



## Softwire Services



Published: 2013-02-15

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.

*Softwire Services*  
Copyright © 2013, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

|                  |  |           |
|------------------|--|-----------|
|                  | About the Documentation . . . . .                                      | ix        |
|                  | Documentation and Release Notes . . . . .                              | ix        |
|                  | Supported Platforms . . . . .  | ix        |
|                  | Using the Examples in This Manual . . . . .                            | ix        |
|                  | Merging a Full Example . . . . .                                       | x         |
|                  | Merging a Snippet . . . . .  | x         |
|                  | Documentation Conventions . . . . .                                    | xi        |
|                  | Documentation Feedback . . . . .                                       | xiii      |
|                  | Requesting Technical Support . . . . .                                 | xiii      |
|                  | Self-Help Online Tools and Resources . . . . .                         | xiii      |
|                  | Opening a Case with JTAC . . . . .                                     | xiv       |
| <b>Part 1</b>    | <b>Overview</b>  |           |
| <b>Chapter 1</b> | <b>Software Services . . . . .</b>                                     | <b>3</b>  |
|                  | Tunneling Services for IPv4-to-IPv6 Transition Overview . . . . .      | 3         |
|                  | 6to4 Overview . . . . .  | 3         |
|                  | Basic 6to4 . . . . .   | 4         |
|                  | 6to4 Anycast . . . . .   | 4         |
|                  | 6to4 Provider-Managed Tunnels . . . . .                                | 5         |
|                  | DS-Lite Softwires—IPv4 over IPv6 . . . . .                             | 5         |
|                  | 6rd Softwires—IPv6 over IPv4 . . . . .                                 | 6         |
| <b>Part 2</b>    | <b>Configuration</b>   |           |
| <b>Chapter 2</b> | <b>Configuration Tasks . . . . .</b>                                   | <b>11</b> |
|                  | Configuring a 6rd Software Concentrator . . . . .                      | 11        |
|                  | Configuring a DS-Lite Software Concentrator . . . . .                  | 11        |
|                  | Configuring Software Rules . . . . .                                   | 12        |
|                  | Configuring Stateful Firewall Rules for 6rd Software . . . . .         | 13        |
|                  | Configuring IPv6 Multicast Interfaces . . . . .                        | 13        |
|                  | Configuring Service Sets for Software . . . . .                        | 14        |
| <b>Chapter 3</b> | <b>Examples . . . . .</b>  | <b>15</b> |
|                  | Example: Basic DS-Lite Configuration . . . . .                         | 15        |
|                  | Example: Basic 6rd Configuration . . . . .                             | 21        |
|                  | Example: Configuring DS-Lite and 6rd in the Same Service Set . . . . . | 25        |
| <b>Chapter 4</b> | <b>Configuration Statements . . . . .</b>                              | <b>33</b> |
|                  | ds-lite . . . . .  | 34        |
|                  | rule (Software) . . . . .  | 35        |
|                  | rule-set (Software) . . . . .  | 35        |

|                  |   |           |
|------------------|---|-----------|
|                  | softwire-concentrator .....                     | 36        |
|                  | softwire-rules .....                            | 36        |
|                  | v6rd .....                                      | 37        |
| <b>Part 3</b>    | <b>Administration</b>                           |           |
| <b>Chapter 5</b> | <b>Softwire Operational Mode Commands .....</b> | <b>41</b> |
|                  | clear services softwire statistics .....        | 42        |
|                  | show services softwire .....                    | 43        |
|                  | show services stateful-firewall flows .....     | 44        |
| <b>Part 4</b>    | <b>Index</b>                                    |           |
|                  | Index .....                                     | 53        |

# List of Figures

|           |                                   |    |
|-----------|-----------------------------------|----|
| Part 1    | Overview                          |    |
| Chapter 1 | Softwire Services .....           | 3  |
|           | Figure 1: 6rd Softwire Flow ..... | 6  |
| Part 2    | Configuration                     |    |
| Chapter 3 | Examples .....                    | 15 |
|           | Figure 2: DS-Lite Topology .....  | 16 |



# List of Tables

|                  |  |           |
|------------------|--|-----------|
|                  | <b>About the Documentation . . . . .</b>                               | <b>ix</b> |
|                  | Table 1: Notice Icons . . . . .  | xi        |
|                  | Table 2: Text and Syntax Conventions . . . . .                         | xi        |
| <b>Part 3</b>    | <b>Administration</b>  |           |
| <b>Chapter 5</b> | <b>Softwire Operational Mode Commands . . . . .</b>                    | <b>41</b> |
|                  | Table 3: show-services-softwire Output Fields . . . . .                | 43        |
|                  | Table 4: show services stateful-firewall flows Output Fields . . . . . | 46        |





# About the Documentation

- [Documentation and Release Notes on page ix](#)
- [Supported Platforms on page ix](#)
- [Using the Examples in This Manual on page ix](#)
- [Documentation Conventions on page xi](#)
- [Documentation Feedback on page xiii](#)
- [Requesting Technical Support on page xiii](#)

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- [M Series](#)
- [T Series](#)
- [MX Series](#)
- [J Series](#)

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

## Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

## Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the CLI User Guide.

## Documentation Conventions

Table 1 on page xi defines notice icons used in this guide.

Table 1: Notice Icons




| Icon  | Meaning            | Description   |
|---|--------------------|---|
|   | Informational note | Indicates important features or instructions.                               |
|  | Caution            | Indicates a situation that might result in loss of data or hardware damage. |
|  | Warning            | Alerts you to the risk of personal injury or death.                         |
|  | Laser warning      | Alerts you to the risk of personal injury from a laser.                     |

Table 2 on page xi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

| Convention                 | Description  | Examples   |
|----------------------------|--|--|
| <b>Bold text like this</b> | Represents text that you type.                         | To enter configuration mode, type the <b>configure</b> command:<br><br>user@host> <b>configure</b> |
| Fixed-width text like this | Represents output that appears on the terminal screen. | user@host> <b>show chassis alarms</b><br>No alarms currently active                                |

Table 2: Text and Syntax Conventions (*continued*)

| Convention                     | Description  | Examples  |
|--------------------------------|--|---|
| <i>Italic text like this</i>   | <ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul> | <ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul> |
| <i>Italic text like this</i>   | Represents variables (options for which you substitute a value) in commands or configuration statements.   | Configure the machine's domain name:<br><br>[edit]<br>root@# <b>set system domain-name</b> <i>domain-name</i>   |
| <b>Text like this</b>          | Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.                          | <ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit protocols ospf area area-id] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>                         |
| < > (angle brackets)           | Enclose optional keywords or variables.  | <b>stub &lt;default-metric metric&gt;;</b>  |
| (pipe symbol)                  | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.             | <b>broadcast   multicast</b><br><br><i>(string1   string2   string3)</i>  |
| # (pound sign)                 | Indicates a comment specified on the same line as the configuration statement to which it applies.   | <b>rsvp { # Required for dynamic MPLS only</b>  |
| [ ] (square brackets)          | Enclose a variable for which you can substitute one or more values.  | <b>community name members [ community-ids ]</b>   |
| Indentation and braces ( { } ) | Identify a level in the configuration hierarchy.   | [edit]<br>routing-options {<br>static {<br>route default {<br>nexthop <i>address</i> ;<br>retain;<br>}<br>}<br>}  |
| ;(semicolon)                   | Identifies a leaf statement at a configuration hierarchy level.  |   |
| <b>J-Web GUI Conventions</b>   |  |   |
| <b>Bold text like this</b>     | Represents J-Web graphical user interface (GUI) items you click or select.   | <ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>   |
| > (bold right angle bracket)   | Separates levels in a hierarchy of J-Web selections.   | In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .  |

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## PART 1

# Overview

- [Softwire Services on page 3](#)





## CHAPTER 1

# Softwire Services

- [Tunneling Services for IPv4-to-IPv6 Transition Overview on page 3](#)

## Tunneling Services for IPv4-to-IPv6 Transition Overview

---

The Junos OS enables service providers to transition to IPv6 by using softwire encapsulation and decapsulation techniques. A softwire is a tunnel that is created between softwire Customer Premises Equipment (CPE). A softwire CPE can share a unique common internal state for multiple softwires, making it a very light and scalable solution. When you use softwires, you need not maintain an interface infrastructure for each softwire, unlike a typical mesh of generic routing encapsulation (GRE) tunnels that would require you to do so. A softwire initiator at the customer end encapsulates native packets and tunnels them to a softwire concentrator at the service provider. The softwire concentrator decapsulates the packets and sends them to their destination. A softwire is created when a softwire concentrator receives the first tunneled packet of a flow and prepares for flow processing. The softwire exists as long as the softwire concentrator is providing flows for routing. A flow counter is maintained; when the number of active flows is 0, the softwire is deleted. Statistics are kept for both flows and softwires.

Softwire addresses are not specifically configured under any physical or virtual interface. Therefore, the number of established softwires does not affect throughput, and scalability is independent of the number of interfaces. The scalability is only limited to the number of flows that the platform (services DPC or PIC) can support.

This topic contains the following sections:

- [6to4 Overview on page 3](#)
- [DS-Lite Softwires—IPv4 over IPv6 on page 5](#)
- [6rd Softwires—IPv6 over IPv4 on page 6](#)

### 6to4 Overview

- [Basic 6to4 on page 4](#)
- [6to4 Anycast on page 4](#)
- [6to4 Provider-Managed Tunnels on page 5](#)

## Basic 6to4

---

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 Internet) without the need to configure explicit tunnels. 6to4 is described in RFC 3056, *Connection of IPv6 Domains via IPv4 Clouds*. 6to4 is especially relevant during the initial phases of deployment to full, native IPv6 connectivity, since IPv6 is not required on nodes between the host and the destination. However, it is intended only as a transition mechanism and is not meant to be used permanently.

6to4 can be used by an individual host, or by a local IPv6 network. When used by a host, it must have a global IPv4 address connected, and the host is responsible for the encapsulation of outgoing IPv6 packets and the decapsulation of incoming 6to4 packets. If the host is configured to forward packets for other clients, often a local network, it is then a router.

There are two kinds of 6to4 virtual routers: border routers and relay routers. A 6to4 border router is an IPv6 router supporting a 6to4 pseudointerface, and is normally the border router between an IPv6 site and a wide-area IPv4 network. A relay router is a 6to4 router configured to support transit routing between 6to4 addresses and pure native IPv6 addresses.

In order for a 6to4 host to communicate with the native IPv6 Internet, its IPv6 default gateway must be set to a 6to4 address which contains the IPv4 address of a 6to4 relay router. To avoid the need for users to set this up manually, the Anycast address of 192.88.99.1 has been allocated to send packets to a 6to4 relay router. Note that when wrapped in 6to4 with the subnet and hosts fields set to zero, this IPv4 address (192.88.99.1) becomes the IPv6 address 2002:c058:6301::. To ensure BGP routing propagation, a short prefix of 192.88.99.0/24 has been allocated for routes pointed at 6to4 relay routers that use this Anycast IP address. Providers willing to provide 6to4 service to their clients or peers should advertise the Anycast prefix like any other IP prefix, and route the prefix to their 6to4 relay.

Packets from the IPv6 Internet to 6to4 systems must be sent to a 6to4 relay router by normal IPv6 routing methods. The specification states that such relay routers must only advertise 2002::/16 and not subdivisions of it to prevent IPv4 routes from polluting the routing tables of IPv6 routers. From there they can then be sent over the IPv4 Internet to the destination.

## 6to4 Anycast

---

Router 6to4 assumes that 6to4 routers and relays are managed and configured cooperatively. In particular, 6to4 sites must configure a relay router to carry the outbound traffic, which becomes the default IPv6 router (except for 2002::/16). The objective of the Anycast variant, defined in RFC 3068, *An Anycast Prefix for 6to4 Relay Routers*, is to avoid the need for such configuration. This makes the solution available for small or domestic users, even those with a single host or simple home gateway instead of a border router. This is achieved by defining 192.88.99.1 as the default IPv4 address for a 6to4 relay, and 2002:c058:6301:: as the default IPv6 router prefix ("well-known prefix") for a 6to4 site.

RFC 6343, *Advisory Guidelines for 6to4 Deployment*, published in August 2011, identifies a wide range of problems associated with the use of unmanaged 6to4 Anycast relay routers.

### 6to4 Provider-Managed Tunnels

---

A solution to many problems associated with unmanaged Anycast 6to4 is presented in IETF informational draft draft-kuarsingh-v6ops-6to4-provider-managed-tunnel-02, *6to4 Provider-Managed Tunnels (PMT)*. That document, a “work in progress,” proposes a solution that allows providers to exercise greater control over the routing of 6to4 traffic.

Anycast 6to4 implies a default configuration for the user site. It does not require any particular user action. It does require an IPv4 Anycast route to be in place to a relay at 192.88.99.1. Traffic does not necessarily return to the same 6to4 gateway because of the the “well-known” 6to4 prefix used and advertised by all 6to4 traffic.

6to4 provider-managed tunnels (PMTs) facilitate the management of 6to4 tunnels using an Anycast configuration. 6to4 PMT enables service providers to improve 6to4 operation when network conditions provide suboptimal performance or break normal 6to4 operation. 6to4 PMT provides a stable provider prefix and forwarding environment by utilizing existing 6to4 relays with an added function of IPv6 prefix translation that controls the flow of return traffic.

The 6to4 managed tunnel model behaves like a standard 6to4 service between the customer IPv6 host or gateway and the 6to4 PMT relay (within the provider domain). The 6to4-PMT relay shares properties with 6rd (RFC5969) by decapsulating and forwarding embedded IPv6 flows, within an IPv4 packet, to the IPv6 Internet. The model provides an additional function which translates the source 6to4 prefix to a provider assigned prefix which is not found in 6rd (RFC5969) or traditional 6to4 operation. The 6to4-PMT relay provides a stateless (or stateful) mapping of the 6to4 prefix to a provider-supplied prefix by mapping the embedded IPv4 address in the 6to4 prefix to the provider prefix.

## DS-Lite Softwires—IPv4 over IPv6

When an Internet service provider (ISP) begins to allocate new subscriber home IPv6 addresses and IPv6-capable equipment, dual-stack lite (DS-Lite) provides a method for the private IPv4 addresses behind the IPv6 customer edge (CE) WAN equipment to reach the IPv4 network. DS-Lite enables IPv4 customers to continue to access the Internet using their current hardware by using a softwire initiator, referred to as a Basic Bridging Broadband (B4), at the customer edge to encapsulate IPv4 packets into IPv6 packets and tunnel them over an IPv6 network to a softwire concentrator, referred to as an Address Family Transition Router (AFTR), for decapsulation. DS-Lite creates the IPv6 softwires that terminate on the services PIC. Packets coming out of the softwire can then have other services such as NAT applied on them.

DS-Lite is supported on Multiservices 100, 400, and 500 PICs on M Series routers and on MX Series routers equipped with Multiservices Dense Port Concentrator (DPCs).



**NOTE:** IPv6 Provider Edge (6PE), or MPLS-enabled IPv6, is available for ISPs with MPLS-enabled networks. These networks now can use Multiprotocol BGP (MP-BGP) to provide connectivity between the DS-Lite B4 and AFTR (or any two IPv6 nodes). DS-Lite properly handles encapsulation and decapsulation despite the presence of additional MPLS header information.

For more information on DS-Lite softwires, see the IETF draft *Dual Stack Lite Broadband Deployments Following IPv4 Exhaustion*.



**NOTE:** The most recent IETF draft documentation for DS-Lite uses new terminology:

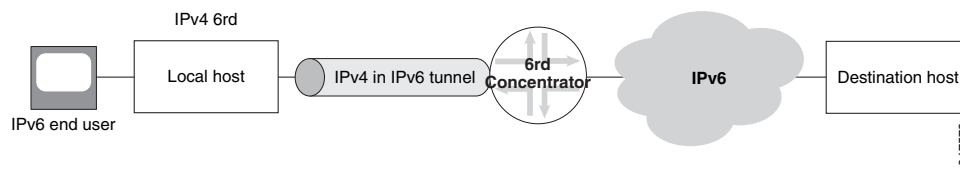
- The term *software initiator* has been replaced by *B4*.
- The term *software concentrator* has been replaced by *AFTR*.

The Junos OS documentation generally uses the original terms when discussing configuration in order to be consistent with the command-line interface (CLI) statements used to configure DS-Lite.

## 6rd Softwires—IPv6 over IPv4

6rd software flow is shown in [Figure 1 on page 6](#).

**Figure 1: 6rd Software Flow**



The Junos OS supports a 6rd software concentrator on a services DPC or PIC to facilitate rapid deployment of IPv6 service to subscribers on native IPv4 CE WANs. IPv6 packets are encapsulated in IPv4 packets by a software initiator at the CE WAN. These packets are tunneled to a software concentrator residing on a multiservices DPC (branch relay). A software is created when IPv4 packets containing IPv6 destination information are received at the software concentrator, which decapsulates IPv6 packets and forwards them for IPv6 routing. All of these functions are performed in a single pass of the services PIC.

In the reverse path, IPv6 packets are sent to the Services DPC where they are encapsulated in IPv4 packets corresponding to the proper software and sent to the CE WAN.

The software concentrator creates softwires as the IPv4 packets are received from the CE WAN side or IPv6 packets are received from the Internet. A 6rd software on the Services DPC is identified by the 3-tuple containing the service set ID, CE software initiator IPv4 address, and software concentrator IPv4 address. IPv6 flows are also created for the encapsulated IPv6 payload, and are associated with the specific software that carried

them in the first place. When the last IPv6 flow associated with a softwire ends, the softwire is deleted. This simplifies configuration and there is no need to create or manage tunnel interfaces.

6rd is supported on Multiservices 100, 400, and 500 PICs on M Series and T Series routers, and on MX Series platforms equipped with Multiservices DPCs.

For more information on 6rd softwires, see RFC 5969, *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification*.

**Related Documentation**

- [Network Address Translation Overview](#)



## PART 2

# Configuration

- [Configuration Tasks on page 11](#)
- [Examples on page 15](#)
- [Configuration Statements on page 33](#)





## CHAPTER 2

# Configuration Tasks

- [Configuring a 6rd Software Concentrator on page 11](#)
- [Configuring a DS-Lite Software Concentrator on page 11](#)
- [Configuring Software Rules on page 12](#)
- [Configuring Stateful Firewall Rules for 6rd Software on page 13](#)
- [Configuring IPv6 Multicast Interfaces on page 13](#)
- [Configuring Service Sets for Software on page 14](#)

## Configuring a 6rd Software Concentrator

---

To configure a 6rd software concentrator:

1. Assign a name to the 6rd software concentrator.

```
[edit services software software-concentrator]  
user@host# edit v6rd v6rd-software-concentrator
```

2. Specify the address of the software tunnel.

```
[edit services software software-concentrator v6rd v6rd-software-concentrator]  
user@host# set software-address address
```

3. Specify the MTU for the software tunnel.

```
[edit services software software-concentrator v6rd v6rd-software-concentrator]  
user@host# set mtu-v4 mtu-v4
```



**TIP:** In this release there is no support for fragmentation and reassembly, therefore the MTUs on the IPv6 and IPV4 network must be properly configured by the administrator.

## Configuring a DS-Lite Software Concentrator

---

To configure a DS-Lite software concentrator:

1. Assign a name to the DS-Lite software concentrator.

```
[edit services software software-concentrator]  
user@host# edit ds-lite ds-lite-software-concentrator
```

2. Specify the address of the software tunnel.

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set software-address address
```

3. Specify the MTU for the software tunnel.

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set mtu-v6 mtu-v6
```



**NOTE:** This option sets the maximum transmission unit when encapsulating IPv4 packets into IPv6. If the final length is greater than the MTU, the IPv6 packet will be fragmented. This option is mandatory since it depends on other network parameters under administrator control.

4. To copy DSCP information from the IPv6 header into the decapsulated IPv4 header, include the **copy-dscp** statement.

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set copy-dscp
```

5. Specify the maximum number of flows for the software

```
[edit services software software-concentrator ds-lite ds-lite-software-concentrator]  
user@host# set flow-limit 1000
```

---

## Configuring Software Rules

You configure software rules to instruct the router how to direct traffic to the addresses specified for 6rd or DS-Lite software concentrators. Software rules do not perform any filtration of the traffic. They do not include a **from** statement, and the only option in the **then** statement is to specify the address of the 6rd or DS-Lite software concentrator.

You can create a software rule consisting of one or more terms and associate a particular 6rd or DS-Lite software concentrator with each term. You can include the software rule in service sets along with other services rules.

To configure a software rule:

1. Assign a name to the rule.

```
[edit services software ]  
user@host# edit rule rule-name
```

2. Specify the match direction.

```
[edit services software rule rule-name]  
user@host# set match-direction (input | output)
```

3. Assign a name for the first term.

```
[edit services software rule rule-name]  
user@host# edit term term-name
```

4. Associate a 6rd or DS-Lite software concentrator with this term.

```
[edit services software rule rule-name term term-name]
```

```
user@host# set then ds-lite name
```

Or

```
user@host# set then v6rd v6rd-software-concentrator
```

5. Repeat Steps 3 and 4 for as many additional terms as needed.

## Configuring Stateful Firewall Rules for 6rd Software

You must configure a stateful firewall rule for use with 6rd softwires. The stateful firewall service is used only to direct packets to the software, not for firewalling purposes. The 6rd software service itself must be stateless. To support stateless processing, you must include an **allow** term in both directions of the stateful firewall policy.

To include a stateful firewall rule for 6rd software processing:

1. Assign a name to the rule.

```
[edit services stateful-firewall]
user@host# edit rule rule-name
```

2. Specify the match direction.

```
[edit services stateful-firewall rule-name]
user@host# set match-direction input-output
```

3. Assign a name for the term.

```
[edit services stateful-firewall rule-name]
user@host# edit term term-name
```

4. Specify that all traffic in both directions should be accepted for the software process.

```
[edit services stateful-firewall rule-name term term-name]
user@host# set then accept
```

## Configuring IPv6 Multicast Interfaces

Configure multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery. This enables the router to process software-initiated flows in both directions.

To configure IPv6 multicast interfaces:

1. Access the software hierarchy.

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

2. Include the **ipv6-multicast-interfaces** statement for an individual interface.

```
[edit services software]
user@host# set ipv6-multicast-interfaces interface-name
```

Or configure all software interfaces as IPv6 multicast.

```
[edit services software]
user@host# set ipv6-multicast-interfaces all
```

## Configuring Service Sets for Software

---

You must include software rules or a software rule set in a service set to enable software processing. You must include a stateful firewall rule for DS-Lite.

To configure service sets for software:

1. Include a software rule or rule set in the service set.

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

2. When using a 6rd software, include a stateful-firewall rule.

```
[edit services service-set service-set-name]
user@host# set stateful-firewall-rules software-rule-name
```

3. You can include a NAT rule for flows originated by DS-Lite softwires.



### NOTE:

Currently a NAT rule configuration is required with a DS-Lite software configuration when you use interface service set configurations; NAT is not required when using next-hop service set configurations. NAT processing from IPv4 to IPv6 address pools and vice versa is not currently supported. FTP, HTTP, and RSTP are supported.

---

For further information, see “Configuring Service Rules.”

## CHAPTER 3

# Examples

- [Example: Basic DS-Lite Configuration on page 15](#)
- [Example: Basic 6rd Configuration on page 21](#)
- [Example: Configuring DS-Lite and 6rd in the Same Service Set on page 25](#)

### Example: Basic DS-Lite Configuration

---

- [Requirements on page 15](#)
- [Configuration Overview and Topology on page 15](#)
- [Configuration on page 16](#)

#### Requirements

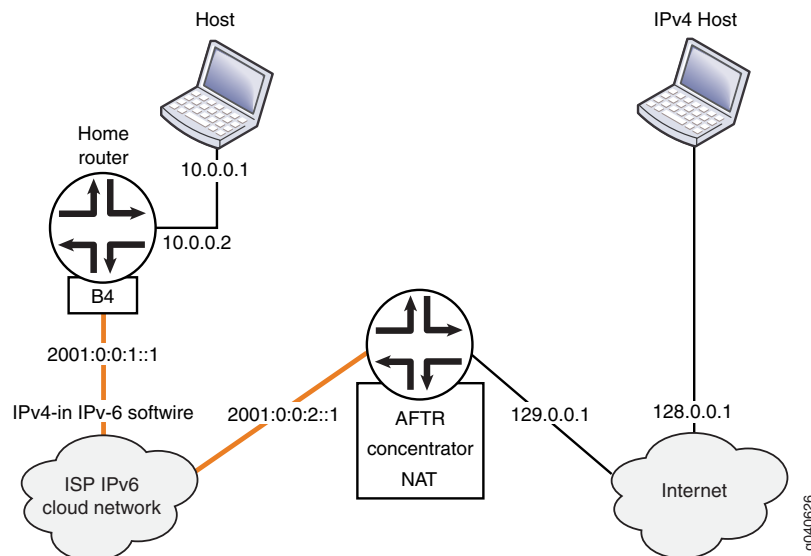
The following hardware components can perform DS-Lite:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

#### Configuration Overview and Topology

This example describes how to configure an MX Series router with an MS-DPC as an AFTR to facilitate the flow shown in [Figure 2 on page 16](#).

Figure 2: DS-Lite Topology



In this example, the DS-Lite softwire concentrator, or AFTR, is an MX Series router with two Gigabit interfaces and a Services DPC. The interface facing the B4 element is ge-3/1/5 and the interface facing the Internet is ge-3/1/0.

## Configuration

- [Chassis Configuration on page 16](#)
- [Interfaces Configuration on page 16](#)
- [Network Address and Port Translation Configuration on page 18](#)
- [Softwire Configuration on page 19](#)
- [Service Set Configuration on page 20](#)

### Chassis Configuration

#### Step-by-Step Procedure

To configure the service PIC (FPC 0 Slot 0) with the Layer 3 service package:

1. Enter the **edit chassis** hierarchy level.  

```
user@host# edit chassis
```
2. Configure the Layer 3 service package.  

```
[edit chassis]
user@host# set fpc 0 pic 0 adaptive-services service-package layer-3
```

### Interfaces Configuration

#### Step-by-Step Procedure

interfaces facing the B4 (softwire initiator) and facing the Internet:

1. Go the **[edit interfaces]** edit hierarchy level for ge-3/1/0, which faces the Internet.  

```
host# edit interfaces ge-3/1/0
```

2. Define the interface.

```
[edit interfaces ge-3/1/0]
user@host# set description AFTR-Internet
user@host# set unit 0 family inet address 128.0.0.2/24
```

3. Go to the **[edit interfaces]** hierarchy level for ge-3/1/5, which faces the B4.

```
user@host# up 1
[edit]
user@host# edit interfaces ge-3/1/5
```

4. Define the interface.

```
[edit interfaces ge-3/1/5]
user@host# set description AFTR-B4
user@host# set unit 0 family inet
user@host# edit unit 0 family inet6
[edit unit 0 family inet6]
user@host# set service input service-set sset
user@host# set service output service-set sset
user@host# set address 2001:0:0:2::1/48
```

5. Go to the **[edit interfaces]** hierarchy level for sp-0/0/0, used to host the DS-Lite AFTR.

```
[edit]
user@host# edit interfaces sp-0/0/0
```

6. Define the interface.

```
[edit interfaces sp-0/0/0]
user@host# set description AFTR-B4
user@host# set unit 0 family inet
user@host# edit unit 0 family inet6
```

```

Results user@host# show interfaces ge-3/1/0
description AFTR-Internet;
unit 0 {
    family inet {
        address 128.0.0.2/24;
    }
}

user@host# show interfaces ge-3/1/5
description AFTR-B4;
unit 0 {
    family inet;
    family inet6 {
        service {
            input {
                service-set sset;
            }
            output {
                service-set sset;
            }
        }
        address 2001:0:0:2::1/48;
    }
}

user@host# show interfaces sp-o/o/o
unit 0 {
    family inet;
    family inet6;
}

```

### Network Address and Port Translation Configuration

---

#### Step-by-Step Procedure

To configure NAPT:

- Go to the **[edit services nat]** hierarchy level.  

```

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

```
- Define a NAT pool p1.  

```

user@host# set pool p1 address 129.0.0.1/32 port automatic

```
- Define a NAT rule, beginning with the match direction.  

```

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

```
- Define a **term** for the rule, beginning with a from clause.  

```

[edit services nat]
user@host# set rule r1 term t1 from source-address 10.0.0.0/16

```
- Define the desired translation in a **then** clause. In this case, use dynamic source translation.  

```

[edit services nat]
user@host# set rule r1 term t1 then translated source-pool p1 translation-type napt-44

```
- (Optional) Configure logging of translation information for the rule.



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

**Results**

```
user@host# show services nat
pool p1 {
  address 129.0.0.1/32;
  port {
    automatic;
  }
}
rule r1 {
  match-direction input;
  term t1 {
    from {
      source-address {
        10.0.0.0/16;
      }
    }
    then {
      translated {
        source-pool p1;
        translation-type {
          napt-44;
        }
      }
      syslog;
    }
  }
}
```

### Software Configuration

**Step-by-Step Procedure** To configure the DS-Lite software concentrator and associated rules:

1. Go to the **[edit services software]** hierarchy level.  

```
user@host# edit services software
```
2. Define the DS-Lite software concentrator.  

```
[edit services software]
user@host# set software-concentrator ds-lite ds-1 software-address 1001::1 mtu-v6 1460
```
3. Define the software rule.  

```
[edit services software]
user@host# set rule r1 match-direction input term t1 then ds-lite ds1.
```

**Results**    `user@host# show services software`

```
software-concentrator {
  ds-lite ds1 {
    software-address 1001::1;
    mtu-v6 1460;
  }
}
rule r1 {
  match-direction input;
  term t1 {
    then {
      ds-lite ds1;
    }
  }
}
```

---

### Service Set Configuration

**Step-by-Step Procedure**    Configure a service set that includes software and NAT rules and specifies either interface-service or next-hop service. This example uses a next-hop service.

1. Go to the **[edit services service-set]** hierarchy level, naming the service set.

```
user@host# edit services service-set sset
```

2. Define the NAT rule to be used for IPv4-to-IPv4 translation.

```
[edit services service-set sset]
```

```
user@host# set nat-rules r1
```

3. Define the software rule to define the software tunnel.

```
[edit services service-set sset]
```

```
user@host# set software-rules r1
```

4. Define the interface service,

```
[edit services service-set sset]
```

```
user@host# set interface-service service-interface sp-0/0/0.0
```



**TIP:** In order to avoid or minimize IPv6 fragmentation, you can configure a TCP maximum segment size (MSS) for your service set.

5. (Optional) Define a TCP MSS.

```
[edit services service-set sset]
```

```
user@host# set tcp-mss 1024
```

```

Results user@host# show services service-set
        syslog {
            host local {
                services any;
            }
        }
        software-rules r1;
        nat-rules r1;
        interface-service {
            service-interface sp-0/0/0;
        }
    }

```

## Example: Basic 6rd Configuration

- [Requirements on page 21](#)
- [Overview on page 21](#)
- [Configuration on page 21](#)

### Requirements

This example describes how a 6rd concentrator can be configured for a 6rd domain, D1, to provide IPv6 Internet connectivity.

The following hardware components can perform 6rd:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

### Overview

This configuration example describes how to configure a basic 6rd tunneling solution.

### Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```

set interfaces ge-1/2/0 unit 0 family inet service input service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet service output service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet address 10.10.10.1/24
set interfaces ge-1/2/0 unit 0 family inet6 service input service-set v6rd-dom1-service-set
set interfaces ge-1/2/0 unit 0 family inet6 service output service-set v6rd-dom1-service-set
set interfaces ge-1/2/2 unit 0 family inet6 address 3abc::1/16
set interfaces sp-0/2/0 unit 0 family inet
set interfaces sp-0/2/0 unit 0 family inet6
set services software software-concentrator v6rd v6rd-dom1 software-address 30.30.30.1
set services software software-concentrator v6rd v6rd-dom1 ipv4-prefix 10.10.10.0/24
set services software software-concentrator v6rd v6rd-dom1 v6rd-prefix 3040::0/16
set services software software-concentrator v6rd v6rd-dom1 mtu-v4 9192

```

```
set services software rule v6rd-dom1 match-direction input
set services software rule v6rd-dom1 term t1 then v6rd v6rd-dom1
set services service-set v6rd-dom1-service-set software-rules v6rd-dom1
set services service-set v6rd-dom1-service-set stateful-firewall-rules r1
set services service-set v6rd-dom1-service-set interface-service service-interface sp-0/2/0
set services stateful-firewall rule r1 match-direction input-output
set services stateful-firewall rule r1 term t1 then accept
```

---

## Chassis Configuration

### Step-by-Step Procedure

To configure the chassis:

1. Define the ingress interface.  

```
user@host# edit interfaces ge-1/2/0
```
2. Configure the ingress interface logical unit and input/output service options.  

```
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet service input service-set v6rd-dom1-service-set
user@host# set unit 0 family inet service output service-set v6rd-dom1-service-set
user@host# set unit 0 family inet6 service input service-set v6rd-dom1-service-set
user@host# set unit 0 family inet6 service output service-set v6rd-dom1-service-set
```
3. Configure the address of the ingress interface.  

```
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet address 10.10.10.1/24
```
4. Define the egress interface.  

```
user@host# up
[edit interfaces]
user@host# edit ge-1/2/2
```
5. Define the logical unit and address for the egress interface.  

```
[edit interfaces ge-1/2/2]
user@host# set unit 0 family inet6 address 3ABC::1/16
```
6. Define the services PIC.  

```
[edit interfaces ge-1/2/2]
user@host# up
[edit interfaces]
user@host# edit sp-0/2/0
```
7. Configure the logical unit for the services PIC.  

```
[edit interfaces sp-0/2/0]
user@host# up
[edit interfaces]
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
```

```

Results [edit interfaces]
user@router# show
sp-0/2/0 {
    unit 0 {
        family inet;
        family inet6;
    }
}
ge-1/2/0 {
    unit 0 {
        family inet {
            service {
                input {
                    service-set v6rd-dom1-service-set;
                }
                output {
                    service-set v6rd-dom1-service-set;
                }
            }
            address 10.10.10.1/24;
        }
        family inet6 {
            service {
                input {
                    service-set v6rd-dom1-service-set;
                }
                output {
                    service-set v6rd-dom1-service-set;
                }
            }
        }
    }
}
ge-1/2/2 {
    unit 0 {
        family inet6 {
            address 3abc::1/16;
        }
    }
}

```

### Software Concentrator, Software Rule, and Stateful Firewall Rule Configuration

#### Step-by-Step Procedure

To configure the software concentrator, software rule, and stateful firewall rule:

1. Define the 6rd software concentrator.
 

```

user@host# top
user@host# edit services software software-concentrator v6rd v6rd-dom1

```
2. Configure the software concentrator properties. Here, software address 30.30.30.1 is the software concentrator IPv4 address, 10.10.10.0/24 is the IPv4 prefix of the CE WAN side, and 3040::0/16 is the IPv6 prefix of the 6rd domain D1.
 

```

[edit services software software-concentrator v6rd v6rd-dom1]
user@host# set software-address 30.30.30.1
user@host# set ipv4-prefix 10.10.10.0/24
user@host# set v6rd-prefix 3040::0/16
user@host# set mtu-v4 9192

```

3. Define the software rule.

```
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# up 2
[edit services software]
user@host# edit rule v6rd-dom1
[edit services software rule v6rd-dom1]
user@host# set match-direction input
[edit services software rule v6rd-dom1]
user@host# set term t1 then v6rd v6rd-dom1
```

4. Define a stateful firewall rule and properties. You must configure a stateful firewall rule that accepts all traffic in both the input and output direction in order for 6rd to work; however, this is not enforced through the CLI. This is because in IPv6, gratuitous IPv6 packets are expected (due to Anycast) and should not be dropped. The service PIC can handle reverse traffic without seeing all forward traffic. This can also happen with service PIC switchover in the middle of a session. By default, the stateful firewall on the service PIC will drop all traffic unless a rule is configured explicitly to allow it.

```
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# up 3
[edit services]
user@host# edit services stateful-firewall
[edit services stateful-firewall]
user@host# edit rule r1
[edit services stateful-firewall rule r1]
user@host# set match-direction input-output
user@host# set term t1 then accept
```

**Results**

```
[edit services software]
user@router# show
software-concentrator {
  v6rd v6rd-dom1 {
    software-address 30.30.30.1;
    ipv4-prefix 10.10.10.0/24;
    v6rd-prefix 3040::0/16;
    mtu-v4 9192;
  }
}
rule v6rd-dom1-r1 {
  match-direction input;
  term t1 {
    then {
      v6rd v6rd-dom1;
    }
  }
}
```

---

### Service Set Configuration

**Step-by-Step Procedure** To configure the service set:

1. Define the service set for 6rd processing.

```
user@host# top
user@host# edit services service-set v6rd-dom1-service-set
```

2. Define the software and stateful firewall rules for the service set.

```
[edit services service-set v6rd-dom1-service-set]
user@host# set software-rules v6rd-dom1
user@host# set stateful-firewall-rules r1
```

3. Define the interface-service for the service set.

```
[edit services service-set v6rd-dom1-service-set]
user@host# set interface-service service-interface sp-0/2/0
```

**Results**

```
[edit service-set v6rd-dom1-service-set]
user@host# show
software-rules v6rd-dom1-r1
  interface-service {
    service-interface sp-0/2/0;
  }
```

## Example: Configuring DS-Lite and 6rd in the Same Service Set

- [Requirements on page 25](#)
- [Overview on page 25](#)
- [Configuration on page 25](#)

### Requirements

The following hardware components can perform DS-Lite:

- M Series Multiservice Edge routers with Multiservices PICs
- T Series Core routers with Multiservices PICs
- MX Series 3D Universal Edge routers with Multiservices DPCs

### Overview

This example describes a software solution that includes DS-Lite and 6rd in the same service set.

### Configuration

#### Chassis Configuration

##### Step-by-Step Procedure

To configure the chassis:

1. Configure the ingress interface.

```
user@host# edit interfaces ge-1/2/0
[edit interfaces ge-1/2/0]
user@host# set unit 0 family inet service input service-set v6rd-dslite-service-set
user@host# set unit 0 family inet service output service-set v6rd-dslite-service-set
user@host# set unit 0 family inet address address 10.10.10.1/24
user@host# set unit 0 family inet6 service input service-set v6rd-dslite-service-set
user@host# set unit 0 family inet6 service output service-set v6rd-dslite-service-set
user@host# set unit 0 family inet6 address address address 2001::1/16
```

Here the service set is applied on the inet (IPv4) and inet6 (IPv6) families of subunit 0. Both DS-Lite IPv6 traffic and 6rd IPv4 traffic hits the service filter and is sent to the services PIC.

2. Configure the egress interface (IPv6 Internet). The IPv4 server that the DS-Lite clients are trying to reach is at 200.200.200.2/24, and the IPv6 server is at 3ABC::2/16.

```
user@host# edit interfaces ge-1/2/2
[edit interfaces ge-1/2/2]
user@host# set unit 0 family inet address 200.200.200.1/24
user@host# set unit 0 family inet6 address 3ABC::1/16
```

3. Configure the services PIC.

```
user@host# edit interfaces sp-3/0/0
[edit interfaces sp-3/0/0]
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
```



**Results** [edit interfaces]  
 user@host# show  
 ge-1/2/0 {  
   unit 0 {  
     family inet {  
       service {  
         input {  
           service-set v6rd-dslite-service-set;  
         }  
         output {  
           service-set v6rd-dslite-service-set;  
         }  
       }  
       address 10.10.10.1/24;  
     }  
     family inet6 {  
       service {  
         input {  
           service-set v6rd-dslite-service-set;  
         }  
         output {  
           service-set v6rd-dslite-service-set;  
         }  
       }  
       address 2001::1/16;  
     }  
   }  
 }  
 ge-1/2/2 {  
   unit 0 {  
     family inet {  
       address 200.200.200.1/24;  
     }  
     family inet6 {  
       address 3ABC::1/16;  
     }  
   }  
 }  
 sp-3/0/0 {  
   unit 0 {  
     family inet;  
     family inet6;  
   }  
 }

### Software Concentrator, Software Rule, Stateful Firewall Rule Configuration

**Step-by-Step Procedure** To configure the software concentrator, software rule, and stateful firewall rule:

1. Configure the DS-Lite and 6rd software concentrators.  

```

user@host# edit services software software-concentrator ds-lite ds1
[edit services software software-concentrator ds-lite ds1]
user@host# set software-address 1001::1
user@host# mtu-v6 9192
user@host# up 1
user@host# edit v6rd v6rd-dom1
[edit services software software-concentrator v6rd v6rd-dom1]
user@host# set software-address 30.30.30.1
user@host# set ipv4-prefix 10.10.10.0/24

```

```
user@host# set v6rd-prefix 3040::0/16
user@host# set mtu-v4 9192
```

2. Configure the software rules.

```
user@host# edit services software rule v6rd-r1]
[edit services software rule v6rd-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd v6rd-dom1
user@host# up 1
user@host# edit services software]
[edit services software]
user@host# edit rule dslite-r1
[edit services software rule dslite-r1]
user@host# set term dslite-t1 then ds-lite ds1
```

The following routes are added by the services PIC daemon on the Routing Engine:

```
user@router# run show route 30.30.30.1
inet.0: 43 destinations, 46 routes (42 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

30.30.30.1/32      *[Static/786432] 00:24:11
                  Service to v6rd-dslite-service-set

[edit]
user@router# run show route 3040::0/16

inet6.0: 23 destinations, 33 routes (23 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3040::/16         *[Static/786432] 00:24:39
                  Service to v6rd-dslite-service-set

user@router# run show route 1001::1
inet6.0: 33 destinations, 43 routes (33 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

1001::1/128      *[Static/1] 1w2d 22:05:41
                  Service to v6rd-dslite-service-set
```

3. Configure a stateful firewall rule.

```
user@host# edit services stateful-firewall rule r1
[edit services stateful-firewall rule r1]
user@host# set match-direction input-output
user@host# set term t1 then accept

[edit services stateful-firewall]
rule r1 {
  match-direction input-output;
  term t1 {
    then {
      accept;
    }
  }
}
```

```

Results [edit services software]
user@host# show
software-concentrator {
  ds-lite ds1 {
    software-address 1001::1;
    mtu-v6 9192;
  }
  v6rd v6rd-dom1 {
    software-address 30.30.30.1;
    ipv4-prefix 10.10.10.0/24;
    v6rd-prefix 3040::0/16;
    mtu-v4 9192;
  }
}
rule v6rd-r1 {
  match-direction input;
  term t1 {
    then {
      v6rd v6rd-dom1;
    }
  }
}
rule dslite-r1 {
  match-direction input;
  term dslite-t1 {
    then {
      ds-lite ds1;
    }
  }
}

```

```

[edit services stateful-firewall]
user@host# show
rule r1 {
  match-direction input-output;
  term t1 {
    then {
      accept;
    }
  }
}

```

### NAT Configuration for DS-Lite

#### Step-by-Step Procedure

To configure NAT for DS-Lite:

1. Configure a NAT pool for DS-Lite.

```

user@host# edit services nat pool dslite-pool
[edit services nat pool dslite-pool]
user@host# set address-range low 33.33.33.1 high 33.33.33.32
user@host# set port automatic

```

2. Configure a NAT rule.

```

user@host# up 1
[edit services nat rule dslite-nat-r1]
user@host# set match-direction input
user@host# set term dslite-nat-t1 from source-address 20.20.0.0/16 then translated
translation-type napt-44

```

**Results** [edit services nat]  
user@host# **show**  
pool dslite-pool {  
 address-range low 33.33.33.1 high 33.33.33.32;  
 port {  
 automatic;  
 }  
}  
rule dslite-nat-r1 {  
 match-direction input;  
 term dslite-nat-t1 {  
 from {  
 source-address {  
 20.20.0.0/16;  
 }  
 }  
 then {  
 translated {  
 source-pool dslite-pool;  
 translation-type {  
 source dynamic;  
 }  
 }  
 }  
 }  
}

Because of this NAT rule, the following NAT routes are installed for the reverse DS-Lite traffic:

```
user@router# run show route 33.33.33.0/24
inet.0: 48 destinations, 52 routes (47 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

33.33.33.1/32      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.2/31      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.4/30      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.8/29      *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.16/28     *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
33.33.33.32/32     *[Static/1] 1w2d 23:08:38
                  Service to v6rd-dslite-service-set
```

The NAT rule triggers address translation for the traffic coming from 20.20.0.0/16 to public address range 33.33.33.1 to 33.33.33.32.

---

### Service Set Configuration

#### Step-by-Step Procedure

This service set has a stateful firewall rule and 6rd rule for 6rd service. The service set also includes a software rule for DS-Lite and a NAT rule to perform address translation for all DS-Lite traffic. The NAT rule performs NAPT translation in the forward direction on the source address and port of the DS-Lite traffic.

To configure the service set:

1. Define the service set.  

```
user@host# edit services service-set v6rd-dslite-service-set
```
2. Configure the service set rules.  

```
[edit services service-set v6rd-dslite-service-set]  
user@host# set software-rules dslite-r1  
user@host# set stateful-firewall-rules r1  
user@host# set nat-rules dslite-nat-r1
```
3. Configure the service set interface-service.  

```
[edit services service-set v6rd-dslite-service-set]  
user@host# set interface-service service-interface sp-3/0/0
```

**Results**

```
[edit services service-set]  
user@host# show  
v6rd-dslite-service-set {  
  software-rules v6rd-r1;  
  software-rules dslite-r1;  
  stateful-firewall-rules r1;  
  nat-rules dslite-nat-r1;  
  interface-service {  
    service-interface sp-3/0/0;  
  }  
}
```



## CHAPTER 4

# Configuration Statements

## ds-lite

---

|                          |   |
|--------------------------|---|
| Syntax                   | <pre>ds-lite <i>ds-lite-software-concentrator</i>{<br/>  auto-update-mtu;<br/>  copy-dscp;<br/>  flow-limit <i>flow-limit</i>;<br/>  mtu-v6 <i>mtu-v6</i>;<br/>  software-address <i>software-address</i>;<br/>}</pre>  |
| Hierarchy Level          | [edit services software <a href="#">software-concentrator</a> ]   |
| Release Information      | <p>Statement introduced in Junos OS Release 10.4.</p> <p><b>auto-update-mtu</b> option introduced in Junos OS Release 10.4.</p> <p><b>copy-dscp</b> option introduced in Junos OS Release 11.2.</p> <p><b>mtu-v6</b> option introduced in Junos OS Release 10.4.</p> <p><b>software-address</b> option introduced in Junos OS Release 10.4.</p>   |
| Description              | Configure settings for a DS-Lite concentrator used to process IPv4 packets encapsulated in IPv6.  |
| Options                  | <p><b><i>ds-lite-software-concentrator</i></b>—Name applied to a DS-Lite software concentrator.</p> <p><b>auto-update-mtu</b>—This option is not currently supported.</p> <p><b>copy-dscp</b>—Copy DSCP information to IPv4 headers during decapsulation.</p> <p><b><i>flow-limit</i></b>—Maximum number of IPv4 flows per software (0 through 16384).</p> <p><b><i>mtu-v6</i></b>—Maximum transmission unit (MTU), in bytes (0 through 9192), for encapsulating IPv4 packets into IPv6. If the final length is greater than the configured value, the IPv6 packet is fragmented.</p> <p><b><i>software-address</i></b>—Address of the DS-Lite software concentrator.</p> |
| Required Privilege Level | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>  |
| Related Documentation    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a DS-Lite Software Concentrator on page 11</a></li></ul>  |



## rule (Software)

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>rule <i>rule-name</i> {     match-direction (input   output);     term <i>term-name</i> {         then {             (ds-lite <i>ds-lite-software-concentrator</i>   v6rd <i>v6rd-software-concentrator</i>);         }     } }</pre>   |
| <b>Hierarchy Level</b>          | [edit services software],<br>[edit services software rule-set <i>rule-set-name</i> ]   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.   |
| <b>Description</b>              | Configure a rule to apply a software concentrator for a flow.  |
| <b>Options</b>                  | <p><b><i>rule-name</i></b>—Identifier for the collection of terms that constitute this rule.</p> <p><b>input</b>—Apply the rule match on the input side of the interface.</p> <p><b>output</b>—Apply the rule match on the output side of the interface.</p> <p>The remaining statements are explained separately.</p> |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Software Rules on page 12</a></li> </ul>  |

## rule-set (Software)

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <pre>rule-set <i>rule-set-name</i> {     rule <i>rule-name</i>; }</pre>   |
| <b>Hierarchy Level</b>          | [edit services software]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.  |
| <b>Description</b>              | Specify the rule set the router uses when applying this service.  |
| <b>Options</b>                  | <p><b><i>rule-set-name</i></b>—Identifier for the collection of rules that constitute this rule set.</p>                |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration. |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring Software Rules on page 12</a></li> </ul>               |

## software-concentrator

---

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>software-concentrator {<br/>  ds-lite ds-lite-software-concentrator {<br/>    auto-update-mtu;<br/>    flow-limit flow-limit;<br/>    mtu-v6 mtu-v6;<br/>    software-address address;<br/>  }<br/>  v6rd v6rd-software-concentrator {<br/>    ipv4-prefix ipv4-prefix;<br/>    v6rd-prefix ipv6-prefix;<br/>    mtu-v4 mtu-v4;<br/>  }<br/>}</pre> |
| <b>Hierarchy Level</b>          | [edit services software]   |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.   |
| <b>Description</b>              | Configure settings for a software concentrator.  |
| <b>Options</b>                  | The statements are explained separately.   |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.  |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring a DS-Lite Software Concentrator on page 11</a></li><li>• <a href="#">Configuring a 6rd Software Concentrator on page 11</a></li></ul>  |

## software-rules

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | (software-rule <i>rule-name</i>   software-rule-sets <i>rule-set-name</i> );  |
| <b>Hierarchy Level</b>          | [edit services service-set <i>service-set-name</i> ]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.  |
| <b>Description</b>              | Specify the DS-Lite or 6rd rules or rule set included in this service set. You can configure multiple rules; however, you can only configure one rule set for each service set. |
| <b>Options</b>                  | <i>rule-name</i> —Identifier for the collection of terms that constitute this rule.<br><br><i>rule-set-name</i> —Identifier for the set of rules to be included.                |
| <b>Required Privilege Level</b> | interface—To view this statement in the configuration.<br>interface-control—To add this statement to the configuration.   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"><li>• <a href="#">Configuring Service Rules</a></li></ul>   |

## v6rd

|                                 |  |
|---------------------------------|--|
| <b>Syntax</b>                   | <pre>v6rd v6rd-softwire-concentrator {   ipv4-prefix <i>ipv4-prefix</i>;   v6rd-prefix <i>ipv6-prefix</i>;   mtu-v4 <i>mtu-v4</i>;   softwire-address <i>ipv4-address</i>; }</pre>   |
| <b>Hierarchy Level</b>          | [edit services softwire <a href="#">softwire-concentrator</a> ]  |
| <b>Release Information</b>      | Statement introduced in Junos OS Release 10.4.   |
| <b>Description</b>              | Configure settings for a 6rd concentrator used to process IPv6 packets encapsulated in IPv4 packets.   |
| <b>Options</b>                  | <p><i>ipv4-prefix</i>—IPv4 prefix of the customer edge (CE) network</p> <p><i>ipv6-prefix</i>—IPv6 prefix of the 6rd domain.</p> <p><i>mtu-v4</i>—Maximum transmission unit (MTU), in bytes (576 through 9192), for IPv6 packets encapsulated into IPv4. If the final length is greater than the configured value, the IPv4 packet will be dropped.</p> <p><i>address</i>—IPv4 address of a softwire concentrator. This is an IPv4 address independent of any interface and on a different prefix.</p> |
| <b>Required Privilege Level</b> | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>   |
| <b>Related Documentation</b>    | <ul style="list-style-type: none"> <li>• <a href="#">Configuring a 6rd Softwire Concentrator on page 11</a></li> </ul>   |



## PART 3

# Administration

- [Softwire Operational Mode Commands on page 41](#)



## CHAPTER 5

# Softwire Operational Mode Commands

## clear services software statistics

---

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <code>clear services software statistics</code><br><code>&lt;interface <i>interface-name</i>&gt;</code>   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.4.  |
| <b>Description</b>              | Clear software statistics.  |
| <b>Options</b>                  | <code>interface <i>interface-name</i></code> — (Optional) Name of the interface servicing the software. When you omit this option, data for all interfaces are cleared. |
| <b>Required Privilege Level</b> | view  |
| <b>List of Sample Output</b>    | <a href="#">clear services software statistics on page 42</a>   |
| <b>Output Fields</b>            | When you enter this command, you are provided feedback on the status of your request.   |

### Sample Output

|   |   |
|---|---|
| <code>clear services software statistics</code> | <code>user@host&gt; clear services software statistics</code> |
|---|---|



## show services software

|                                 |   |
|---------------------------------|---|
| <b>Syntax</b>                   | <b>show services software</b><br><b>&lt;count&gt;</b>   |
| <b>Release Information</b>      | Command introduced in Junos OS Release 10.4.<br><count> option added in Junos OS Release 11.2.  |
| <b>Description</b>              | Display information about software services. Information is displayed on both 6rd and DS-Lite services.   |
| <b>Options</b>                  | <b>count</b> <i>interface-name</i> —(Optional) Display the current software counts for a service set for both DS-Lite and 6rd.  |
| <b>Required Privilege Level</b> | view  |
| <b>List of Sample Output</b>    | <a href="#">show services software on page 43</a><br><a href="#">show services software count on page 43</a>  |
| <b>Output Fields</b>            | <a href="#">Table 3 on page 43</a> lists the output fields for the <b>command-name</b> command. Output fields are listed in the approximate order in which they appear. |

**Table 3: show-services-software Output Fields**

| Field Name         | Field Description  | Level of Output |
|--------------------|--|-----------------|
| <b>Interface</b>   | Interface for which information is displayed.                | All levels      |
| <b>Service Set</b> | Service set containing the software rules for the interface. | All levels      |
| <b>Software</b>    | Name of the software concentrator.                           | All levels      |
| <b>Direction</b>   | Direction of the flow.                                       | All levels      |
| <b>Flow count</b>  | Number of flows.   | All levels      |

## Sample Output

```

show services software  user@host> show services software
                        Interface: sp-3/0/0, Service set: v6rd-dom1-dom3-service-set
                        Software
                        10.10.10.2      ->      30.30.30.1      Direction      Flow count
                                           I              13

show services software  user@host> show services software count
count                  Interface      Service set      DS-Lite      6RD
                        sp-0/0/0      dslite-svc-set1  2            0

```

## show services stateful-firewall flows

---

**Syntax**    `show services stateful-firewall flows`  
              `<brief | extensive | summary | terse>`  
              `<application-protocol protocol>`  
              `<count>`  
              `<destination-port destination-port>`  
              `<destination-prefix destination-prefix>`  
              `<interface interface-name>`  
              `<limit number>`  
              `<protocol protocol>`  
              `<service-set service-set>`  
              `<source-port source-port>`  
              `<source-prefix source-prefix>`

**Release Information**    Command introduced before Junos OS Release 7.4.  
                              **pgcp** option introduced in Junos OS Release 8.4.  
                              **application-protocol** option introduced in Junos OS Release 10.4.

**Description**    Display stateful firewall flow table entries. When the interface is used for software processing, the type of software concentrator (**DS-LITE** or **6rd**) is shown, and frame counts are provided.

**Options**    **none**—Display standard information about all stateful firewall flows.

**brief | extensive | summary | terse**—(Optional) Display the specified level of output.

**application-protocol *application-protocol***—(Optional) Display information about one of the following application-level gateway (ALG) protocol types:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment (DCE) remote procedure call (RPC) protocol



.....  
**NOTE:** Use this option to select Microsoft Remote Procedure Call (MSRPC).  
.....

- **dce-rpc-portmap**—Distributed Computing Environment (DCE) remote procedure call (RPC) portmap protocol
- **dns**—Domain Name Service protocol
- **exec**—Remote execution protocol
- **ftp**—File Transfer Protocol
- **h323**—H.323 protocol
- **icmp**—Internet Control Message Protocol
- **iioip**—Internet Inter-ORB Protocol

- **ip**—Internet protocol
- **netbios**—NetBIOS protocol
- **netshow**—Netshow protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **realaudio**—RealAudio protocol
- **rpc**—Remote Procedure Call protocol



**NOTE:** Use this option to select Sun Microsystems Remote Procedure Call protocol (SunRPC).

- **rpc-portmap**—Remote Procedure Call portmap protocol
- **rtsp**—Real-Time Streaming Protocol
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **talk**—Talk protocol
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

**count**—(Optional) Display a count of the matching entries.

**destination-port *destination-port***—(Optional) Display information for a particular destination port. The range of values is from 0 to 65535.

**destination-prefix *destination-prefix***—(Optional) Display information for a particular destination prefix.

**interface *interface-name***—(Optional) Display information about a particular interface.  
On M Series and T Series routers, *interface-name* can be **ms-fpc/pic/port** or **rspnumber**.  
On J Series routers, *interface-name* is **ms-pim/0/port**.

**limit *number***—(Optional) Maximum number of entries to display.

**protocol *protocol***—(Optional) Display information about one of the following IP types:

- **number**—Numeric protocol value from 0 to 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol

- **icmp**—Internet Control Message Protocol
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-within-IP Encapsulation Protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

**service-set *service-set***—(Optional) Display information for a particular service set.

**source-port *source-port***—(Optional) Display information for a particular source port. The range of values is from 0 to 65535.

**source-prefix *source-prefix***—(Optional) Display information for a particular source prefix.

**Required Privilege Level** view

**Related Documentation** • clear services stateful-firewall flows

**List of Sample Output** [show services stateful-firewall flows on page 48](#)  
[show services stateful-firewall flows \(For Software Flows\) on page 48](#)  
[show services stateful-firewall flows brief on page 48](#)  
[show services stateful-firewall flows extensive on page 48](#)  
[show services stateful-firewall flows count on page 49](#)  
[show services stateful-firewall flows destination port on page 49](#)  
[show services stateful-firewall flows source port on page 49](#)  
[show services stateful-firewall flows \(Twice NAT\) on page 49](#)

**Output Fields** [Table 4 on page 46](#) lists the output fields for the **show services stateful-firewall flows** command. Output fields are listed in the approximate order in which they appear.

**Table 4: show services stateful-firewall flows Output Fields**

| Field Name               | Field Description   |
|--------------------------|---|
| <b>Interface</b>         | Name of the interface.  |
| <b>Service set</b>       | Name of a service set. Individual empty service sets are not displayed. If no service set has any flows, a flow table header is displayed for each service set. |
| <b>Flow Count</b>        | Number of flows in a session.   |
| <b>Flow or Flow Prot</b> | Protocol used for this flow.  |

Table 4: show services stateful-firewall flows Output Fields (*continued*)

| Field Name | Field Description   |
|------------|---|
| Source     | Source prefix of the flow in the format <i>source-prefix:port</i> . For ICMP flows, port information is not displayed.  |
| Dest       | Destination prefix of the flow. For ICMP flows, port information is not displayed.  |
| State      | Status of the flow: <ul style="list-style-type: none"><li>• <b>Drop</b>—Drop all packets in the flow without response.</li><li>• <b>Forward</b>—Forward the packet in the flow without looking at it.</li><li>• <b>Reject</b>—Drop all packets in the flow with response.</li><li>• <b>Watch</b>—Inspect packets in the flow.</li></ul> |
| Dir        | Direction of the flow: input (I) or output (O).   |
| Frm count  | Number of frames in the flow.   |

## Sample Output

### show services stateful-firewall flows

```
user@host> show services stateful-firewall flows
Interface: ms-1/3/0, Service set: green
```

```
Flow
Prot    Source                Dest                State    Dir    Frm count
TCP     10.58.255.178:23    ->    10.59.16.100:4000 Forward  0
TCP     10.58.255.50:33005-> 10.58.255.178:23 Forward  I      1
Source NAT 10.58.255.50:33005-> 10.59.16.100:4000
Destin NAT 10.58.255.178:23    ->    0.0.0.0:4000
```

### show services stateful-firewall flows (For Software Flows)

When a service set includes software processing, the following output format is used for the software flows:

```
user@host> show services stateful-firewall flows
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow
TCP     200.200.200.2:80    ->    44.44.44.1:1025 Forward  0      219942
NAT dest 44.44.44.1:1025    ->    20.20.1.4:1025
Software 2001::2          ->    1001::1
TCP     20.20.1.2:1025    ->    200.200.200.2:80 Forward  I      110244
NAT source 20.20.1.2:1025 ->    44.44.44.1:1024
Software 2001::2          ->    1001::1
TCP     200.200.200.2:80 ->    44.44.44.1:1024 Forward  0      219140
NAT dest 44.44.44.1:1024 ->    20.20.1.2:1025
Software 2001::2          ->    1001::1
DS-LITE 2001::2          ->    1001::1 Forward  I      988729
TCP     200.200.200.2:80 ->    44.44.44.1:1026 Forward  0      218906
NAT dest 44.44.44.1:1026 ->    20.20.1.3:1025
Software 2001::2          ->    1001::1
TCP     20.20.1.3:1025 ->    200.200.200.2:80 Forward  I      110303
NAT source 20.20.1.3:1025 ->    44.44.44.1:1026
Software 2001::2          ->    1001::1
TCP     20.20.1.4:1025 ->    200.200.200.2:80 Forward  I      110944
NAT source 20.20.1.4:1025 ->    44.44.44.1:1025
Software 2001::2          ->    1001::1
```

### show services stateful-firewall flows brief

The output for the **show services stateful-firewall flows brief** command is identical to that for the **show services stateful-firewall flows** command. For sample output, see [show services stateful-firewall flows](#).

### show services stateful-firewall flows extensive

```
user@host> show services stateful-firewall flows extensive
Interface: ms-0/3/0, Service set: ss_nat
```

```
Flow
count
TCP     16.1.0.1:2330    ->    16.49.0.1:21      Forward  I
8
NAT source 16.1.0.1:2330    ->    16.41.0.1:2330
NAT dest 16.49.0.1:21     ->    16.99.0.1:21
Byte count: 455, TCP established, TCP window size: 57344
TCP acknowledge: 3251737524, TCP tickle enabled, tcp_tickle: 0
Flow role: Master, Timeout: 720
TCP     16.99.0.1:21    ->    16.41.0.1:2330    Forward  0
5
NAT source 16.99.0.1:21    ->    16.49.0.1:21
```

```

      NAT dest      16.41.0.1:2330  ->      16.1.0.1:2330
Byte count: 480, TCP established, TCP window size: 57344
TCP acknowledge: 463128048, TCP tickle enabled, tcp_tickle: 0
Flow role: Responder, Timeout: 720

```

#### show services stateful-firewall flows count

```

user@host> show services stateful-firewall flows count
Interface      Service set      Flow Count
ms-1/3/0       green            2

```

#### show services stateful-firewall flows destination port

```

user@router> show services stateful-firewall flows destination-port 21
Interface: ms-0/3/0, Service set: svc_set_trust
Flow
State      Dir      Frm count
Interface: ms-0/3/0, Service set: svc_set_untrust
Flow
TCP      10.50.10.2:2143  ->      10.50.20.2:21  Watch  0      0

```

#### show services stateful-firewall flows source port

```

user@router> show services stateful-firewall flows source-port 2143
Interface: ms-0/3/0, Service set: svc_set_trust
Flow
State      Dir      Frm count
Interface: ms-0/3/0, Service set: svc_set_untrust
Flow
TCP      10.50.10.2:2143  ->      10.50.20.2:21  Watch  0      0

```

#### show services stateful-firewall flows (Twice NAT)

```

user@router> show services stateful-firewall flows
Flow
UDP      40.0.0.8:23439  ->      80.0.0.1:16485  Watch  I      20
  NAT source      40.0.0.8:23439  ->      172.16.1.10:1028
  NAT dest        80.0.0.1:16485  ->      192.16.1.10:22415
UDP      192.16.1.10:22415  ->      172.16.1.10:1028  Watch  0      20
  NAT source      192.16.1.10:22415  ->      80.0.0.1:16485
  NAT dest        172.16.1.10:1028  ->      40.0.0.8:23439

```





## PART 4

# Index

- [Index on page 53](#)



# Index

## Symbols

|  |     |
|--|-----|
| #, comments in configuration statements..... | xii |
| ( ), in syntax descriptions.....             | xii |
| < >, in syntax descriptions.....             | xii |
| [ ], in configuration statements.....        | xii |
| { }, in configuration statements.....        | xii |
| (pipe), in syntax descriptions.....          | xii |

## B

|  |     |
|--|-----|
| braces, in configuration statements..... | xii |
| brackets                                 |     |
| angle, in syntax descriptions.....       | xii |
| square, in configuration statements..... | xii |

## C

|   |      |
|---|------|
| clear services software statistics command..... | 42   |
| comments, in configuration statements.....      | xii  |
| conventions                                     |      |
| text and syntax.....                            | xi   |
| curly braces, in configuration statements.....  | xii  |
| customer support.....                           | xiii |
| contacting JTAC.....                            | xiii |

## D

|                        |      |
|------------------------|------|
| documentation          |      |
| comments on.....       | xiii |
| ds-lite statement..... | 34   |
| usage guidelines.....  | 11   |

## F

|                       |    |
|-----------------------|----|
| font conventions..... | xi |
|-----------------------|----|

## M

|                  |      |
|------------------|------|
| manuals          |      |
| comments on..... | xiii |

## P

|  |     |
|--|-----|
| parentheses, in syntax descriptions..... | xii |
|--|-----|

## R

|                    |        |
|--------------------|--------|
| rule statement     |        |
| software.....      | 12, 35 |
| rule-set statement |        |
| software.....      | 35     |

## S

|  |    |
|--|----|
| show services software command.....      | 43 |
| show services stateful-firewall flows    |    |
| command.....                             | 44 |
| software-concentrator statement.....     | 36 |
| software-rules statement.....            | 36 |
| stateful firewall                        |    |
| flows                                    |    |
| displaying.....                          | 44 |
| support, technical See technical support |    |
| syntax conventions.....                  | xi |

## T

|                      |      |
|----------------------|------|
| technical support    |      |
| contacting JTAC..... | xiii |

## V

|                       |    |
|-----------------------|----|
| v6rd statement.....   | 37 |
| usage guidelines..... | 11 |

