rate Threshold	66
Saving Your Configuration	67
FA Service Thresholds	69
Configuring FA Service Thresholds	70
Saving Your Configuration	71
FNG Thresholds	73
Configuring FNG Thresholds	74
Saving Your Configuration	75
HA Service Thresholds	77

Saving Your Configuration.....	78
Context-Level HA Service Thresholds	79
Configuring Context-Level HA Service Thresholds.....	79
HA Service-Level HA Service Thresholds.....	80
Configuring HA Service-Level HA Service Thresholds	80
IP Pool Utilization Thresholds	81
Saving Your Configuration.....	83
Context-Level IP Pool and Group Thresholds.....	84
Configuring Context-Level IP Pool and Group Thresholds	84
IP Address Pool-Level Thresholds	85
Configuring IP Address Pool-Level Thresholds	85
MME Service Thresholds	87
Saving Your Configuration.....	88
System-Level MME Service Thresholds	89
Configuring System-level MME Service Thresholds	89
Network Address Translation Thresholds	91
Configuring NAT Thresholds	92
Enabling Thresholds.....	92
Configuring Threshold Poll Interval	92
Configuring Thresholds Limits.....	92
Saving Your Configuration.....	94
Packet Processing Thresholds	95
Saving Your Configuration.....	96
Filtered/Dropped Packet Thresholds	97
Configuring Filtered/Dropped Packet Thresholds	97
Forwarded Packet Thresholds	98
Configuring Forwarded Packet Thresholds.....	98
PDG/TTG Thresholds.....	99
Configuring PDG/TTG Thresholds	100
Saving Your Configuration.....	101
PDIF Thresholds.....	103
Configuring PDIF Thresholds	104
Saving Your Configuration.....	105
PDSN Service Thresholds.....	107
Saving Your Configuration.....	108
Context-Level PDSN Service Thresholds	109
Configuring Context-Level PDSN Service Thresholds.....	109
PDSN Service-Level PDSN Service Thresholds.....	110
Configuring PDSN Service-Level PDSN Service Thresholds	110
Per-service Session Thresholds	113
Saving Your Configuration.....	114
Per-PDSN Service Thresholds	115
Configuring Per-PDSN Service Thresholds	115
Per-HA Service Thresholds	116
Configuring Per-HA Service Thresholds	116
Per-GGSN Service Thresholds	117
Configuring Per-GGSN Service Thresholds	117
Per-LNS Service Thresholds.....	118
Configuring Per-LNS Service Thresholds	118
Per-GPRS Service Thresholds.....	119

Configuring Per-GPRS Service Thresholds	119
Per-GPRS Service PDP Contexts Thresholds	120
Configuring Per-GPRS Service PDP Contexts Thresholds	120
Per-SGSN Service Thresholds	121
Configuring Per-SGSN Service Thresholds	121
Per-SGSN Service PDP Contexts Thresholds	122
Configuring Per-SGSN Service PDP Contexts Thresholds	122
Port Utilization Thresholds	123
Saving Your Configuration	124
Receive Port Utilization Thresholds	125
Configuring Receive Port Utilization Thresholds	125
Transmit Port Utilization Thresholds	126
Configuring Transmit Port Utilization Thresholds	126
High Port Activity Thresholds	127
Configuring High Port Activity Thresholds	127
Session License Utilization Thresholds	129
Configuring Session License Utilization Thresholds	130
Saving Your Configuration	131
Stateful Firewall Thresholds	133
Configuring Stateful Firewall Thresholds	134
Enabling Thresholds	134
Configuring Threshold Polling Intervals	134
Configuring Thresholds Limits	134
Saving Your Configuration	135
Subscriber Thresholds	137
Saving Your Configuration	138
Total Subscriber Thresholds	139
Configuring Total Subscriber Thresholds	139
Active Subscriber Thresholds	140
Configuring Active Subscriber Thresholds	140
System Management Card CompactFlash Memory Thresholds	141
Saving Your Configuration	142
Total Session Thresholds	143
Saving Your Configuration	144
Total PDSN Session Thresholds	145
Configuring Total PDSN Session Thresholds	145
Total GGSN Session Thresholds	146
Configuring Total GGSN Session Thresholds	146
Total GPRS Session Thresholds	147
Configuring Total GPRS Session Thresholds	147
Total GPRS PDP Contexts Thresholds	148
Configuring Total GPRS PDP Context Thresholds	148
Total HA Session Thresholds	149
Configuring Total HA Session Thresholds	149
Total HNB-GW Session Thresholds	150
Configuring Total HNB Session Thresholds	150
Configuring Total UE Session Thresholds	150
Configuring Total Iu Session Thresholds	150
Total HSGW Session Thresholds	152
Configuring Total HSGW Session Thresholds	152
Total LMA Session Thresholds	153

Configuring Total LMA Session Thresholds	153
Total LNS Session Thresholds	154
Configuring Total LNS Session Thresholds	154
Total MME Session Thresholds	155
Configuring Total MME Session Thresholds	155
Total P-GW Session Thresholds	156
Configuring Total P-GW Session Thresholds	156
Total SGSN Session Thresholds	157
Configuring Total SGSN Session Thresholds	157
Total SGSN PDP Contexts Thresholds	158
Configuring Total SGSN PDP Context Thresholds	158
Total S-GW Session Thresholds	159
Configuring Total S-GW Session Thresholds	159
Traffic Performance Optimizer Thresholds	161
Configuring TPO Thresholds	162
Enabling TPO Thresholds	162
Configuring Threshold Poll Interval	162
Configuring Thresholds Limits	162
Saving Your Configuration	163

About this Guide





This document pertains to the features and functionality that run on and/or that are related to the Cisco® ASR 5x00 Chassis.

This preface includes the following sections:

- [Conventions Used](#)
- [Contacting Customer Support](#)
- [Additional Information](#)

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.
	Electrostatic Discharge (ESD)	Warns you to take proper grounding precautions before handling ESD sensitive components or devices.

Typeface Conventions	Description
Text represented as a screen display	This typeface represents text that appears on your terminal screen, for example: Login:
Text represented as commands	This typeface represents commands that you enter at the CLI, for example: show ip access-list This document always gives the full form of a command in lowercase letters. Commands are <u>not</u> 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 <i>slot_number</i> 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 <i>variable</i> }	Required keywords and variables are surrounded by braces. They must be entered as part of the command syntax.
[keyword or <i>variable</i>]	Optional keywords or variables that may or may not be used are surrounded by brackets.

Command Syntax Conventions	Description
	<p>Some commands support alternative variables. These “options” are documented within braces or brackets by separating each variable with a vertical bar.</p> <p>These variables can be used in conjunction with required or optional keywords or variables. For example:</p> <pre>{ nonce timestamp }</pre> <p>OR</p> <pre>[count <i>number_of_packets</i> size <i>number_of_bytes</i>]</pre>

Contacting Customer Support

Go to <http://www.cisco.com/cisco/web/support/> to submit a service request. A valid Cisco account (username and password) is required to access this site. Please contact your Cisco account representative for additional information.

Additional Information

Refer to the following guides for supplemental information about the system:

- *Command Line Interface Reference*
- *Statistics and Counters Reference*
- *Thresholding Configuration Guide*
- *SNMP MIB Reference*
- *Cisco Web Element Manager Installation and Administration Guide*
- Product-specific and feature-specific administration guides
- *Release Notes* that accompany updates and upgrades to StarOS

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.

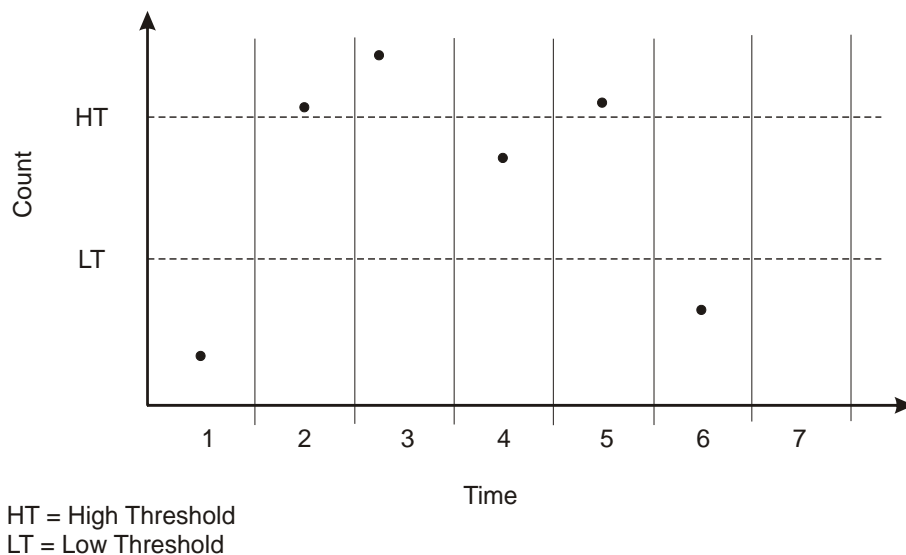
In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded HT.

- **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





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
- HNB-GW Service Sessions:
 - Total HNB Sessions
 - Total UE Sessions
 - Total Iu Sessions
- 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

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
Archive Queue size	Enables the generation of alerts or alarms per Session Manager instance based on the queue size for AAA (RADIUS and/or GTPP) accounting messages being archived during the polling interval.	AAA Accounting Message Archive Queue 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 message archive size threshold 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 Message Archive Queue Size Thresholds

The Session Manager can buffer around 26400 CDRs per Session Manager instance in ASR5K. Once the above limit is breached the oldest CDRs will be purged to make room for the new CDRs. Since purging can happen as soon as the Session Manager queue size reaches the maximum allowed limit, there is a need for the alarms to be generated during this scenario.

Accounting message archive queue size thresholds generate alerts or alarms per Session Manager instance based on the queue percentage of accounting messages archived in the buffer. The alarm will typically be generated when the message archival begins, and as and when the buffer is filled up to say, 25%, 50% and 90% during the specified polling interval.



Important: AcctArchiveStarted trap will be generated if the queue size exceeds 15% of the maximum number of session manager items per instance. The queue size is indicative of the maximum of ACS manager queue size and session manager queue size.

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

- **Enter condition:** Actual queue percentage of archived messages \geq High Threshold
- **Clear condition:** Actual queue percentage 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 Queue Size Threshold

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

configure

```
threshold aaa-acct-archive-queue-size1 <high_thresh> [ clear <low_thresh> ]

threshold aaa-acct-archive-queue-size2 <high_thresh> [ clear <low_thresh> ]

threshold aaa-acct-archive-queue-size3 <high_thresh> [ clear <low_thresh> ]

threshold monitoring aaa-acct-archive-queue

threshold poll aaa-acct-archive-queue-size1 interval <time>

threshold poll aaa-acct-archive-queue-size2 interval <time>

threshold poll aaa-acct-archive-queue-size3 interval <time>

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 \geq 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:

configure

```
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:

configure

```
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 \geq 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:

configure

```
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 \geq 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 retry 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 \geq 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 3

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 4

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 \geq 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 \geq 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 5

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 \geq 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 confilt-block interval <interval>
    threshold poll confilt-rating interval <interval>
end
```

Configuring Threshold Limits

To configure threshold limits use the following configuration:

```
configure
    threshold confilt-block <high_thresh> [ clear <low_thresh> ]
    threshold confilt-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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 6

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
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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 \geq 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 \geq 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 \geq 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 \geq 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 7

CSCF Service Thresholds

CSCF Service thresholds generate alerts or alarms for the average number of calls setup. A threshold can be configured to report this information for an individual CSCF service. Thresholds can also be configured for several other conditions for individual CSCF services.

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

- **Enter condition:** Actual average of call setups or actual number of errors \geq 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. Polling intervals are set on a system level.

Configuring CSCF Thresholds

This section describes how to enable and configure CSCF Service thresholds.

Enabling CSCF Service Thresholds

To enable threshold monitoring for a CSCF service, use the following configuration:

```
configure
  context <context_name>
    cscf-service <name>
      threshold monitoring
    end
```

Configuring CSCF Service Thresholds

The following thresholds can be configured for a CSCF Service:

- Number of CSCF call setup failures
- Number of total active CSCF calls
- Number of CSCF call setup failures due to no-resource
- Number of CSCF Presence errors
- Number of CSCF Registration Authentication failures
- Number of CSCF call setup failures due to TCP error
- Number of CSCF calls per polling interval
- Number of CSCF registrations per polling interval
- Number of total CSCF active registrations
- Maximum number of route-failures, after which the alarm/alert will be raised

Use the following example to configure these thresholds:

```
configuration
  context <context_name>
    cscf-service <name>
      threshold call-setup-failures <high_thresh> [ clear <low_thresh>]
      threshold call-total-active <high_thresh> [ clear <low_thresh> ]
      threshold error-no-resource <high_thresh> [ clear <low_thresh>]
```

```

threshold error-presence <high_thresh> [ clear <low_thresh>]

threshold error-reg-auth <high_thresh> [ clear <low_thresh>]

threshold error-tcp <high_thresh> [ clear <low_thresh>]

threshold invite-rcvd-rate <high_thresh> [ clear <low_thresh>]

threshold reg-rcvd-rate <high_thresh> [ clear <low_thresh>]

threshold reg-total-active <high_thresh> [ clear <low_thresh>]

threshold route-failures <high_thresh> [ clear <low_thresh>]

end

```

Configuring Threshold Poll Intervals

The following threshold poll intervals can be configured for the CSCF Service:

- CSCF call setup failures
- CSCF total active calls
- CSCF calls
- CSCF registrations
- CSCF service route failures
- CSCF no resource errors
- CSCF presence errors
- CSCF Reg-Auth errors
- CSCF TCP errors
- CSCF total active registrations

Use the following example to configure these threshold poll intervals:

```

configuration

threshold poll call-setup-failures interval <dur>

threshold poll call-total-active interval <dur>

threshold poll cscf-invite-rcvd interval <dur>

threshold poll cscf-reg-rcvd interval <dur>

threshold poll cscf-service-route-failures interval <dur>

threshold poll error-no-resource interval <dur>

threshold poll error-presence interval <dur>

threshold poll error-reg-auth interval <dur>

```

```
threshold poll error-tcp interval <dur>

threshold poll reg-total-active interval <dur>

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 10

FNG Thresholds

Thresholds generate alerts or alarms based on either the total number of FNG 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.

The 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 FNG Thresholds

Use the following configuration example to configure FNG threshold monitoring:

```
configure

[ no | default ] threshold monitoring fng-service

[ default ] threshold fng-current-sessions <high_thresh> [ clear <low_thresh> ]

[ default ] threshold poll fng-current-sessions interval <time>

end
```

Usage thresholds are provided for monitoring the overall FNG usage on an ASR 5000 chassis. These commands are used to monitor the total number of FNG sessions, both active and inactive, over an entire chassis.

In the commands above, *<high_thresh>* configures the total number of FNG sessions on an ASR 5000 chassis, both active and inactive. *<high_thresh>* is any integer from 0 to 300000. There is no default, but 0 means that there is no threshold monitoring.

The **clear** *<low_thresh>* command clears any percentage of the number of sessions being monitored using the *<high_thresh>* variable defined above. *<low_thresh>* is any integer from 0 to 300000.

The following example configures a monitoring threshold of 300000 active and inactive FNG sessions on an ASR 5000 chassis:

```
threshold fng-current-sessions 300000
```

This turns out to be too many, so the following command clears 100000:

```
threshold fng-current-sessions 300000 clear 100000
```

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 11

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 12

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: <ul style="list-style-type: none">• 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	<p>The following thresholds can be configured for each IP address pool:</p> <ul style="list-style-type: none">• Percent-available for the group that the IP pool belongs to;• Percent-free;• Percent-hold;• Percent-release; and• Percent-used. <p>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.</p>	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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 13

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 14

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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 15

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 16

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

[ default ] threshold poll pdg-current-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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 17

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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 18

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 a11-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 19

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 \geq 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 \geq 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-GPRS Service Thresholds

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

configure

```
threshold per-service-gprs-sessions <high_thresh> [ clear <low_thresh> ]
```

```
threshold poll per-service-gprs-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 \geq 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 \geq 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 \geq 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 20

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 \geq 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 21

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 22

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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 23

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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 \geq 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 24

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 \geq 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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Chapter 25

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
HNB-GW Services	Enables the generation of alerts or alarms based on the total number of HNB, UE, Iu sessions (active and dormant) facilitated by all HNB-GW services counted during the polling interval.	Total HNB-GW 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 MME services counted during the polling interval.	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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

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 \geq 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 subscriber
```

```
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 \geq 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>
```

```
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 \geq 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>
```

```
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 \geq 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>
```

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 \geq 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 subscriber
```

```
end
```

Total HNB-GW Session Thresholds

Total HNB-GW service session thresholds generate alerts or alarms based on the total number of IuH, IuCS, and IuPS sessions facilitated by all HNB-GW services configured on the system during the specified polling interval. Thresholds for IuH session is provided for HNB and UE separately.

Alerts or alarms are triggered for the total of all IuH, IuCS, or IuPS 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 HNB Session Thresholds

Use the following example to configure the thresholds for total HNB sessions over IuH interface between HNB and HNB-GW service on HNB-GW node:

configure

```
threshold total-hnbgw-hnb-sessions <high_thresh> [ clear <low_thresh> ]
```

```
threshold poll total-hnbgw-hnb-sessions interval <time>
```

```
threshold monitoring hnbgw-service
```

```
end
```

Configuring Total UE Session Thresholds

Use the following example to configure the thresholds for total UE sessions over IuH interface between HNB and HNB-GW service on HNB-GW node:

configure

```
threshold total-hnbgw-ue-sessions <high_thresh> [ clear <low_thresh> ]
```

```
threshold poll total-hnbgw-ue-sessions interval <time>
```

```
threshold monitoring hnbgw-service
```

```
end
```

Configuring Total Iu Session Thresholds

Use the following example to configure the thresholds for total IuPS and/or IuCS sessions over Iu interface between HNB-GW and CN node:

configure

```
threshold total-hnbgw-iu-sessions <high_thresh> [ clear <low_thresh> ]  
threshold poll total-hnbgw-iu-sessions interval <time>  
threshold monitoring hnbgw-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 \geq 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 \geq 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 \geq 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 subscriber
```

```
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 \geq 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-mme-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 \geq 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 \geq 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>
```

```
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 \geq 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>
```

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 \geq 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
```


Chapter 26

Traffic Performance Optimizer Thresholds

Thresholds generate alerts or alarms based on either the total number of Traffic Performance Optimizer (TPO) 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 \geq 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. The 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. The default interval value is 900 seconds.

Configuring TPO Thresholds

This section describes how to enable and configure TPO thresholds.

Enabling TPO Thresholds

To enable TPO thresholds use the following configuration:

```
configure
    threshold monitoring tpo
end
```

Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

```
configure
    threshold poll tpo-dns-failure interval <interval>
    threshold poll tpo-low-compression-gain interval <interval>
    threshold poll tpo-rto-timeout interval <interval>
end
```

Configuring Thresholds Limits

To configure threshold limits use the following configuration:

```
configure
    threshold tpo-dns-failure <high_thresh> clear <low_thresh>
    threshold tpo-low-compression-gain <high_thresh> clear <low_thresh>
    threshold tpo-rto-timeout <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 to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.