# Thresholding Configuration Guide, StarOS Release 21.27

**First Published:** 2022-04-14

**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

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 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.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.

# CONTENTS


PREFACE

**About this Guide** xiii

About this Guide xiv

Conventions Used xiv

Supported Documents and Resources xv

Related Documentation xv

Obtaining Documentation xvi

Contacting Customer Support xvi

CHAPTER 1

**Thresholding Overview** 1

Thresholding Overview 1

CHAPTER 2

**AAA Thresholds** 7

AAA Thresholds 7

Saving Your Configuration 8

AAA Accounting Message Archive Size Thresholds 8

Configuring AAA Accounting Message Archive Size Threshold 8

AAA Accounting Message Archive Queue Size Thresholds 9

Configuring AAA Accounting Message Archive Queue Size Threshold 9

AAA Accounting Failure Thresholds 9

Configuring AAA Accounting Failure Threshold 10

AAA Accounting Failure Rate Thresholds 10

Configuring AAA Accounting Failure Rate Threshold 10

AAA Authentication Failure Thresholds 10

Configuring AAA Authentication Failure Threshold 11

AAA Authentication Failure Rate Thresholds 11

Configuring AAA Authentication Failure Rate Threshold 11

AAA Request Message Retry Rate Thresholds 11
Configuring AAA Authentication Failure Rate Threshold 12
AAA Manager Request Queue Threshold 12
Configuring AAA Manager Request Queue Threshold 12

CHAPTER 3 ASNGW Thresholds 13
ASN GW Service Thresholds 13
Saving Your Configuration 13
System-Level ASN GW Service Thresholds 13
Configuring System-level ASN GW Service Thresholds 14

CHAPTER 4 Call Setup Thresholds 15
Call Setup Thresholds 15
Saving Your Configuration 16
Call Setup Thresholds 16
Configuring Call Setup Thresholds 17
Call Setup Failure Thresholds 17
Configuring Call Setup Failure Thresholds 17
eGTP-C S2b Setup Fail Rate Thresholds 17
Configuring eGTP-C S2b Setup Fail Rate Thresholds 18
eGTP-C S5 Setup Fail Rate Thresholds 18
Configuring eGTP-C S5 Setup Fail Rate Thresholds 18
RP Setup Failure Rate Thresholds 18
Configuring RP Setup Failure Rate Thresholds 19
PPP Setup Failure Rate Thresholds 19
Configuring PPP Setup Failure Rate Thresholds 19
No Resource Call Reject Thresholds 19
Configuring No Resource Call Reject Thresholds 20

CHAPTER 5 Content Filtering Thresholds 21
Content Filtering Thresholds 21
Configuring Content Filtering Thresholds 21
Enabling Thresholds 21
Configuring Threshold Poll Interval 22

Configuring Threshold Limits 22
Saving Your Configuration 22

CHAPTER 6 CPU Resource Thresholds 23
CPU Resource Thresholds 23
Saving Your Configuration 24
10-second Average of Total Processing Card CPU Utilization Thresholds 24
Configuring 10-second Average of Processing Card CPU Thresholds 25
Processing Card CPU Available Memory Thresholds 25
Configuring Processing Card CPU Available Memory Thresholds 25
Processing Card CPU Load Thresholds 25
Configuring Processing Card CPU Load Thresholds 26
Processing Card CPU Memory Usage Thresholds 26
Configuring Processing Card CPU Memory Usage Thresholds 26
Processing Card CPU Session Throughput Thresholds 26
Configuring Processing Card CPU Session Throughput Thresholds 27
Processing Card CPU Utilization Thresholds 27
Configuring Processing Card CPU Utilization Thresholds 27
System Management Card CPU Memory Usage Thresholds 27
Configuring System Management Card CPU Memory Usage Thresholds 28
System Management Card CPU Utilization Thresholds 28
Configuring System Management Card CPU Utilization Thresholds 28
ORBS Software Task CPU Usage Warning-Level Thresholds 28
Configuring ORBS Software Task CPU Usage Warning-Level Thresholds 28
ORBS Software Task CPU Usage Critical-Level Thresholds 29
Configuring ORBS Software Task CPU Usage Critical-Level Thresholds 29

CHAPTER 7 CSCF Service Thresholds 31
CSCF Service Thresholds 31
Configuring CSCF Thresholds 31
Enabling CSCF Service Thresholds 32
Configuring CSCF Service Thresholds 32
Configuring Threshold Poll Intervals 32
Saving Your Configuration 33

CHAPTER 8 **Disconnect-Reasons Thresholds** 35

Disconnect-Reasons Thresholds 35

Configuring Disconnect-Reasons Thresholds 35

threshold disconnect-reason 36

threshold poll disconnect-reason 36

threshold monitoring 36

Saving Your Configuration 37

CHAPTER 9 **Diameter Thresholds** 39

Diameter Thresholds 39

Configuring Diameter Thresholds 39

DCCA Bad Answers Threshold 40

Configuring DCCA Bad Answers Threshold 40

DCCA Protocol Errors Threshold 40

Configuring DCCA Protocol Errors Threshold 40

DCCA Rating Failure Threshold 40

Configuring DCCA Rating Failure Threshold 41

DCCA Unknown Rating Group Threshold 41

Configuring DCCA Unknown Rating Group Threshold 41

Diameter Retry Rate Threshold 41

Configuring Diameter Retry Rate Threshold 42

Saving Your Configuration 42

CHAPTER 10 **ECS Thresholds** 43

ECS Thresholds 43

Configuring ECS Thresholds 43

CDR File Space Threshold 44

Configuring CDR File Space Threshold 44

DNS-learnt IPv4 Threshold 44

Configuring DNS-Learnt IPv4 Threshold 44

DNS-learnt IPv6 Threshold 45

Configuring DNS-Learnt IPv6 Threshold 45

EDR File Space Threshold 45

Configuring EDR File Space Threshold 45
Dropped EDR/UDR Flow Control Threshold 46
Configuring Dropped EDR/UDR Flow Control Threshold 46
Saving Your Configuration 46

CHAPTER 11 ePDG Thresholds 47
EPDG Thresholds 47
Configuring ePDG Thresholds 47
Saving Your Configuration 48
Configuring IKEv2 tunnel setup attempts 48

CHAPTER 12 FA Thresholds 49
FA Service Thresholds 49
Configuring FA Service Thresholds 49
Saving Your Configuration 50

CHAPTER 13 FNG Thresholds 51
FNG Thresholds 51
Configuring FNG Thresholds 51
Saving Your Configuration 52

CHAPTER 14 HA Thresholds 53
HA Service Thresholds 53
Saving Your Configuration 54
Context-Level HA Service Thresholds 54
Configuring Context-Level HA Service Thresholds 54
HA Service-Level HA Service Thresholds 54
Configuring HA Service-Level HA Service Thresholds 55

CHAPTER 15 HeNBGW Thresholds 57
HeNB-GW Service Thresholds 57
Saving Your Configuration 57
System-Level HeNB-GW Service Thresholds 58

Configuring System-level HeNB-GW Service Thresholds 58

CHAPTER 16 **IP Pool Thresholds 59**

IP Pool Utilization Thresholds 59

Saving Your Configuration 60

Context-Level IP Pool and Group Thresholds 61

Configuring Context-Level IP Pool and Group Thresholds 61

IP Address Pool-Level Thresholds 61

Configuring IP Address Pool-Level Thresholds 62

CHAPTER 17 **MME Service Thresholds 63**

MME Service Thresholds 63

Saving Your Configuration 63

System-Level MME Service Thresholds 63

Configuring System-level MME Service Thresholds 64

CHAPTER 18 **Network Address Translation Thresholds 65**

Network Address Translation Thresholds 65

Configuring NAT Thresholds 65

Enabling Thresholds 65

Configuring Threshold Poll Interval 66

Configuring Thresholds Limits 66

Saving Your Configuration 66

CHAPTER 19 **Packet Processing Thresholds 67**

Packet Processing Thresholds 67

Saving Your Configuration 67

Filtered/Dropped Packet Thresholds 67

Configuring Filtered/Dropped Packet Thresholds 68

Forwarded Packet Thresholds 68

Configuring Forwarded Packet Thresholds 68

CHAPTER 20 **PDG/TTG Thresholds 69**

PDG/TTG Thresholds 69
Configuring PDG/TTG Thresholds 69
Saving Your Configuration 70

CHAPTER 21 PDIF Thresholds 71
PDIF Thresholds 71
Configuring PDIF Thresholds 71
Saving Your Configuration 72

CHAPTER 22 PDSN Thresholds 73
PDSN Service Thresholds 73
Saving Your Configuration 74
Context-Level PDSN Service Thresholds 74
Configuring Context-Level PDSN Service Thresholds 74
PDSN Service-Level PDSN Service Thresholds 74
Configuring PDSN Service-Level PDSN Service Thresholds 75

CHAPTER 23 Per-Service Session Thresholds 77
Per-service Session Thresholds 77
Saving Your Configuration 78
Per-PDSN Service Thresholds 78
Configuring Per-PDSN Service Thresholds 78
Per-HA Service Thresholds 79
Configuring Per-HA Service Thresholds 79
Per-GGSN Service Thresholds 79
Configuring Per-GGSN Service Thresholds 79
Per-LNS Service Thresholds 80
Configuring Per-LNS Service Thresholds 80
Per-GPRS Service Thresholds 80
Configuring Per-GPRS Service Thresholds 80
Per-GPRS Service PDP Contexts Thresholds 81
Configuring Per-GPRS Service PDP Contexts Thresholds 81
Per-SGSN Service Thresholds 81
Configuring Per-SGSN Service Thresholds 81

Per-SGSN Service PDP Contexts Thresholds 82
Configuring Per-SGSN Service PDP Contexts Thresholds 82

CHAPTER 24 **Port Utilization Thresholds 83**
Port Utilization Thresholds 83
Saving Your Configuration 83
Receive Port Utilization Thresholds 84
Configuring Receive Port Utilization Thresholds 84
Transmit Port Utilization Thresholds 84
Configuring Transmit Port Utilization Thresholds 84
High Port Activity Thresholds 85
Configuring High Port Activity Thresholds 85

CHAPTER 25 **SaMOG Thresholds 87**
SaMOG Thresholds 87
Configuring SaMOG Thresholds 87
Saving Your Configuration 87

CHAPTER 26 **Session License Utilization Thresholds 89**
Session License Utilization Thresholds 89
Configuring Session License Utilization Thresholds 89
Saving Your Configuration 90

CHAPTER 27 **Stateful Firewall Thresholds 91**
Stateful Firewall Thresholds 91
Configuring Stateful Firewall Thresholds 91
Enabling Thresholds 91
Configuring Threshold Polling Intervals 92
Configuring Thresholds Limits 92
Saving Your Configuration 92

CHAPTER 28 **Subscriber Thresholds 93**
Subscriber Thresholds 93

Saving Your Configuration 93
Total Subscriber Thresholds 93
Configuring Total Subscriber Thresholds 94
Active Subscriber Thresholds 94
Configuring Active Subscriber Thresholds 94

CHAPTER 29 **System Management Card CompactFlash Memory Thresholds 95**
System Management Card CompactFlash Memory Thresholds 95
Saving Your Configuration 95

CHAPTER 30 **Total Session Thresholds 97**
Total Session Thresholds 97
Saving Your Configuration 99
Total PDSN Session Thresholds 99
Configuring Total PDSN Session Thresholds 99
Total GGSN Session Thresholds 99
Configuring Total GGSN Session Thresholds 100
Total GPRS Session Thresholds 100
Configuring Total GPRS Session Thresholds 100
Total GPRS PDP Contexts Thresholds 100
Configuring Total GPRS PDP Context Thresholds 101
Total HA Session Thresholds 101
Configuring Total HA Session Thresholds 101
Total HeNB-GW Session Thresholds 101
Configuring Total HeNB Session Thresholds 102
Configuring Total UE Session Thresholds 102
Total HNB-GW Session Thresholds 102
Configuring Total HNB Session Thresholds 102
Configuring Total UE Session Thresholds 0 103
Configuring Total Iu Session Thresholds 103
Total HSGW Session Thresholds 103
Configuring Total HSGW Session Thresholds 103
Total LMA Session Thresholds 104
Configuring Total LMA Session Thresholds 104

Total LNS Session Thresholds 104
Configuring Total LNS Session Thresholds 104
Total MME Session Thresholds 105
Configuring Total MME Session Thresholds 105
Total P-GW Session Thresholds 105
Configuring Total P-GW Session Thresholds 105
Total SAEGW Session Thresholds 106
Configuring Total SAEGW Session Thresholds 106
Total SGSN Session Thresholds 106
Configuring Total SGSN Session Thresholds 106
Total SGSN PDP Contexts Thresholds 107
Configuring Total SGSN PDP Context Thresholds 107
Total S-GW Session Thresholds 107
Configuring Total S-GW Session Thresholds 107

# About this Guide

**Note** Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with CUPS products. References to any CUPS products or features are for informational purposes only. Please contact your Cisco Account or Support representative for any questions about parity between this product and any CUPS products.

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

**Note** The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *Thresholding Configuration Guide* and its document conventions.

This document provides descriptive information on StarOS thresholds and thresholding mechanism, used to monitor all StarOS functions and services for conditions and events that could potentially cause errors or outages.

Refer to the *Thresholding Overview* section for more information about the structure and content of this reference.


- About this Guide, on page xiv
- Conventions Used, on page xiv
- Supported Documents and Resources, on page xv

• Contacting Customer Support , on page xvi

# About this Guide

**Note** Control and User Plane Separation (CUPS) represents a significant architectural change in the way StarOS-based products are deployed in the 3G, 4G, and 5G networks. Unless otherwise specified, it should not be assumed that any constructs (including, but not limited to, commands, statistics, attributes, MIB objects, alarms, logs, services) referenced in this document imply functional parity with CUPS products. References to any CUPS products or features are for informational purposes only. Please contact your Cisco Account or Support representative for any questions about parity between this product and any CUPS products.

**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

**Note** The HA, HSGW, PDSN, and SecGW products have reached end of life and are not supported in this release. Any references to these products (specific or implied) their components or functions including CLI commands and parameters in this document are coincidental and are not supported. Full details on the end of life for these products are available at https://www.cisco.com/c/en/us/products/collateral/wireless/asr-5000-series/eos-eol-notice-c51-740422.html.

This preface describes the *Thresholding Configuration Guide* and its document conventions.

This document provides descriptive information on StarOS thresholds and thresholding mechanism, used to monitor all StarOS functions and services for conditions and events that could potentially cause errors or outages.

Refer to the *Thresholding Overview* section for more information about the structure and content of this reference.

# Conventions Used

The following tables describe the conventions used throughout this documentation.

| Notice Type | Description |
|---|---|
| Information Note | Provides information about important features or instructions. |
| Caution | Alerts you of potential damage to a program, device, or system. |

| Notice Type | Description |
|---|---|
| Warning | Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards. |

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

# Supported Documents and Resources

## Related Documentation

The most up-to-date information for this product is available in the product *Release Notes* provided with each software release.

The following related product documents are also available:

- *AAA Interface Administration and Reference*
- *ASR 5500 Installation Guide*
- *Command Line Interface Reference*
- *GTPP Interface Administration and Reference*
- *IPSec Reference*
- Platform-specific System Administration Guides

- Product-specific Administration Guides
- *Release Change Reference*
- *SNMP MIB Reference*
- *Statistics and Counters Reference*
- *Statistics and Counters Reference - Bulk Statistics Descriptions*

## Obtaining Documentation

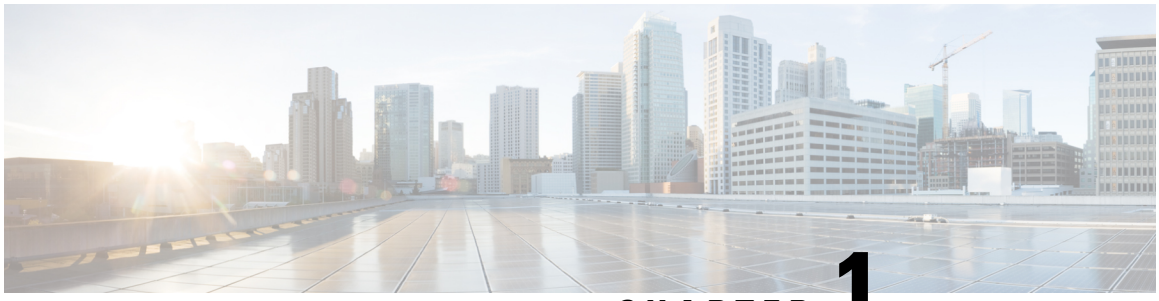
The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

# Contacting Customer Support

Use the information in this section to contact customer support.

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



CHAPTER 1

# Thresholding Overview


- Thresholding Overview, on page 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.

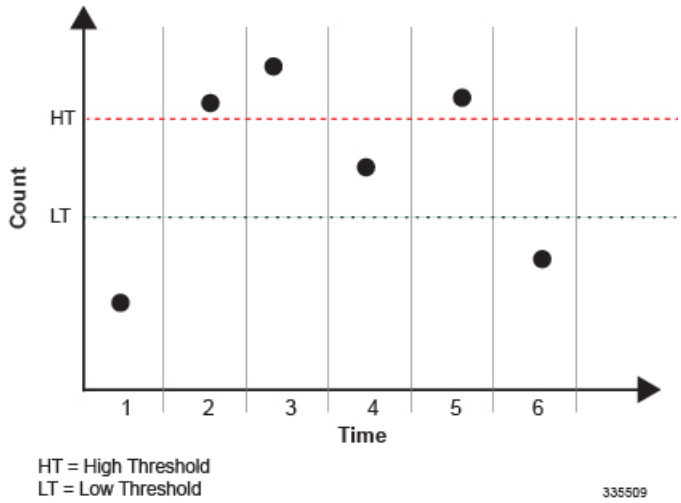
  In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded HT.

- **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*




**Note** 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.

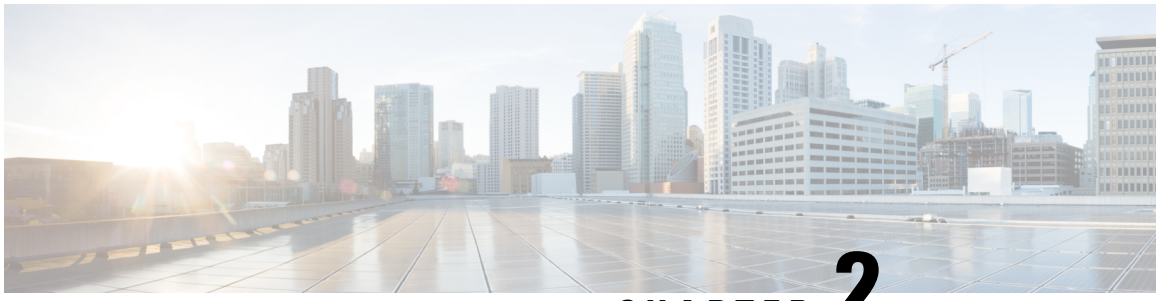
  "Outstanding" alarms are reported to through the system\'s alarm subsystem and are viewable through the system\'s CLI.

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 |

Thresholding Overview



CHAPTER 2

# AAA Thresholds


- AAA Thresholds, on page 7
- Saving Your Configuration, on page 8
- AAA Accounting Message Archive Size Thresholds, on page 8
- AAA Accounting Message Archive Queue Size Thresholds, on page 9
- AAA Accounting Failure Thresholds, on page 9
- AAA Accounting Failure Rate Thresholds, on page 10
- AAA Authentication Failure Thresholds, on page 10
- AAA Authentication Failure Rate Thresholds, on page 11
- AAA Request Message Retry Rate Thresholds, on page 11
- AAA Manager Request Queue Threshold, on page 12


## AAA Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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. |
| Accounting Failures | Enables the generation of alerts or alarms based on the number of failed AAA accounting requests that occur during the polling interval. |
| Accounting Failure Rate | Enables the generation of alerts or alarms based on the percentage of AAA accounting requests that failed during the polling interval. |
| Authentication Failures | Enables the generation of alerts or alarms based on the number of failed AAA authentication requests that occur during the polling interval. |

| Value | Description |
|---|---|
| Authentication Failure Rate | Enables the generation of alerts or alarms based on the percentage of AAA authentication requests that failed during the polling interval. |
| 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 Manager Request Queue Usage | Enables the generation of alarms or alerts when the AAA Manager request queue usage reaches a specified percentage level. |

# 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 ASR 5500. 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.

**Note** 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 > or = 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 > or = High Threshold

- **Clear condition:** Actual number of failures < Low Threshold

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

## Configuring AAA Accounting Failure Threshold

Use the following example to configure AAA accounting failure threshold:

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

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

## Configuring AAA Authentication Failure Threshold

Use the following example to configure AAA authentication failure threshold:

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

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

## Configuring AAA Authentication Failure Rate Threshold

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

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

# AAA Request Message Retry Rate Thresholds

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

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

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

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

## Configuring AAA Authentication Failure Rate Threshold

Use the following example for configuring AAA request message 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:

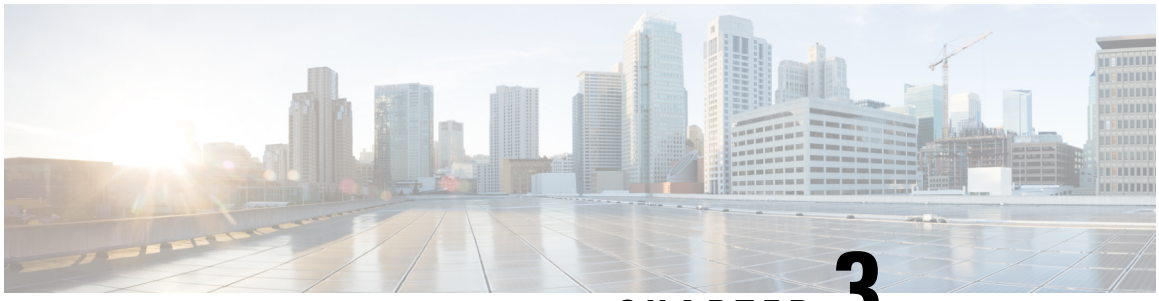
- **Enter condition:** Actual AAA Manager request queue percentage used > or = High Threshold
- **Clear condition:** Actual AAA Manager request queue percentage used < Low Threshold

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

## Configuring AAA Manager Request Queue Threshold

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

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



CHAPTER 3

# ASNGW Thresholds


- ASN GW Service Thresholds, on page 13
- Saving Your Configuration, on page 13
- System-Level ASN GW Service Thresholds, on page 13


## 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.

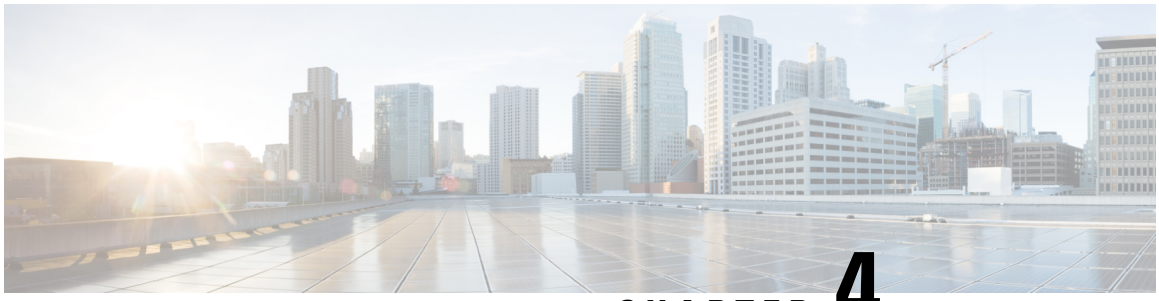
Following thresholds can be configured for the ASN GW service-level:

- 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


- Call Setup Thresholds, on page 15
- Saving Your Configuration, on page 16
- Call Setup Thresholds, on page 16
- Call Setup Failure Thresholds, on page 17
- eGTP-C S2b Setup Fail Rate Thresholds, on page 17
- eGTP-C S5 Setup Fail Rate Thresholds, on page 18
- RP Setup Failure Rate Thresholds, on page 18
- PPP Setup Failure Rate Thresholds, on page 19
- No Resource Call Reject Thresholds, on page 19


## Call Setup Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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. |
| eGTP-C S2b setup failure rate | Enables the generation of alerts or alarms based on the rate at which eGTP-C S2b setup failures are experienced by the system during the polling interval. |
| eGTP-C S5 setup failure rate | Enables the generation of alerts or alarms based on the rate at which eGTP-C S5 setup failures are experienced by the system during the polling interval. |
| 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. |

| Value | Description |
|---|---|
| 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. |
| 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. |

# 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 |
|---|---|
| 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. |
| 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. |
| eGTP-C S2b setup failure rate | Enables the generation of alerts or alarms based on the rate at which eGTP-C S2b setup failures are experienced by the system during the polling interval. |
| eGTP-C S5 setup failure rate | Enables the generation of alerts or alarms based on the rate at which eGTP-C S5 setup failures are experienced by the system during the polling interval. |
| 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. |
| 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. |
| 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. |

## Configuring Call Setup Thresholds

Use the following example to configure call setup thresholds:

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

# Call Setup Failure Thresholds

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

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

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

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

## Configuring Call Setup Failure Thresholds

Use the following example for configuring call setup failure thresholding:

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

# eGTP-C S2b Setup Fail Rate Thresholds

eGTP-C S2b setup fail rate thresholds generate alerts or alarms based on the rate of eGTP-C S2b setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by this formula: 1 - (Create Session Response Accept / Create Session Request).

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

- **Enter condition:** Actual number of eGTP-C S2b setup failures > or = High Threshold
- **Clear condition:** Actual number of eGTP-C S2b 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 eGTP-C S2b Setup Fail Rate Thresholds

Use the following example for configuring eGTP-C S2b setup fail rate thresholds:

```
configure
   threshold egtpc-s2b-setup-fail-rate high_thresh [ clear low_thresh ]
   threshold poll egtpc-s2b-setup-fail-rate interval duration
   threshold monitoring call-setup
   end
```

# eGTP-C S5 Setup Fail Rate Thresholds

eGTP-C S5 setup fail rate thresholds generate alerts or alarms based on the rate of eGTP-C S5 setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by this formula: 1 - (Create Session Response Accept / Create Session Request).

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

- **Enter condition:** Actual number of eGTP-C S5 setup failures > or = High Threshold
- **Clear condition:** Actual number of eGTP-C S5 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 eGTP-C S5 Setup Fail Rate Thresholds

Use the following example for configuring eGTP-C S5 setup fail rate thresholds:

```
configure
   threshold egtpc-s5-setup-fail-rate high_thresh [ clear low_thresh ]
   threshold poll egtpc-s5-setup-fail-rate interval duration
   threshold monitoring call-setup
   end
```

# RP Setup Failure Rate Thresholds

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

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

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

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

## Configuring RP Setup Failure Rate Thresholds

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

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

# PPP Setup Failure Rate Thresholds

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

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

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

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

## Configuring PPP Setup Failure Rate Thresholds

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

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

# No Resource Call Reject Thresholds

No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (CPU, memory, etc.) during the specified polling interval.

Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

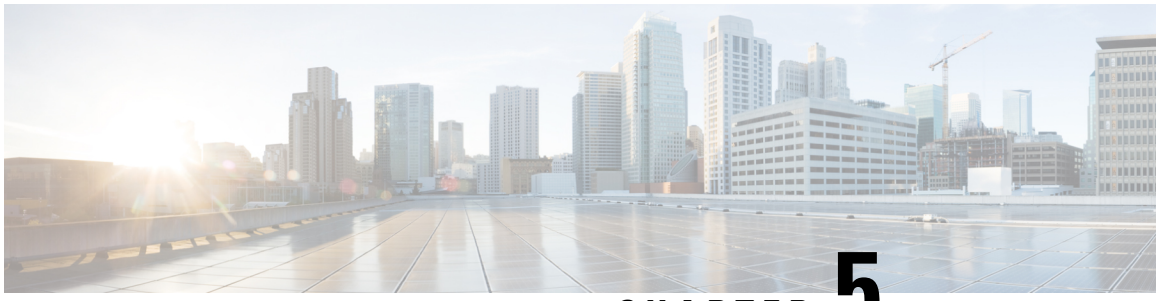
- **Enter condition:** Actual number of calls rejected due to no resources > or = High Threshold
- **Clear condition:** Actual number of calls rejected due to no resources < Low Threshold

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

# Configuring No Resource Call Reject Thresholds

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

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



CHAPTER 5

# Content Filtering Thresholds


- Content Filtering Thresholds, on page 21
- Configuring Content Filtering Thresholds, on page 21
- Saving Your Configuration, on page 22


## Content Filtering Thresholds

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

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

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

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

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

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

## Configuring Content Filtering Thresholds

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

### Enabling Thresholds

To enable thresholds use the following configuration:

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

# Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

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

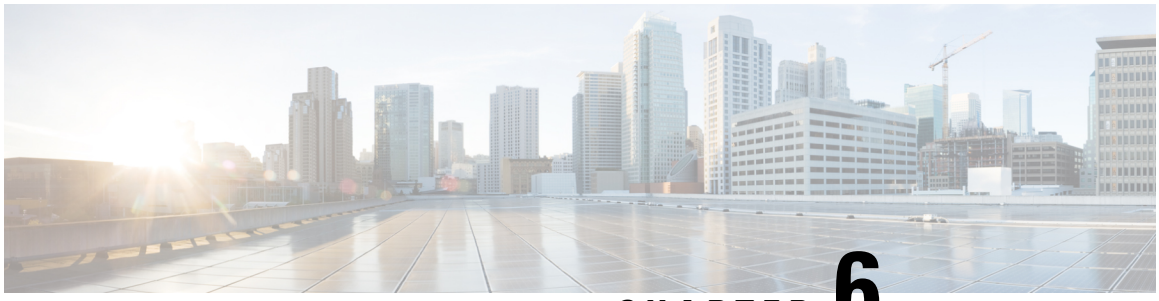
# Configuring Threshold Limits

To configure threshold limits use the following configuration:

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

# Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration 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


- CPU Resource Thresholds, on page 23
- Saving Your Configuration, on page 24
- 10-second Average of Total Processing Card CPU Utilization Thresholds, on page 24
- Processing Card CPU Available Memory Thresholds, on page 25
- Processing Card CPU Load Thresholds, on page 25
- Processing Card CPU Memory Usage Thresholds, on page 26
- Processing Card CPU Session Throughput Thresholds, on page 26
- Processing Card CPU Utilization Thresholds, on page 27
- System Management Card CPU Memory Usage Thresholds, on page 27
- System Management Card CPU Utilization Thresholds, on page 28
- ORBS Software Task CPU Usage Warning-Level Thresholds, on page 28
- ORBS Software Task CPU Usage Critical-Level Thresholds, on page 29


## CPU Resource Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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 load | Enables the generation of alerts or alarms based on processing card CPU load using a 5 minute average measurement. |
| 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. |

| Value | Description |
|---|---|
| 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 utilization | Enables the generation of alerts or alarms based on the utilization percentage for each processing card CPU during the polling interval. |
| 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 utilization | Enables the generation of alerts or alarms based on the utilization percentage for each active system management card CPU during the polling interval. |
| 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 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. |

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

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

## Configuring Processing Card CPU Load Thresholds

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

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

# Processing Card CPU Memory Usage Thresholds

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

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

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

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

## Configuring Processing Card CPU Memory Usage Thresholds

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

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

# Processing Card CPU Session Throughput Thresholds

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

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

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

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

## Configuring Processing Card CPU Session Throughput Thresholds

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

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

# Processing Card CPU Utilization Thresholds

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

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

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

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

## Configuring Processing Card CPU Utilization Thresholds

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

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

# System Management Card CPU Memory Usage Thresholds

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

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

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

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

## Configuring System Management Card CPU Memory Usage Thresholds

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

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

# System Management Card CPU Utilization Thresholds

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

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

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

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

## Configuring System Management Card CPU Utilization Thresholds

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

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

# ORBS Software Task CPU Usage Warning-Level Thresholds

Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of system management card CPU resources it is consuming at the time of polling.

Warning-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage > High Threshold
- **Clear condition:** Actual CPU usage percentage = or < Low Threshold

## Configuring ORBS Software Task CPU Usage Warning-Level Thresholds

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

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

# ORBS Software Task CPU Usage Critical-Level Thresholds

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of system management card CPU resources it is consuming at the time of polling.

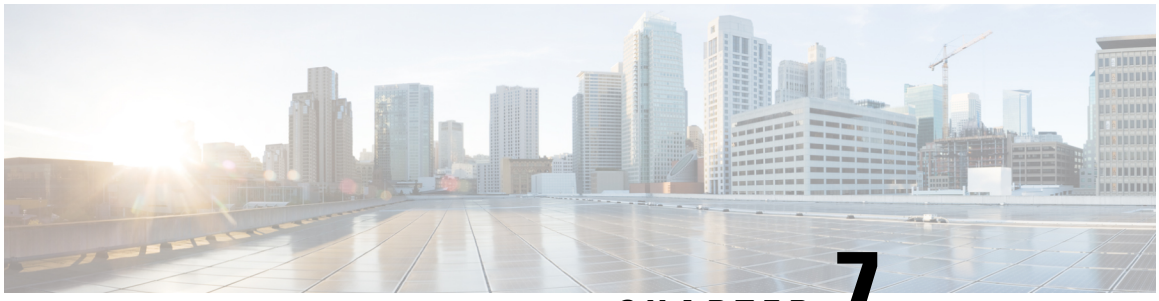
Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage > High Threshold
- **Clear condition:** Actual CPU usage percentage = or < Low Threshold

## Configuring ORBS Software Task CPU Usage Critical-Level Thresholds

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

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



CHAPTER 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 > 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. Polling intervals are set on a system level.


- CSCF Service Thresholds, on page 31
- Configuring CSCF Thresholds, on page 31
- Saving Your Configuration, on page 33


# 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 > 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. 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:

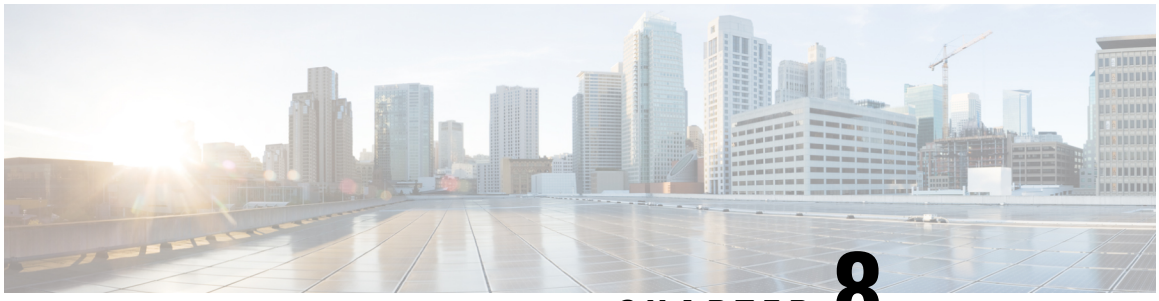
- CSCF call setup failures
- CSCF total active calls
- CSCF calls
- CSCF registrations
- CSCF service route failures
- CSCF no resource errors
- CSCF presence errors
- CSCF Reg-Auth errors
- CSCF TCP errors
- CSCF total active registrations

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

# Disconnect-Reasons Thresholds

An operator can set alarms based on threshold parameters for up to 30 specific session disconnect reasons. An alarm notification and SNMP trap are generated whenever a disconnect reason threshold is exceeded.

The **show session disconnect-reasons verbose** command displays the name and associated reason number of all disconnect reasons (600+).

Alerts or alarms are triggered for a specific disconnect type based on the following rules:

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


- Disconnect-Reasons Thresholds, on page 35
- Configuring Disconnect-Reasons Thresholds, on page 35
- Saving Your Configuration, on page 37



# Disconnect-Reasons Thresholds

An operator can set alarms based on threshold parameters for up to 30 specific session disconnect reasons. An alarm notification and SNMP trap are generated whenever a disconnect reason threshold is exceeded.

The **show session disconnect-reasons verbose** command displays the name and associated reason number of all disconnect reasons (600+).

Alerts or alarms are triggered for a specific disconnect type based on the following rules:

- **Enter condition:** Actual number of disconnects > or = High Threshold
- **Clear condition:** Actual number of disconnects < 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 Disconnect-Reasons Thresholds

This section describes how to enable and configure session disconnect-reason thresholds.

# threshold disconnect-reason

Use the following configuration example to configure alarm and clear thresholds based on the number of disconnects per specified disconnect reason on a chassis.

```
configure
   threshold disconnect-reason disc-reason_name high_thresh [ clear  low_thresh
]
   end
```

**Note** The operator can configure a maximum of 30 types of disconnect reasons for monitoring. When the number of disconnects per disconnect reason crosses the threshold, a trap is generated.

# threshold poll disconnect-reason

Use the following configuration example to configure a polling period for a specific disconnect reason.

```
configure
   [ default ] threshold poll disconnect-reason disc-reason_name interval
polling_interval_seconds
   end
```

*polling_interval_seconds* is specified as an integer divisible by 30 within the range of 300 (five minutes) to 60000 (1000 minutes).

**Important** The operator can configure a maximum of 30 types of disconnect reasons for monitoring. When the number of disconnects per disconnect reason crosses the threshold, a trap is generated.

# threshold monitoring

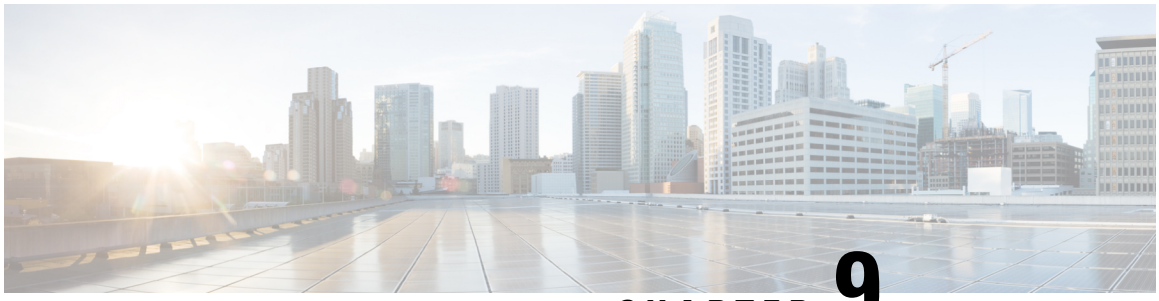
Use the following configuration example to enable or disable monitoring of disconnect reasons.

```
configure
   [ no | default ] threshold monitoring disconnect-reason
   end
```

**Important** The operator can configure a maximum of 30 types of disconnect reasons for monitoring. When the number of disconnects per disconnect reason crosses the threshold, a trap is generated.

# Saving Your Configuration

When you configure thresholds they are not persistent 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 **save configuration** command. 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

# Diameter Thresholds


- Diameter Thresholds, on page 39
- Configuring Diameter Thresholds, on page 39
- Saving Your Configuration, on page 42


## Diameter Thresholds

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

| Threshold | Description |
|---|---|
| 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 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 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 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. |
| Diameter Retry Rate | Enables generation of alerts or alarms based on the percentage of Diameter requests that were re-tried during a polling interval. |

## Configuring Diameter Thresholds

This section describes how to enable and configure Diameter thresholds.

# DCCA Bad Answers Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring DCCA Bad Answers Threshold

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

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

# DCCA Protocol Errors Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring DCCA Protocol Errors Threshold

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

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

# DCCA Rating Failure Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

### Configuring DCCA Rating Failure Threshold

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

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

## DCCA Unknown Rating Group Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

### Configuring DCCA Unknown Rating Group Threshold

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

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

## Diameter Retry Rate Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

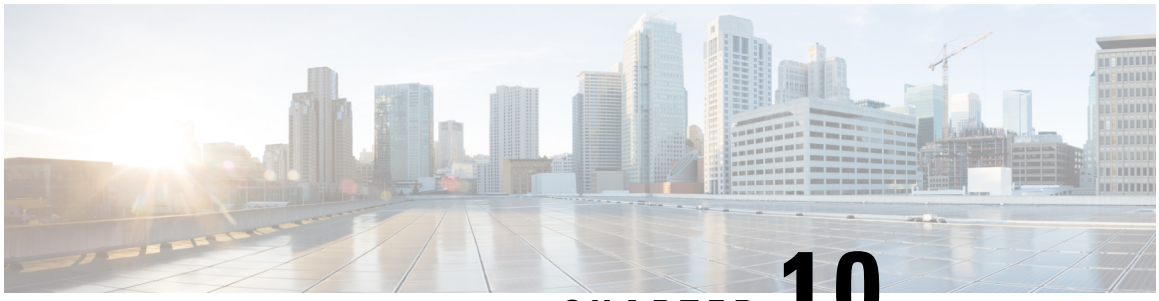
## Configuring Diameter Retry Rate Threshold

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

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

# Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration 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

# ECS Thresholds


- ECS Thresholds, on page 43
- Configuring ECS Thresholds, on page 43
- Saving Your Configuration, on page 46


## ECS Thresholds

Threshold monitoring can be enabled for the ECS thresholds as described in the following table.

| Threshold | Description |
|---|---|
| CDR File Space | Enables generation of alerts or alarms based on the percentage of total file space allocated for Charging Data Records (CDRs) used during the polling interval. |
| DNS-learnt IPv4 for ACS DNS Snooping feature | Enables generation of alerts or alarms based on the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature. |
| DNS-learnt IPv6 for ACS DNS Snooping feature | Enables generation of alerts or alarms based on the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature. |
| EDR File Space | Enables generation of alerts or alarms based on the percentage of total file space allocated for Event Data Records (EDRs) used during the polling interval. |
| Dropped EDR/UDR Flow Control | Enables generation of alerts or alarms based on the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control. |

## Configuring ECS Thresholds

This section describes how to enable and configure ECS thresholds.

# CDR File Space Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring CDR File Space Threshold

To configure the CDR File Space threshold use the following configuration:

```
configure
 threshold cdr-file-space <high_thresh> [ clear  <low_thresh> ]
 threshold poll cdr-file-space interval <seconds>
 threshold monitoring ecs
 end
```

# DNS-learnt IPv4 Threshold

DNS-learnt IPv4 threshold generates alerts or alarms based on the percentage of total DNS-learnt IPv4 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring DNS-Learnt IPv4 Threshold

To configure the DNS-Learnt IPv4 threshold use the following configuration:

```
configure
 threshold dns-learnt-ipv4-max-entries  <high_thresh> [ clear  <low_thresh> ]
 threshold poll dns-learnt-ipv4-max-entries <seconds>
 threshold monitoring ecs
 end
```

# DNS-learnt IPv6 Threshold

DNS-learnt IPv6 threshold generates alerts or alarms based on the percentage of total DNS-learnt IPv6 entries in relation to the ACS DNS Snooping feature.

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring DNS-Learnt IPv6 Threshold

To configure the DNS-Learnt IPv6 threshold use the following configuration:

```
configure
 threshold dns-learnt-ipv6-max-entries <high_thresh> [ clear <low_thresh> ]
 threshold poll dns-learnt-ipv6-max-entries <seconds>
 threshold monitoring ecs
 end
```

# EDR File Space Threshold

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

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring EDR File Space Threshold

To configure the EDR File Space threshold use the following configuration:

```
configure
 threshold edr-file-space <high_thresh> [ clear <low_thresh> ]
 threshold poll edr-file-space interval <seconds>
 threshold monitoring ecs
 end
```

# Dropped EDR/UDR Flow Control Threshold

Dropped EDR/UDR Flow Control threshold generates alerts or alarms based on the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control.

Alerts or alarms are triggered based on the following rules:

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

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

## Configuring Dropped EDR/UDR Flow Control Threshold

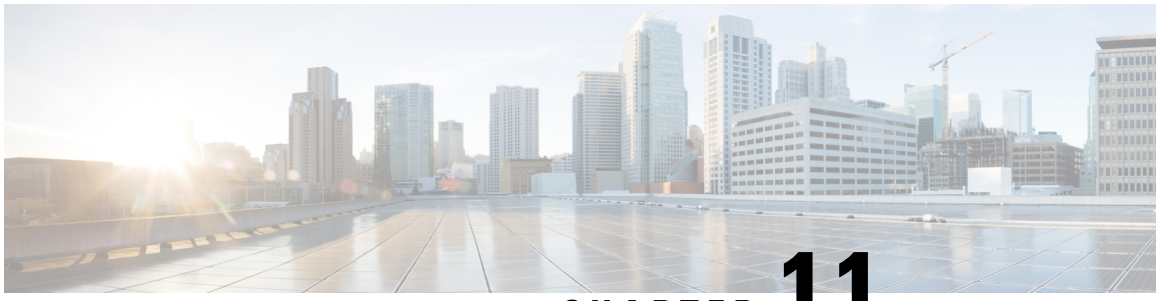
To configure the Dropped EDR/UDR Flow Control threshold use the following configuration:

```
configure
 threshold edr-udr-dropped-flow-control  <high_thresh> [ clear  <low_thresh> ]

 threshold poll edr-udr-dropped-flow-control <seconds>
 threshold monitoring ecs
 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 11

# ePDG Thresholds


- EPDG Thresholds, on page 47
- Configuring ePDG Thresholds, on page 47
- Saving Your Configuration, on page 48
- Configuring IKEv2 tunnel setup attempts , on page 48


## EPDG Thresholds

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

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

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

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

Default ePDG threshold polling interval value is 5 Min.

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 ePDG Thresholds

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

```
configure
     [ no ] threshold monitoring epdg-service
 threshold  epdg-current-sessions current_epdg_sessions_threshold clear
alarm_clear_threshold
 default threshold  epdg-current-sessions
 threshold poll epdg-current-sessions interval threshold_polling_interval
 default threshold poll epdg-current-sessions interval
      end
```

# Saving Your Configuration

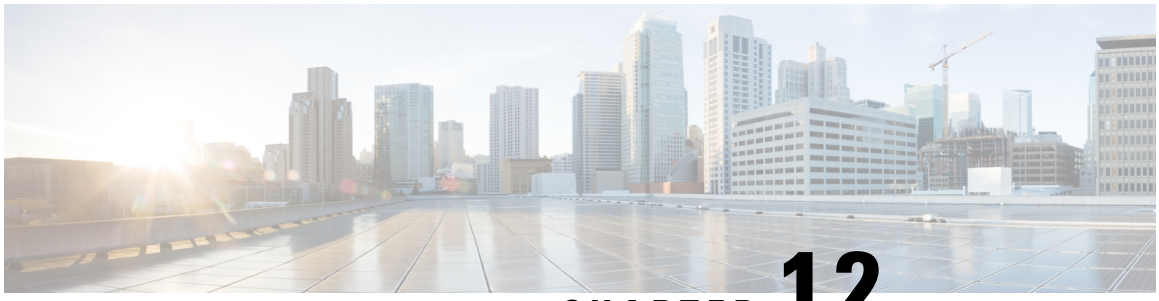
When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

# Configuring IKEv2 tunnel setup attempts

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

```
configure
        context epdg context
          epdg-service epdg_service_name
          no  threshold ikev2-setup-attempts threshold_value  clear clear_value

        exit threshold poll epdg-current-sessions interval
      exit
```



CHAPTER 12

# FA Thresholds


- FA Service Thresholds, on page 49
- Configuring FA Service Thresholds, on page 49
- Saving Your Configuration, on page 50


## 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 ≥ 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.

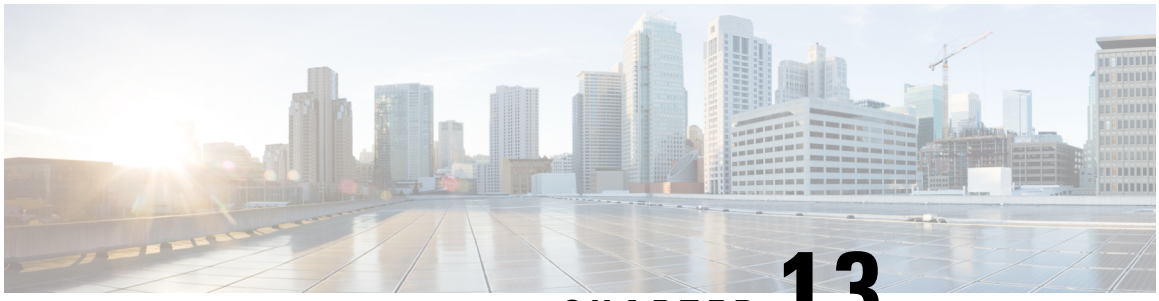
## Configuring FA Service Thresholds

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 13

# FNG Thresholds


- FNG Thresholds, on page 51
- Configuring FNG Thresholds, on page 51
- Saving Your Configuration, on page 52


## 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 5500 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 5500 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 5500 chassis:

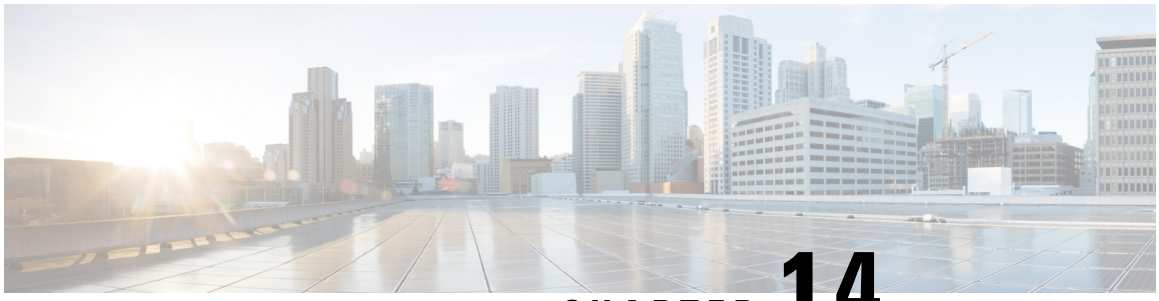
```
threshold fng-current-sessions 300000
```

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 14

# HA Thresholds


- HA Service Thresholds, on page 53
- Saving Your Configuration, on page 54
- Context-Level HA Service Thresholds, on page 54
- HA Service-Level HA Service Thresholds, on page 54


## 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 |
|---|---|
| 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. |
| 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. |

# 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

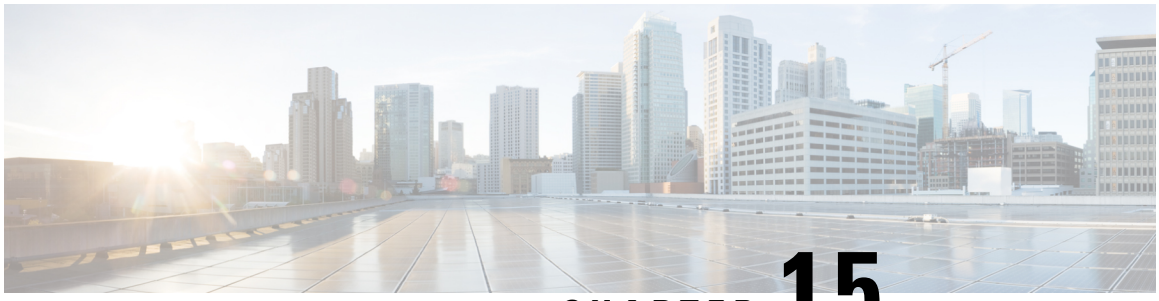
There are 10 thresholds that can be configured for the HA service-level:

- 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 15

# HeNBGW Thresholds


- HeNB-GW Service Thresholds, on page 57
- Saving Your Configuration, on page 57
- System-Level HeNB-GW Service Thresholds, on page 58


## HeNB-GW Service Thresholds

HeNB-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 HeNB-GW service. Thresholds can also be configured for session registration response failures, discarded interface registration requests, discarded network entry registration acknowledgments for HeNB-GW services.

Threshold counter limits are configured for HeNB-GW HeNB SCTP association, HeNB-GW UE sessions, and HeNB-GW Paging messages with poll interval value.

On reaching the threshold limits in the configured interval, if threshold monitoring is enabled for the HeNB-GW service(s), threshold notifications get generated as SNMP traps. If threshold monitoring is disabled for the HeNB-GW service(s), even on reaching the threshold limits, no notification gets generated.

Alerts or alarms are triggered for these HeNB-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 HeNB-GW Service Thresholds

The system-level thresholds for HeNB-GW Service-Level can be configured to monitor thresholds for HeNB-GW Paging messages.

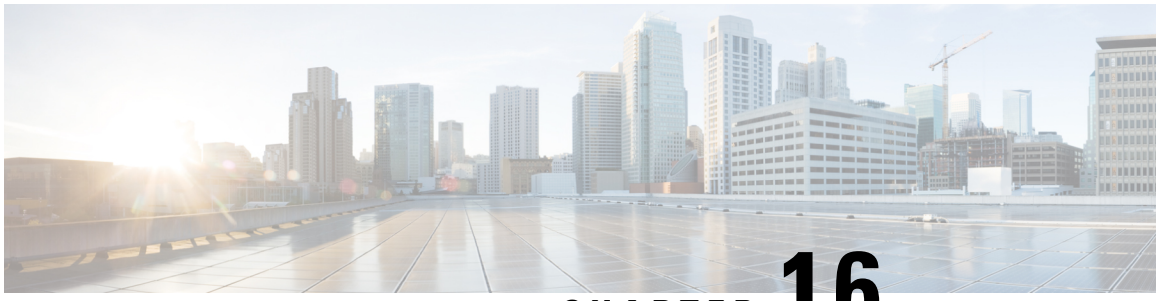
Following thresholds can be configured for the HeNB-GW service-level:

- Number of HeNB-GW Paging Messages
- Total number of subscribers threshold for HeNB-GW HeNB sessions
- Total number of subscribers threshold for HeNB-GW UE sessions

## Configuring System-level HeNB-GW Service Thresholds

Use the following example to configure and enable these thresholds:

```
configuration
 threshold henbgw-paging-messages  <high_thresh> [ clear <low_thresh>]
 threshold total-henbgw-henb-sessions  <high_thresh> [ clear <low_thresh>]
 threshold total-henbgw-ue-sessions  <high_thresh> [ clear <low_thresh>]
 threshold poll henbgw-paging-messages interval <dur>
 threshold poll total-henbgw-henb-sessions interval <dur>
 threshold poll total-henbgw-ue-sessions interval <dur>
 threshold monitoring henbgw-service
 end
```



CHAPTER 16

# IP Pool Thresholds


- IP Pool Utilization Thresholds, on page 59
- Saving Your Configuration, on page 60
- Context-Level IP Pool and Group Thresholds, on page 61
- IP Address Pool-Level Thresholds, on page 61


## 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 |
|---|---|
| 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. |
| | IP Pool: The following thresholds can be configured for all IP address pools configured within a given system context:<br>• Percent-free;<br>• Percent-hold;<br>• Percent-release;<br>• Percent-used.<br>**NOTE:** Separate alerts or alarms are generated for each pool that experiences an event. |
| IP address pool-level | The following thresholds can be configured for each IP address pool:<br>• Percent-available for the group that the IP pool belongs to;<br>• Percent-free;<br>• Percent-hold;<br>• Percent-release; and<br>• Percent-used.<br>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. |

# 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, on page 61 for setting thresholds for individual IP pools.

**Note** 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.

**Note** 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.

**Note** 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:

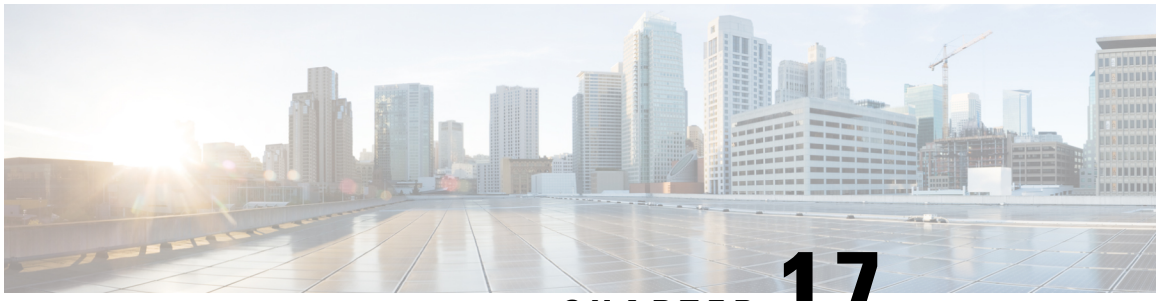
- Enter condition (low threshold) set to 40 percent
- Clear condition (high threshold) set to 60 percent

- 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 17

# MME Service Thresholds


- MME Service Thresholds, on page 63
- Saving Your Configuration, on page 63
- System-Level MME Service Thresholds, on page 63


## 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.

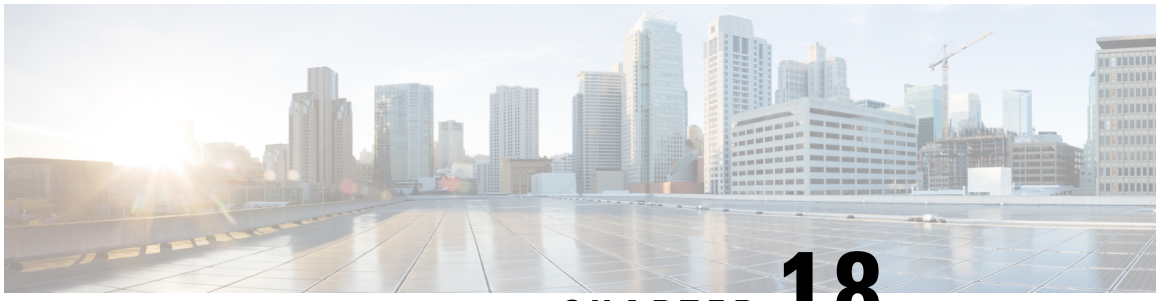
Following thresholds can be configured for the entire MME (all services together), for a configured polling period:

- Number of Sessions
- 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 18

# Network Address Translation Thresholds


- Network Address Translation Thresholds, on page 65
- Configuring NAT Thresholds, on page 65
- Saving Your Configuration, on page 66


## Network Address Translation Thresholds

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

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

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

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

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

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

## Configuring NAT Thresholds

This section describes how to enable and configure NAT thresholds.

### Enabling Thresholds

To enable thresholds use the following configuration:

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

Notes:

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

# Configuring Threshold Poll Interval

To configure threshold poll interval use the following configuration:

```
configure
     threshold poll ip-pool-used interval  <interval>
     threshold poll nat-pkt-drop 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:

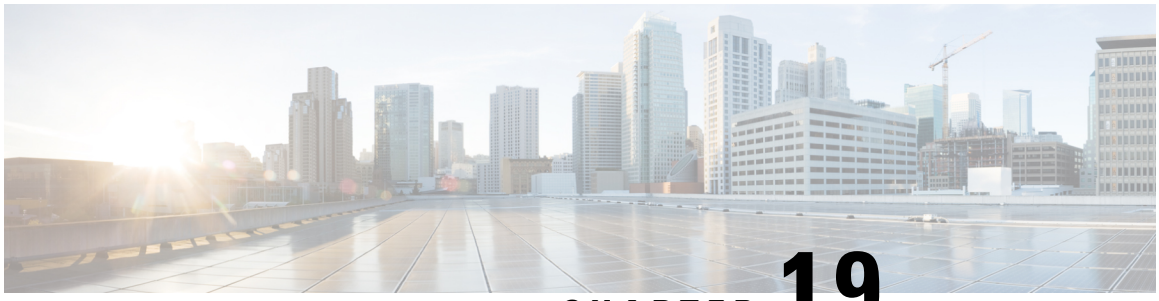
```
configure
     context <context_name>
          threshold ip-pool-free <high_thresh> [ clear <low_thresh> ]
          ip-pool-hold <high_thresh> [ clear <low_thresh> ]
          ip-pool-release <high_thresh> [ clear <low_thresh> ]
          ip-pool-used <high_thresh> [ clear <low_thresh> ]
          exit
     threshold nat-pkt-drop <high_thresh> [ clear <low_thresh> ]
     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 19

# Packet Processing Thresholds


- Packet Processing Thresholds, on page 67
- Saving Your Configuration, on page 67
- Filtered/Dropped Packet Thresholds, on page 67
- Forwarded Packet Thresholds, on page 68


## Packet Processing Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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. |

## 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 > or = High Threshold

- **Clear condition:** Actual number of filtered/dropped packets < Low Threshold

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

**Note** 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.

**Note** Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

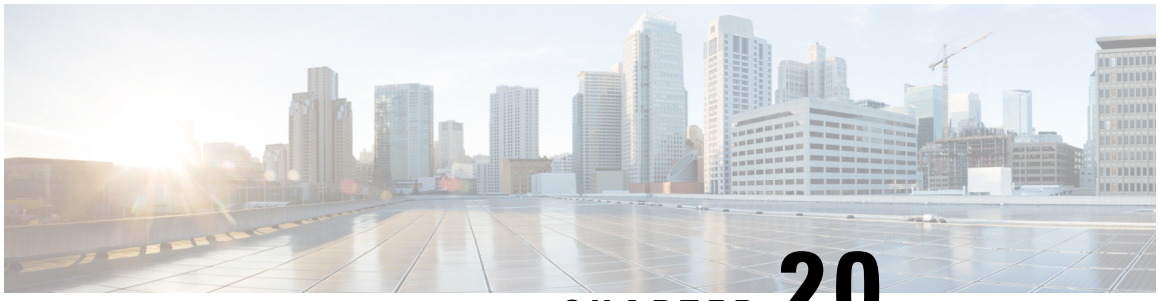
- **Enter condition:** Actual number of forwarded packets > or = High Threshold
- **Clear condition:** Actual number of forwarded packets < Low Threshold

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

## Configuring Forwarded Packet Thresholds

Use the following example to configure the forwarded packet thresholds:

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



CHAPTER 20

# PDG/TTG Thresholds


- PDG/TTG Thresholds, on page 69
- Configuring PDG/TTG Thresholds, on page 69
- Saving Your Configuration, on page 70


## 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

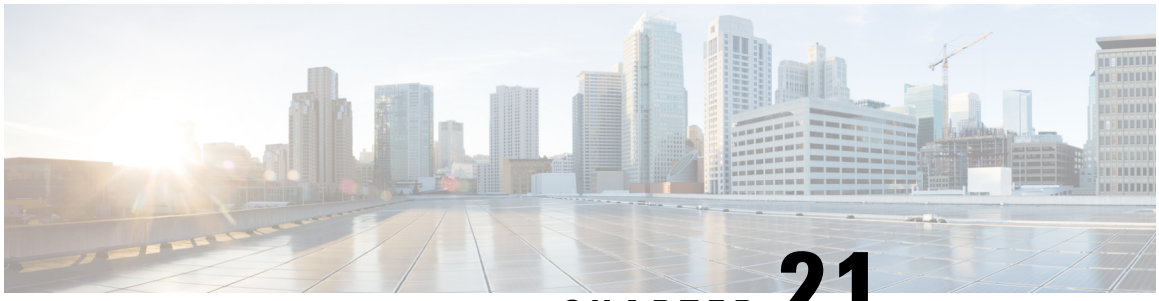
Use the following configuration example to enable, disable and configure PDG/TTG threshold monitoring.

```
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 21

# PDIF Thresholds


- PDIF Thresholds, on page 71
- Configuring PDIF Thresholds, on page 71
- Saving Your Configuration, on page 72


## PDIF Thresholds

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

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

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

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

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

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

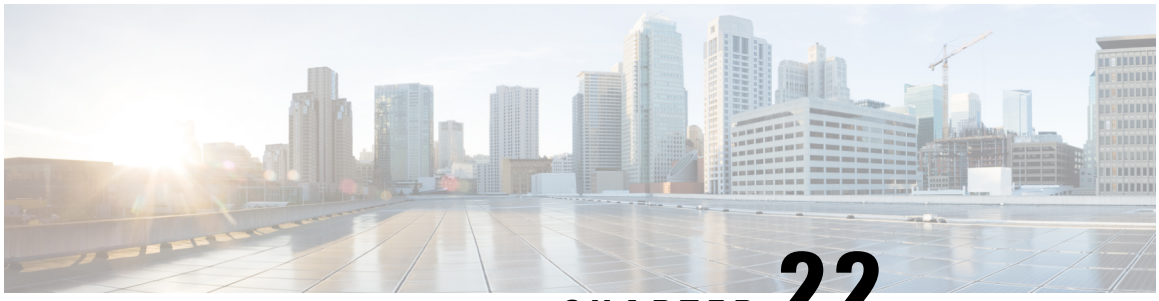
## Configuring PDIF Thresholds

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

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

# Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration 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

# PDSN Thresholds


- PDSN Service Thresholds, on page 73
- Saving Your Configuration, on page 74
- Context-Level PDSN Service Thresholds, on page 74
- PDSN Service-Level PDSN Service Thresholds, on page 74


## 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 |
|---|---|
| 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. |

| Method | Description |
|---|---|
| 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. |

# 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:

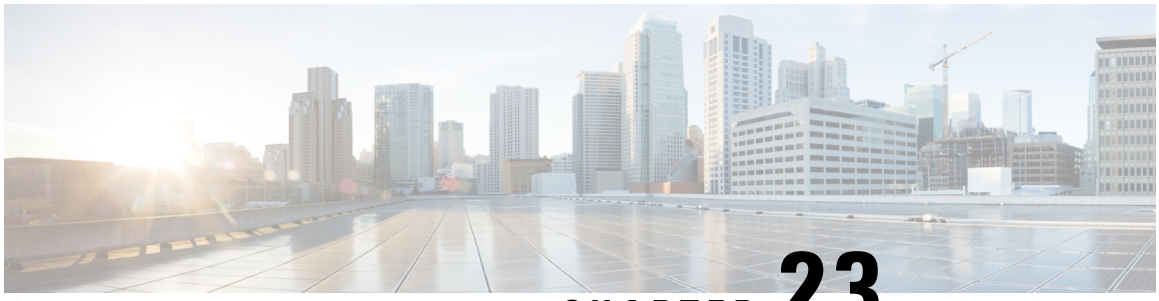
- Average Calls Setup Per Second

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



CHAPTER 23

# Per-Service Session Thresholds


- Per-service Session Thresholds, on page 77
- Saving Your Configuration, on page 78
- Per-PDSN Service Thresholds, on page 78
- Per-HA Service Thresholds, on page 79
- Per-GGSN Service Thresholds, on page 79
- Per-LNS Service Thresholds, on page 80
- Per-GPRS Service Thresholds, on page 80
- Per-GPRS Service PDP Contexts Thresholds, on page 81
- Per-SGSN Service Thresholds, on page 81
- Per-SGSN Service PDP Contexts Thresholds, on page 82


## Per-service Session Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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. |
| 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. |
| 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. |

| Value | Description |
|---|---|
| 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. |
| 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. |

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

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

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

## Configuring Per-PDSN Service Thresholds

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

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

# Per-HA Service Thresholds

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

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

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

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

## Configuring Per-HA Service Thresholds

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

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

# Per-GGSN Service Thresholds

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

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

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

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

## Configuring Per-GGSN Service Thresholds

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

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

# Per-LNS Service Thresholds

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

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

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

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

## Configuring Per-LNS Service Thresholds

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

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

# Per-GPRS Service Thresholds

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

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

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

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

## Configuring Per-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 > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < Low Threshold

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

## Configuring Per-GPRS Service PDP Contexts Thresholds

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

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

# Per-SGSN Service Thresholds

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

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

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

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

## Configuring Per-SGSN Service Thresholds

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

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

# Per-SGSN Service PDP Contexts Thresholds

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

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

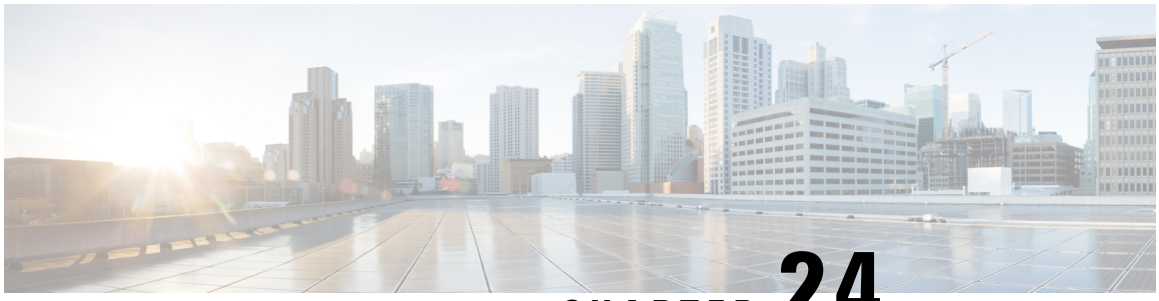
- **Enter condition:** Actual total number of PDP contexts > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < Low Threshold

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

## Configuring Per-SGSN Service PDP Contexts Thresholds

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

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



CHAPTER 24

# Port Utilization Thresholds


- Port Utilization Thresholds, on page 83
- Saving Your Configuration, on page 83
- Receive Port Utilization Thresholds, on page 84
- Transmit Port Utilization Thresholds, on page 84
- High Port Activity Thresholds, on page 85


## Port Utilization Thresholds

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

| Value | Description |
|---|---|
| Receive port utilization | Enables the generation of alerts or alarms based on the port utilization percentage for data received during the polling interval. |
| Transmit port utilization | Enables the generation of alerts or alarms based on the port utilization percentage for data transmitted during the polling interval. |
| High port activity | Enables the generation of alerts or alarms based on the overall port utilization percentage during the polling interval. |

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

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

## Configuring Receive Port Utilization Thresholds

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

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

# Transmit Port Utilization Thresholds

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

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

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

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

## Configuring Transmit Port Utilization Thresholds

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

```
configure
 threshold poll port-tx-utilization interval  <seconds>
 port <port-type> <slot/port>
```

```
threshold tx-utilization <high_thresh_> [ clear <low_thresh_> ]
threshold monitoring
           end
```

# High Port Activity Thresholds

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

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

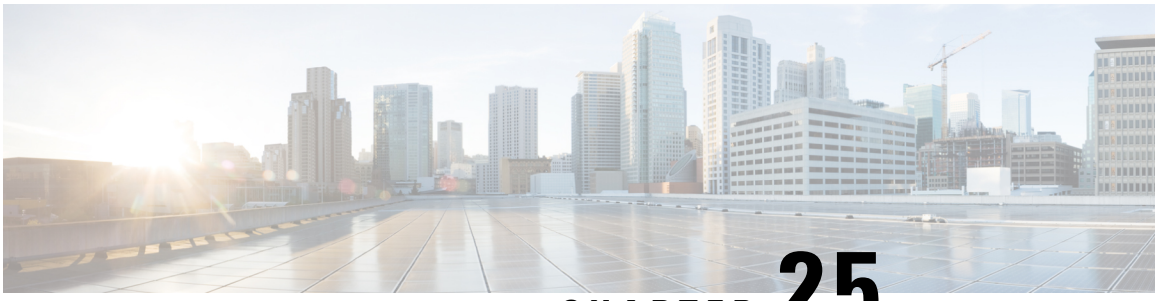
- **Enter condition:** Actual percent peak utilization of a port > or = High Threshold
- **Clear condition:** Actual percent peak utilization of a port < Low Threshold

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

## Configuring High Port Activity Thresholds

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

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



CHAPTER 25

# SaMOG Thresholds


- SaMOG Thresholds, on page 87
- Configuring SaMOG Thresholds, on page 87
- Saving Your Configuration, on page 87


## SaMOG Thresholds

Per-samog-service threshold generate alerts or alarms based on either the total number of SaMOG sessions facilitated by any samog-service configured on the system duringf the specified polling interval

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

- **Enter Condition:** Actual total number of SaMOG sessions > or = High Threshold
- **Clear Condition:** Actual total number of SaMOG sessions < Low Threshold

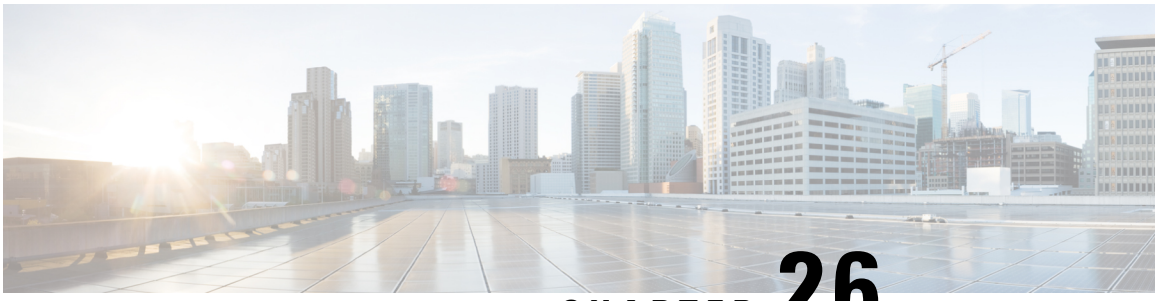
## Configuring SaMOG Thresholds

Use the following configuration example for the samog-service session count threshold crossing alerts:

```
configure
 threshold per-service-samog-sessions <high_thresh> [ clear <low_thresh> ]
 threshold poll per-service-samog-sessions interval <dur>
 threshold monitoring subscriber
 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 26

# Session License Utilization Thresholds


- Session License Utilization Thresholds, on page 89
- Configuring Session License Utilization Thresholds, on page 89
- Saving Your Configuration, on page 90


## 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.

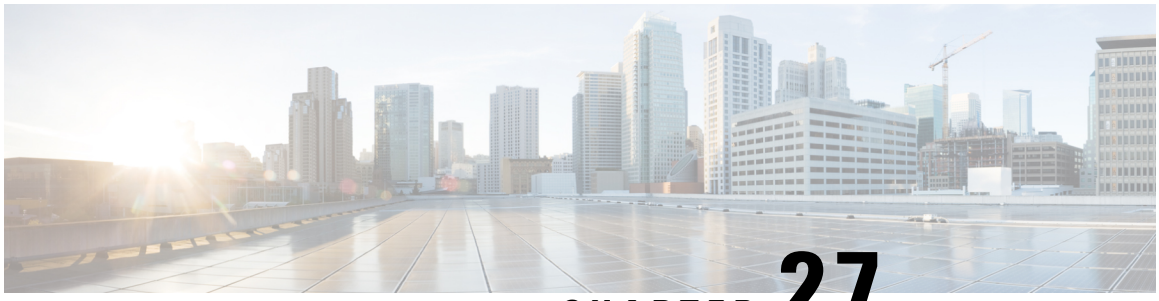
## Configuring Session License Utilization Thresholds

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 27

# Stateful Firewall Thresholds


- Stateful Firewall Thresholds, on page 91
- Configuring Stateful Firewall Thresholds, on page 91
- Saving Your Configuration, on page 92


## Stateful Firewall Thresholds

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

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

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

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

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

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

## Configuring Stateful Firewall Thresholds

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

### Enabling Thresholds

To enable thresholds use the following configuration:

```
configure
 threshold monitoring firewall
 end
```

# Configuring Threshold Polling Intervals

To configure threshold poll interval use the following configuration:

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

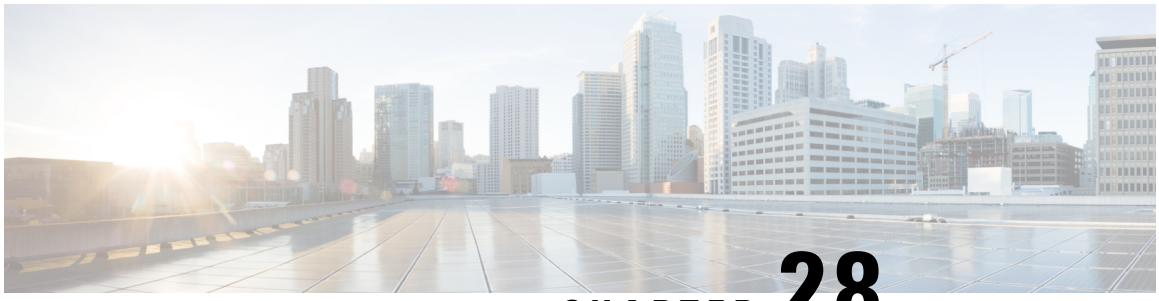
# Configuring Thresholds Limits

To configure threshold limits use the following configuration:

```
configure
 threshold fw-deny-rule <high_thresh> [ clear <low_thresh> ]
 threshold fw-dos-attack <high_thresh> [ clear <low_thresh> ]
 threshold fw-drop-packet <high_thresh> [ clear <low_thresh> ]
 threshold fw-no-rule <high_thresh> [ clear <low_thresh> ]
 end
```

# Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration 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 28

# Subscriber Thresholds


- Subscriber Thresholds, on page 93
- Saving Your Configuration, on page 93
- Total Subscriber Thresholds, on page 93
- Active Subscriber Thresholds, on page 94


## Subscriber Thresholds

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

| Value | Description |
|---|---|
| Total subscribers | Enables the generation of alerts or alarms based on the total number subscriber sessions (active and dormant) counted during the polling interval. |
| Active subscribers | Enables the generation of alerts or alarms based on the total number of subscribers with active sessions counted during 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*.

## Total Subscriber Thresholds

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

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

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

- **Clear condition:** Actual total number of subscriber sessions < Low Threshold

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

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

## Configuring Total Subscriber Thresholds

Use the following example to configure the total subscriber thresholds:

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

# Active Subscriber Thresholds

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

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

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

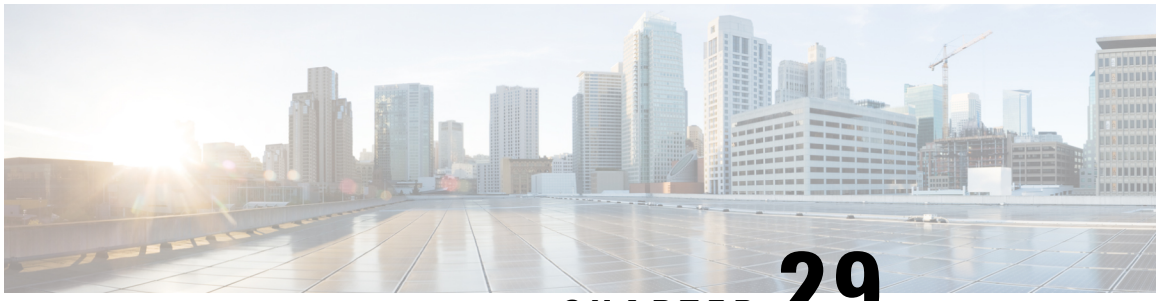
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

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

## Configuring Active Subscriber Thresholds

Use the following example to configure the active subscriber thresholds:

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



CHAPTER 29

# System Management Card CompactFlash Memory Thresholds


- System Management Card CompactFlash Memory Thresholds, on page 95
- Saving Your Configuration, on page 95


## System Management Card CompactFlash Memory Thresholds

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

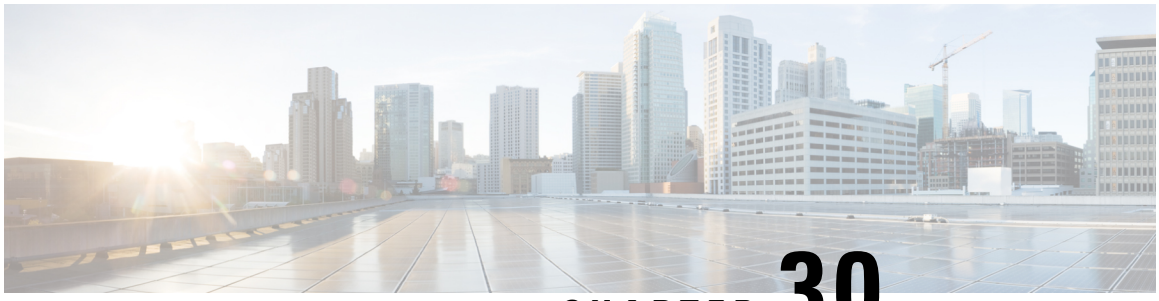
Alerts or alarms are triggered for CompactFlash memory utilization based on the following rules:

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

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

## Saving Your Configuration

When you configure thresholds they are not permanent unless you save the changes. When you have completed configuring thresholds, save your configuration 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 30

# Total Session Thresholds


- Total Session Thresholds, on page 97
- Saving Your Configuration, on page 99
- Total PDSN Session Thresholds, on page 99
- Total GGSN Session Thresholds, on page 99
- Total GPRS Session Thresholds, on page 100
- Total GPRS PDP Contexts Thresholds, on page 100
- Total HA Session Thresholds, on page 101
- Total HeNB-GW Session Thresholds, on page 101
- Total HNB-GW Session Thresholds, on page 102
- Total HSGW Session Thresholds, on page 103
- Total LMA Session Thresholds, on page 104
- Total LNS Session Thresholds, on page 104
- Total MME Session Thresholds, on page 105
- Total P-GW Session Thresholds, on page 105
- Total SAEGW Session Thresholds, on page 106
- Total SGSN Session Thresholds, on page 106
- Total SGSN PDP Contexts Thresholds, on page 107
- Total S-GW Session Thresholds, on page 107


## Total Session Thresholds

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

| Value | Description |
|---|---|
| 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. |
| 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. |

| Value | Description |
|---|---|
| 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. |
| 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. |
| HeNB-GW Services | Enables the generation of alerts or alarms based on the total number of HeNB and UE sessions (active and dormant) facilitated by all HeNB-GW services counted during the polling interval. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| 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. |
| SAEGW Service | Enables the generation of alerts or alarms based on the total number of sessions (active and dormant) facilitated by all SAEGW services counted during the polling interval. |

| Value | Description |
|---|---|
| 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. |
| 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. |

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

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

## Configuring Total PDSN Session Thresholds

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

```
configure
 threshold total-pdsn-sessions <high_thresh> [ clear <low_thresh> ]
 threshold poll total-pdsn-sessions interval <time>
 threshold monitoring 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 > or = High Threshold
- **Clear condition:** Actual total number of PDP contexts < Low Threshold

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

## Configuring Total GGSN Session Thresholds

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

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

# Total GPRS Session Thresholds

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

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

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

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

## Configuring Total GPRS Session Thresholds

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

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

# Total GPRS PDP Contexts Thresholds

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

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

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

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

## Configuring Total GPRS PDP Context Thresholds

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

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

# Total HA Session Thresholds

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

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

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

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

## Configuring Total HA Session Thresholds

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

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

# Total HeNB-GW Session Thresholds

**Important** In Release 20, 21.0 and 21.1, HeNBGW is not supported. For more information, contact your Cisco account representative.

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

Alerts or alarms are triggered for the total of all 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 HeNB 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-henbgw-henb-sessions <high_thresh> [ clear <low_thresh> ]
 threshold poll total-henbgw-henb-sessions interval <time>
 threshold monitoring henbgw-service
      end
```

## Configuring Total UE Session Thresholds

Use the following example to configure the thresholds for total HeNB-GW UE sessions:

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

# Total HNB-GW Session Thresholds

**Important** In Release 20 and later, HNBGW is not supported. For more information, contact your Cisco account representative.

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 seperately.

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 0

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

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

## Configuring Total HSGW Session Thresholds

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

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

# Total LMA Session Thresholds

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

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

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

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

## Configuring Total LMA Session Thresholds

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

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

# Total LNS Session Thresholds

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

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

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

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

## Configuring Total LNS Session Thresholds

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

```
configure
      threshold total-lns-sessions <high_thresh> [ clear <low_thresh> ]
      threshold poll total-lns-sessions interval <time>
      threshold monitoring 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 > or = High Threshold
- **Clear condition:** Actual total number of sessions < Low Threshold

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

## Configuring Total MME Session Thresholds

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

```
configure
 threshold total-mme-sessions <high_thresh> [ clear <low_thresh> ]
 threshold poll total-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 > or = High Threshold
- **Clear condition:** Actual total number of sessions < Low Threshold

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

## Configuring Total P-GW Session Thresholds

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

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

# Total SAEGW Session Thresholds

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

Alerts or alarms are triggered for the total of all SAEGW 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 SAEGW Session Thresholds

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

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

# Total SGSN Session Thresholds

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

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

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

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

## Configuring Total SGSN Session Thresholds

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

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

# Total SGSN PDP Contexts Thresholds

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

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

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

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

## Configuring Total SGSN PDP Context Thresholds

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

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

# Total S-GW Session Thresholds

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

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

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

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

## Configuring Total S-GW Session Thresholds

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

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