

Network Address Translation for JSF



Published: 2011-05-06

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Network Address Translation for JSF
Copyright © 2011, Juniper Networks, Inc.
All rights reserved.

Revision History
May 2011—R1 Network Address Translation for JSF 11.2

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

- a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.
- b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.
- c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.
- d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.
- e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is "commercial computer software" and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14 (ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License ("GPL") or the GNU Library General Public License ("LGPL")), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at <http://www.gnu.org/licenses/gpl.html>, and a copy of the LGPL at <http://www.gnu.org/licenses/lgpl.html>.

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

Part 1	Overview
Chapter 1	Network Address Translation 3
	Network Address Translation Overview for JSF 3
	Translation Types 4
	IPv4 to IPv4 Traditional NAT 4
	Basic NAT 5
	NAPT 5
	Basic NAT 5
	NAPT 6
	Dynamic NAT 6
	Static Destination NAT 6
Part 2	Configuration
Chapter 2	Configuration Tasks 11
	Configuring Addresses and Ports for Use in NAT Rules 11
	Configuring Pools of Addresses and Ports 11
	Pool Configuration Constraints for NAT 12
	Specifying Destination and Source Prefixes 12
	Requirements for NAT Addresses 13
	Configuring NAT Rules 14
	Configuring Match Direction for NAT Rules 15
	Configuring Match Conditions in NAT Rules 15
	Configuring Actions in NAT Rules 17
	Configuring NAT Rule Sets 19
	Configuring Juniper Service Framework – Network Address Translation Package, Rules, and Services Set 19
	Configuring the JSF NAT Package 20
	Configuring the NAT Rule and NAT Pool 22
	Configuring the Services Set for NAT 24
	Configuring Static Source Translation in IPv4 Networks 26
	Configuring the NAT Pool and Rule 26
	Configuring the Service Set for NAT 27
	Configuring Trace Options 28
	Configuring Dynamic Source Address and Port Translation in IPv4 Networks . . . 29
	Configuring Dynamic Address-Only Source Translation in IPv4 Networks 31
	Configuring Static Destination Address Translation in IPv4 Networks 34

Chapter 3	NAT Rules Examples	37
	Example: Configuring Dynamic Address-only Source Translation	37
	Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network	38
	Example: Configuring Dynamic Source Translation (NAPT)	38
	Example: Configuring Dynamic Source Translation for an IPv4 Network	39
	Example: Configuring Static Source Translation	39
	Example: Configuring Dynamic and Static Source Translation	40
	Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges	41
	Example: Configuring NAT Rules Without Defining a Pool	41
	Example: Preventing Translation of Specific Addresses	42
	Example: Configuring NAT for Multicast Traffic	42
	Rendezvous Point Configuration	43
	Router 1 Configuration	46
	Example: Configuring Static Destination Address Translation	46
Chapter 4	Configuration Statements	49
	address	49
	address-allocation	49
	address-range	50
	application-sets	50
	applications	51
	destination-address	51
	destination-address-range	52
	destination-pool	52
	destination-prefix	53
	destination-prefix-list	53
	from	54
	hint	55
	match-direction	55
	no-translation	56
	pgcp	56
	pool	57
	port	58
	ports-per-session	58
	remotely-controlled	59
	rule	60
	rule-set	61
	services	61
	source-address	62
	source-address-range	62
	source-pool	63
	source-prefix	63
	source-prefix-list	64
	syslog	64
	term	65
	then	66
	translated	67

	translation-type	68
	transport	68
Part 3	Administration	
Chapter 5	Network Address Translation Operational Mode Commands	71
	show services nat pool	72
Part 4	Troubleshooting	
Chapter 6	Knowledge Base	77
Part 5	Index	
	Index	81
	Index of Statements and Commands	85

List of Figures

Part 2

Configuration

Chapter 3

NAT Rules Examples 37

Figure 1: Configuring NAT for Multicast Traffic 42

List of Tables

Part 3

Administration

Chapter 5

Network Address Translation Operational Mode Commands 71

Table 1: show services nat pool Output Fields 72

PART 1

Overview

- Network Address Translation on page 3

CHAPTER 1

Network Address Translation

- Network Address Translation Overview for JSF on page 3
- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Network Address Translation Overview for JSF

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks.

NAT is supported on Junos Services Framework (JSF). JSF is a unified framework for the integration of services on Junos OS-based platforms.



NOTE: Junos operating system (Junos OS) supports NAT on IPv4 and IPv6 networks. However, JSF does not support NAT on IPv6 networks. Therefore, ensure that IPv4 networks are used for configuring NAT on JSF.

For more information about NAT, refer to the following topics:

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Translation Types

The Multiservices PIC interfaces support the following types of translation:

- Static-source translation—Allows you to hide a private network without using NAPT (Network Address Port Translation). It features one-to-one mapping between the original address and the translated address, and mapping is configured statically. For more information, see “Basic NAT” on page 5.
- Dynamic-source translation—Includes two options: dynamic address-only source translation and Network Address Port Translation (NAPT).
 - Dynamic address-only source translation—A NAT address is picked up dynamically from a source NAT pool and the mapping from the original source address to the translated address is maintained as long as there is at least one active flow that uses this mapping. For more information, see “Dynamic NAT” on page 6.
 - NAPT—Both the original source address and the source port are translated. The translated address and port are picked up from the corresponding NAT pool. For more information, see “NAPT” on page 6.
- Static destination translation—Allows you to make selected private servers accessible. It features one-to-one mapping between the translated address and the destination address, and mapping is configured statically. For more information, see “Static Destination NAT” on page 6.

Junos OS supports NAT functionality described in the following RFCs and Internet drafts:

- RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*
- RFC 4787, *NAT Behavioral Requirements for Unicast UDP*
- RFC 5382, *NAT Behavioral Requirements for TCP*
- RFC 5508, *NAT Behavioral Requirements for ICMP*

Related Documentation

- IPv4 to IPv4 Traditional NAT on page 4
- Basic NAT on page 5
- NAPT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

IPv4 to IPv4 Traditional NAT

Basic Network Address Translation or Basic NAT is a method by which IP addresses are mapped from one group to another, transparent to end users. Network Address Port Translation or NAPT is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. Together, these two operations, referred

to as traditional NAT, provide a mechanism to connect a realm with private addresses to an external realm with globally unique registered addresses.

Traditional NAT, specified in RFC 3022, *Traditional IP Network Address Translator*, is fully supported by Junos OS. In addition, network address port translation (NAPT) is supported for source addresses.

Basic NAT

With Basic NAT, a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, Basic NAT translates source IP addresses and related fields such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, the destination IP address and the checksums listed above are translated.

NAPT

Use Network Address Port Translation (NAPT) to enable the components of the private network to share a single external address. NAPT translates the transport identifier (for example, TCP port number, UDP port number, or ICMP query ID) of the private network into a single external address. NAPT can be combined with Basic NAT to use a pool of external addresses in conjunction with port translation.

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier (TCP/UDP port or ICMP query ID), and related fields, such as IP, TCP, UDP, and ICMP header checksums. For inbound packets, the destination IP address, the destination transport identifier, and the IP and transport header checksums are translated.

Related Documentation

- Translation Types on page 4
- Dynamic NAT on page 6
- Static Destination NAT on page 6

Basic NAT

With Basic NAT, a block of external addresses are set aside for translating addresses of hosts in a private domain as they originate sessions to the external domain. For packets outbound from the private network, the Basic NAT translates source IP address and related fields such as IP, TCP, UDP and ICMP header checksums. For inbound packets, the destination IP address and the checksums as listed above are translated.

Related Documentation

- Translation Types on page 4
- IPv4 to IPv4 Traditional NAT on page 4
- NAPT on page 6
- Dynamic NAT on page 6
- Static Destination NAT on page 6

NAPT

Network address port translation (NAPT) is a mechanism that allows a private network to share a single external address. NAPT translates the transport identifier (for example, the TCP and UDP port numbers or the ICMP query ID) of the private network into a single external address. NAPT can be combined with Basic NAT to use a pool of external addresses in conjunction with port translation.

For packets outbound from the private network, NAPT translates the source IP address, source transport identifier (TCP/UDP port or ICMP query ID) and related fields, such as IP, TCP, UDP and ICMP header checksums. For inbound packets, the destination IP address, destination transport identifier and the IP and transport header checksums are translated.

- Related Documentation**
- Translation Types on page 4
 - IPv4 to IPv4 Traditional NAT on page 4
 - Basic NAT on page 5
 - Dynamic NAT on page 6
 - Static Destination NAT on page 6

Dynamic NAT

Dynamic NAT is a mechanism with which a private IP address (source) is mapped to a public IP address drawing from a pool of registered (public) IP addresses. NAT addresses from the pool are assigned dynamically. Assigning addresses dynamically also allows a few public IP addresses to be used by several private hosts in contrast with an equal-sized pool required by source static NAT.

For more information about dynamic address translation, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*

- Related Documentation**
- Translation Types on page 4
 - IPv4 to IPv4 Traditional NAT on page 4
 - Basic NAT on page 5
 - NAPT on page 6
 - Static Destination NAT on page 6

Static Destination NAT

Static destination NAT translates the destination address for external traffic to an address specified in a destination pool. The destination pool contains one address and no port configuration.

For more information about static address translation, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

- Related Documentation**
- Translation Types on page 4
 - IPv4 to IPv4 Traditional NAT on page 4
 - Basic NAT on page 5
 - NAT on page 6
 - Dynamic NAT on page 6

PART 2

Configuration

- Configuration Tasks on page 11
- NAT Rules Examples on page 37
- Configuration Statements on page 49

CHAPTER 2

Configuration Tasks

- Configuring Addresses and Ports for Use in NAT Rules on page 11
- Configuring NAT Rules on page 14
- Configuring NAT Rule Sets on page 19
- Configuring Juniper Service Framework – Network Address Translation Package, Rules, and Services Set on page 19
- Configuring Static Source Translation in IPv4 Networks on page 26
- Configuring Dynamic Source Address and Port Translation in IPv4 Networks on page 29
- Configuring Dynamic Address-Only Source Translation in IPv4 Networks on page 31
- Configuring Static Destination Address Translation in IPv4 Networks on page 34

Configuring Addresses and Ports for Use in NAT Rules

For information about configuring translated addresses, see the following sections:

- Configuring Pools of Addresses and Ports on page 11
- Specifying Destination and Source Prefixes on page 12

Configuring Pools of Addresses and Ports

To configure pools for NAT, you need to specify a destination pool or a source pool. You use the **pool** statement to define the addresses that constitute the pool. You can define the pool by specifying addresses (or prefixes), address ranges, and ports that need to be used for network address translation.

To configure a NAT pool, include the **pool** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
pool nat-pool-name {
  address ip-prefix </prefix-length>;
  address-range low minimum-value high maximum-value;
  port (automatic | range low minimum-value high maximum-value)
    preserve-parity
    preserve-range {
  }
}
```

The **address** statement specifies the addresses that constitute the pool. Using this statement, you define the pool by specifying the IP address and IP address prefix.

The **address-range** statement also specifies the addresses that constitute the pool. Using this statement, you define the pool by specifying an address range. In an address range, the **low** value must be a lower number than the **high** value. When multiple address ranges and prefixes are configured, the prefixes are depleted first, followed by the address ranges.

The **port** statement specifies port assignment for the translated addresses. To configure automatic assignment of ports, include the **port automatic** statement at the **[edit services nat pool nat-pool-name]** hierarchy level. To configure a specific range of port numbers, include the **port range low minimum-value high maximum-value** statement at the **[edit services nat pool nat-pool-name]** hierarchy level. By default, Junos OS allocates NAT ports sequentially. To change the way ports are allocated, you can use the **preserve-parity** command, which allocates even ports for packets with even destination ports and odd ports for packets with odd destination ports, or the **preserve-range** command, which allocates ports within a range from 0 through 1023 assuming the original packet contains a destination port in the reserved range. This behavior is applicable to control sessions and not data sessions.

Pool Configuration Constraints for NAT

You must consider the following constraints when configuring a pool for NAT:

- For static source NAT and dynamic source NAT, you can specify multiple IPv4 addresses (or prefixes) and IPv4 address ranges. Up to 32 prefixes or address ranges (or a combination) can be supported within a single pool.
- For static source NAT, the prefixes and address ranges cannot overlap between separate pools.
- For static destination NAT, you can specify multiple address prefixes and address ranges in a single term. Multiple destination NAT terms can share a destination NAT pool. However, the netmask or range for the **from** address must be smaller or equal to the netmask or range for the destination pool address. If you define the pool to be larger than required, some addresses are not used. For example, if you define the pool size as 100 addresses and the rule specifies only 80 addresses, the last 20 addresses in the pool are not used.
- When you specify a port for dynamic source NAT, address ranges are limited to a maximum of 65,000 addresses, for a total of (65,000 x 65,535) or 4,259,775,000 flows. A dynamic NAT pool with no address port translation supports up to 65,535 addresses. There is no limit on the pool size for static source NAT.
- With Network Address Port Translation (NAPT), you can configure up to 32 address ranges with up to 65,536 addresses each.

For constraints on specific translation types, see “Configuring Actions in NAT Rules” on page 17.

Specifying Destination and Source Prefixes

You can directly specify the destination or source prefix used in network address translation without configuring a pool.

To configure the information, include the **rule** statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  term term-name {
    then {
      translated {
        destination-prefix prefix;
      }
    }
  }
}
```

Requirements for NAT Addresses

When configuring NAT addresses, keep in mind the following requirements:

- The following addresses, while valid in **inet.0**, cannot be used for NAT translation:
 - **0.0.0.0/32**
 - **127.0.0.0/8** (loopback)
 - **128.0.0.0/16** (martian)
 - **191.255.0.0/16** (martian)
 - **192.0.0.0/24** (martian)
 - **223.255.255.0/24** (martian)
 - **224.0.0.0/4** (multicast)
 - **240.0.0.0/4** (reserved)
 - **255.255.255.255** (broadcast)
- You can specify one or more IPv4 address prefixes in the **pool** statement and in the **from** clause of the NAT rule term. This enables you to configure source translation from a private subnet to a public subnet without defining a rule term for each address in the subnet. Destination translation cannot be configured by this method.
- When you configure static source NAT, the **address** prefix size you configure at the **[edit services nat pool pool-name]** hierarchy level must be larger than the **source-address** prefix range configured at the **[edit services nat rule rule-name term term-name from]** hierarchy level. The **source-address** prefix range must also map to a single subnet or range of IPv4 addresses in the **pool** statement. Any pool addresses that are not used by the **source-address** prefix range are left unused; pools cannot be shared.



NOTE: When you include a NAT configuration that changes IP addresses, the configuration might affect forwarding path features elsewhere in your router configuration, such as source class usage (SCU), destination class usage (DCU), filter-based forwarding, or other features that target specific IP addresses or prefixes.

NAT configuration might also affect routing protocols operation, because the protocol peering, neighbor, and interface addresses can be altered when routing protocols packets transit the Multiservices PIC.

Related Documentation

- Network Address Translation Overview for JSF on page 3
- Example: Configuring Dynamic Address-only Source Translation on page 37
- Example: Configuring Dynamic Source Translation (NAPT) on page 38
- Example: Configuring Static Source Translation on page 39
- Example: Configuring Dynamic and Static Source Translation on page 40
- Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges on page 41
- Example: Configuring NAT Rules Without Defining a Pool on page 41

Configuring NAT Rules

To configure a NAT rule, include the **rule** *rule-name* statement at the **[edit services nat]** hierarchy level:

```
[edit services nat]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      application-sets set-name;
      applications [ application-names ];
      destination-address (address | any-unicast) <except>;
      destination-address-range low minimum-value high maximum-value <except>;
      destination-prefix-list list-name <except>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
      source-prefix-list list-name <except>;
    }
    then {
      no-translation;
      translated {
        destination-pool nat-pool-name;
        destination-prefix prefix;
        source-pool nat-pool-name;
        source-prefix prefix;
        translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
      }
    }
  }
}
```

```

        syslog;
    }
}

```

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied.

In addition, each NAT rule consists of a set of terms, similar to a firewall filter. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software.

The following sections explain how to configure the components of NAT rules:

- Configuring Match Direction for NAT Rules on page 15
- Configuring Match Conditions in NAT Rules on page 15
- Configuring Actions in NAT Rules on page 17

Configuring Match Direction for NAT Rules

Each rule must include a **match-direction** statement that specifies the direction in which the match is applied. To configure where the match is applied, include the **match-direction** statement at the **[edit services nat rule rule-name]** hierarchy level:

```

[edit services nat rule rule-name]
  match-direction (input | output);

```

The match direction is used with respect to the traffic flow through the Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it. The criteria for determining packet direction is as follows:

- With an interface service set, packet direction is determined by whether a packet is entering or leaving the interface on which the service set is applied.
- With a next-hop service set, packet direction is determined by the interface used to route the packet to the Multiservices PIC. If the inside interface is used to route the packet, the packet direction is input. If the outside interface is used to direct the packet to the PIC, the packet direction is output..
- On the Multiservices PIC, a flow lookup is performed. If no flow is found, rule processing is performed. All rules in the service set are considered. During rule processing, the packet direction is compared against rule directions. Only rules with direction information that matches the packet direction are considered.

Configuring Match Conditions in NAT Rules

To configure NAT match conditions, include the **from** statement at the **[edit services nat rule rule-name term term-name]** hierarchy level:

```

[edit services nat rule rule-name term term-name]
  from {

```

```
application-sets set-name;
applications [ application-names ];
destination-address (address | any-unicast) <except>;
destination-address-range low minimum-value high maximum-value <except>;
destination-prefix-list list-name <except>;
source-address (address | any-unicast) <except>;
source-address-range low minimum-value high maximum-value <except>;
source-prefix-list list-name <except>;
}
```

To configure traditional NAT, you can use the destination address, a range of destination addresses, the source address, or a range of source addresses as a match condition, in the same way that you would configure a firewall filter; for more information, see the [Junos OS Routing Policy Configuration Guide](#).

Alternatively, you can specify a list of source or destination prefixes by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or **source-prefix-list** statement in the NAT rule.



NOTE: If you configure a service set with a destination NAT rule, the address configured in the **from** condition must be translated. If the service set is deleted from the interface and you want traffic destined to the address to be forwarded without translation, you must explicitly deactivate either the service set or the NAT rule within the service set.

You can include application protocol definitions that you have configured at the **[edit applications]** hierarchy level:

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services nat rule rule-name term term-name from]** hierarchy level.
- To apply one or more sets of application protocol definitions that you have defined, include the **application-sets** statement at the **[edit services nat rule rule-name term term-name from]** hierarchy level.



NOTE: If you include one of the statements that specifies application protocols, the router derives port and protocol information from the corresponding configuration at the **[edit applications]** hierarchy level; you cannot specify these properties as match conditions. When matched rules include more than one ALG, the more specific ALG takes effect; for example, if the stateful firewall rule includes TCP and the NAT rule includes FTP, the NAT rule takes precedence.

You can configure ALGs for ICMP and trace route under stateful firewall and NAT.

By default, NAT can restore IP, TCP, and UDP headers embedded in the payload of ICMP error messages. You can include the **protocol tcp** and **protocol udp** statements with the **application** statement for NAT configurations.

Configuring Actions in NAT Rules

To configure NAT actions, include the **then** statement at the **[edit services nat rule rule-name term term-name]** hierarchy level:

```
[edit services nat rule rule-name term term-name]
then {
  >no-translation;
  syslog;
  translated {
    destination-pool nat-pool-name;
    destination-prefix prefix;
    source-pool nat-pool-name;
    source-prefix prefix;
    translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
  }
}
```

The **no-translation** statement allows you to specify addresses that you want to be excluded from NAT.

The **syslog** statement enables you to record an alert in the system logging facility.

The **destination-pool**, **destination-prefix**, **source-pool**, and **source-prefix** statements specify addressing information that you define by including the **pool** statement at the **[edit services nat]** hierarchy level; for more information, see “Configuring Addresses and Ports for Use in NAT Rules” on page 11.

The **translation-type** statement specifies the type of network address translation used for source or destination traffic. Choices are **basic-nat44**, **dynamic-nat44**, **napt44**, or **dnat-44**, which are explained in the following list. For more information, see “Network Address Translation Overview for JSF” on page 3.



NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in IPv4 networks. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in IPv6 networks. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not mentioned here.

- **basic-nat44**—Implement static translation of source IP addresses without port mapping. You must configure the **from destination-address** statement in the match condition for the rule. The size of the address range specified in the statement must be the same or smaller than the destination pool. You must specify either a **destination-pool** or a **destination-prefix**. The referenced pool can contain multiple addresses but no **port** configuration.



NOTE: In an interface service set, all packets destined for the **destination-address** specified in the match condition are automatically routed to the services PIC, even if no service set is associated with the interface.

- **dynamic-nat44**—Implement dynamic translation of source IP addresses without port mapping. You must specify a **source-pool** name. The referenced pool must include an **address** configuration (for address-only translation).

The **dynamic-nat44** option supports translating up to 64,000 addresses to a smaller size pool. The requests from the source address range are assigned to the addresses in the pool until the pool is used up, and any additional requests are rejected. A NAT address assigned to a host is used for all concurrent sessions from that host. The address is released to the pool only after all the sessions for that host expire. This feature enables the router to share a few public IP addresses between several private hosts. Since all the private hosts might not simultaneously create sessions, they can share a few public IP addresses.

- **napt44**—Implement dynamic address translation for destination traffic with port mapping. You must specify a **source-pool** name. The referenced pool must include a port configuration (for NAPT). The **napt44** option supports translating up to 32 addresses to a smaller size pool.

If you specify **port automatic** or a port range, NAPT is used. If a port is not defined, the port value defaults to 1.

- **dnat-44**—Implement static translation of destination IP addresses without port mapping. The size of the pool address space must be greater than or equal to the source address space. You must specify a **source-pool** name. The referenced pool can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of source addresses in the **from** statement. You must include exactly one **source-address** value at the **[edit services nat rule rule-name term term-name from]** hierarchy level; if it is a prefix, the size must be less than or equal to the pool prefix size. Any addresses in the pool that are not matched in the **source-address** value remain unused, because a pool cannot be shared among multiple terms or rules.



NOTE: When configuring NAT, if any traffic is destined for the following addresses and does not match a NAT flow or NAT rule, the traffic is dropped:

- Addresses specified in the **from destination-address** statement, when you are using destination translation
- Addresses specified in the source NAT pool when you are using source translation

For more information on NAT methods, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

Related Documentation

- Network Address Translation Overview for JSF on page 3
- Configuring Addresses and Ports for Use in NAT Rules on page 11
- Configuring NAT Rule Sets on page 19

Configuring NAT Rule Sets

The **rule-set** statement defines a collection of NAT rules that determine what actions the router software performs on packets in the data stream. You define each rule by specifying a rule name and configuring terms. Then, you specify the order of the rules by including the **rule-set** statement at the **[edit services nat]** hierarchy level with a **rule** statement for each rule:

```
rule-set rule-set-name {
  rule rule-name;
}
```

The router software processes the rules in the order in which you specify them in the configuration. If a term in a rule matches the packet, the router performs the corresponding action and the rule processing stops. If no term in a rule matches the packet, processing continues to the next rule in the rule set. If none of the rules matches the packet, no NAT action is performed on the packet. If a packet is destined to a NAT pool address, it is dropped.

Configuring Juniper Service Framework – Network Address Translation Package, Rules, and Services Set

Network Address Translation (NAT) is a mechanism for concealing a set of host addresses on a private network behind a pool of public addresses. It can be used as a security measure to protect the host addresses from direct targeting in network attacks. The Junos operating system (Junos OS) supports NAT on IPv4 networks. To use Junos Services Framework (JSF) to run NAT, you must configure the **jservices-nat** package at the

hierarchy level. In addition, you must configure NAT rules and a service set with a Multiservice interface. This topic includes the following tasks:

1. Configuring the JSF NAT Package on page 20
2. Configuring the NAT Rule and NAT Pool on page 22
3. Configuring the Services Set for NAT on page 24

Configuring the JSF NAT Package

To configure the JSF-NAT package:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit chassis
```

2. In the hierarchy level, configure the FPC and PIC.

```
[edit chassis]
user@host# edit fpc slot pic slot
```

In this example, the FPC is in slot 1 and the PIC is in slot 0:

```
[edit chassis]
user@host# edit fpc 1 pic 0
```

3. Configure the number of cores dedicated to run control functionality.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider control-cores
control-cores
```

In this example, the number of control cores is 1.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider control-cores
1
```

4. Configure the number of processing cores dedicated to data.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider data-cores
data-cores
```

In this example, the number of data cores is 7.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider data-cores 7
```

5. Configure the size of the object cache in megabytes (MB). Only values in increments of 128 MB are allowed and the maximum value of the object cache can be 1280 MB.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider
object-cache-size object-cache-size
```

In this example, the size of the object cache is 512 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider
object-cache-size 512
```

6. Configure the size of the policy database in megabytes (MB).

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider policy-db-size
policy-db-size
```

In this example, the size of the policy database is 64 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider policy-db-size
64
```

7. Configure the package.

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider package
package
```

In this example, the package is `jservices-nat`.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider package
jservices-nat
```

8. Configure the extension provider system log, to enable PIC system logging to record or view system log messages:

```
[edit chassis fpc slot pic slot]
user@host# set adaptive-services service-package extension-provider syslog syslog
```

In this example, the system log is set to `daemon any` and `external any`:

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog daemon
any
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider syslog external
any
```

9. Verify the configuration.

```
[edit chassis]
user@host# show chassis
fpc 1 {
  pic 0 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 7;
          object-cache-size 512;
          policy-db-size 64;
          package jservices-nat;
          syslog {
            daemon any;
            external any;
```

```
}  
}  
}  
}  
}
```

Configuring the NAT Rule and NAT Pool

To configure the NAT pool and NAT rule:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit services
```

2. Configure the NAT pool.

```
[edit services]  
user@host# set nat pool pool
```

In this example, the NAT pool is **p1**.

```
[edit services]  
user@host# set nat pool p1
```

3. Configure the NAT pool address.

```
[edit services]  
user@host# set nat pool p1 address address
```

In this example, the NAT pool address is **20.1.1.10/32**.

```
[edit services]  
user@host# set nat pool p1 address 20.1.1.10/32;
```

4. Configure the NAT pool port.

```
[edit services]  
user@host# set nat pool p1 port port;
```

In this example, the NAT pool port is **automatic**.

```
[edit services]  
user@host# set nat pool p1 port automatic;
```

5. Configure the rule.

```
[edit services]  
user@host# set nat rule rule
```

In this example, the rule is **r1**.

```
[edit services]  
user@host# set nat rule r1
```

6. Configure the match direction.

```
[edit services]  
user@host# set nat rule r1 match-direction match-direction
```

In this example, the match direction is **input**.

```
[edit services]
```

```
user@host# set nat rule r1 match-direction input
```

7. Configure the term.

```
[edit services]
user@host# set nat rule r1 term term
```

In this example, the term is **t1**.

```
[edit services]
user@host# set nat rule r1 term t1
```

8. Configure the input conditions for the NAT term.

```
[edit services]
user@host# set nat rule r1 term t1 from from
```

In this example, the input conditions are **applications junos-tftp** and **applications junos-rsh**.

```
[edit services]
user@host# set nat rule r1 term t1 from applications junos-tftp
[edit services]
user@host# set nat rule r1 term t1 from applications junos-rsh
```

9. Configure the NAT term action.

```
[edit services]
user@host# set nat rule r1 term then then
```

In this example, the term action is **translated**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated
```

10. Configure the properties for translated traffic.

```
[edit services]
user@host# set nat rule r1 term then translated translated
```

In this example, the property for the translated traffic is **source-pool p1**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated source-pool p1
```

11. Configure the properties for translated traffic transaction type.

```
[edit services]
user@host# set nat rule r1 term then translated translation-type translation type
```

In this example, the property for the translated traffic is **dynamic-nat44**.

```
[edit services]
user@host# set nat rule r1 term t1 then translated translation-type dynamic-nat44
```

12. Verify the configuration:

```
[edit services]
user@host# show
}
nat {
  pool p1 {
    address 20.1.1.10/32;
    port {
```

```
        automatic;
    }
}
rule r1 {
    match-direction input;
    term t1 {
        from {
            applications [ junos-tftp junos-rsh ];
        }
        then {
            translated {
                source-pool p1;
                translation-type dynamic-nat44;
            }
        }
    }
}
```

Configuring the Services Set for NAT

To configure the services set for NAT:

1. In configuration mode, go to the following hierarchy level:

```
user@host# edit services
```

2. Configure the service set with a rule.

```
[edit services]
user@host# edit service-set service-set
```

In this example, the service set with rule is **nat-ss**.

```
[edit services]
user@host# edit service-set nat-ss
```

3. Configure the service set message rate limit.

```
[edit services service-set nat ss]
user@host# edit syslog syslog
```

In this example, the service set message rate limit is set to **syslog**, which is the maximum number of system log messages per second allowed from this interface.

```
[edit services service-set nat-ss]
user@host# edit syslog
```

4. Configure the host attributes.

```
[edit services service-set nat ss syslog]
user@host# edit host host
```

In this example, the host is **host-local**.

```
[edit services service-set nat-ss syslog]
user@host# edit host host-local
```

5. Configure the services with services attributes.

```
[edit services service-set nat-ss syslog host host-local]
user@host# set services services
```

In this example, the services attributes is **any**.

```
[edit services service-set nat-ss syslog host host-local]
user@host# set services any
```

6. Configure the service set with NAT rules.

```
[edit services service-set nat ss]
user@host# edit nat-rules nat-rules
```

In this example, the NAT rules is **r1**.

```
[edit services service-set nat-ss]
user@host# edit nat-rules r1
```

7. Configure the interface.

```
[edit services service-set nat ss]
user@host# edit interface interface
```

In this example, the interface is **interface-service**.

```
[edit services service-set nat-ss]
user@host# edit interface interface-service
```

8. Configure the service interface.

```
[edit services service-set nat-ss interface-service]
user@host# set service-interfaceservice-interface
```

In this example, the interface is **ms-1/0/0**.

```
[edit services service-set nat-ss interface-service]
user@host# set service-interface ms-1/0/0
```

9. Verify the configuration.

```
[edit services]
user@host# show services
service-set nat-ss {
    syslog {
        host local {
            services any;
        }
    }
    nat-rules r1;
    interface-service {
        service-interface ms-1/0/0;
    }
}
```

Configuring Static Source Translation in IPv4 Networks

To configure the translation type as **basic-nat44**, you must configure the NAT pool and rule, service set with service interface, and trace options. This topic includes the following tasks:

1. Configuring the NAT Pool and Rule on page 26
2. Configuring the Service Set for NAT on page 27
3. Configuring Trace Options on page 28

Configuring the NAT Pool and Rule

To configure the NAT pool, rule, and term:

1. In configuration mode, go to the **[edit services nat]** hierarchy level:

```
[edit]
user@host# edit services nat
```

2. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool name address address
```

In the following example, the pool name is **src_pool** and the address is **10.10.10.2/32**.

```
[edit services nat]
user@host# set pool src_pool address 10.10.10.2/32
```

3. Configure the NAT rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the NAT rule name is **rule-basic-nat44** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 match-direction input
```

4. Configure the source address in the **from** statement.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term term-name from from
```

In the following example, the term name is **t1** and the input condition is **source-address 3.1.1.2/32**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 from source-address 3.1.1.2/32
```

5. Configure the NAT term action and properties of the translated traffic.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then term-action translated-property
```


In the following example, the term action is **translated** and the property of the translated traffic is **source-pool src_pool**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated source-pool src_pool
```

6. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
translation-type
```

In the following example, the translation type is **basic-nat44**.

```
[edit services nat]
user@host# set rule rule-basic-nat44 term t1 then translated translation-type
basic-nat44
```

7. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level:

```
[edit services]
user@host# show
nat {
  pool src_pool {
    address 10.10.10.2/32;
  }
  rule rule-basic-nat44 {
    match-direction input;
    term t1 {
      from {
        source-address {
          3.1.1.2/32;
        }
      }
      then {
        translated {
          source-pool src_pool;
          translation-type {
            basic-nat44;
          }
        }
      }
    }
  }
}
```

Configuring the Service Set for NAT

To configure the service set for NAT:

1. In configuration mode, go to the **[edit services]** hierarchy level:

```
[edit]
user@host# edit services
```

2. Configure the service set.

```
[edit services]
user@host# edit service-set service-set-name
```

In the following example, the service set name is **s1**.

```
[edit services]
user@host# edit service-set s1
```

3. For the **s1** service set, set the reference to the NAT rules configured at the **[edit services nat]** hierarchy level.

```
[edit services service-set s1]
user@host# set nat-rules rule-name
```

In the following example, the rule name is **rule-basic-nat44**.

```
[edit services service-set s1]
user@host# set nat-rules rule-basic-nat44
```

4. Configure the service interface.

```
[edit services service-set s1]
user@host# set interface-service service-interface service-interface-name
```

In the following example, the service interface name is **ms-1/2/0**.

```
[edit services service-set s1]
user@host# set interface-service service-interface ms-1/2/0
```

5. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-basic-nat44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
```

Configuring Trace Options

To configure the trace options at the **[edit services adaptive-services-pics]** hierarchy level:

1. In configuration mode, go to the **[edit services adaptive-services-pics]** hierarchy level:

```
[edit]
user@host# edit services adaptive-services-pics
```

2. Configure the trace options:

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

3. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
```

```
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

Configuring Dynamic Source Address and Port Translation in IPv4 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP (Transmission Control Protocol/User Datagram Protocol) ports are translated into a single network address and its TCP/UDP ports. This translation can be configured in both IPv4 and IPv6 networks. This section describes the steps for configuring NAPT in IPv4 networks.

To configure NAPT, you need to configure a rule at the **[edit services nat]** hierarchy level for dynamically translating the source IPv4 addresses.

To configure the NAPT in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level:

```
[edit]
user@host# edit services
```

2. Configure the service set and NAT rule.

```
[edit services]
user@host# set service-set service-set-name nat-rules rule-name
```

In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-napt-44**.

```
[edit services]
user@host# set service-set s1 nat-rules rule-napt-44
```

3. Go to the **[interface-service]** hierarchy level of the service set.

```
[edit services]
user@host# edit service-set s1 interface-service
```

4. Configure the service interface.

```
[edit services service-set s1 interface service]
user@host# set service-interface service-interface-name
```

In the following example, the name of the service interface is **ms-0/1/0**.



NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1 interface service]
```

```
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **napt-pool** and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool napt-pool address 10.10.10.0
```

7. Configure the port.

```
[edit services nat]
user@host# set pool pool-name port port-type
```

In the following example, the port type is selected as **automatic**.

```
[edit services nat]
user@host# set pool napt-pool port automatic
```

8. Configure the rule and the match direction.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction
```

In the following example, the name of the rule is **rule-napt-44** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input
```

9. Configure the term, the action for the translated traffic, and the translation type.

```
[edit services nat]
user@host# set rule rule-name term term-name then translated translated-action
translation-type translation-type
```

In the following example, the name of the term is **t1**, the action for the translated traffic is **translated**, the name of the source pool is **napt-pool**, and the translation type is **napt-44**.

```
[edit services nat]
user@host# set rule rule-napt-44 match-direction input term t1 then translated
source-pool napt-pool translation-type napt-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
```

```
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-napt-44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool napt-pool {
    address 10.10.10.0/32;
    port {
      automatic;
    }
  }
  rule rule-napt-44 {
    match-direction input;
    term t1 {
      then {
        translated {
          source-pool napt-pool;
          translation-type {
            napt-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

Related Documentation • Example: Configuring Dynamic Source Translation for an IPv4 Network on page 39

Configuring Dynamic Address-Only Source Translation in IPv4 Networks

In IPv4 networks, dynamic address translation (dynamic NAT) is a mechanism to dynamically translate the destination traffic without port mapping. To use dynamic NAT, you must specify a source pool name, which includes an address configuration.

To configure dynamic NAT in IPv4 networks:

1. In configuration mode, navigate to the **[edit services]** hierarchy level.

```
[edit]
user@host# edit services
```

2. Configure the service set and NAT rule.

```
[edit services]
```

```
user@host# set service-set service-set-name nat-rules rule-name
```

In the following example, the name of the service set is **s1**, and the name of the NAT rule is **rule-dynamic-nat44**.

```
[edit services]
user@host# set service-set s1 nat-rules rule-dynamic-nat44
```

3. Go to the **[interface-service]** hierarchy level for the service set.

```
[edit services]
user@host# edit service-set s1 interface-service
```

4. Configure the service interface.

```
[edit services service-set s1 interface-service]
user@host# set service-interface service-interface-name
```

In the following example, the name of the service interface is **ms-0/1/0**.



NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface-service]
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1 interface-service]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, the name of the pool is **source-dynamic-pool**, and the address is **10.10.10.0**.

```
[edit services nat]
user@host# set pool source-dynamic-pool address 10.10.10.0
```

7. Configure the rule, match direction, term, and source address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
source-address address
```

In the following example, the name of the rule is **rule-dynamic-nat44**, the match direction is **input**, the name of the term is **t1**, and the source address is **3.1.1.0**.

```
[edit services nat]
user@host# set rule rule-dynamic-nat44 match-direction input match-direction t1
from source-address 3.1.1.0
```

8. Go to the **[edit rule rule-dynamic-nat-44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dynamic-nat44 term t1
```

9. Configure the source pool and the translation type.

```
[edit services nat rule rule-dynamic-nat44 term t1]
user@host# set then translated source-pool src-pool-name translation-type
translation-type
```

In the following example, the name of the source pool is **source-dynamic-pool** and the translation type is **dynamic-nat44**.

```
[edit services nat rule rule-dynamic-nat44 term t1]
user@host# set then translated source-pool source-dynamic-pool translation-type
dynamic-nat44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat rule rule-dynamic-nat44 term t1]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-dynamic-nat44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool source-dynamic-pool {
    address 10.1.1.0/24;
  }
  rule rule-dynamic-nat44 {
    match-direction input;
    term t1 {
      from {
        source-address {
          3.1.1.0/24;
        }
      }
      then {
        translated {
          destination-pool source-dynamic-pool;
          translation-type {
            dynamic-nat44;
          }
        }
      }
    }
  }
}
```

```
    }  
  }  
  adaptive-services-pics {  
    traceoptions {  
      flag all;  
    }  
  }  
}
```

**Related
Documentation**

- Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network on page 38

Configuring Static Destination Address Translation in IPv4 Networks

In IPv4 networks, destination address translation is a mechanism to implement address translation for destination traffic without port mapping. To use destination address translation, the size of the pool address space must be greater than or equal to the destination address space. You must specify a name for the **destination-pool** statement, which can contain multiple addresses, ranges, or prefixes, as long as the number of NAT addresses in the pool is larger than the number of destination addresses in the **from** statement.

To configure destination address translation in IPv4 networks:

1. In configuration mode, go to the **[edit services]** hierarchy level.

```
[edit]  
user@host# edit services
```

2. Configure the service set and the NAT rule.

```
[edit services]  
user@host# set service-set service-set-name nat-rules rule-name
```

In the following example, the name of the service set is **s1** and the name of the NAT rule is **rule-dnat44**.

```
[edit services]  
user@host# set service-set s1 nat-rules rule-dnat44
```

3. Go to the **[interface-service]** hierarchy level of the service set.

```
[edit services]  
user@host# edit service-set s1 interface-service
```

4. Configure the service interface.

```
[edit services service-set s1 interface-service]  
user@host# set service-interface service-interface-name
```

In the following example, the name of the service interface is **ms-0/1/0**.



NOTE: If the service interface is not present in the router, or the specified interface is not functional, the following command can result in an error.

```
[edit services service-set s1 interface-service]
```



```
user@host# set service-interface ms-0/1/0
```

5. Go to the **[edit services nat]** hierarchy level. Issue the following command from the top of the services hierarchy, or use the **top** keyword.

```
[edit services service-set s1]
user@host# top edit services nat
```

6. Configure the NAT pool with an address.

```
[edit services nat]
user@host# set pool pool-name address address
```

In the following example, **dest-pool** is used as the pool name and **4.1.1.2** as the address.

```
user@host# set pool dest-pool address 4.1.1.2
```

7. Configure the rule, match direction, term, and destination address.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from
destination-address address
```

In the following example, the name of the rule is **rule-dnat44**, the match direction is **input**, the name of the term is **t1**, and the address is **20.20.20.20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from
destination-address 20.20.20.20
```

8. Go to the **[edit services nat rule rule-dnat44 term t1]** hierarchy level.

```
[edit services nat]
user@host# edit rule rule-dnat44 term t1
```

9. Configure the destination pool and the translation type.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool-name translation-type
translation-type
```

In the following example, the destination pool name is **dest-pool**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then translated destination-pool dest-pool translation-type dnat-44
```

10. Go to the **[edit services adaptive-services-pics]** hierarchy level. In the following command, the **top** keyword ensures that the command is run from the top of the hierarchy.

```
[edit services nat rule rule-dnat44 term t1]
user@host# top edit services adaptive-services-pics
```

11. Configure the trace options.

```
[edit services adaptive-services-pics]
user@host# set traceoptions flag tracing parameter
```

In the following example, the tracing parameter is configured as **all**.

```
[edit services adaptive-services-pics]
```

```
user@host# set traceoptions flag all
```

12. Verify the configuration by using the **show** command at the **[edit services]** hierarchy level.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-dnat44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool dest-pool {
    address 4.1.1.2/32;
  }
  rule rule-dnat44 {
    match-direction input;
    term t1 {
      from {
        destination-address {
          20.20.20.20/32;
        }
      }
      then {
        translated {
          destination-pool dest-pool;
          translation-type {
            dnat-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}
```

Related Documentation

- [Example: Configuring Static Destination Address Translation on page 46](#)

CHAPTER 3

NAT Rules Examples

- Example: Configuring Dynamic Address-only Source Translation on page 37
- Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network on page 38
- Example: Configuring Dynamic Source Translation (NAPT) on page 38
- Example: Configuring Dynamic Source Translation for an IPv4 Network on page 39
- Example: Configuring Static Source Translation on page 39
- Example: Configuring Dynamic and Static Source Translation on page 40
- Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges on page 41
- Example: Configuring NAT Rules Without Defining a Pool on page 41
- Example: Preventing Translation of Specific Addresses on page 42
- Example: Configuring NAT for Multicast Traffic on page 42
- Example: Configuring Static Destination Address Translation on page 46

Example: Configuring Dynamic Address-only Source Translation

The following example configures dynamic address-only source translation:

```
[edit services nat]
pool public {
  address-range low 192.16.2.1 high 192.16.2.32;
}
rule Private-Public {
  match-direction input;
  term Translate {
    then {
      translated {
        source-pool public;
        translation-type source dynamic;
      }
    }
  }
}
```

Example: Configuring Dynamic Address-Only Source Translation in an IPv4 Network

The following example configures the translation type as **dynamic-nat44**.

```
[edit services]
user@host# show
service-set s1 {
    nat-rules rule-dynamic-nat44;
    interface-service {
        service-interface ms-0/1/0;
    }
}
nat {
    pool source-dynamic-pool {
        address 10.1.1.0/24;
    }
    rule rule-dynamic-nat44 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    3.1.1.0/24;
                }
            }
            then {
                translated {
                    destination-pool source-dynamic-pool;
                    translation-type {
                        dynamic-nat44;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

Example: Configuring Dynamic Source Translation (NAPT)

The following example configures dynamic source (address and port) translation, or NAPT:

```
[edit services nat]
pool public {
    address-range low 192.16.2.1 high 192.16.2.32;
    port automatic;
}
rule Private-Public {
    match-direction input;
    term Translate {
        then {
            translated {
                source-pool public;
            }
        }
    }
}
```

```

        translation-type source dynamic;
    }
}
}

```



NOTE: The only difference between the configurations for dynamic address-only source translation and NAT is the inclusion of the `port` statement for NAT.

Example: Configuring Dynamic Source Translation for an IPv4 Network

The following example configures the translation type as **napt-44**.

```

[edit services]
user@host# show
service-set s1 {
  nat-rules rule-napt-44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool napt-pool {
    address 10.10.10.0/32;
    port {
      automatic;
    }
  }
  rule rule-napt-44 {
    match-direction input;
    term t1 {
      then {
        translated {
          source-pool napt-pool;
          translation-type {
            napt-44;
          }
        }
      }
    }
  }
}
adaptive-services-pics {
  traceoptions {
    flag all;
  }
}

```

Example: Configuring Static Source Translation

The following configuration sets up one-to-one mapping between a private subnet and a public subnet:

```
[edit services nat]
pool mypool {
  address 192.16.1.0/28; # public subnet
}
rule src-nat {
  match-direction input;
  term t1 {
    from {
      source-address 10.150.1.0/28; # private subnet
    }
    then {
      translated {
        source-pool mypool;
        translation-type source static;
      }
    }
  }
}
```

Example: Configuring Dynamic and Static Source Translation

In the following configuration, **term1** configures source address translation for traffic from any private address to any public address. The translation is applied for all services. **term2** performs destination address translation for Hypertext Transfer Protocol (HTTP) traffic from any public address to the server's virtual IP address. The virtual server IP address is translated to an internal IP address.

```
[edit services nat]
rule my-nat-rule {
  match-direction input;
  term my-term1 {
    from {
      source-address private;
      destination-address public;
    }
    then {
      translated {
        source-pool my-pool; # pick address from a pool
        translation-type source dynamic; # dynamic NAT with port translation
      }
    }
  }
  term my-term2 {
    from {
      destination-address 192.168.137.3; # my server's virtual address
      application http;
    }
    then {
      translated {
        destination-pool nat-pool-name;
        translation-type destination static; # static destination NAT
      }
    }
  }
}
```

Example: Configuring Static Source Translation with Multiple Prefixes and Address Ranges

The following configuration creates a static pool with an address prefix and an address range and uses static source NAT translation.

```
[edit services nat]
pool p1 {
  address 30.30.30.252/30;
  address-range low 20.20.20.1 high 20.20.20.2;
}
rule r1 {
  match-direction input;
  term {
    from {
      source-address {
        10.10.10.252/30;
      }
    }
    then {
      translated {
        source-pool p1;
        translation-type source static;
      }
    }
  }
}
```

Example: Configuring NAT Rules Without Defining a Pool

The following configuration performs network address translation using the source prefix 20.20.10.0/24 without defining a pool.

```
[edit services nat]
rule src-nat {
  match-direction input;
  term t1 {
    then {
      translation-type source dynamic;
      source-prefix 20.20.10.0/24;
    }
  }
}
```

The following configuration performs network address translation using the destination prefix 20.20.10.0/32 without defining a pool.

```
[edit services nat]
rule src-nat {
  match-direction input;
  term t1 {
    from {
      destination-address 10.10.10.10/32;
    }
    then {
```

```

        translation-type destination static;
        destination-prefix 20.20.10.0/24;
    }
}
}
}

```

Example: Preventing Translation of Specific Addresses

The following configuration specifies that network address translation is not performed on incoming traffic from the source address **192.168.20.24/32**. Dynamic NAT is performed on all other incoming traffic.

```

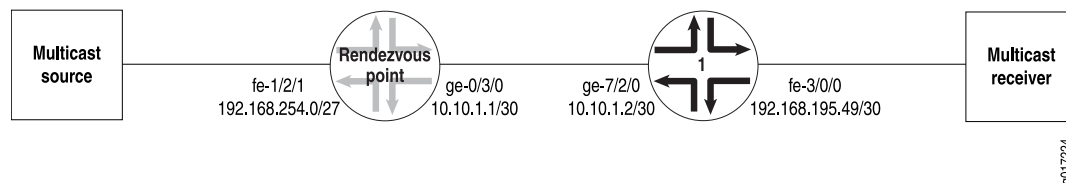
[edit services nat]
pool my-pool {
    address-range low 10.10.10.1 high 10.10.10.16;
    port-automatic;
}
rule src-nat {
    match-direction input;
    term t0 {
        from {
            source-address 192.168.20.24/32;
        }
        then {
            no-translation;
        }
    }
    term t1 {
        then {
            translated {
                translation-type source dynamic;
                source-pool my-pool;
            }
        }
    }
}
}

```

Example: Configuring NAT for Multicast Traffic

Figure 1 on page 42 illustrates the network setup for the following configuration, which allows IP multicast traffic to be sent to the Adaptive Services (AS) or MultiServices PIC.

Figure 1: Configuring NAT for Multicast Traffic



- Rendezvous Point Configuration on page 43
- Router 1 Configuration on page 46

Rendezvous Point Configuration

On the rendezvous point (RP), all incoming traffic from the multicast source at **192.168.254.0/27** is sent to the static NAT pool **mcast_pool**, where its source is translated to **20.20.20.0/27**. The service set **nat_ss** is a next-hop service set that allows IP multicast traffic to be sent to the AS or MultiServices PIC. The inside interface on the PIC is **sp-1/1/0.1** and the outside interface is **sp-1/1/0.2**.

```
[edit services]
nat {
  pool mcast_pool {
    address 20.20.20.0/27;
  }
  rule nat_rule_1 {
    match-direction input;
    term 1 {
      from {
        source-address 192.168.254.0/27;
      }
    }
    then {
      translated {
        source-pool mcast_pool;
        translation-type source static;
      }
      syslog;
    }
  }
}
service-set nat_ss {
  allow-multicast;
  nat-rules nat_rule_1;
  next-hop-service {
    inside-service-interface sp-1/1/0.1;
    outside-service-interface sp-1/1/0.2;
  }
}
```

The Gigabit Ethernet interface **ge-0/3/0** carries traffic out of the RP to Router 1. The adaptive services interface **sp-1/1/0** has two logical interfaces: **unit 1** is the inside interface for next-hop services and **unit 2** is the outside interface for next-hop services. Multicast source traffic comes in on the Fast Ethernet interface **fe-1/2/1**, which has the firewall filter **fbf** applied to incoming traffic.

```
[edit interfaces]
ge-0/3/0 {
  unit 0 {
    family inet {
      address 10.10.1.1/30;
    }
  }
}
sp-1/1/0 {
  unit 0 {
    family inet;
```

```
    }
    unit 1 {
        family inet;
        service-domain inside;
    }
    unit 2 {
        family inet;
        service-domain outside;
    }
}
fe-1/2/1 {
    unit 0 {
        family inet {
            filter {
                input fbf;
            }
            address 192.168.254.27/27;
        }
    }
}
```

Multicast packets can only be directed to the AS or MultiServices PIC using a next-hop service set. In the case of NAT, you must also configure a VRF. Therefore, the routing instance **stage** is created as a “dummy” forwarding instance. To direct incoming packets to **stage**, you configure filter-based forwarding through a firewall filter called **fbf**, which is applied to the incoming interface **fe-1/2/1**. A lookup is performed in **stage.inet.0**, which has a multicast static route that is installed with the next hop pointing to the PIC’s inside interface. All multicast traffic matching this route is sent to the PIC.

```
[edit firewall]
filter fbf {
    term 1 {
        then {
            routing-instance stage;
        }
    }
}
```

The routing instance **stage** forwards IP multicast traffic to the inside interface **sp-1/1/0.1** on the AS or MultiServices PIC:

```
[edit]
routing-instances stage {
    instance-type forwarding;
    routing-options {
        static {
            route 224.0.0.0/4 next-hop sp-1/1/0.1;
        }
    }
}
```

You enable OSPF and Protocol Independent Multicast (PIM) on the Fast Ethernet and Gigabit Ethernet logical interfaces over which IP multicast traffic enters and leaves the RP. You also enable PIM on the outside interface (**sp-1/1/0.2**) of the next-hop service set.

```
[edit protocols]
```

```

ospf {
  area 0.0.0.0 {
    interface fe-1/2/1.0 {
      passive;
    }
    interface lo0.0;
    interface ge-0/3/0.0;
  }
}
pim {
  rp {
    local {
      address 10.255.14.160;
    }
  }
  interface fe-1/2/1.0;
  interface lo0.0;
  interface ge-0/3/0.0;
  interface sp-1/1/0.2;
}

```

As with any filter-based forwarding configuration, in order for the static route in the forwarding instance **stage** to have a reachable next hop, you must configure routing table groups so that all interface routes are copied from **inet.0** to the routing table in the forwarding instance. You configure routing tables **inet.0** and **stage.inet.0** as members of **fbf_rib_group**, so that all interface routes are imported into both tables.

```

[edit routing-options]
interface-routes {
  rib-group inet fbf_rib_group;
}
rib-groups fbf_rib_group {
  import-rib [ inet.0 stage.inet.0 ];
}
multicast {
  rpf-check-policy no_rpf;
}

```

Reverse path forwarding (RPF) checking must be disabled for the multicast group on which source NAT is applied. You can disable RPF checking for specific multicast groups by configuring a policy similar to the one in the example that follows. In this case, the **no_rpf** policy disables RPF check for multicast groups belonging to **224.0.0.0/4**.

```

[edit policy-options]
policy-statement no_rpf {
  term 1 {
    from {
      route-filter 224.0.0.0/4 orlonger;
    }
    then reject;
  }
}

```

Router 1 Configuration

The Internet Group Management Protocol (IGMP), OSPF, and PIM configuration on Router 1 is as follows. Because of IGMP static group configuration, traffic is forwarded out **fe-3/0/0.0** to the multicast receiver without receiving membership reports from host members.

```
[edit protocols]
igmp {
  interface fe-3/0/0.0 {
  }
}
ospf {
  area 0.0.0.0 {
    interface fe-3/0/0.0 {
      passive;
    }
    interface lo0.0;
    interface ge-7/2/0.0;
  }
  pim {
    rp {
      static {
        address 10.255.14.160;
      }
    }
    interface fe-3/0/0.0;
    interface lo0.0;
    interface ge-7/2/0.0;
  }
}
```

The routing option creates a static route to the NAT pool, **mcast_pool**, on the RP.

```
[edit routing-options]
static {
  route 20.20.20.0/27 next-hop 10.10.1.1;
}
```

Example: Configuring Static Destination Address Translation

The following example configures the translation type as **dnat-44**.

```
[edit services]
user@host# show
service-set s1 {
  nat-rules rule-dnat44;
  interface-service {
    service-interface ms-0/1/0;
  }
}
nat {
  pool dest-pool {
    address 4.1.1.2/32;
  }
  rule rule-dnat44 {
    match-direction input;
  }
}
```

```
term t1 {  
  from {  
    destination-address {  
      20.20.20.20/32;  
    }  
  }  
  then {  
    translated {  
      destination-pool dest-pool;  
      translation-type {  
        dnat-44;  
      }  
    }  
  }  
}  
}  
}  
adaptive-services-pics {  
  traceoptions {  
    flag all;  
  }  
}
```


CHAPTER 4

Configuration Statements

address

Syntax	<code>address ip-prefix </prefix-length>;</code>
Hierarchy Level	<code>[edit services nat pool nat-pool-name]</code>
Release Information	Statement introduced before Junos OS Release 7.4. <i>prefix</i> option enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the NAT pool prefix value.
Options	<i>prefix</i> —Specify an IPv4 prefix value.
Usage Guidelines	See “Configuring Addresses and Ports for Use in NAT Rules” on page 11.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

address-allocation

Syntax	<code>address-allocation round-robin</code>
Hierarchy Level	<code>[edit services nat pool pool-name]</code>
Release Information	Statement introduced in Junos OS Release 11.2.
Description	When you use round-robin allocation, one port is allocated from each address in a range before repeating the process for each address in the next range. After ports have been allocated for all addresses in the last range, the allocation process wraps around and allocates the next unused port for addresses in the first range.
Usage Guidelines	See “Configuring Addresses and Ports for Use in NAT Rules” on page 11.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

address-range

Syntax	<code>address-range low <i>minimum-value</i> high <i>maximum-value</i>;</code>
Hierarchy Level	<code>[edit services nat pool <i>nat-pool-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the NAT pool address range.
Options	<i>minimum-value</i> —Lower boundary for the IPv4 address range. <i>maximum-value</i> —Upper boundary for the IPv4 address range.
Usage Guidelines	See “Configuring Addresses and Ports for Use in NAT Rules” on page 11.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

application-sets

Syntax	<code>applications-sets <i>set-name</i>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define one or more target application sets.
Options	<i>set-name</i> —Name of the target application set.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

applications

Syntax	<code>applications [<i>application-names</i>];</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define one or more application protocols to which the NAT services apply.
Options	<i>application-name</i> —Name of the target application.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-address

Syntax	<code>destination-address (<i>address</i> any-unicast) <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced before Junos OS Release 7.4. any-unicast and except options introduced in Junos OS Release 7.6. address option enhanced to support IPv4 and addresses in Junos OS Release 8.5.
Description	Specify the destination address for rule matching.
Options	<i>address</i> —Destination IPv4 or address or prefix value. <i>any-unicast</i> —Any unicast packet. <i>except</i> —(Optional) Prevent the specified address, prefix, or unicast packets from being translated.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-address-range

Syntax	<code>destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 7.6. <i>minimum-value</i> and <i>maximum-value</i> options enhanced to support IPv4 and addresses in Junos OS Release 8.5.
Description	Specify the destination address range for rule matching.
Options	<i>minimum-value</i> —Lower boundary for the IPv4 address range. <i>maximum-value</i> —Upper boundary for the IPv4 address range. <i>except</i> —(Optional) Prevent the specified address range from being translated.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-pool

Syntax	<code>destination-pool <i>nat-pool-name</i>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> then translated]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the destination address pool for translated traffic.
Options	<i>nat-pool-name</i> —Destination pool name.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-prefix

Syntax	<code>destination-prefix <i>destination-prefix</i>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> then translated]</code>
Release Information	Statement introduced in Junos OS Release 7.6. <i>destination-prefix</i> option enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the destination prefix for translated traffic.
Options	<i>destination-prefix</i> —IPv4 destination prefix value.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

destination-prefix-list

Syntax	<code>destination-prefix-list <i>list-name</i> <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 8.2.
Description	Specify the destination prefix list for rule matching. You configure the prefix list by including the prefix-list statement at the [edit policy-options] hierarchy level.
Options	<i>list-name</i> —Destination prefix list. except —(Optional) Exclude the specified prefix list from rule matching.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Junos OS Routing Policy Configuration Guide

from

Syntax	<pre>from { application-sets <i>set-name</i>; applications [<i>application-names</i>]; destination-address (<i>address</i> any-unicast) <except>; destination-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; destination-prefix-list <i>list-name</i> <except>; source-address (<i>address</i> any-unicast) <except>; source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>; }</pre>
Hierarchy Level	[edit services nat rule <i>rule-name</i> term <i>term-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify input conditions for the NAT term.
Options	<p>For information on match conditions, see the description of firewall filter match conditions in the Junos OS Routing Policy Configuration Guide.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

hint

Syntax	hint [<i>hint-strings</i>];
Hierarchy Level	[edit services nat pool <i>nat-pool-name</i> pgcp]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure a hint that enables the BGF to choose a NAT pool by direction rather than by virtual interface. The BGF matches the configured hint with a termination hint located in the Direction field of a nonstandard termination ID.
Default	When no hint is configured, the BGF can choose any NAT pool associated with the virtual interface.
Options	hint-string —Alphanumeric string of up to 3 characters that the BGF uses to match with a termination hint located in the Direction field of a nonstandard termination ID. You can also include underscores (_) and hyphens (-) within the string. To specify a list of hints, use the format: [hint <i>xx</i> hint <i>yy</i>].
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Session Border Control Solutions Guide Using BGF and IMSG

match-direction

Syntax	match-direction (input output);
Hierarchy Level	[edit services nat rule <i>rule-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the direction in which the rule match is applied.
Options	input —Apply the rule match on input. output —Apply the rule match on output.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

no-translation

Syntax	no-translation;
Hierarchy Level	[edit services nat rule <i>rule-name</i> term <i>term-name</i> then]
Release Information	Statement introduced in Junos OS Release 7.6.
Description	Specify that traffic is not to be translated.
Options	none
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

pgcp

Syntax	<pre>pgcp { hint [<i>hint-strings</i>]; ports-per-session <i>ports</i>; remotely-controlled; transport [<i>transport-protocols</i>]; }</pre>
Hierarchy Level	[edit services nat pool <i>nat-pool-name</i>]
Release Information	Statement introduced in Junos OS Release 8.4. remotely-controlled and ports-per-session statements added in Junos OS Release 8.5. hint statement added in Junos OS Release 9.0.
Description	Specify that the NAT pool is used exclusively by the BGF.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Session Border Control Solutions Guide Using BGF and IMSG

pool

Syntax	<pre> pool <i>nat-pool-name</i> { address <i>ip-prefix</i> </prefix-length>; address-allocation round-robin; address-range low <i>minimum-value</i> high <i>maximum-value</i>; mapping-timeout <i>seconds</i>; pgcp { hint [<i>hint-strings</i>]; ports-per-session <i>ports</i>; remotely-controlled; transport [<i>transport-protocols</i>]; } port (automatic range low <i>minimum-value</i> high <i>maximum-value</i>); } </pre>
Hierarchy Level	[edit services nat]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>pgcp statement added in Junos OS Release 8.4.</p> <p>remotely-controlled and ports-per-session statements added in Junos OS Release 8.5.</p> <p>hint statement added in Junos OS Release 9.0.</p> <p>address-allocation statement added in Junos OS Release 11.2.</p>
Description	Specify the NAT name and properties.
Options	<p><i>nat-pool-name</i>—Identifier for the NAT address pool.</p> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “Configuring Addresses and Ports for Use in NAT Rules” on page 11.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

port

Syntax	<code>port (automatic range low <i>minimum-value</i> high <i>maximum-value</i>) { }</code>
Hierarchy Level	<code>[edit services nat pool <i>nat-pool-name</i>]</code>
Release Information	port statement introduced before Junos OS Release 7.4. random-allocation statement introduced in Junos OS Release 9.3.
Description	Specify the NAT pool port or range. You can configure an automatically assigned port or specify a range with minimum and maximum values.
Options	automatic —Router-assigned port. <i>minimum-value</i> —Lower boundary for the port range. <i>maximum-value</i> —Upper boundary for the port range.
Usage Guidelines	See “Configuring Addresses and Ports for Use in NAT Rules” on page 11.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

ports-per-session

Syntax	<code>ports-per-session <i>ports</i>;</code>
Hierarchy Level	<code>[edit services nat pool <i>nat-pool-name</i> pgcp]</code>
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Configure the number of ports required to support Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP), Real-Time Streaming Protocol (RTSP), forward error correction (FEC) for voice and video flows on the Multiservices PIC.
Options	<i>number-of-ports</i> —Number of ports to enable: 2 or 4 for combined voice and video services. Default: 2
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Session Border Control Solutions Guide Using BGF and IMSG

remotely-controlled

Syntax	remotely-controlled;
Hierarchy Level	[edit services nat pool <i>nat-pool-name</i> pgcp]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Configure the addresses and ports in a NAT pool to be remotely controlled by the gateway controller.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Session Border Control Solutions Guide Using BGF and IMSG

rule

```
Syntax  rule rule-name {
        match-direction (input | output);
        term term-name {
            from {
                application-sets set-name;
                applications [ application-names ];
                destination-address (address | any-unicast) <except>;
                destination-address-range low minimum-value high maximum-value <except>;
                destination-prefix-list list-name <except>;
                source-address (address | any-unicast) <except>;
                source-address-range low minimum-value high maximum-value <except>;
            }
            then {
                no-translation;
                translated {
                    address-pooling paired;
                    destination-pool nat-pool-name;
                    destination-prefix destination-prefix;
                    dns-alg-pool dns-alg-pool;
                    dns-alg-prefix dns-alg-prefix;
                    filtering-type endpoint-independent;
                    mapping-type endpoint-independent;
                    overload-pool overload-pool;
                    overload-prefix overload-prefix;
                    source-pool nat-pool-name;
                    source-prefix source-prefix;
                    translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
                }
                syslog;
            }
        }
    }
```

Hierarchy Level [edit services nat],
[edit services nat rule-set rule-set-name]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the rule the router uses when applying this service.



NOTE: The translation types `basic-nat44`, `dynamic-nat44`, `napt44`, and `dnat-44` are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types `basic-nat-pt`, `basic-nat66`, `napt-66`, `napt-pt`, and `stateful-nat64`. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options	<i>rule-name</i> —Identifier for the collection of terms that comprise this rule.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

rule-set

Syntax	<pre>rule-set <i>rule-set-name</i> { [rule <i>rule-names</i>]; }</pre>
Hierarchy Level	[edit services nat]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the rule set the router uses when applying this service.
Options	<i>rule-set-name</i> —Identifier for the collection of rules that constitute this rule set.
Usage Guidelines	See “Configuring NAT Rule Sets” on page 19.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

services

Syntax	<pre>services nat { ... }</pre>
Hierarchy Level	[edit]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the service rules to be applied to traffic.
Options	nat —Identifies the NAT set of rules statements.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

source-address

Syntax	<code>source-address (<i>address</i> any-unicast) <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced before Junos OS Release 7.4. any-unicast and except options introduced in Junos OS Release 7.6. address option enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the source address for rule matching.
Options	address —Source IPv4 address or prefix value. any-unicast —Any unicast packet. except —(Optional) Prevent the specified address or unicast packets from being translated.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-address-range

Syntax	<code>source-address-range low <i>minimum-value</i> high <i>maximum-value</i> <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 7.6. minimum-value and maximum-value options enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the source address range for rule matching.
Options	minimum-value —Lower boundary for the IPv4 address range. maximum-value —Upper boundary for the IPv4 address range. except —(Optional) Prevent the specified address range from being translated.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-pool

Syntax	<code>source-pool <i>nat-pool-name</i>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> then translated]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the source address pool for translated traffic.
Options	<i>nat-pool-name</i> —Source pool name.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-prefix

Syntax	<code>source-prefix <i>source-prefix</i>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> then translated]</code>
Release Information	Statement introduced in Junos OS Release 7.6. <i>source-prefix</i> option enhanced to support IPv4 addresses in Junos OS Release 8.5.
Description	Specify the source prefix for translated traffic.
Options	<i>source-prefix</i> —IPv4 source prefix value.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

source-prefix-list

Syntax	<code>source-prefix-list <i>list-name</i> <except>;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> from]</code>
Release Information	Statement introduced in Junos OS Release 8.2.
Description	Specify the source prefix list for rule matching. You configure the prefix list by including the prefix-list statement at the [edit policy-options] hierarchy level.
Options	<i>list-name</i> —Destination prefix list. except —(Optional) Exclude the specified prefix list from rule matching.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Junos OS Routing Policy Configuration Guide

syslog

Syntax	<code>syslog;</code>
Hierarchy Level	<code>[edit services nat rule <i>rule-name</i> term <i>term-name</i> then]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Enable system logging. The system log information from the Multiservices PIC is passed to the kernel for logging in the /var/log directory.
Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

term

```
Syntax  term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address (address | any-unicast) <except>;
            destination-address-range low minimum-value high maximum-value <except>;
            destination-prefix-list list-name <except>;
            source-address (address | any-unicast) <except>;
            source-address-range low minimum-value high maximum-value <except>;
        }
        then {
            no-translation;
            translated {
                address-pooling paired;
                destination-pool nat-pool-name;
                destination-prefix destination-prefix;
                dns-alg-pool dns-alg-pool;
                dns-alg-prefix dns-alg-prefix;
                filtering-type endpoint-independent;
                mapping-type endpoint-independent;
                overload-pool overload-pool;
                overload-prefix overload-prefix;
                source-pool nat-pool-name;
                source-prefix source-prefix;
                translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
            }
            syslog;
        }
    }
```

Hierarchy Level [edit services nat rule *rule-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the NAT term properties.



NOTE: The translation types `basic-nat44`, `dynamic-nat44`, `napt44`, and `dnat-44` are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types `basic-nat-pt`, `basic-nat66`, `napt-66`, `napt-pt`, and `stateful-nat64`. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options *term-name*—Identifier for the term.

Usage Guidelines See “Configuring NAT Rules” on page 14.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

then

Syntax

```

then {
  no-translation;
  translated {
    address-pooling paired;
    destination-pool nat-pool-name;
    destination-prefix destination-prefix;
    dns-alg-pool dns-alg-pool;
    dns-alg-prefix dns-alg-prefix;
    filtering-type endpoint-independent;
    mapping-type endpoint-independent;
    overload-pool overload-pool;
    overload-prefix overload-prefix;
    source-pool nat-pool-name;
    source-prefix source-prefix;
    translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
  }
  syslog;
}
```

Hierarchy Level [edit services nat rule *rule-name* term *term-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the NAT term actions.



NOTE: The translation types `basic-nat44`, `dynamic-nat44`, `napt44`, and `dnat-44` are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types `basic-nat-pt`, `basic-nat66`, `napt-66`, `napt-pt`, and `stateful-nat64`. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options The remaining statements are explained separately.

Usage Guidelines See “Configuring NAT Rules” on page 14.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

translated

Syntax translated {
 address-pooling paired;
 destination-pool *nat-pool-name*;
 dns-alg-pool *dns-alg-pool*;
 dns-alg-prefix *dns-alg-prefix*;
 filtering-type endpoint-independent;
 mapping-type endpoint-independent;
 source-pool *nat-pool-name*;
 translation-type (basic-nat44 | dynamic-nat44 | napt44 | dnat-44);
 }

Hierarchy Level [edit services nat rule *rule-name* term *term-name* then]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define properties for translated traffic.



NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the syntax above.

Options The remaining statements are explained separately.

Usage Guidelines See "Configuring NAT Rules" on page 14.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

translation-type

Syntax	<code>translation-type <i>translation type</i></code>
Hierarchy Level	[edit services nat rule <i>rule-name</i> term <i>term-name</i> then translated]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the NAT types for traditional NAT.
Options	<i>translation type</i> —You can specify basic-nat44 , dynamic-nat44 , napt44 , or dnat-44 .



NOTE: The translation types **basic-nat44**, **dynamic-nat44**, **napt44**, and **dnat-44** are used for configuring NAT in an IPv4 network. Apart from these translation types, Junos OS also supports the translation types **basic-nat-pt**, **basic-nat66**, **napt-66**, **napt-pt**, and **stateful-nat64**. These translation types are used for configuring NAT in an IPv6 network. Because Junos Services Framework (JSF) does not support configuring NAT in IPv6 networks, these translation types are not displayed in the options above.

Usage Guidelines	See “Configuring NAT Rules” on page 14.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

transport

Syntax	<code>transport [<i>transport-protocols</i>];</code>
Hierarchy Level	[edit services nat pool <i>nat-pool-name</i> pgcp]
Release Information	Statement introduced in Junos OS Release 9.2.
Description	Configure the BGF to select a NAT pool based on transport protocol type.
Options	[<i>transport-protocol</i>]—One or more transport protocols. Values: rtp-avp, tcp, udp Syntax: One or more protocols. If you specify more than one protocol, you must enclose all protocols in brackets.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Session Border Control Solutions Guide Using BGF and IMSG

PART 3

Administration

- Network Address Translation Operational Mode Commands on page 71

CHAPTER 5

Network Address Translation Operational Mode Commands

show services nat pool

Syntax	<pre>show services nat pool <brief detail> <pool-name> pgcp <ports-per-session remotely-controlled></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>pgcp option added in Junos OS Release 8.5.</p>
Description	Display information about Network Address Translation (NAT) pools.
Options	<p>none—Display standard information about all NAT pools.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>pool-name—(Optional) Display information about the specified NAT pool.</p> <p>pgcp—(Optional) Display information about a NAT pool that is exclusive to the BGF.</p> <p>ports-per-session—(Optional) Display the number of ports allocated per session from the NAT pool.</p> <p>remotely-controlled—(Optional) Display if the NAT pool is explicitly specified by the gateway controller.</p>
Required Privilege Level	view
List of Sample Output	<p>show services nat pool brief on page 73</p> <p>show services nat pool detail on page 73</p>
Output Fields	Table 1 on page 72 lists the output fields for the show services nat pool command. Output fields are listed in the approximate order in which they appear.

Table 1: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an Multiservices interface.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed, but if none of the service sets has any flows, a flow table header is printed for each service set.	All levels
NAT pool	Name of the Network Address Translation pool.	All levels
Type or Translation type	Address translation type: basic-nat44 , dynamic-nat44 , napt44 , or dnat-44 .	All levels
Address or Address range	IPv4 address range of the pool.	All levels

Table 1: show services nat pool Output Fields (*continued*)

Field Name	Field Description	Level of Output
Port or Port range	Port range of the pool. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	All levels
Ports used' or Ports in use	Number of ports allocated in this pool with this name. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	All levels
Out of port errors	Number of port allocation errors. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	detail
Max ports used	Maximum number of ports used. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	detail
Addresses in use	Number of addresses in use for dynamic source address NAT pools.	detail

Sample Output

```

show services nat pool brief user@host> show services nat pool brief
                             Interface: ms-1/3/0, Service set: blue
                             NAT pool Type      Address                               Port      Ports used
                             pool1    DNAT-44   100.100.100.100-100.100.100.100
                             pool2    NAPT-44   200.200.200.200-200.200.200.200
                             pool3    DYNAMIC  NAT44  210.210.210.210-210.210.210.230 65530-65535      0

show services nat pool detail user@host> show services nat pool detail
                             Interface: ms-1/2/0, Service set: nat-2-internet-rsp0
                             NAT pool: src-nat-pool-pl01, Translation type: DNAT-44
                             Address range: 1.1.1.0-1.1.1.0
                             Address range: 2.2.2.2-2.2.2.2
                             Port range: 512-65535, Ports in use: 0, Out of port errors: 0, Max ports
                             used: 0

```


PART 4

Troubleshooting

- Knowledge Base on page 77

CHAPTER 6

Knowledge Base

PART 5

Index

- Index on page 81
- Index of Statements and Commands on page 85

Index

A

address statement	
NAT.....	49
usage guidelines.....	11
address-allocation statement.....	49
address-range statement	
NAT.....	50
application-sets statement	
NAT.....	50
usage guidelines.....	15
applications statement	
NAT.....	51
usage guidelines.....	15

B

Basic NAT Overview.....	5
basic-nat44 option	
configuring.....	26

D

destination NAT	
configuring.....	34
example.....	46
destination-address statement	
NAT.....	51
usage guidelines.....	15
destination-address-range statement	
NAT.....	52
usage guidelines.....	15
destination-pool statement.....	52
usage guidelines.....	17
destination-prefix statement.....	53
destination-prefix-list statement	
NAT.....	53
dnat-44 option	
example.....	46
usage guidelines.....	34
dynamic address- only source translation	
configuring.....	31

dynamic address-only source translation	
example.....	38
dynamic NAT	
configuring.....	31
example.....	38
Dynamic NAT Overview.....	6
dynamic-nat44 option	
example.....	38
usage guidelines.....	31

F

from statement	
NAT.....	54
usage guidelines.....	14, 15

H

hint statement.....	55
---------------------	----

I

IPv4	
napt-44 option.....	29
napt-44 option, example.....	39
translation type	
basic-nat44 option.....	26
IPv4 dynamic source translation	
configuring.....	29
example.....	39
IPv4 to IPv4 Traditional NAT Overview.....	4

M

match-direction statement	
NAT.....	55
usage guidelines.....	14

N

NAPT Overview.....	5, 6
napt-44 option	
example.....	39
usage guidelines.....	29

NAT		remotely-controlled statement.....	59
action statements.....	17	rule statement	
address configuration.....	11	NAT.....	60
applications.....	15	usage guidelines.....	14
basic NAT, overview.....	5	rule-set statement	
destination NAT.....	34	NAT.....	61
example.....	46	usage guidelines.....	19
dynamic address- only source translation.....	31	S	
dynamic address-only source translation.....	38	services statement	
dynamic NAT.....	31	NAT.....	61
example.....	38	show services nat pool command.....	72
dynamic NAT, overview.....	6	source-address statement	
dynamic source translation.....	29	NAT.....	62
dynamic source translation, example.....	39	usage guidelines.....	15
match conditions.....	15	source-address-range statement	
NAPT, overview.....	5, 6	NAT.....	62
rule sets.....	19	usage guidelines.....	15
static destination address translation.....	34	source-pool statement.....	63
example.....	46	usage guidelines.....	17
static destination NAT, overview.....	6	source-prefix statement.....	63
status information, displaying.....	72	source-prefix-list statement	
traditional NAT, overview.....	4	NAT.....	64
translation types overview.....	4	static destination address translation	
Network Address Port Translation (NAPT)		configuring.....	34
configuring.....	29	example.....	46
example.....	39	static destination NAT overview.....	6
IPv4.....	29	syslog statement	
IPv4 example.....	39	NAT.....	64
no-translation statement.....	56	usage guidelines.....	17
usage guidelines.....	17	T	
O		term statement	
overload-pool statement		NAT.....	65
usage guidelines.....	17	usage guidelines.....	14
overload-prefix statement		then statement	
usage guidelines.....	17	NAT.....	66
P		usage guidelines.....	14
pgcp statement		traditional NAT	
NAT.....	56	basic NAT, overview.....	5
pool statement.....	57	traditonal NAT	
usage guidelines.....	11	NAPT, overview.....	5, 6
port statement		translated statement.....	67
NAT.....	58	usage guidelines.....	17
usage guidelines.....	11	translation types overview.....	4
ports-per-session statement.....	58	translation-type statement	
R		basic-nat44 option.....	26
random-allocation statement.....	58	dnat-44 option, configuring.....	34
		dnat-44 option, example.....	46

dynamic-nat44, configuring.....	31
dynamic-nat44, example.....	38
napt-44 option, configuring.....	29
napt-44 option, example.....	39
usage guidelines.....	17
transport statement	
NAT.....	68

Index of Statements and Commands

A

address statement	
NAT	49
address-allocation statement.....	49
address-range statement	
NAT	50
application-sets statement	
NAT	50
applications statement	
NAT	51

D

destination-address statement	
NAT	51
destination-address-range statement	
NAT	52
destination-pool statement.....	52
destination-prefix statement.....	53
destination-prefix-list statement	
NAT	53

F

from statement	
NAT	54

H

hint statement.....	55
---------------------	----

M

match-direction statement	
NAT	55

N

no-translation statement.....	56
-------------------------------	----

P

pgcp statement	
NAT	56
pool statement.....	57

port statement	
NAT	58
ports-per-session statement.....	58

R

random-allocation statement.....	58
remotely-controlled statement.....	59
rule statement	
NAT	60
rule-set statement	
NAT	61

S

services statement	
NAT	61
show services nat pool command.....	72
source-address statement	
NAT	62
source-address-range statement	
NAT	62
source-pool statement.....	63
source-prefix statement.....	63
source-prefix-list statement	
NAT	64
syslog statement	
NAT	64

T

term statement	
NAT	65
then statement	
NAT	66
translated statement.....	67
transport statement	
NAT	68

