



Cisco ASR 5000 Series Network Address Translation Administration Guide Addendum Version 12.2

Last Updated January 09, 2012

Americas Headquarters

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

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

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

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

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

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

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

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

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

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

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

Cisco ASR 5000 Series Network Address Translation Administration Guide Addendum

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

CONTENTS





About this Guide	V
Conventions Used.....	vi
Contacting Customer Support	viii
Affected Documents	9
NAT ICSR Flow Checkpointing.....	11
NAT ICSR Flow Checkpointing Overview.....	12
NAT ICSR Flow Checkpointing Configuration	13
CLI Command Reference.....	14
Firewall-and-NAT Policy Configuration Mode Commands.....	14
nat icsr-flow-recovery	14
Statistics and Counters Reference	15
show active-charging fw-and-nat policy name	15

About this Guide

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

Conventions Used

The following tables describe the conventions used throughout this documentation.

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

Typeface Conventions	Description
Text represented as a <code>screen display</code>	This typeface represents displays that appear on your terminal screen, for example: <code>Login:</code>
Text represented as commands	This typeface represents commands that you enter, for example: <code>show ip access-list</code> 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: <code>show card slot_number</code> <code>slot_number</code> is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New

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

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

Contacting Customer Support

Use the information in this section to contact customer support.

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

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



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

Chapter 1

Affected Documents

This addendum provides new and/or expanded information pertaining to the Network Address Translation documentation delivered as part of the 12.2 release.

Documentation updates provided in this addendum pertain to the documents listed in the following table and correspond to the stated release date(s):

Document	Part Number	Release Date
<i>Cisco ASR 5000 Series Network Address Translation Administration Guide: Version 12.2</i>	OL-25618-01	October 17, 2011
<i>Cisco ASR 5000 Series Command Line Interface Reference: Version 12.2</i>	OL-25551-01	October 17, 2011
<i>Cisco ASR 5000 Series Statistics and Counters Reference: Version 12.2</i>	OL-25556-01	October 17, 2011

Chapter 2

NAT ICSR Flow Checkpointing

This chapter describes the NAT ICSR Flow-recovery Checkpointing feature.

This chapter covers the following topics:

- [NAT ICSR Flow Checkpointing Overview](#)
- [NAT ICSR Flow Checkpointing Configuration](#)
- [CLI Command Reference](#)
- [Statistics and Counters Reference](#)

NAT ICSR Flow Checkpointing Overview

The ICSR feature provides the highest possible availability for continuous call processing without interrupting subscriber services. This feature allows the operator to utilize geographically distant gateways for redundancy purposes. In the event of a node or gateway failure, ICSR allows sessions to be transparently routed around the failure, thus maintaining the user experience and also session information and state.

ICSR is accomplished through the use of redundant chassis. The chassis are configured as primary and backup, with one being active and one standby. Both chassis are connected to the same AAA server. A checkpoint duration timer is used to control when subscriber data is sent from the active chassis to the standby chassis. If the active chassis handling the call traffic goes out of service, the standby chassis transitions to the active state and continues processing the call traffic without interrupting the subscriber session. The chassis determines which is active through a propriety TCP-based connection called a redundancy link. This link is used to exchange Hello messages between the primary and backup chassis and must be maintained for proper system operation.

For NAT flow recovery, the following behaviour is supported:

- One-to-one NAT: Since NAT IP address being used for one-to-one NAT is recovered and as one-to-one NAT does not change the port, on-going flows will be recovered as part of Firewall Flow Recovery algorithm.
- Many-to-one NAT: On-going flows will not be recovered as the port numbers being used for flows across chassis peers/SessMgr peers are not preserved. It is now possible to enable/disable the checkpointing of NATed flows and control the type of flows to be checkpointed based on criteria. Check pointing is done only for TCP and UDP flows. Many-to-one NAT flow recovery is also supported for ICSR.
- Bypass NAT Flow: On-going flows will be recovered as part of Firewall Flow Recovery algorithm.

The NAT Flow checkpointing is done when the checkpoint criteria present in the Firewall-and-NAT policy is met. In the current 12.2 release, support is provided to enable or disable all the NAT ICSR Flow checkpointing.

NAT ICSR Flow Checkpointing Configuration

To enable/disable and configure NAT Flow checkpointing for ICSR, use the following configuration:

configure

```
active-charging service <acs_service_name>

fw-and-nat policy <policy_name>

[ default | no ] nat icsr-flow-recovery

end
```

Notes:

- For more information on Active Charging Service configuration, refer to the *Cisco ASR 5000 Series Enhanced Charging Services Administration Guide*.
- By default, NAT Flow-recovery checkpointing for ICSR is disabled.

CLI Command Reference

This section provides details of new CLI commands required to enable or disable NAT ICSR Flow checkpointing.

Firewall-and-NAT Policy Configuration Mode Commands

nat icsr-flow-recovery

This command enables/disables the NAT ICSR Flow checkpointing support for subscribers in a Firewall-and-NAT policy.

Product

NAT

Privilege

Security Administrator, Administrator

Syntax

```
[ default | no ] nat icsr-flow-recovery
```

default

Configures the default setting.

Default: Disabled. Same as **no nat icsr-flow-recovery**.

no

Disables the NAT ICSR Flow checkpointing.

Usage

Use this command to enable/disable all NAT ICSR Flow checkpointing for subscribers using this policy.

Example

The following command enables NAT ICSR Flow checkpointing:

```
nat icsr-flow-recovery
```

Statistics and Counters Reference

This section provides details of new statistics in support of NAT ICSR Flow-recovery checkpointing.

show active-charging fw-and-nat policy name

Table 1. show active-charging fw-and-nat policy name Command Output Descriptions

Field	Description
ICSR Flow-recovery Status	
Non-ALG	Indicates whether ICSR flow-recovery is enabled or disabled for non-ALGs in the Firewall-and-NAT policy.
SIP-ALG	Indicates whether ICSR flow-recovery is enabled or disabled for SIP ALG in the Firewall-and-NAT policy.