JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Adaptive Services Interfaces User Guide for Routing Devices

Published
2020-09-22

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Junos® OS Adaptive Services Interfaces User Guide for Routing Devices

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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

3

Transitioning to IPv6 Using Softwires

8

Configuring Inter-Chassis MS-MPC and MS-MIC Redundancy for NAT and Stateful Firewall

9

Configuring Interface Redundancy and Bundling on LSQ Interfaces

About the Documentation

IN THIS SECTION

Use this guide to configure and monitor the following services:

- Network Address Translation (NAT)
- Stateful firewalls
- URL filtering
- Intrusion detection service (IDS)
- IP Security (IPsec)
- Application Layer Gateways (ALGs)
- Class of service (CoS) for packets transiting service cards
- Voice services
- Load balancing of server traffic

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 https://www.juniper.net/documentation/.

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 https://www.juniper.net/books.

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.xsl;
           }
       }
   }
   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.xsl; }
   ```

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 CLI Explorer.

Documentation Conventions

Table 1 on page xlviii 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.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

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

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (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.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

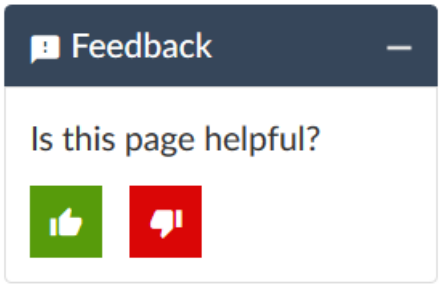
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Juniper Care or Partner Support Services 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- 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 https://support.juniper.net/support/requesting-support/.

1

PART

Overview

CHAPTER 1

Adaptive Services Overview

IN THIS CHAPTER

Adaptive Services Overview

MultiServices PICs and MultiServices Dense Port Concentrators (MS-DPCs) provide *adaptive services interfaces*, which allow you to coordinate multiple services on a single PIC by configuring a set of services and applications. MultiServices PICs and MS-DPCs offer a special range of services you configure in one or more service sets.

The MultiServices PIC is available in three versions, the MultiServices 100, the MultiServices 400, and the MultiServices 500, which differ in memory size and performance. All versions offer enhanced performance in comparison with AS PICs. MultiServices PICs are supported on M Series and T Series routers except M20 routers.

The MultiServices DPC is available for MX Series routers; it includes a subset of the functionality supported on the MultiServices PIC. Currently the MultiServices DPC supports the following Layer 3 services: stateful firewall, NAT, IDS, IPsec, active flow monitoring, RPM, and generic routing encapsulation (GRE) tunnels (including GRE key and fragmentation); it also supports graceful Routing Engine switchover (GRES) and Dynamic Applicaton Awareness for Junos OS. For more information about supported packages, see *Enabling Service Packages*.

It is also possible to group several Multiservices PICs into an aggregated Multiservices (AMS) system. An AMS configuration eliminates the need for separate routers within a system. The primary benefit of having an AMS configuration is the ability to support load balancing of traffic across multiple services PICs. Starting with Junos OS 11.4, all MX Series routers will support high availability (HA) and Network Address Translation (NAT) on AMS infrastructure. See “Configuring Load Balancing on AMS Infrastructure” on page 1004 for more information.

NOTE: The MultiServices PICs are polling based and not interrupt based; as a result, a high value in the **show chassis pic** "Interrupt load average" field may not mean that the PIC has reached its maximum limit of processing.

The following services are configured within a service set and are available only on adaptive services interfaces:

- Stateful firewall—A type of firewall filter that considers state information derived from previous communications and other applications when evaluating traffic.
- Network Address Translation (NAT)—A security procedure for concealing host addresses on a private network behind a pool of public addresses.
- Intrusion detection service (IDS)—A set of tools for detecting, redirecting, and preventing certain kinds of network attack and intrusion.
- IP Security (IPsec)—A set of tools for configuring manual or dynamic security associations (SAs) for encryption of data traffic.
- Class of service (CoS)—A subset of CoS functionality for services interfaces, limited to DiffServ code point (DSCP) marking and forwarding-class assignment. CoS BA classification is not supported on services interfaces.

The configuration for these services comprises a series of rules that you can arrange in order of precedence as a *rule set*. Each rule follows the structure of a firewall filter, with a **from** statement containing input or match conditions and a **then** statement containing actions to be taken if the match conditions are met.

The following services are also configured on the MultiServices PICs and MS-DPCs, but do not use the rule set definition:

- Layer 2 Tunneling Protocol (L2TP)—A tool for setting up secure tunnels using Point-to-Point Protocol (PPP) encapsulation across Layer 2 networks.
- Link Services Intelligent Queuing (LSQ)—Interfaces that support Junos OS class-of-service (CoS) components, link fragmentation and interleaving (LFI) (FRF.12), Multilink Frame Relay (MLFR) user-to-network interface (UNI) network-to-network interface (NNI) (FRF.16), and Multilink PPP (MLPPP).
- Voice services—A feature that uses the Compressed Real-Time Transport Protocol (CRTP) to enable voice over IP traffic to use low-speed links more effectively.

In addition, Junos OS includes the following tools for configuring services:

- Application protocols definition—Allows you to configure properties of application protocols that are subject to processing by router services, and group the application definitions into application sets.
- Service-set definition—Allows you to configure combinations of directional rules and default settings that control the behavior of each service in the service set.

> **NOTE:** Logging of adaptive services interfaces messages to an external server by means of the **fxp0** port is not supported on M Series routers. The architecture does not support system logging traffic out of a management interface. Instead, access to an external server is supported on a Packet Forwarding Engine interface.

RELATED DOCUMENTATION

Services PICs-Overview

Packet Flow Through the Adaptive Services or Multiservices PIC | 4

Enabling Service Packages

Services Configuration Procedure

Supported Platforms

Packet Flow Through the Adaptive Services or Multiservices PIC

You can optionally configure service sets to be applied at one of the following three points while the packets transit the router:

- An interface service set applied at the inbound interface.
- A next-hop service set applied at the forwarding table.
- An interface service set applied at the outbound interface.

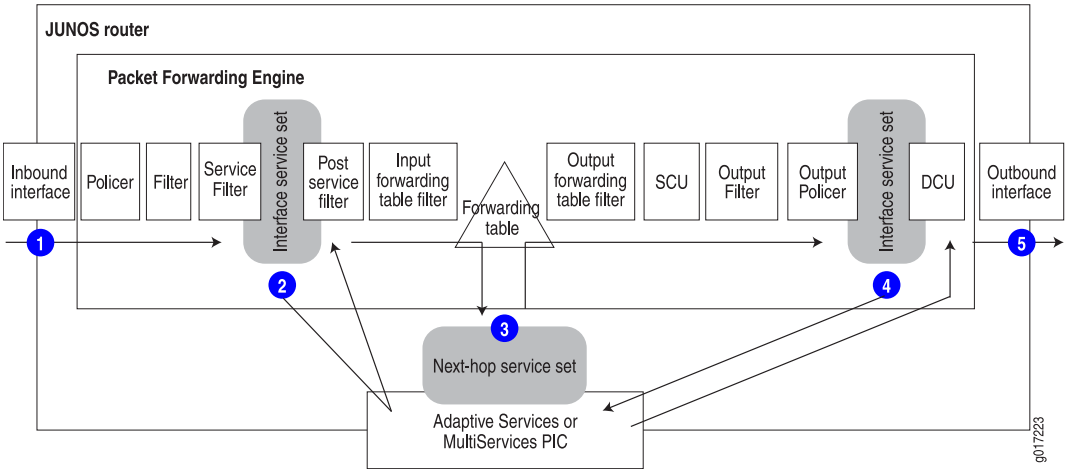
The packet flow is as follows, graphically displayed in Figure 1 on page 5. (You can configure a service set as either an interface service set or a next-hop service set.)

1. Packets enter the router on the inbound interface.
2. A policer, filter, service filter, service set, postservice filter, and input forwarding-table filter are applied sequentially to the traffic; these are all optional items in the configuration. If an interface service set is applied, the packets are forwarded to the AS or MultiServices PIC for services processing and then sent back to the Packet Forwarding Engine; if a service filter is also applied, only packets matching the service filter are sent to the PIC. The optional postservice filter is applied and postprocessing takes place.
3. A next-hop service set can be applied to the VPN routing and forwarding (VRF) table or to **inet.0**. If it is applied, packets are sent to the PIC for services processing and sent back to the Packet Forwarding Engine.

NOTE: For NAT, the next-hop service set can only be applied to the VRF table. For all other services, the next-hop service set can be applied to either the VRF table or to **inet.0**.

4. On the output interface, an output filter, output policer, and interface service set can be applied sequentially to the traffic if you have configured any of these items. If an interface service set is applied, the traffic is forwarded to the PIC for processing and sent back to the Packet Forwarding Engine, which then forwards the traffic.
5. Packets exit the router.

Figure 1: Packet Flow Through the Adaptive Services or MultiServices PIC



NOTE: When an AS PIC experiences persistent back pressure as a result of high traffic volume for 3 seconds, the condition triggers an automatic core dump and reboot of the PIC to help clear the blockage. A system log message at level LOG_ERR is generated. This mechanism applies to both Layer 2 and Layer 3 service packages.

RELATED DOCUMENTATION

Services PICs-Overview

Adaptive Services Overview | 2

Supported Platforms

Services Configuration Procedure

CHAPTER 2

Adaptive Services Configuration Overview

IN THIS CHAPTER

Understanding Service Sets

Junos OS enables you to create service sets that define a collection of services to be performed by an Adaptive Services interface (AS) or Multiservices line cards (MS-DPC, MS-MIC, and MS-MPC). You can configure the service set either as an interface-style service set or as a next-hop-style service set.

An interface service set is used as an action modifier across an entire interface. You can use an interface-style service set when you want to apply services to packets passing through an interface.

A next-hop service set is a route-based method of applying a particular service. Only packets destined for a specific next hop are serviced by the creation of explicit static routes. This configuration is useful when services need to be applied to an entire virtual private network (VPN) routing and forwarding (VRF) table, or when routing decisions determine that services need to be performed. When a next-hop service is configured, the service interface is considered to be a two-legged module with one leg configured to be the inside interface (inside the network) and the other configured as the outside interface (outside the network).

To configure service sets, include the following statements at the **[edit services]** hierarchy level:

```
[edit services]
service-set service-set-name {
    (ids-rules rule-names | ids-rule-sets rule-set-name);
    (ipsec-vpn-rules rule-names | ipsec-vpn-rule-sets rule-set-name);
    max-session-setup-rate max-setup-rate;
    (nat-rules rule-names | nat-rule-sets rule-set-name);
    (pgcp-rules rule-names | pgcp-rule-sets rule-set-name);
    (ptsp-rules rule-names | ptsp-rule-sets rule-set-name);
    (stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
    allow-multicast;
    extension-service service-name {
        provider-specific rules;
    }
    interface-service {
        service-interface interface-name;
    }
    ipsec-vpn-options {
        anti-replay-window-size bits;
        clear-dont-fragment-bit;
        ike-access-profile profile-name;
        local-gateway address;
        no-anti-replay;
        passive-mode-tunneling;
        trusted-ca [ ca-profile-names ];
        tunnel-mtu bytes;
    }
    max-flows number;
    next-hop-service {
        inside-service-interface interface-name.unit-number;
        outside-service-interface interface-name.unit-number;
        service-interface-pool name;
    }
```

```
    syslog {
        host hostname {
            services severity-level;
            facility-override facility-name;
            log-prefix prefix-value;
        }
    }
}
adaptive-services-pics {
    traceoptions {
        file filename <files number> <match regex> <size size> <(world-readable | no-world-readable)>;
        flag flag;
    }
}
logging {
    traceoptions {
        file filename <files number> <match regex> <size size> <(world-readable | no-world-readable)>;
        flag flag;
    }
}
```

RELATED DOCUMENTATION

- Configuring Service Sets to be Applied to Services Interfaces | 9
- Configuring Service Rules | 21
- Configuring IPsec Service Sets | 698
- Configuring Service Set Limitations | 23
- Configuring System Logging for Service Sets | 36
- Enabling Services PICs to Accept Multicast Traffic | 25
- Tracing Services PIC Operations | 38
- Example: Configuring Service Sets | 28

Configuring Service Sets to be Applied to Services Interfaces

IN THIS SECTION

You configure a services interface to specify the adaptive services interface on which the service is to be performed. Services interfaces are used with either of the service set types described in the following sections.

Configuring Interface Service Sets

An interface service set is used as an action modifier across an entire interface. To configure the services interface, include the **interface-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

```
[edit services service-set service-set-name]
interface-service {
   service-interface interface-name;
}
```

Only the device name is needed, because the router software manages logical unit numbers automatically. The services interface must be an adaptive services interface for which you have configured **unit 0 family inet** at the **[edit interfaces *interface-name*** hierarchy level.

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces installed on the router. When you apply the service set to an interface, it automatically ensures that packets are directed to the PIC.

To associate a defined service set with an interface, include a **service-set** statement with the **input** or **output** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
input {
   service-set service-set-name <service-filter filter-name>;
```

```
    post-service-filter filter-name;
}
output {
    service-set service-set-name <service-filter filter-name>;
}
```

If a packet is entering the interface, the match direction is **input**. If a packet is leaving the interface, the match direction is **output**. The service set retains the input interface information even after services are applied, so that functions such as filter-class forwarding and destination class usage (DCU) that depend on input interface information continue to work.

You configure the same service set on the input and output sides of the interface. You can optionally include filters associated with each service set to refine the target and additionally process the traffic. If you include the **service-set** statement without a **service-filter** definition, the router software assumes the match condition is true and selects the service set for processing automatically.

NOTE: If you configure service sets with filters, they must be configured on the input and output sides of the interface.

You can include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order in which they appear in the configuration. The system executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions. A maximum of six service sets can be applied to an interface. When you apply multiple service sets to an interface, you must also configure and apply a service filter to the interface.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the **post-service-filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service input]** hierarchy level:

```
post-service-filter filter-name;
```

The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

For an example, see “Example: Configuring Service Sets” on page 28.

NOTE: With interface-style service sets that are configured with Junos OS extension-provide packages, the traffic fails to get serviced when the ingress interface is part of a VRF instance and the service interface is not part of the same VRF instance.

NOTE: When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the **bypass-traffic-on-pic-failure** statement at the **[edit services service-set *service-set-name* service-set-options]** hierarchy level. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured. This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations using IDP service sets. This forwarding feature worked only with the Packet Forwarding Engine (PFE) initially. Starting with Junos OS Release 11.3, the packet-forwarding feature is extended to packets generated by the Routing Engine for bypass service sets as well.

Configuring Next-Hop Service Sets

A next-hop service set is a route-based method of applying a particular service. Only packets destined for a specific next hop are serviced by the creation of explicit static routes. This configuration is useful when services need to be applied to an entire virtual private network (VPN) routing and forwarding (VRF) table, or when routing decisions determine that services need to be performed.

When a next-hop service is configured, the AS or Multiservices PIC is considered to be a two-legged module with one leg configured to be the inside interface (inside the network) and the other configured as the outside interface (outside the network).

NOTE: You can create IFL indexes greater than 8000 only if the interface service set is not configured.

To configure the domain, include the **service-domain** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
service-domain (inside | outside);
```

The **service-domain** setting must match the configuration for the next-hop service inside and outside interfaces. To configure the inside and outside interfaces, include the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level. The interfaces you specify must be logical interfaces on the same AS PIC. You cannot configure **unit 0** for this purpose, and the logical interface you choose must not be used by another service set.

```
next-hop-service {
    inside-service-interface interface-name.unit-number;
    outside-service-interface interface-name.unit-number;
}
```

Traffic on which the service is applied is forced to the inside interface using a static route. For example:

```
routing-options {
    static {
        route 10.1.2.3 next-hop sp-1/1/0.1;
    }
}
```

After the service is applied, traffic exits by way of the outside interface. A lookup is then performed in the Packet Forwarding Engine (PFE) to send the packet out of the AS or Multiservices PIC.

The reverse traffic enters the outside interface, is serviced, and sent to the inside interface. The inside interface forwards the traffic out of the AS or Multiservices PIC.

Determining Traffic Direction

When you configure next-hop service sets, the AS PIC functions as a two-part interface, in which one part is the *inside* interface and the other part is the *outside* interface. The following sequence of actions takes place:

1. To associate the two parts with logical interfaces, you configure two logical interfaces with the **service-domain** statement, one with the **inside** value and one with the **outside** value, to mark them as either an inside or outside service interface.
2. The router forwards the traffic to be serviced to the inside interface, using the next-hop lookup table.
3. After the service is applied, the traffic exits from the outside interface. A route lookup is then performed on the packets to be sent out of the router.
4. When the reverse traffic returns on the outside interface, the applied service is undone; for example, IPsec traffic is decrypted or NAT addresses are unmasked. The serviced packets then emerge on the inside interface, the router performs a route lookup, and the traffic exits the router.

A service rule's match direction, whether input, output, or input/output, is applied with respect to the traffic flow through the AS PIC, not through a specific inside or outside interface.

When a packet is sent to an AS PIC, packet direction information is carried along with it. This is true for both interface style and next-hop style service sets.

Interface Style Service Sets

Packet direction is determined by whether a packet is entering or leaving any Packet Forwarding Engine interface (with respect to the forwarding plane) on which the **interface-service** statement is applied. This is similar to the input and output direction for stateless firewall filters.

The match direction can also depend on the network topology. For example, you might route all the external traffic through one interface that is used to protect the other interfaces on the router, and configure various services on this interface specifically. Alternatively, you might use one interface for priority traffic and configure special services on it, but not care about protecting traffic on the other interfaces.

Next-Hop Style Service Sets

Packet direction is determined by the AS PIC interface used to route packets to the AS PIC. If you use the **inside-interface** statement to route traffic, then the packet direction is **input**. If you use the **outside-interface** statement to direct packets to the AS PIC, then the packet direction is **output**.

The interface to which you apply the service sets affects the match direction. For example, apply the following configuration:

```
sp-1/1/0 unit 1 service-domain inside;
sp-1/1/0 unit 2 service-domain outside;
```

If you configure **match-direction input**, you include the following statements:

```
[edit]
services service-set test1 next-hop-service inside-service-interface sp-1/0/0.1;
services service-set test1 next-hop-service outside-service-interface sp-1/0/0.2;
services ipsec-vpn rule test-ipsec-rule match-direction input;
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.1;
```

If you configure **match-direction output**, you include the following statements:

```
[edit]
services service-set test2 next-hop-service inside-service-interface sp-1/0/0.1;
services service-set test2 next-hop-service outside-service-interface sp-1/0/0.2;
services ipsec-vpn rule test-ipsec-rule match-direction output;
routing-options static route 10.0.0.0/24 next-hop sp-1/1/0.2;
```

The essential difference between the two configurations is the change in the match direction and the static routes' next hop, pointing to either the AS PIC's inside or outside interface.

RELATED DOCUMENTATION

Service Filters in ACX Series

When you apply a service set to the traffic at an inline services interface, you can optionally use service filters to refine the target of the set of services and also to process traffic. Service filters enable you to manipulate traffic by performing packet filtering to a defined set of services on an inline services interface before the traffic is delivered to its destination. In ACX Series routers, you can apply a service filter to traffic before packets are accepted for input service processing.

> **NOTE:** In ACX Series routers, the **service-set** filters are implemented using ternary content addressable memory (TCAM) space. The allocated TCAM space is shared by the bridge family filter. The same space is shared by the NNI-Address-Overload-Reverse filter (for each service set that is configured with address overloading, the internal filters are configured for the given overloaded IP address and the port range to redirect the matched reverse-nat (public to private) traffic to the service). From a scaling perspective, the allocated 124 hardware TCAM entries are shared by these features and the allocation of TCAM entries works on a first-come-first-serve basis mode.

RELATED DOCUMENTATION

Guidelines for Applying Service Filters

IN THIS SECTION

This topic covers the following information:

Restrictions for Inline Services Interfaces

You can apply a service filter to IPv4 traffic associated with a service set at an *inline services interface* only.

ACX Series routers do not support post-service filters.

Statement Hierarchy for Applying Service Filters

You can enable packet filtering of IPv4 traffic before a packet is accepted for input service processing. To do this, apply a service filter to the inline services interface input in conjunction with an interface service set.

The following configuration shows the hierarchy levels at which you can apply the service filters to inline services interfaces:

```
[edit]
interfaces {
    interface-name {
        unit unit-number {
```

```
            family (inet | inet6) {
               service {
                  input {
                     service-set service-set-name service-filter service-filter-name;
                  }
                  output {
                     [ service-set service-set-name <service-filter filter-name> ];
                  }
               }
            }
         }
      }
   }
```

Associating Service Rules with Inline Services Interfaces

To define and group the service rules be applied to an inline services interface, you define an *interface service set* by including the **service-set** ***service-set-name*** statement at the **[edit services]** hierarchy level.

To apply an interface service set to the input of an inline services interface, you include the **service-set** ***service-set-name*** at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *unit-number* input]**

Filtering Traffic Before Accepting Packets for Service Processing

To filter IPv4 traffic before accepting packets for input service processing, include the **service-set** ***service-set-name*** **service-filter** ***service-filter-name*** at the following hierarchy level:

- **[edit interfaces *interface-name* unit *unit-number* family inet service input]**

For the ***service-set-name***, specify a service set configured at the **[edit services service-set]** hierarchy level.

The service set retains the input interface information even after services are applied, so that functions such as filter-class forwarding that depend on input interface information continue to work.

The following requirements apply to filtering inbound or outbound traffic before accepting packets for service processing:

- You configure the same service set on the input and output sides of the interface.
- If you include the **service-set** statement without an optional **service-filter** definition, Junos OS assumes that the match condition is true and selects the service set for processing automatically.
- The service filter is applied only if a service set is configured and selected.

RELATED DOCUMENTATION

Enabling Inline Services Interface on ACX Series | 116

Understanding Service Sets

Service Filters in ACX Series | 14

Service Filter Match Conditions for IPv4 Traffic | 17

Service Filter Actions | 18

Configuring Service Sets to Be Applied to Services Interfaces

Configuring Queuing and Scheduling on Inline Services Interface | 20

Service Filter Match Conditions for IPv4 Traffic

In ACX Series, service filters support only a subset of the stateless firewall filter match conditions for IPv4 traffic. Table 3 on page 17 describes the service filter match conditions.

Table 3: Service Filter Match Conditions for IPv4 Traffic

Match Condition	Description	Protocol Families
destination-address ***address***	Match the IP destination address field.	**family inet**
destination-port ***number***	Match the UDP or TCP destination port field. You cannot specify both the **port** and **destination-port** match conditions in the same term. If you configure this match condition for IPv4 traffic, we recommend that you also configure the **protocol udp** or **protocol tcp** match statement in the same term to specify which protocol is being used on the port.	**family inet**
ip-options ***values***	Match the 8-bit IP option field, if present, to the specified value or list of values.	**family inet**
protocol ***number***	Match the IP protocol type field.	**family inet**
source-address ***address***	Match the IP source address.	**family inet**

Table 3: Service Filter Match Conditions for IPv4 Traffic *(continued)*

Match Condition	Description	Protocol Families
source-port *number*	Match the UDP or TCP source port field. If you configure this match condition for IPv4 traffic, we recommend that you also configure the **protocol udp** or **protocol tcp** match statement in the same term to specify which protocol is being used on the port.	**family inet**
tcp-flags *value*	Match one or more of the low-order 6 bits in the 8-bit TCP flags field in the TCP header. If you configure this match condition for IPv4 traffic, we recommend that you also configure the **protocol tcp** match statement in the same term to specify that the TCP protocol is being used on the port.	**family inet**

RELATED DOCUMENTATION

- Enabling Inline Services Interface on ACX Series | **116**
- *Understanding Service Sets*
- Service Filters in ACX Series | **14**
- Guidelines for Applying Service Filters | **15**
- Service Filter Actions | **18**
- *Configuring Service Sets to Be Applied to Services Interfaces*
- Configuring Queuing and Scheduling on Inline Services Interface | **20**

Service Filter Actions

ACX Series support different sets of terminating and nonterminating actions that you can configure in a service filter term.

> **NOTE:** Service filters do not support the **next term** action.

Table 4 on page 19 describes the terminating actions you can configure in a service filter term.

Table 4: Terminating Actions for Service Filters

Terminating Action	Description	Protocol Families
service	Direct the packet to service processing.	**inet**

Table 5 on page 19 describes the nonterminating actions you can configure in a service filter term.

Table 5: Nonterminating Actions for Service Filters

Nonterminating Action	Description	Protocol Families
accept	Accept the packet.	**inet**
count ***counter-name***	Count the packet in the named counter.	**inet**
log	Log the packet header information in a buffer within the Packet Forwarding Engine. You can access this information by issuing the **show firewall log** command at the command-line interface (CLI).	**inet**
port-mirror	Port-mirror the packet based on the specified family.	**inet**

RELATED DOCUMENTATION

Enabling Inline Services Interface on ACX Series | 116

Understanding Service Sets

Service Filters in ACX Series | 14

Guidelines for Applying Service Filters | 15

Service Filter Match Conditions for IPv4 Traffic | 17

Configuring Service Sets to Be Applied to Services Interfaces

Configuring Queuing and Scheduling on Inline Services Interface | 20

Configuring Queuing and Scheduling on Inline Services Interface

To configure queuing and scheduling on an inline services interface, you need to include **scheduler-map** statement at the **[edit class-of-services interfaces si-/0/0/0]** hierarchy level.

```
[edit class-of-service]
scheduler-maps <scheduler-map-name>;
interfaces si-0/0/0; {
scheduler-map <scheduler-map-name>;
}
```

The **queue-number** *7* of the inline services interface has *strict-high* priority because the timing packets received by ACX Series routers gets assigned to this queue. You can explicitly override this strict-high priority by assigning an explicit scheduler for **queue-number** *7* in the **scheduler-map** statement attached to inline services interface as shown below:

```
[edit class-of-service]
forwarding-classes {
   class <class-name> queue-number 7;
}
interfaces {
   si-0/0/0{
   scheduler-map scheduler-map-name;
   }
}
scheduler-maps {
   <map-name> {
   forwarding-class <class-name> scheduler <scheduler-name>;
   }
}
schedulers {
   <scheduler-name> {
   priority low ;
   }
}
```

The following are the CoS limitations for inline services:

- Inline services packets classified with packet loss priority as *medium-high* in the ingress path are treated as *high* on the egress path.
- When both timing and NAT services are enabled on the router, you should not classify NAT traffic into a forwarding class mapped with **queue-number** *7*, because if you do so, the performance of timing services can degrade.

- If a scheduler with **queue-number** *7* in the **scheduler-map** statement is attached to an inline services interface, then the scheduler should be configured with *strict* priority, else the timing performance can degrade.

RELATED DOCUMENTATION

Network Address Translation Overview on ACX Series | **96**

Network Address Port Translation Overview | **98**

Enabling Inline Services Interface on ACX Series | **116**

Understanding Service Sets

Service Filters in ACX Series | **14**

Network Address Translation Address Overload in ACX Series | **98**

Network Address Translation Constraints on ACX | **100**

Configuring Address Pools for Network Address Port Translation (NAPT) Overview | **115**

Configuring Service Sets to Be Applied to Services Interfaces

Configuring Service Rules

You specify the collection of rules and rule sets that constitute the service set. The router performs rule sets in the order in which they appear in the configuration. You can include only one rule set for each service type. You configure the rule names and content for each service type at the **[edit services *name*]** hierarchy level for each type:

- You configure intrusion detection service (IDS) rules at the **[edit services ids]** hierarchy level; for more information, see "Configuring IDS Rules on an MS-DPC" on page 583 for MS-DPC cards and "Configuring Protection Against Network Attacks on an MS-MPC" on page 601 for MS-MPC cards.
- You configure IP Security (IPsec) rules at the **[edit services ipsec-vpn]** hierarchy level; for more information, see "Understanding Junos VPN Site Secure" on page 618..
- You configure Network Address Translation (NAT) rules at the **[edit services nat]** hierarchy level; for more information, see "Junos Address Aware Network Addressing Overview" on page 78..
- You configure packet-triggered subscribers and policy control (PTSP) rules at the **[edit services ptsp]** hierarchy level; for more information, see *Configuring PTSP Service Rules*.

- You configure softwire rules for DS-Lite or 6rd softwires at the **[edit services softwire]** hierarchy level; for more information, see "Configuring Softwire Rules" on page 381.
- You configure stateful firewall rules at the **[edit services stateful-firewall]** hierarchy level; for more information, see "Configuring Stateful Firewall Rules" on page 546.

To configure the rules and rule sets that constitute a service set, include the following statements at the **[edit services service-set *service-set-name*]** hierarchy level:

```
([ ids-rules rule-names ] |ids-rule-sets rule-set-name);
([ ipsec-vpn-rules rule-names ] | ipsec-vpn-rule-sets rule-set-name);
([ nat-rules rule-names ] | nat-rule-sets rule-set-name);
([ pgcp-rules rule-names] | pgcp-rule-sets rule-set-name);
([softwire-rules rule-names] | softwire-rule-sets rule-set-name);
([ stateful-firewall-rules rule-names ] | stateful-firewall-rule-sets rule-set-name);
```

For each service type, you can include one or more individual rules, or one rule set.

If you configure a service set with IPsec rules, it must not contain rules for any other services. You can, however, configure another service set containing rules for the other services and apply both service sets to the same interface.

NOTE: You can also include Junos Application Aware (previously known as Dynamic Application Awareness) functionality within service sets. To do this, you must include an **idp-profile** statement at the **[edit services service-set]** hierarchy level, along with application identification (APPID) rules, and, as appropriate, application-aware access list (AACL) rules and a **policy-decision-statistics-profile**. Only one service sets can be applied to a single interface when Junos Application Aware functionality is used. For more information, see "Configuring IDS Rules on an MS-DPC" on page 583, *APPID Overview*, and *Application Aware Services Interfaces User Guide for Routing Devices*.

RELATED DOCUMENTATION

Understanding Service Sets | 6

Configuring Service Sets to be Applied to Services Interfaces | 9

Configuring Service Set Limitations | 23

Configuring System Logging for Service Sets | 36

Configuring Service Set Limitations

You can set the following limitations on service set capacity:

- You can limit the maximum number of flows allowed per service set. To configure the maximum value, include the **max-flows** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

  ```
  [edit services service-set service-set-name]
  max-flows number;
  ```

  The **max-flows** statement permits you to assign a single flow limit value. For IDS service sets only, you can specify various types of flow limits with a finer degree of control. For more information, see the description of the **session-limit** statement in "Configuring IDS Rule Sets on an MS-DPC" on page 592.

  > **NOTE:** When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the **max-flow** value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the **max-flow** value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective **max-flow** value of 4000.

- You can limit the maximum segment size (MSS) allowed by the Transmission Control Protocol (TCP). To configure the maximum value, include the **tcp-mss** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

  ```
  [edit services service-set service-set-name]
  tcp-mss number;
  ```

  The TCP protocol negotiates an MSS value during session connection establishment between two peers. The MSS value negotiated is primarily based on the MTU of the interfaces to which the communicating peers are directly connected to. However in the network, due to variation in link MTU on the path taken by the TCP packets, some packets that are still well within the MSS value may be fragmented when the concerned packet's size exceeds the link's MTU.

  If the router receives a TCP packet with the SYN bit and MSS option set and the MSS option specified in the packet is larger than the MSS value specified by the **tcp-mss** statement, the router replaces the MSS value in the packet with the lower value specified by the **tcp-mss** statement. The range for the **tcp-mss *mss-value*** parameter is from **536** through **65535**.

  To view statistics of SYN packets received and SYN packets whose MSS value, is modified, issue the **show services service-sets statistics tcp-mss** operational mode command. For more information on this topic, see the *Junos OS Administration Library*.

- Starting in Junos OS Release 17.1R1, you can limit the session setup rate per service set for an MS-MPC. To configure the maximum setup rate allowed, include the **max-session-setup-rate** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

  ```
  [edit services service-set service-set-name]
  max-session-setup-rate (number | numberk);
  ```

  The maximum session setup rate is the maximum number of session setups allowed per second. After this rate is reached, any additional session setup attempts are dropped.

  The range for the **max-session-setup-rate** *number* is 1 through 429,496,729. You can also express the setup rate as thousands of sessions by using *number*k. Starting in Junos OS Release 18.4R1, 1k=1000 for the **max-session-setup-rate**. Prior to Junos OS Release 18.4R1, 1k=1024. If you do not include the **max-session-setup-rate** statement, the session setup rate is not limited.

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1, 1k=1000 for the **max-session-setup-rate**.
17.1R1	Starting in Junos OS Release 17.1R1, you can limit the session setup rate per service set for an MS-MPC.

RELATED DOCUMENTATION

Understanding Service Sets | 6

Configuring Service Sets to be Applied to Services Interfaces | 9

Configuring Service Rules | 21

Configuring System Logging for Service Sets | 36

Configuring Service Interface Pools

To configure a service interface pool, include the following statements at the **[edit services service-interface-pools]** hierarchy level:

```
[edit services service-interface-pools]
pool pool-name {
    interface interface-name.unit-number;
```

```
}
```

RELATED DOCUMENTATION

- Configuring Service Sets to be Applied to Services Interfaces | 9

Enabling Services PICs to Accept Multicast Traffic

To allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC, include the **allow-multicast** statement at the **[edit services service-set *service-set-name*]** hierarchy level. If this statement is not included, multicast traffic is dropped by default. This statement applies only to multicast traffic using a next-hop service set; interface service set configuration is not supported. Only unidirectional flows are created for multicast packets.

RELATED DOCUMENTATION

- Understanding Service Sets | 6
- Configuring Service Sets to be Applied to Services Interfaces | 9
- Configuring Service Rules | 21
- Example: Configuring Service Sets | 28
- Example: Configuring NAT for Multicast Traffic | 157

Applying Filters and Services to Interfaces

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces on the router. To associate a defined service set with an interface, include the **service-set** statement with the **input** or **output** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number family inet service]
input {
    service-set service-set-name <service-filter filter-name>;
    post-service-filter filter-name;
```

```
}
output {
    service-set service-set-name <service-filter filter-name>;
}
```

NOTE: When you enable services on an interface, reverse-path forwarding is not supported. You cannot configure services on the management interface (**fxp0**) or the loopback interface (**lo0**).

You can configure different service sets on the input and output sides of the interface. However, for service sets with bidirectional service rules, you must include the same service set definition in both the **input** and **output** statements. Any service set you include in the **service** statement must be configured with the **interface-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level; for more information, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.

NOTE: If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an Internet Control Message Protocol (ICMP) error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

Configuring Service Filters

You can optionally include filters associated with each service set to refine the target and additionally process the traffic. If you include the **service-set** statement without a **service-filter** definition, the router software assumes that the match condition is true and selects the service set for processing automatically.

To configure service filters, include the **firewall** statement at the **[edit]** hierarchy level:

```
firewall {
    family inet {
        service-filter filter-name {
```

```
            term term-name {
               from {
                  match-conditions;
               }
               then {
                  action;
                  action-modifiers;
               }
            }
         }
      }
   }
```

NOTE: You must specify **inet** as the address family to configure a service filter.

You configure service filters in a similar way to firewall filters. Service filters have the same match conditions as firewall filters, but the following specific actions:

- **count**—Add the packet to a counter total.
- **log**—Log the packet.
- **port-mirror**—Port-mirror the packet.
- **sample**—Sample the packet.
- **service**—Forward the packet for service processing.
- **skip**—Omit the packet from service processing.

For more information about configuring firewall filters, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

You can also include more than one service set definition on each side of the interface. If you include multiple service sets, the router software evaluates them in the order specified in the configuration. It executes the first service set for which it finds a match in the service filter and ignores the subsequent definitions.

An additional statement allows you to specify a filter for processing the traffic after the input service set is executed. To configure this type of filter, include the **post-service-filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service input]** hierarchy level:

```
post-service-filter filter-name;
```

> **NOTE:** The software performs postservice filtering only when it has selected and executed a service set. If the traffic does not meet the match criteria for any of the configured service sets, the postservice filter is ignored. The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

For an example of applying a service set to an interface, see "Examples: Configuring Services Interfaces" on page 32.

For more information on applying filters to interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*. For general information on filters, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

> **NOTE:** After NAT processing is applied to packets, they are not subject to output service filters. The service filters affect only untranslated traffic.

RELATED DOCUMENTATION

Services PICs-Overview

Configuring Service Sets to be Applied to Services Interfaces | 9

Examples: Configuring Services Interfaces | 32

Example: Configuring Service Sets

Apply two service sets, **my-input-service-set** and **my-output-service-set**, on an interface-wide basis. All traffic has **my-input-service-set** applied to it. After the service set is applied, additional filtering is done using **my_post_service_input_filter**.

```
[edit interfaces fe-0/1/0]
unit 0 {
    family inet {
        service {
            input {
                service-set my-input-service-set;
                post-service-filter my_post_service_input_filter;
```

```
        }
        output {
            service-set my-output-service-set;
        }
    }
  }
}
```

RELATED DOCUMENTATION

Understanding Service Sets | 6

Configuring Service Sets to be Applied to Services Interfaces | 9

Configuring AS or Multiservices PIC Redundancy

You can configure AS or Multiservices PIC redundancy on M Series and T Series routers, except TX Matrix routers, that have multiple AS or Multiservices PICs. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary AS or Multiservices PIC is restored, it remains on standby and does not preempt the secondary PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.

Failover to the secondary PIC occurs under the following conditions:

- The primary PIC, FPC, or Packet Forwarding Engine goes down, resets, or is physically removed from the router.
- The PIC or FPC is taken offline using the **request chassis pic fpc-slot *slot-number* pic-slot *slot-number* offline** or **request chassis fpc slot *slot-number* offline** command. For more information, see the CLI Explorer.
- The driver watchdog timer expires.
- The **request interface switchover** command is issued. For more information, see the CLI Explorer.

NOTE: Adaptive Services and Multiservices PICs in Layer-2 mode (running Layer 2 services) are not rebooted when a MAC flow-control situation is detected.

NOTE: When you perform a switchover from a primary PIC to a secondary or standby PIC or a revert operation by issuing **request interfaces (revert | switchover)** command for redundancy services PICs (**rsp**), the PIC that was previously the active PIC before the switchover or reversion is automatically rebooted. The reboot of the PIC that was previously active and functioning as the primary PIC does not disrupt traffic forwarding.

The physical interface type **rsp** specifies the pairings between primary and secondary **sp** interfaces to enable redundancy. To configure an AS or Multiservices PIC as the backup, include the **redundancy-options** statement at the **[edit interfaces rsp*number*]** hierarchy level:

```
[edit interfaces rspnumber]
redundancy-options {
    primary sp-fpc/pic/port;
    secondary sp-fpc/pic/port;
    hot-standby;
}
```

For the **rsp** interface, *number* can be from 0 through 15.

NOTE: You can include a similar redundancy configuration for Link Services IQ (LSQ) PICs at the **[edit interfaces rlsq*number*]** hierarchy level. For more information, see "Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces" on page 912.

The following constraints apply to redundant AS or Multiservices PIC configurations:

- The services supported in redundancy configurations include stateful firewall, NAT, IDS, and IPsec. Services mounted on the AS or Multiservices PIC that use interface types other than **sp-** interfaces, such as tunneling and voice services, are not supported. For information on flow monitoring redundancy, see *Configuring Services Interface Redundancy with Flow Monitoring*.

  > **NOTE:** For IPsec functionality, the router no longer needs to renegotiate security associations (SAs) during warm standby PIC switchover. Instead, the warm standby feature has been made stateful by periodically setting a checkpoint between the working state of the PIC and the Routing Engine, which should lessen the downtime during switchover. If you prefer to retain the earlier behavior, you can include the **clear-ipsec-sas-on-pic-restart** statement at the **[edit services ipsec-vpn]** hierarchy level. If you enable this capability, the router renegotiates the IPsec SAs on warm standby PIC switchover. For more information, see "Configuring Security Associations" on page 639.

- We recommend that you pair the same model type in RSP configurations, such as two ASMs or two AS2 PICs. If you pair unlike models, the two PICs may perform differently.
- You can specify an AS or Multiservices PIC (**sp** interface) as the primary for only one **rsp** interface.
- An **sp** interface can be a secondary for multiple **rsp** interfaces. However, the same **sp** interface cannot be configured as a primary interface in one **rsp** configuration and as a secondary in another configuration.
- When the secondary PIC is active, if another primary PIC that is paired with it in an **rsp** configuration fails, no failover takes place.
- When you configure an AS or Multiservices PIC within a redundant configuration, the **sp** interface cannot have any configured services. Apply the configurations at the **[edit interfaces rsp*number*]** hierarchy level, using, for example, the **unit** and **services-options** statements. Exceptions include the **multiservice-options** statement used in flow monitoring configurations, which can be configured separately for the primary and secondary **sp** interfaces, and the **traceoptions** statement.
- All the operational mode commands that apply to **sp** interfaces also apply to **rsp** interfaces. You can issue **show** commands for the **rsp** interface or the primary and secondary **sp** interfaces.
- If a secondary PIC fails while it is in use, the **rsp** interface returns to the " not present" state. If the primary PIC comes up later, service is restored to it.
- For redundant Multiservices (rms-) interfaces, similar to the configuration of other bundle interfaces, the properties of the Multiservices (ms-) member interfaces, such as the logical unit and the address family, are inherited from the underlying rms- interface. If you previously configured the member ms- interface properties separately, and attempt to configure the rms- interface properties by using the relevant statements at the **[edit interfaces rms*number*]** hierarchy level, an error occurs when you perform a commit check operation. You must configure the properties of interfaces that are part of the rms- interface only by using the statements at the **[edit interfaces rms*number*]** hierarchy level.

RELATED DOCUMENTATION

Services PICs-Overview

Examples: Configuring Services Interfaces | **32**

Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

Enabling Session Offloading for Multiservices DPCs

The Junos OS enables you to configure session offloading for Multiservices DPCs on MX Series routers. This enables Fast Update Filters (FUF) at the PIC level for a multiservices interface (**ms-*fpc-pic-port***). To configure session offloading, include the **session-offload** statement at the **[edit chassis fpc *slot-number* pic *number* adaptive-services service-package extension-provider]** hierarchy level:

```
[edit chassis fpc slot-number pic number adaptive-services service-package extension-provider]
session-offload;
```

Currently, session offloading is supported only for a maximum of one multiservices interface.

NOTE: When session offloading is enabled for a Multiservices PIC, we recommend that you limit dynamic application awareness features for Intrusion Detection and Prevention (IDP) only for that interface.

RELATED DOCUMENTATION

session-offload | **1465**

Examples: Configuring Services Interfaces

Apply the **my-service-set** service set on an interface-wide basis. All traffic that is accepted by **my_input_filter** has **my-input-service-set** applied to it. After the service set is applied, additional filtering is done using the **my_post_service_input_filter** filter.

```
[edit interfaces fe-0/1/0]
unit 0 {
```

```
    family inet {
        filter {
            input my_input_filter;
            output my_output_filter;
        }
        service {
            input {
                service-set my-input-service-set;
                post-service-filter my_post_service_input_filter;
            }
            output {
                service-set my-output-service-set;
            }
        }
    }
}
```

Configure two redundancy interfaces, **rsp0** and **rsp1**, and associated services.

```
[edit interfaces]
rsp0 {
    redundancy-options {
        primary sp-0/0/0;
        secondary sp-1/3/0;
    }
    unit 0 {
        family inet;
    }
    unit 30 {
        family inet;
        service-domain inside;
    }
    unit 31 {
        family inet;
        service-domain outside;
    }
}
rsp1 {
    redundancy-options {
        primary sp-0/1/0;
        secondary sp-1/3/0;
    }
    unit 0 {
        family inet;
```

```
    }
    unit 20 {
        family inet;
        service-domain inside;
    }
    unit 21 {
        family inet;
        service-domain outside;
    }
}
[edit services]
service-set null-sfw-with-nat {
    stateful-firewall-rules allow-all;
    nat-rules rule1;
    next-hop-service {
        inside-service-interface rsp0.30;
        outside-service-interface rsp0.31;
    }
}
[edit routing-instances]
vpna {
    interface rsp0.0;
}
```

RELATED DOCUMENTATION

- *Services PICs-Overview*
- Configuring the Address and Domain for Services Interfaces | **34**
- *Configuring Default Timeout Settings for Services Interfaces*
- *Configuring System Logging for Services Interfaces*
- Applying Filters and Services to Interfaces | **25**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

Configuring the Address and Domain for Services Interfaces

On the AS or Multiservices PIC, you configure a source address for system log messages by including the **address** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```
address address {
   ...
}
```

Assign an IP address to the interface by configuring the ***address*** value. The AS or Multiservices PIC generally supports only IP version 4 (IPv4) addresses configured using the **family inet** statement, but IPsec services support IP version 6 (IPv6) addresses as well, configured using the **family inet6** statement.

NOTE: If you configure the same address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration, the remaining address configurations are ignored and can leave interfaces without an address. Interfaces that do not have an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

For example, in the following configuration the address configuration of interface xe-0/0/1.0 is ignored:

```
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/24;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
     family inet {
       address 192.168.1.1/24;
     }
  }
}
```

For more information on configuring the same address on multiple interfaces, see *Configuring the Interface Address*.

For information on other addressing properties you can configure that are not specific to service interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

The **service-domain** statement specifies whether the interface is used within the network or to communicate with remote devices. The software uses this setting to determine which default stateful firewall rules to

apply, and to determine the default direction for service rules. To configure the domain, include the **service-domain** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
service-domain (inside | outside);
```

If you are configuring the interface in a next-hop service-set definition, the **service-domain** setting must match the configuration for the **inside-service-interface** and **outside-service-interface** statements; for more information, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.

RELATED DOCUMENTATION

- *Configuring Default Timeout Settings for Services Interfaces*
- *Configuring System Logging for Services Interfaces*
- Examples: Configuring Services Interfaces | **32**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

Configuring System Logging for Service Sets

You specify properties that control how system log messages are generated for the service set. These values override the values configured at the **[edit interfaces *interface-name* services-options]** hierarchy level.

To configure service-set-specific system logging values, include the **syslog** statement at the **[edit services service-set *service-set-name*]** hierarchy level:

```
syslog {
    host hostname {
        class class-name
        facility-override facility-name;
        log-prefix prefix-value;
        port port-number
        services severity-level;
        source-address source-address
    }
}
```

Configure the **host** statement with a hostname or an IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that

triggered session establishment) is delivered. You can specify only one system logging hostname. The **source-address** parameter is supported on the ms, rms, and mams interfaces.

Starting in Junos OS Release 17.4R1, you can configure up to a maximum of four system log servers (combination of local system log hosts and remote system log collectors) for each service set under **[edit services service-set *service-set-name*]** hierarchy level.

> **NOTE:** Junos OS does not support the exporting of system log messages to an external system log server through the fxp.0 interface; this is because the high transmission rate of system log messages and the limited bandwidth of the fxp.0 interface can cause several problems. The external system log server must be reachable through a routable interface.

Table 6 on page 37 lists the severity levels that you can specify in configuration statements at the **[edit services service-set *service-set-name* syslog host *hostname*]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Table 6: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or non-error conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log NAT functionality, set the level to **info**.

For more information about system log messages, see the System Log Explorer.

To select the class of messages to be logged to the specified system log host, include the **class** statement at the **[edit services service-set *service-set-name* syslog host *hostname*]** hierarchy level:

```
class class-name;
```

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services service-set *service-set-name* syslog host *hostname*]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities are: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services service-set *service-set-name* syslog host *hostname*]** hierarchy level:

```
log-prefix prefix-value;
```

RELATED DOCUMENTATION

Understanding Service Sets | 6

Configuring Service Sets to be Applied to Services Interfaces | 9

Tracing Services PIC Operations | 38

Tracing Services PIC Operations

IN THIS SECTION

Tracing operations track all adaptive services operations and record them in a log file. The logged error descriptions provide detailed information to help you solve problems faster.

By default, no events are traced. If you include the **traceoptions** statement at the **[edit services adaptive-services-pics]** or **[edit services logging]** hierarchy level, the default tracing behavior is the following:

- Important events are logged in a file called **serviced** located in the **/var/log** directory.
- When the file **serviced** reaches 128 kilobytes (KB), it is renamed **serviced.0**, then **serviced.2**, and so on, until there are three trace files. Then the oldest trace file (**serviced.2**) is overwritten. (For more information about how log files are created, see the System Log Explorer.)
- Log files can be accessed only by the user who configures the tracing operation.

You cannot change the directory (**/var/log**) in which trace files are located. However, you can customize the other trace file settings by including the following statements:

```
file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
flag {
    all;
    command-queued;
    config;
    handshake;
    init;
    interfaces;
    mib;
    removed-client;
    show;
}
```

You include these statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level.

These statements are described in the following sections:

Configuring the Adaptive Services Log Filename

By default, the name of the file that records trace output is **serviced**. You can specify a different name by including the **file** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file filename;
```

Configuring the Number and Size of Adaptive Services Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed ***filename*.0**, then ***filename*.1**, and so on, until there are three trace files. Then the oldest trace file (***filename*.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (***filename***) reaches 2 MB, ***filename*** is renamed ***filename*.0**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0** is renamed ***filename*.1** and ***filename*** is renamed ***filename*.0**. This process repeats until there are 20 trace files. Then the oldest file (***filename*.19**) is overwritten by the newest file (***filename*.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10 KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the **file world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> world-readable;
```

To explicitly set the default behavior, include the **file no-world-readable** statement at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
file <filename> no-world-readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events.

You can refine the output by including the **match** statement at the **[edit services adaptive-services-pics traceoptions file *filename*]** or **[edit services logging traceoptions]** hierarchy level and specifying a regular expression (regex) to be matched:

```
file <filename> match regular-expression;
```

Configuring the Trace Operations

By default, if the **traceoptions** configuration is present, only important events are logged. You can configure the trace operations to be logged by including the following statements at the **[edit services adaptive-services-pics traceoptions]** or **[edit services logging traceoptions]** hierarchy level:

```
flag {
    all;
    configuration;
    routing-protocol;
    routing-socket;
    snmp;
}
```

Table 7 on page 41 describes the meaning of the adaptive services tracing flags.

Table 7: Adaptive Services Tracing Flags

Flag	Description	Default Setting
all	Trace all operations.	Off
command-queued	Trace command enqueue events.	Off
config	Log reading of the configuration at the **[edit services]** hierarchy level.	Off
handshake	Trace handshake events.	Off
init	Trace initialization events.	Off
interfaces	Trace interface events.	Off
mib	Trace GGSN SNMP MIB events.	Off
removed-client	Trace client cleanup events.	Off
show	Trace CLI command servicing.	Off

To display the end of the log, issue the **show log serviced | last** operational mode command:

```
[edit]
user@host# run show log serviced | last
```

RELATED DOCUMENTATION

Understanding Service Sets | 6

Configuring Service Sets to be Applied to Services Interfaces | 9

Configuring System Logging for Service Sets | 36

Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces

Two configuration options are available to prevent excessive consumption of computational CPU cycles on a services PIC caused by the handling of large numbers of fragmented packets. Such fragment handling can be exploited in DOS attacks. The **fragment-limit** option establishes a maximum number of fragments for a packet. When this number is exceeded, the packet is dropped. The **reassembly-timeout** specifies the maximum time from the receipt of the first and latest fragments in a packet. When the number is exceeded, the packet is dropped.

To configure fragmentation control for MS-DPC and MS-PIC service interfaces:

1. In configuration mode, go to the **[edit interfaces *interface-name* services-options** hierarchy level.

   ```
   edit interfaces interface-name services-options
   ```

2. Configure the fragment limit.

   ```
   [ edit services interface-name services-options]
   set fragment-limit number-of-fragments
   ```

3. Configure the reassembly timeout.

   ```
   [ edit services interface-name services-options]
   set reassembly-timeout number-of-fragments
   ```

CHAPTER 3

Plug-in Adaptive Services

IN THIS CHAPTER

DNS Request Filtering for Disallowed Website Domains

IN THIS SECTION

Overview of DNS Request Filtering

IN THIS SECTION

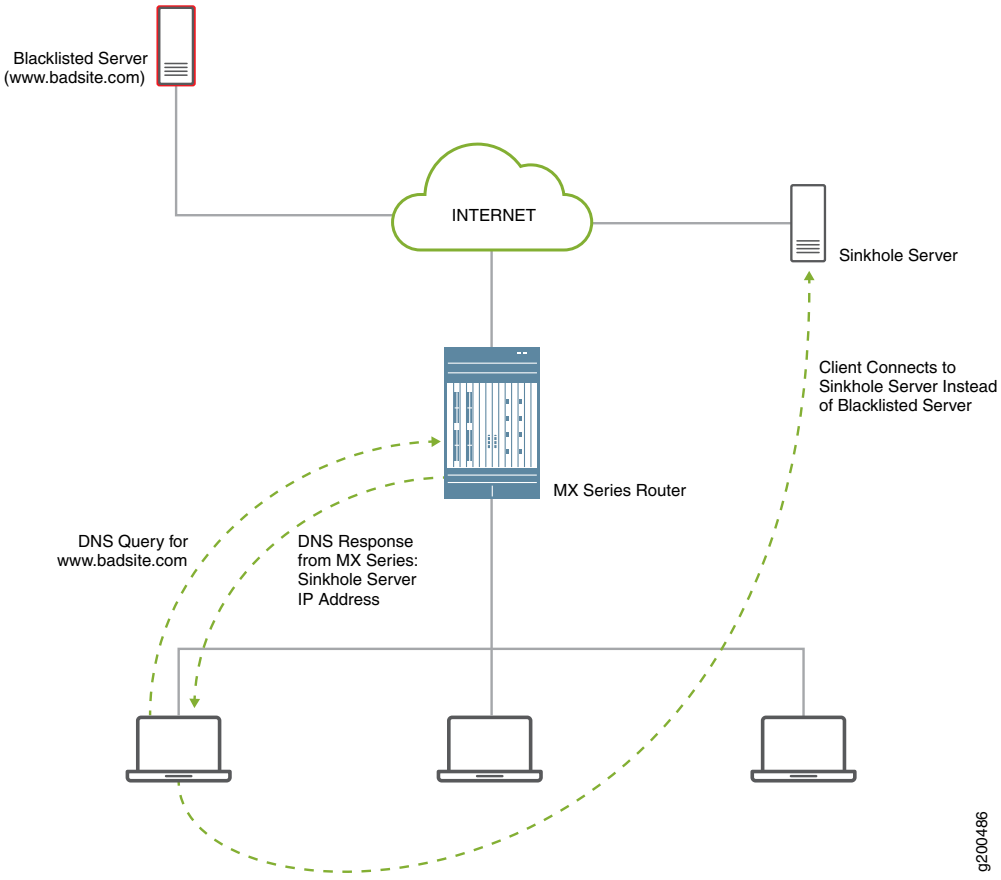
Starting in Junos OS Release 18.3R1, you can configure DNS filtering to identify DNS requests for disallowed website domains. Starting in Junos OS Release 19.3R2, you can configure DNS filtering if you are running Next Gen Services with the MX-SPC3 services card. Next Gen Services are supported on MX240, MX480 and MX960 routers. For DNS request types A, AAAA, MX, CNAME, TXT, SRV, and ANY, you configure the action to take for a DNS request for a disallowed domain. You can either:

- Block access to the website by sending a DNS response that contains the IP address or fully qualified domain name (FQDN) of a DNS sinkhole server. This ensures that when the client attempts to send traffic to the disallowed domain, the traffic instead goes to the sinkhole server (see Figure 2 on page 44).
- Log the request and allow access.

For other DNS request types for a disallowed domain, the request is logged and access is allowed.

The actions that the sinkhole server takes are not controlled by the DNS request filtering feature; you are responsible for configuring the sinkhole server actions. For example, the sinkhole server could send a message to the requestor that the domain is not reachable and prevent access to the disallowed domain.

Figure 2: DNS Request for Disallowed Domain



Benefits

DNS filtering redirects DNS requests for disallowed website domains to sinkhole servers, while preventing anyone operating the system from seeing the list of disallowed domains. This is because the disallowed domain names are in an encrypted format.

Disallowed Domain Filter Database File

DNS request filtering requires a disallowed domain filter database .txt file, which identifies each disallowed domain name, the action to take on a DNS request for the disallowed domain, and the IP address or fully qualified domain name (FQDN) of a DNS sinkhole server.

DNS Filter Profile

You configure a DNS filter profile to specify which disallowed domain filter database file to use. You can also specify the interfaces on which DNS request filtering is performed, limit the filtering to requests for specific DNS servers, and limit the filtering to requests from specific source IP address prefixes.

How to Configure DNS Request Filtering

IN THIS SECTION

To filter DNS requests for disallowed website domains, perform the following:

How to Configure a Domain Filter Database

Create one or more domain filter database files that include an entry for each disallowed domain. Each entry specifies what to do with a DNS request for a disallowed website domain.

To configure a domain filter database file:

1. Create the name for the file. The database file name can have a maximum length of 64 characters and must have a **.txt** extension.

2. Add a file header with a format such as **20170314_01:domain,sinkhole_ip,v6_sinkhole,sinkhole_fqdn,id,action**.

3. Add an entry in the file for each disallowed domain. You can include a maximum of 10,000 domain entries. Each entry in the database file has the following items:

   hashed-domain-name,IPv4 sinkhole address, IPv6 sinkhole address, sinkhole FQDN, ID, action

where:

- **hashed-domain-name** is a hashed value of the disallowed domain name (64 hexadecimal characters). The hash method and hash key that you use to produce the hashed domain value are needed when you configure DNS filtering with the Junos OS CLI.
- **IPv4 sinkhole address** is the address of the DNS sinkhole server for IPv4 DNS requests.
- **IPv6 sinkhole address** is the address of the DNS sinkhole server for IPv6 DNS requests.
- **sinkhole FQDN** is the fully qualified domain name of the DNS sinkhole server.
- **ID** is a 32-bit number that uniquely associates the entry with the hashed domain name.
- **action** is the action to apply to a DNS request that matches the disallowed domain name. If you enter **replace**, the MX Series router sends the client a DNS response with the IP address or FQDN of the DNS sinkhole server. If you enter **report**, the DNS request is logged and then sent to the DNS server.

4. In the last line of the file, include the file hash, which you calculate by using the same key and hash method that you used to produce the hashed domain names.

5. Save the database files on the Routing Engine in the **/var/db/url-filterd** directory.

6. Validate the domain filter database file.

```
user@host> request services web-filter validate dns-filter-file-name filename hash-key key-string hash-method
  hash-method-name
```

7. If you make any changes to the database file, apply the changes.

```
user@host> request services web-filter update dns-filter-database filename
```

How to Configure a DNS Filter Profile

A DNS filter profile includes general settings for filtering DNS requests for disallowed website domains, and includes up to 32 templates. The template settings apply to DNS requests on specific uplink and downlink logical interfaces or routing instances, or to DNS requests from specific source IP address prefixes, and override the corresponding settings at the DNS profile level. You can configure up to eight DNS filter profiles.

To configure a DNS filter profile:

1. Configure the name for a DNS filter profile:

```
[edit]
user@host# edit services web-filter profile profile-name
```

The maximum number of profiles is 8.

2. Configure the interval for logging per-client statistics for DNS filtering. The range is 0 through 60 minutes and the default is 5 minutes.

```
[edit services web-filter profile profile-name]
user@host# set global-dns-stats-log-timer minutes
```

3. Configure general DNS filtering settings for the profile. These values are used if a DNS request does not match a specific template.

   a. Specify the name of the domain filter database to use when filtering DNS requests.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set database-file filename
```

   b. (Optional) To limit DNS filtering to DNS requests that are destined for specific DNS servers, specify up to three IP addresses (IPv4 or IPv6).

```
[edit services web-filter profile profile-name dns-filter]
user@host# set dns-server [ ip-address ]
```

   c. Specify the format for the hash key.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set hash-key ascii-text
```

   d. Specify the hash key that you used to create the hashed domain name in the domain filter database file.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set hash-key key-string
```

   e. Specify the hash method that was used to create the hashed domain name in the domain filter database file.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set hash-method hash-method-name
```

   The only supported hash method is **hmac-sha2-256**.

f. Configure the interval for logging statistics for DNS requests and for sinkhole actions performed for each customer IP address. The range is 1 through 60 minutes and the default is 5 minutes.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set statistics-log-timer minutes
```

g. Configure the time to live while sending the DNS response after taking the DNS sinkhole action. The range is 0 through 86,400 seconds and the default is 1800.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set dns-resp-ttl seconds
```

h. Configure the level of subdomains that are searched for a match. The range is 0 through 10. A value of 0 indicates that subdomains are not searched.

```
[edit services web-filter profile profile-name dns-filter]
user@host# set wildcarding-level level
```

For example, if you set the **wildcarding-level** to 4 and the database file includes an entry for **example.com**, the following comparisons are made for a DNS request that arrives with the domain **198.51.100.0.example.com**:

- **198.51.100.0.example.com**: no match
- **51.100.0.example.com**: no match for one level down
- **100.0.example.com**: no match for two levels down
- **0.example.com**: no match for three levels down
- **example.com**: match for four levels down

4. Configure a template. You can configure a maximum of 8 templates in a profile. Each template identifies filter settings for DNS requests on specific uplink and downlink logical interfaces or routing instances, or for DNS requests from specific source IP address prefixes.

a. Configure the name for the template.

```
[edit services web-filter profile profile-name]
user@host# set dns-filter-template template-name
```

b. (Optional) Specify the client-facing logical interfaces (uplink) to which the DNS filtering is applied.

```
[edit services web-filter profile profile-name dns-filter-template template-name]
```

```
user@host# set client-interfaces client-interface-name
```

c. (Optional) Specify the server-facing logical interfaces (downlink) to which the DNS filtering is applied.

```
[edit services web-filter profile profile-name dns-filter-template template-name]
user@host# set server-interfaces server-interface-name
```

d. (Optional) Specify the routing instance for the client-facing logical interface to which the DNS filtering is applied.

```
[edit services web-filter profile profile-name dns-filter-template template-name]
user@host# set client-routing-instance client-routing-instance-name
```

e. (Optional) Specify the routing instance for the server-facing logical interface to which DNS filtering is applied.

```
[edit services web-filter profile profile-name dns-filter-template template-name]
user@host# set server-routing-instance server-routing-instance-name
```

NOTE: If you configure the client and server interfaces or the client and server routing instances, implicit filters are installed on the interfaces or routing instances to direct DNS traffic to the services PIC for DNS filtering. If you configure neither the client and server interfaces nor the routing instances, you must provide a way to direct DNS traffic to the services PIC (for example, via routes).

f. Specify the name of the domain filter database to use when filtering DNS requests.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set database-file filename
```

g. (Optional) To limit DNS filtering to DNS requests that are destined for specific DNS servers, specify up to three IP addresses (IPv4 or IPv6).

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set dns-server ip-address
```

h. Specify the hash method that was used to create the hashed domain name in the domain filter database file.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set hash-method hash-method-name
```

The only supported hash method is **hmac-sha2-256**.

i. Specify the hash key that was used to create the hashed domain name in the domain filter database file.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set hash-key key-string
```

j. Configure the interval for logging statistics for DNS requests and for sinkhole actions performed for each customer IP address. The range is 1 through 60 minutes and the default is 5 minutes.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set statistics-log-timer minutes
```

k. Configure the time to live while sending the DNS response after taking the DNS sinkhole action. The range is 0 through 86,400 seconds and the default is 1800.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set dns-resp-ttl seconds
```

l. Configure the level of subdomains that are searched for a match. The range is 0 through 10. A value of 0 indicates that subdomains are not searched.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set wildcarding-level level
```

For example, if you set the **wildcarding-level** to 4 and the database file includes an entry for **example.com**, the following comparisons are made for a DNS request that arrives with the domain **198.51.100.0.example.com**:

- **198.51.100.0.example.com**: no match
- **51.100.0.example.com**: no match for one level down
- **100.0.example.com**: no match for two levels down

- **0.example.com**: no match for three levels down
- **example.com**: match for four levels down

m. (Optional) Specify the response error code for SRV and TXT query types.

```
[edit services web-filter profile profile-name dns-filter-template template-name dns-filter]
user@host# set txt-resp-err-code (Noerror | Refused)
user@host# set srv-resp-err-code (Noerror | Refused)
```

n. Configure a term for the template. You can configure a maximum of 64 terms in a template.

```
[edit services web-filter profile profile-name dns-filter-template template-name]
user@host# set term term-name
```

o. (Optional) Specify the source IP address prefixes of DNS requests you want to filter. You can configure a maximum of 64 prefixes in a term.

```
[edit services web-filter profile profile-name dns-filter-template template-name term term-name]
user@host# set from src-ip-prefix source-prefix
```

p. Specify that the sinkhole action identified in the domain filter database is performed on disallowed DNS requests.

```
[edit services web-filter profile profile-name dns-filter-template template-name term term-name]
user@host# set then dns-sinkhole
```

How to Configure a Service Set for DNS Filtering

- Associate the DNS filter profile with a next-hop service set and enable logging for DNS filtering. The service interface can be an ms- or vms- interface Next Gen Services with MX-SPC3 services card), or it can be an aggregated multiservices (AMS) interface.

```
[edit services service-set service-set-name]
user@host# set web-filter-profile profile-name
user@host# set syslog host hostname class urlf-logs
user@host# set next-hop-service inside-service-interface interface-name.unit-number
user@host# set next-hop-service outside-service-interface interface-name.unit-number
```

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, you can configure DNS filtering if you are running Next Gen Services with the MX-SPC3 services card. Next Gen Services are supported on MX240, MX480 and MX960 routers.

URL Filtering Overview

IN THIS SECTION

You can use URL filtering to determine which Web content is not accessible to users.

Components of this feature include the following:

- URL filter database file
- Configuration of one or more templates (up to eight per profile)
- URL Filter Plug-in (jservices-urlf)
- URL filtering daemon (url-filterd)

The URL filter database file is stored on the Routing Engine and contains all the disallowed URLs. Configured *templates* define which traffic to monitor, what criteria to match, and which actions to take. You configure the templates and the location of the URL filter database file in a *profile*.

Starting in Junos OS Release 17.2R2 and 17.4R1, for Adaptive Services, you can disable the filtering of HTTP traffic that contains an embedded IP address (for example, http:/10.1.1.1) belonging to a disallowed domain name in the URL filter database.Starting in Junos OS Release 19.3R2, this same functionaly is supported for Next Gen Services on MX240, MX480, and MX960.

To enable the URL filtering feature, you must configure **jservices-urlf** as the ***package-name*** at the **[edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]** hierarchy level. Once enabled, jservices-urlf maintains the URL filtering profile and receives all traffic to be filtered, the filtering criteria, and the action to be taken on the filtered traffic.

The URL filtering daemon (url-filterd), which also resides on the Routing Engine, resolves the domain name of each URL in the URL filter database to a list of IPv4 and IPv6 addresses. It then downloads the list of IP addresses to the service PIC, which runs jservices-urlf. Then url-filterd interacts with the Dynamic Firewall process (dfwd) to install filters on the Packet Forwarding Engine to punt the selected traffic from the Packet Forwarding Engine to the service PIC.

As new HTTP and HTTPS traffic reaches the router, a decision is made based on the information in the URL filter database file. The filtering rules are checked and either the router accepts the traffic and passes it on or blocks the traffic. If the traffic is blocked, one of the following configured actions is taken:

- An HTTP redirect is sent to the user.
- A custom page is sent to the user.
- An HTTP status code is sent to the user.
- A TCP reset is sent.

Accept is also an option. In this case, the traffic is not blocked.

For more details on the URL filtering feature, see the following sections:

URL Filter Database File

The URL filter database file contains entries of URLs and IP addresses. Create the URL filter database file in the format indicated in Table 8 on page 53 and locate it on the Routing Engine in the **/var/db/url-filterd** directory.

Table 8: URL Filter Database File Format

Entry	Description	Example
FQDN	Fully qualified domain name.	www.badword.com/jjj/bad.jpg
URL	Full string URL without the Layer 7 protocol.	www.yahoo.com/*badword*/
IPv4 address	HTTP request on a specific IPv4 address.	10.1.1.199
IPv6 address	HTTP request on a specific IPv6 address.	1::1

You must specify a custom URL filter database in the profile. If needed, you can also assign a custom URL filter database file with any template, and that database takes precedence over the database configured at the profile level.

If you change the contents of the URL filter database file, use the **request services (url-filter | web-filter) update** command. Other commands to help maintain the URL filter database file include the following:

- **request services (url-filter | web-filter) delete**
- **request services (url-filter | web-filter) force**
- **request services (url-filter | web-filter) validate**

URL Filter Profile Caveats

The URL filter profile consists of from one to eight templates. Each template consists of a set of configured logical interfaces where traffic is monitored for URL filtering and one or more terms.

A *term* is a set of match criteria with actions to be taken if the match criteria is met. You must configure at least one term to configure URL filtering. Each term consists of a **from** statement and a **then** statement, where the **from** statement defines the source IP prefixes and destination ports that are monitored. The **then** statement specifies the action to be taken. If you omit the **from** statement, any source IP prefix and any destination port are considered to match. But you can omit only one **from** statement per template or per profile.

Example configuration of multiple terms without from statements

```
template1 {
    client-interfaces [ xe-4/0/3.35 xe-4/0/3.36 ];
    server-interfaces xe-4/0/0.31;
    dns-source-interface xe-4/0/0.1;
    dns-routing-instance data_vr;
    routing-instance data_vr2;
    dns-server 50.0.0.3;
    dns-retries 3;
    url-filter-database url_database.txt;
    term term1 {
        then {
            tcp-reset;
        }
    }
    term term2 {
        then {
            redirect-url www.google.com;
        }
    }
}
```

If you omit more than one **from** statement per template, you will get the following error message on commit:

```
URLFD_CONFIG_FAILURE: Configuration not valid:
Cannot have two wild card terms in template template1
error: configuration check-out failed
```

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, this same functionaly is supported for Next Gen Services on MX240, MX480, and MX960.
17.2R2	Starting in Junos OS Release 17.2R2 and 17.4R1, for Adaptive Services, you can disable the filtering of HTTP traffic that contains an embedded IP address (for example, http:/10.1.1.1) belonging to a disallowed domain name in the URL filter database.

RELATED DOCUMENTATION

- Configuring URL Filtering | 55
- request services url-filter update url-filter-database file | 1707
- request services url-filter force dns-resolution | 1705
- request services url-filter delete gencfg-data | 1704
- request services url-filter validate | 1708

Configuring URL Filtering

URL filtering is configured on a service PIC. The interfaces you are dealing with are services interfaces (which use the **ms** prefix) or aggregated multiservices (AMS) interfaces (which use the **ams** prefix). For more information on AMS interfaces, see the *Adaptive Services Interfaces User Guide for Routing Devices* starting with "Understanding Aggregated Multiservices Interfaces" on page 994.

To configure the URL filtering feature, you must first configure **jservices-urlf** as the ***package-name*** at the **[edit chassis fpc *slot-number* pic *pic-number* adaptive-services service-package extension-provider]** hierarchy level. For more information on configuring the **extension-provider package *package-name*** configuration statement, see the **package (Loading on PIC)** statement.

A URL filtering *profile* is a collection of templates. Each template consists of a set of criteria that defines which URLs are disallowed and how the recipient is notified.

To configure the URL profile:

1. Assign a name to the URL profile.

   ```
   [edit]
   user@host# edit services (web-filter | url-filter) profile profile-name
   ```

   Starting in Junos OS Release 18.3R1, for Adaptive Services. configure the profile at the **[edit services web-filter]** hierarchy level. Before Junos OS Release 18.3R1, configure the profile at the **[edit services url-filter]** hierarchy level.Starting in Junos OS Release 19.3R2, this same functionality is available for Next Gen Serices on MX240, MX480, and MX960.

2. Specify the name of the URL filter database to use.

   ```
   [edit services (web-filter | url-filter) profile profile-name]
   user@host# set url-filter-database filename
   ```

3. Configure one or more templates for the profile.

   To configure each template:

   a. Name the template.

   ```
   [edit services (web-filter | url-filter) profile profile-name]
   user@host# set (url-filter-template template-name | template template-name)
   ```

   NOTE: Starting in Junos OS Release 18.3R1, configure the template with the **url-filter-template** statement. Before Junos OS Release 18.3R1, configure the template with the **template** statement.

   b. Go to that new template hierarchy level.

   ```
   [edit services (web-filter | url-filter) profile profile-name]
   user@host# edit (url-filter-template template-name | template template-name)
   ```

   c. Specify the name of the URL filter database to use.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set url-filter-database filename
```

d. Specify the loopback interface for which the source IP address is picked for sending DNS queries.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set dns-source-interface loopback-interface-name
```

e. Disable the filtering of HTTP traffic that contains an embedded IP address (for example, http:/10.1.1.1) belonging to a disallowed domain name in the URL filter database.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set disable-url-filtering
```

f. Configure the DNS resolution time interval in minutes.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set dns-resolution-interval minutes
```

g. Configure the number of retries for a DNS query in case the query fails or times out.

```
[edit services (web-filter | url-filter) profile profile-name]
user@host# set dns-retries number
```

h. Specify the IP addresses (IPv4 or IPv6) of DNS servers to which the DNS queries are sent.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set dns-server [ip-address]
```

i. Specify the client-facing logical interfaces on which the URL filtering is configured.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set client-interfaces [ client-interface-name ]
```

j. Specify the server-facing logical interfaces on which the URL filtering is configured.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set server-interfaces [ server-interface-name ]
```

k. Specify the routing instance on which the URL filtering is configured.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set routing-instance routing-instance-name
```

l. Specify the routing instance on which the DNS server is reachable.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# dns-routing-instance dns-routing-instance-name
```

4. Configure the term information.

   Terms are used in filters to segment the policy or filter into small match and action pairs.

   a. Name the term.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# set term term-name
```

   b. Go to the new term hierarchy level.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name)]
user@host# edit term term-name
```

   c. Specify the source IP address prefixes for traffic you want to filter.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name) term term-name]
user@host# set from src-ip-prefix [prefix]
```

d. Specify the destination ports for traffic you want to filter.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name) term term-name]
user@host# set from dest-port [port]
```

e. Configure an action to take.

```
[edit services (web-filter | url-filter) profile profile-name (url-filter-template template-name | template
    template-name) term term-name]
user@host# set then action
```

The action can be one of the following:

custom-page *custom-page*—Send a custom page string to the user.

http-status-code *http-status-code*—Send an HTTP status code to the user.

redirect-url *redirect-url*—Send an HTTP redirect to the user.

tcp-reset—Send a TCP reset to the user.

5. Associate the URL profile with a next-hop service set.

NOTE: For URL filtering, you must configure the service set as a next-hop service set.

```
[edit]
user@host# set services service-set service-set-name (web-filter-profile profile-name | url-filter-profile
    profile-name)
user@host# set services service-set service-set-name next-hop-service inside-service-interface
    interface-name.unit-number
user@host# set services service-set service-set-name next-hop-service outside-service-interface
    interface-name.unit-number
```

NOTE: The service interface can also be of the **ams** prefix. If you are using **ams** interfaces at the **[edit services service-set *service-set-name]*** hierarchy level for the URL filter, you must also configure the **load-balancing-options hash-keys** statement at the **[edit interfaces *ams-interface-name* unit *number*]** hierarchy level. .

NOTE: Starting in Junos OS Release 18.3R1, configure the service set with the **web-filter-profile** statement. Before Junos OS Release 18.3R1, configure the service set with the **url-filter-profile** statement.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, this same functionality is available for Next Gen Serices on MX240, MX480, and MX960.
18.3R1	Starting in Junos OS Release 18.3R1, for Adaptive Services. configure the profile at the **[edit services web-filter]** hierarchy level. Before Junos OS Release 18.3R1, configure the profile at the **[edit services url-filter]** hierarchy level.

RELATED DOCUMENTATION

URL Filtering Overview | 52

Configuring Service Sets to be Applied to Services Interfaces | 9

Exchanging Data More Efficiently Using TCP Fast Open

TCP Fast Open (TFO) is an update to TCP that saves up to one full round-trip time (RTT) over the standard three-way connection handshake during a TCP session. TFO support is for MS-MPC and MS-MIC.

The standard three-way connection handshake involves three sets of send and receive messages between two hosts and the following exchange of SYN (synchronize) and ACK (acknowledgement) packets:

1. Host A sends a TCP SYN packet to Host B. Host B receives it.
2. Host B sends a SYN-ACK packet to Host A. Host A receives it.

3. Host A sends an ACK packet to Host B. Host B receives it.

In standard TCP, although data can be carried in SYN packets, this data cannot be delivered until the three-way handshake is completed. TFO removes this constraint and allows data in SYN packets to be delivered to the application, yielding significant latency improvement.

The key component of TFO is the Fast Open Cookie (cookie), which is a Message Authentication Code (MAC) tag generated by the server. The client requests a cookie in one regular TCP connection, then uses it for future TCP connections to exchange data during the handshake.

The TFO option is used to request or to send a TFO cookie. When a cookie is not present or is empty, the option is used by the client to request a cookie from the server. When the cookie is present, the option is used to pass the cookie from the server to the client or from the client back to the server.

The following list outlines how the client requests a TFO cookie:

1. The client sends a SYN with a TFO option that has the cookie field empty.
2. The server generates a cookie and sends it through the TFO option of a SYN-ACK packet.
3. The client caches the cookie for future TFO connections.

Thereafter, the two devices perform a TFO exchange:

1. The client sends a SYN with data and the cookie in the TFO option.
2. The server validates the cookie:
   - If the cookie is valid, the server sends a SYN-ACK acknowledging both the SYN and the data.

     The server then delivers the data to the application.
   - Otherwise, the server drops the data and sends a SYN-ACK acknowledging only the SYN sequence number.

The rest of the connection proceeds like a normal TCP connection. The client can repeat many TFO operations once it acquires a cookie (until the cookie is expired by the server). Thus, TFO is useful for applications in which the same client reconnects to the same server multiple times and exchanges data.

RELATED DOCUMENTATION

tcp-fast-open | **1510**

Configuring TFO | **62**

Configuring TFO

IN THIS SECTION

In this topic, the three modes of TCP Fast Open (TFO) are described and examples given. The case of using NAT with TFO is also covered.

Three Modes for TFO

No configuration is required to use TFO. TFO is enabled by default. In default mode, all TFO packets are forwarded by the service PIC. Besides the default, there are two other modes for TFO that you configure through the CLI:

- Drop TFO—If this mode is set, no TFO packets are forwarded.
- Disable TFO—If this mode is set, any SYN or SYN ACK packet carrying TFO, data, or both, will be stripped of the TFO and the data before being forwarded.

The TFO option is enabled per service set. The service set can be either a next-hop service set or an interface-style service set. Following is an example interface-style service set configuration:

```
[edit]
services {
   service-set ss2 {
      stateful-firewall-rules sfw_rule;
      interface-service {
         service-interface ms-2/3/0;
      }
   }
   stateful-firewall {
      rule sfw_rule {
         match-direction input-output;
         term 0 {
            from {
               source-address {
                  any-ipv4;
               }
```

```
            destination-address {
              any-ipv4;
            }
            then {
              accept;
            }
          }
        }
      }
    }
  }
```

In this instance, TFO is enabled by default (no TFO configuration). The output for the **show services service-sets statistics tcp** command is as follows:

`user@host>` **show services service-sets statistics tcp**

```
Interface: ms-2/3/0
  Service set: ss2
    TCP open/close statistics:
      TCP first packet non-syn: 0
      TCP first packet reset: 0
      TCP first packet FIN: 0
      TCP non syn discard: 0
      TCP extension alloc fail: 0
      TFO SYN with cookie request: 1
      TFO SYN with cookie: 0
      TFO SYN ACK with cookie: 0
      TFO packets forwarded: 0
      TFO packets dropped: 1
      TFO packets stripped: 0
```

If you drop TFO enabled packets, you have the following configuration and output:

```
[edit]
services {
  service-set ss2 {
    service-set-options {
      tcp-fast-open drop;
    }
    stateful-firewall-rules sfw_rule;
```

```
      interface-service {
        service-interface ms-2/3/0;
      }
    }
  }
```

`user@host>` **show services service-sets statistics tcp**

```
Interface: ms-2/3/0
  Service set: ss2
    TCP open/close statistics:
      TCP first packet non-syn: 0
      TCP first packet reset: 0
      TCP first packet FIN: 0
      TCP non syn discard: 0
      TCP extension alloc fail: 0
      TFO SYN with cookie request: 1
      TFO SYN with cookie: 0
      TFO SYN ACK with cookie: 0
      TFO packets forwarded: 0
      TFO packets dropped: 1
      TFO packets stripped: 0
```

If you strip the TFO option, the configuration and output change accordingly:

```
[edit]
services {
  service-set ss2 {
    service-set-options {
      tcp-fast-open disabled;
    }
    stateful-firewall-rules sfw_rule;
    interface-service {
      service-interface ms-2/3/0;
    }
  }
}
```

`user@host>` **show services service-sets statistics tcp**

```
Interface: ms-2/3/0
  Service set: ss2
    TCP open/close statistics:
      TCP first packet non-syn: 0
      TCP first packet reset: 0
      TCP first packet FIN: 0
      TCP non syn discard: 0
      TCP extension alloc fail: 0
      TFO SYN with cookie request: 1
      TFO SYN with cookie: 0
      TFO SYN ACK with cookie: 0
      TFO packets forwarded: 0
      TFO packets dropped: 0
      TFO packets stripped: 1
```

Using NAT and TFO

If NAT is configured in the service set and you are using TFO, you should configure address-pooling paired (APP). APP allows a private IP address to be mapped to the same public IP address from a NAT pool for all its sessions.

If you do not configure APP, NAT can give a different IP address to the client from the same NAT pool than the one it sent to the server before. The server does not recognize the IP address, drops the TFO option, and replies with SYN ACK and the data the client sent is not acknowledged. Therefore, even though the connection is successful and no packet is lost, the benefit of TFO is lost. But if client comes back with the same IP address, the server recognizes it and acknowledges the data. Therefore, always enable APP with a high mapping timeout value with TFO.

To configure APP:

1. Configure APP:

   ```
   set services nat rule rule-name term term-name then translated address-pooling paired
   ```

2. Configure a high mapping timeout value:

   ```
   set services nat pool nat-pool-name mapping-timeout seconds
   ```

RELATED DOCUMENTATION

Integration of Juniper ATP Cloud and Web filtering on MX Routers

IN THIS SECTION

Overview

IN THIS SECTION

Juniper Sky™ Advanced Threat Prevention (Juniper ATP Cloud) is integrated with MX series routers to protect all hosts in your network against evolving security threats by employing cloud-based threat detection software with a next-generation firewall system.

This topic provides an overview of Juniper ATP Cloud, Policy Enforcer, Security Intelligence, Web filtering, and their benefits when integrated on MX Series routers (MX240, MX480 and MX960).

Benefits

- Simplifies deployment and enhances the anti-threat capabilities when integrated with the MX routers.
- Delivers protection against “zero-day” threats using a combination of tools to provide robust coverage against sophisticated, evasive threats.
- Checks inbound and outbound traffic with policy enhancements that allow users to stop malware, quarantine infected systems, prevent data exfiltration, and disrupt lateral movement.
- Supports High Availability to provide uninterrupted service.

- Provides scalability to handle increasing loads that require more computing resources, increased network bandwidth to receive more customer submissions, and a large storage for malware.
- Provides deep inspection, actionable reporting, and inline malware blocking.

Understanding Policy Enforcer and Juniper ATP Cloud

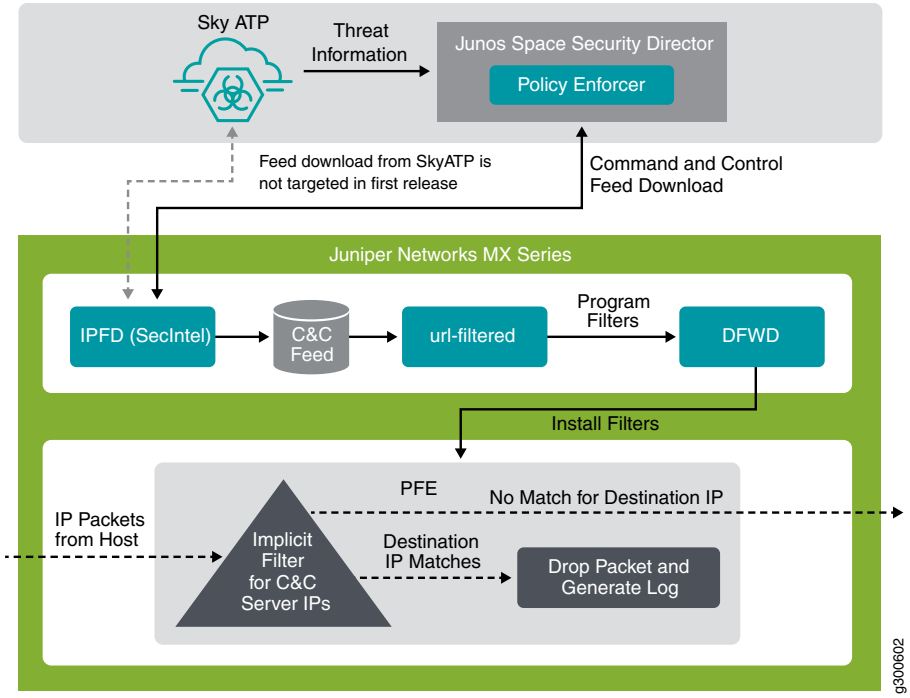
Juniper Networks Security Director comprises a feature called the Policy Enforcer (PE) that enables it to learn from threat conditions, automate the policy creation, and to dynamically deploy enforcement to Juniper devices in the network.

Figure 3 on page 68 illustrates the traffic flow between the PE, the Juniper ATP Cloud, and the MX router which functions as a firewall.

- Policy Enforcer (PE) learns from threat conditions, automates the policy creation, and deploys enforcement to Juniper devices in the network.
- Juniper Sky™ Advanced Threat Prevention (Juniper ATP Cloud) protects all hosts in your network by employing cloud-based threat detection software with a next-generation firewall system.
- MX router fetches the threat intelligence feeds from Policy Enforcer (PE) and implements those policies to quarantine compromised hosts. It comprises of the following important components:
  - Security Intelligence process
  - Web Filtering process
  - Firewall process

Figure 3: System Architecture

ERROR: Unresolved graphic fileref="" not found in "//cmsxml/default/main/supplemental/STAGING/images/".



To understand the functionality of the system architecture consider the following example—if a user downloads a file from the Internet and that file passes through an MX firewall, the file can be sent to the Juniper ATP Cloud cloud for malware inspection (depending on your configuration settings.) If the file is determined to be malware, PE identifies the IP address and MAC address of the host that downloaded the file. Based on a user-defined policy, that host can be put into a quarantine VLAN or blocked from accessing the Internet.

MX Series routers (MX240, MX480, and MX960) can be integrated with the Juniper ATP Cloud to prevent compromised hosts (botnets) from communicating with command and control servers:

- Starting in Junos OS Release 18.4R1 with the Adaptive Services as an Inline security capability
- Starting in Junos OS Release 19.3R2 with the Next Gen Services as an Inline security capability

Security Intelligence (SecIntel) - Overview

The Security Intelligence process (IPFD), is responsible for downloading the security intelligence feeds and parsing from the feed connector or ATP Cloud cloud feed server. The IPFD process on the MX platforms fetches the command and control IPv4/IPv6 feeds from Policy Enforcer. C&C feeds are essentially a list of servers that are known command and control servers for botnets. The list also includes servers that are

known sources for malware downloads. The information thus fetched is saved in a file (**urlf_si_cc_db.txt**) created under the **/var/db/url-filterd** directory.

The file format of the disallowed IPs sent by IPFD to the web filtering process is as follows:

IPv4 address | IPv6 address, threat-level.

The ***threat-level*** is an integer ranging from 1 to 10 to indicate the threat level of files scanned for malware and for infected hosts. Here, 1 represents the lowest threat level and 10 represents the highest threat level.

For example: 178.10.19.20, 4

Here, 178.10.19.20 indicates the disallowed IP and 4 indicates the ***threat-level***.

The C&C feed database is synced onto the backup Routing Engine. IPFD then shares the information to the web filtering process (url-filterd). The web filtering process reads the file contents and configures the filters accordingly.

Configuring Security Intelligence to Download the CC Feed from Policy Enforcer

To download the command and control IPv4/IPv6 feeds from Juniper ATP Cloud/Policy Enforcer, include the **security-intelligence** statement at the **[edit services]** hierarchy as shown in the following example:

```
security-intelligence {
    authentication {
        auth-token 7QGSBL5ZRKR5UHUZ2X2R6QLHB656D5EN;
    }
    url https://10.92.83.245:443/api/v1/manifest.xml;
    traceoptions {
        file security-inteligence.log size 1g;
        level all;
        flag all;
    }
}
```

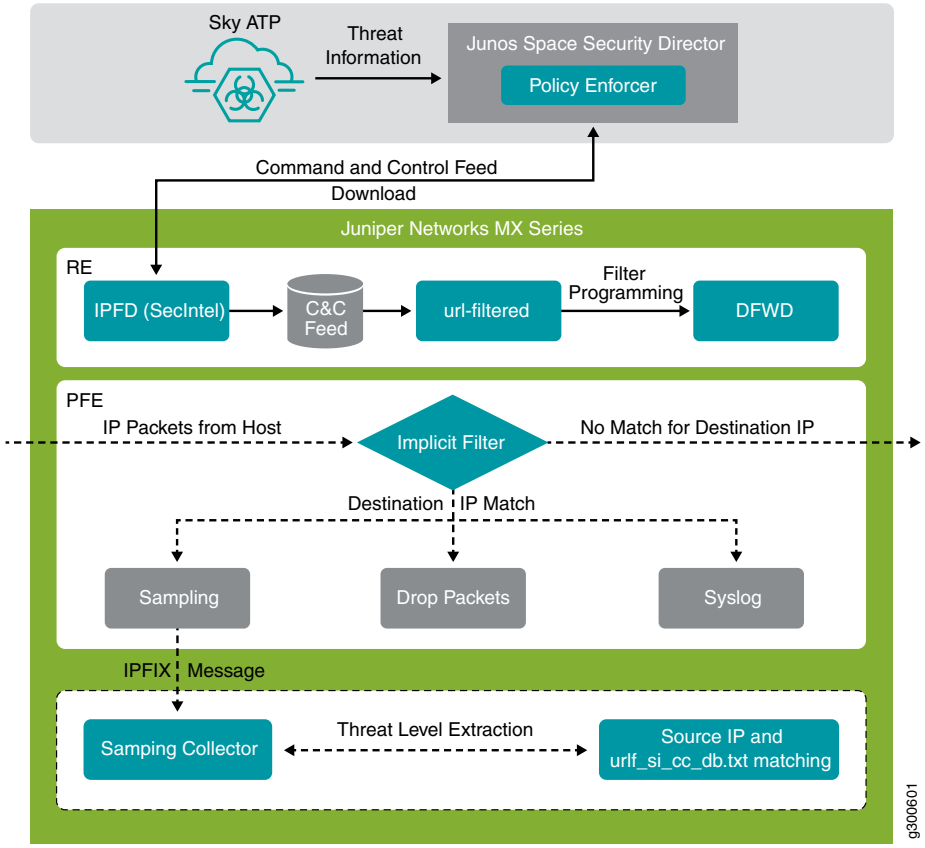
Web Filtering (URL-Filterd) - Overview

The web filtering process reads the file contents fetched from the IPFD and configures the filters on the Packet Forwarding Engine accordingly. The web filtering process enforces the command and control feeds by programming the filters in the Packet Forwarding Engine to block the packets destined to the blocked IP addresses and to generate logs for reporting the incident.

Figure 4 on page 70 illustrates the way C&C feed is fetched by the IPFD and then processed by the web filtering process.

Figure 4: Web Filtering

ERROR: Unresolved graphic fileref="" not found in "//cmsxml/default/main/supplemental/STAGING/images/".



The web filter profile can have more than one templates. Each template consists of a set of configured logical interfaces for Web filtering and one or more terms. A term is a set of match criteria with actions to be taken if the match criteria is met. To configure the web filter profile to use dynamically fetched C&C feed, you can configure the **security-intelligence-policy** command under the **[edit services web-filter profile *profile-name*** hierarchy level. You need not configure a term for a **security-intelligence-policy** based web filter profiles.

You can configure the following threat level actions for the web filter profile at the **edit web-filter profile *profile-name* security-intelligence-policy threat-level *threat-level* threat-action** hierarchy level:

- **drop**
- **drop-and-log**
- **log**

You can configure only one **threat-action** for each **threat level**. If the **threat-action** is not configured for a particular **threat level**, the default **threat-action** is **accept**.

SEE ALSO

security-intelligence-policy | 1444
security-intelligence | 1442

Configuring the Web Filter Profile for Sampling

Starting in Junos OS Release 19.3R1, web filtering process (url-filterd) supports inline sampling of packets as a threat level action. The packets are dropped, logged, and sampled based on the threat-action you configure. For scaled scenarios, sampling of packets is preferred over the logging option. Along with the existing threat level actions, you can configure the following threat level actions on the web filter profile at the **edit web-filter profile** ***profile-name*** **security-intelligence-policy threat-level** ***threat-level*** **threat-action** hierarchy level:

- **drop-and-sample**
- **drop-log-and-sample**
- **log-and-sample**
- **sample**

The inline flow monitoring samples the packets and sends the flow records in IPFIX format to a flow collector. You can derive the threat level for the sampled packets received at the external collector by matching the received IP from the sampled packets with the corresponding IP entry in **/var/db/url-filterd/urlf_si_cc_db.txt**. You can configure sampling using any of the following methods:

- Associate a sampling instance with the FPC on which the media interface is present at the **[edit chassis]** hierarchy level. If you are configuring sampling of IPv4 flows, IPv6 flows, or VPLS flows, you can configure the flow hash table size for each family.
- Configure the template properties for inline flow monitoring at the **[edit services flow-monitoring** hierarchy level.
- Configure a sampling instance and associate the flow-server IP address, port number, flow export rate, and specify the collectors at the **[edit forwarding-options** hierarchy level.

Associate a Sampling Instance with the FPC

To associate the defined instance with a particular FPC, MPC, or DPC, you include the **sampling-instance** statement at the **[edit chassis fpc number]** hierarchy level, as shown in the following example:

```
chassis {
    redundancy {
        graceful-switchover;
    }
    fpc 0 {
        pic0 {
            inline-services {
                bandwidth 10g;
            }
            }
        }
        pic 2 {
            inline-services {
                bandwidth 10g;
            }
        }
        pic 3 {
            inline-services {
                bandwidth 10g;
            }
        }
        sampling-instance 1to1;
        inline-services{
        flow-table-size {
            ipv4-flow-table-size 5;
            ipv6flow-table-size 5;
        }
    }
}
```

Configure a Sampling Instance and Associate the Template With the Sampling Instance.

To configure the template properties for inline flow monitoring, include the following statements at the **edit services flow-monitoring** hierarchy level as shown in the following example:

```
services {
    flow-monitoring {
        version-ipfix {
        template ipv4 {
        flow-active-timeout 60;
    flow-inactive-timeout 60;
        template-refresh-rate {
            packets 48000;
            seconds 60;
```

```
        }
        option-refresh-rate {
            packets 48000;
            seconds 60;
            }
        ipv4-template;
        template ipv6 {
            flow-active-timeout 60;
            flow-inactive-timeout 60;
            template-refresh-rate {
                packets 48000;
                seconds 60;
                }
                ipv6-template;
            }
        }
}
```

Configure the sample instance and associate the flow-server IP address and other parameters.

To configure a sampling instance and associate the flow-server IP address and other parameters. include the following statements at the **[edit forwarding-options]** hierarchy, as shown in the following example:

```
forwarding-options {
    sampling {
        traceoptions {
            file ipfix.log size 10k;
        }
    instance {
        1to1 {
        input {
        rate 1;
    }
    family inet {
        output {
            flow-server 192.168.9.194;
            port 2055;;
            autonomous-system-type origin;
            version-ipfix {
                template {
            ipv4;
        }
        }
        }
```

```
        inline-jflow {
        source-address 192.168.9.195;
        }
        }
    }
    family inet6 {
        output {
            flow-server 192.168.9.194;
            port 2000;
            autonomous-system-type origin;
            version-ipfix {
                template {
            ipv6;
        }
        }
        }
        inline-jflow {
        source-address 192.168.9.195;
        }
        }
    }
    }
}
```

Example: Configuring Web-filter Profile to Define Different Threat-Levels

```
web-filter {
    profile Profile1 ;
    security-intelligence-policy{
    file-type txt;
    threat-level 7 {
        threat-action {
        log-and-sample;
        }
    }
    threat-level 8 {
        threat-action {
        drop-log-and-sample;
        }
    }
    threat-level 10 {
        threat-action {
        drop-log-and-sample;
        }
```

```
    }
    threat-level 5{
      threat-action {
      drop-log-and-sample;
      }
    }
    threat-level 6 {
      threat-action {
      drop-log-and-sample;
      }
    }
    threat-level 9{
      threat-action {
      drop-log-and-sample;
      }
    }
    }
    url-filter-template template1 {
      client-interfaces ge-0/0/4.0;
      client-routing-instance inet.0;
    }
    }
    traceoptions {
      file webfilter_log size 1g;
      level all;
      flag all;
    }
    }
}
```

SEE ALSO

security-intelligence-policy | **1444**

Configuring Traffic Sampling on MX, M and T Series Routers

2

PART

Translating IP Addresses Using NAT

CHAPTER 4

NAT Overview

IN THIS CHAPTER

Junos Address Aware Network Addressing Overview

IN THIS SECTION

Junos Address Aware Network Addressing provides Network Address Translation (NAT) functionality for translating IP addresses. This is particularly important because the Internet Assigned Numbers Authority (IANA) allocated the last large block of IPv4 addresses in early 2011.

This topic includes the following sections:

Benefits of NAT

NAT supports a wide range of networking goals, including:

- Concealing a set of host addresses on a private network behind a pool of public addresses to protect the host addresses from direct targeting in network attacks and to avoid IPv4 address exhaustion
- Providing the tools to transition to IPv6 based on business requirements and to ensure uninterrupted subscriber and service growth
- Providing IPv4–IPv6 coexistence

NAT Concept and Facilities Overview

Junos Address Aware Network Addressing provides carrier-grade NAT (CGN) for IPv4 and IPv6 networks, and facilitates the transit of traffic between different types of networks.

Junos Address Aware Network Addressing supports a diverse set of NAT translation options:

- Static-source translation—Allows you to hide a private network. It features a one-to-one mapping between the original address and the translated address; the mapping is configured statically. For more information, see “Basic NAT” on page 80.
- Deterministic NAPT—Eliminates the need for address translation logging by ensuring that the original source IPv4 or IPv6 address and port always map to the same post-NAT IPv4 address and port range.
- Dynamic-source translation— Includes two options: dynamic address-only source translation and Network Address Port Translation (NAPT):
  - Dynamic address-only source translation— mdash;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 82.
  - 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 80.
- Static destination translation—Allows you to make selected private servers accessible. It features a one-to-one mapping between the translated address and the destination address; the mapping is configured statically. For more information, see “Static Destination NAT” on page 81.

- Protocol translation—Allows you to assign addresses from a pool on a static or dynamic basis as sessions are initiated across IPv4 or IPv6 boundaries. For more information, see "Configuring NAT-PT" on page 225, "NAT-PT with DNS ALG" on page 82, and "Stateful NAT64" on page 83.
- Encapsulation of IPv4 packets into IPv6 packets using softwires—Enables packets to travel over softwires to a carrier-grade NAT endpoint where they undergo source-NAT processing to hide the original source address. For more information, see "Tunneling Services for IPv4-to-IPv6 Transition Overview" on page 375.

Junos Address Aware Network Addressing supports NAT functionality described in IETF RFCs and Internet drafts, as shown in " *Supported NAT and SIP Standards*" in *Standards Reference*.

> **NOTE:** Not all types of NAT are supported on all interface types. See "Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card" on page 87, which lists features available on supported interfaces.

IPv4-to-IPv4 Basic 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 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 Address Aware Network Addressing. In addition, NAPT is supported for source addresses.

Basic NAT

With Basic NAT, a block of external addresses is 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, Basic NAT translates the destination IP address and the checksums listed above.

Hairpinning is supported for basic NAT.

NAPT

Use 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, NAPT translates the destination IP address, the destination transport identifier, and the IP and transport header checksums.

On MX Series routers with MS-MICs and MS-MPCs, if you configure a NAPT44 NAT rule and the source IP address of a spoofed packet is equal to the NAT pool and the NAT rule match condition fails, the packet is continuously looped between the services PIC and the Packet Forwarding Engine. We recommend that you manually clear the session and create a filter to block NAT pool IP spoofing under such conditions.

Hairpinning is supported for NAPT.

Deterministic NAPT

Use deterministic NAPT44 to ensure that the original source IPv4 address and port always map to the same post-NAT IPv4 address and port range, and that the reverse mapping of a given translated external IPv4 address and port are always mapped to the same internal IP address. This eliminates the need for address translation logging. Starting in Junos OS Release 17.4R1, deterministic NAPT64 is supported on the MS-MPC and MS-MIC. Deterministic NAPT64 ensures that the original source IPv6 address and port always map to the same post-NAT IPv4 address and port range, and that the reverse mapping of a given translated external IPv4 address and port are always mapped to the same internal IPv6 address.

Static Destination NAT

Use static destination NAT to translate 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 destination NAT, see RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*.

Twice NAT

In Twice NAT, both the source and destination addresses are subject to translation as packets traverse the NAT router. The source information to be translated can be either address only or address and port. For example, you would use Twice NAT when you are connecting two networks in which all or some addresses in one network overlap with addresses in another network (whether the network is private or public). In traditional NAT, only one of the addresses is translated.

To configure Twice NAT, you must specify both a destination address and a source address for the match direction, pool or prefix, and translation type.

You can configure application-level gateways (ALGs) for ICMP and traceroute under stateful firewall, NAT, or class-of-service (CoS) rules when Twice NAT is configured in the same service set. These ALGs cannot be applied to flows created by the Packet Gateway Control Protocol (PGCP). Twice NAT does not support other ALGs. By default, the Twice NAT feature can affect IP, TCP, and UDP headers embedded in the payload of ICMP error messages.

Twice NAT, specified in RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations*, is fully supported by Junos Address Aware Network Addressing.

IPv6 NAT

IPv6-to-IPv6 NAT (NAT66), defined in Internet draft draft-mrw-behave-nat66-01, *IPv6-to-IPv6 Network Address Translation (NAT66)*, is fully supported by Junos Address Aware Network Addressing.

Application-Level Gateway (ALG) Support

Junos Address Aware Network Addressing supports a number of ALGs. You can use NAT rules to filter incoming traffic based on ALGS. For more information, see "Network Address Translation Rules Overview" on page 106.

NAT-PT with DNS ALG

NAT-PT and Domain Name System (DNS) ALG are used to facilitate communication between IPv6 hosts and IPv4 hosts. Using a pool of IPv4 addresses, NAT-PT assigns addresses from that pool to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4 or IPv6 boundaries. Inbound and outbound sessions must traverse the same NAT-PT router so that it can track those sessions. RFC 2766, *Network Address Translation - Protocol Translation (NAT-PT)*, recommends the use of NAT-PT for translation between IPv6-only nodes and IPv4-only nodes, and *not* for IPv6-to-IPv6 translation between IPv6 nodes or IPv4-to-IPv4 translation between IPv4 nodes.

DNS is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. The DNS ALG is an application-specific agent that allows an IPv6 node to communicate with an IPv4 node and vice versa.

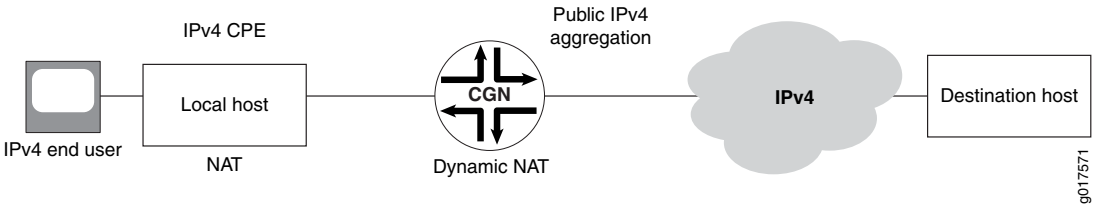
When DNS ALG is employed with NAT-PT, the DNS ALG translates IPv6 addresses in DNS queries and responses to the corresponding IPv4 addresses and vice versa. IPv4 name-to-address mappings are held in the DNS with "A" queries. IPv6 name-to-address mappings are held in the DNS with "AAAA" queries.

> **NOTE:** For IPv6 DNS queries, use the **do-not-translate-AAAA-query-to-A-query** statement at the **[edit applications application *application-name*]** hierarchy level.

Dynamic NAT

Dynamic NAT flow is shown in Figure 5 on page 83.

Figure 5: Dynamic NAT Flow



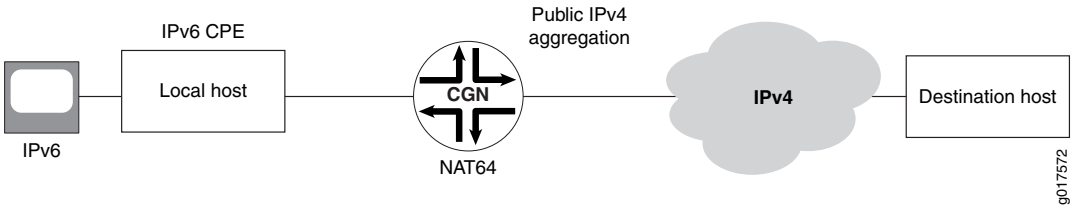
With dynamic NAT, you can map a private IP address (source) to a public IP address drawing from a pool of registered (public) IP addresses. NAT addresses from the pool are assigned dynamically. Assigning addresses dynamically also allows a few public IP addresses to be used by several private hosts, 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*.

Stateful NAT64

Stateful NAT64 flow is shown in Figure 6 on page 83.

Figure 6: Stateful NAT64 Flow



Stateful NAT64 is a mechanism to move to an IPv6 network and at the same time deal with IPv4 address depletion. By allowing IPv6-only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP, several IPv6-only clients can share the same public IPv4 server address. To allow sharing of the IPv4 server address, NAT64 translates incoming IPv6 packets into IPv4 (and vice versa).

When stateful NAT64 is used in conjunction with DNS64, no changes are usually required in the IPv6 client or the IPv4 server. DNS64 is out of scope of this document because it is normally implemented as an enhancement to currently deployed DNS servers.

Stateful NAT64, specified in RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*, is fully supported by Junos Address Aware Network Addressing.

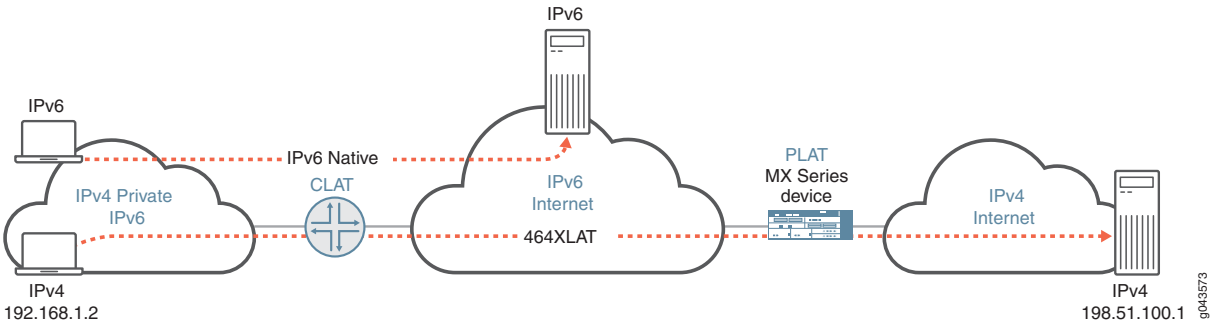
464XLAT

Starting in Junos OS Release 17.1R1, you can configure a 464XLAT Provider-Side Translater (PLAT). This is supported only on MS-MICs and MS-MPCs. 464XLAT provides a simple and scalable technique for an

IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. 464XLAT only suports IPv4 in the client-server model, so it does not support IPv4 peer-to-peer communication or inbound IPv4 connections.

A customer-side translator (CLAT), which is not a Juniper Networks product, translates the IPv4 packet to IPv6 by embedding the IPv4 source and destination addresses in IPv6 /96 prefixes, and sends the packet over an IPv6 network to the PLAT. The PLAT translates the packet to IPv4, and sends the packet to the IPv4 host over an IPv4 network (see Figure 7 on page 84).

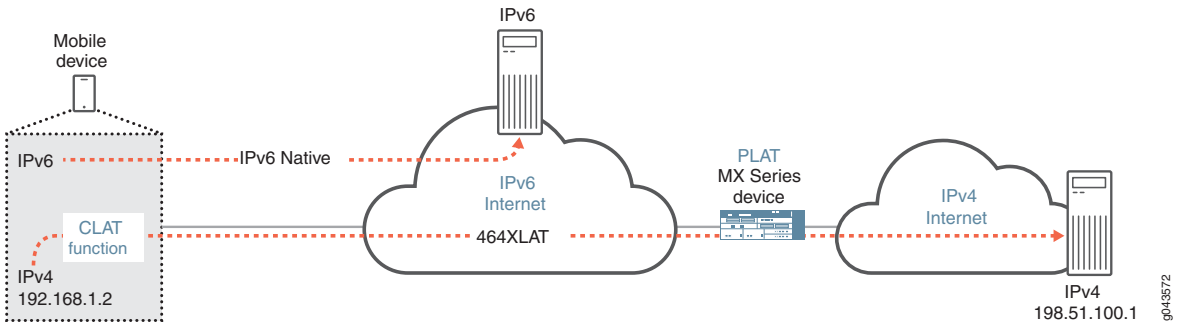
Figure 7: 464XLAT Wireline Flow



XLAT464 provides the advantages of not having to maintain an IPv4 network and not having to assign additional public IPv4 addresses.

The CLAT can reside on the end user mobile device in an IPv6-only mobile network, allowing mobile network providers to roll out IPv6 for their users *and* support IPv4-only applications on mobile devices (see Figure 8 on page 84).

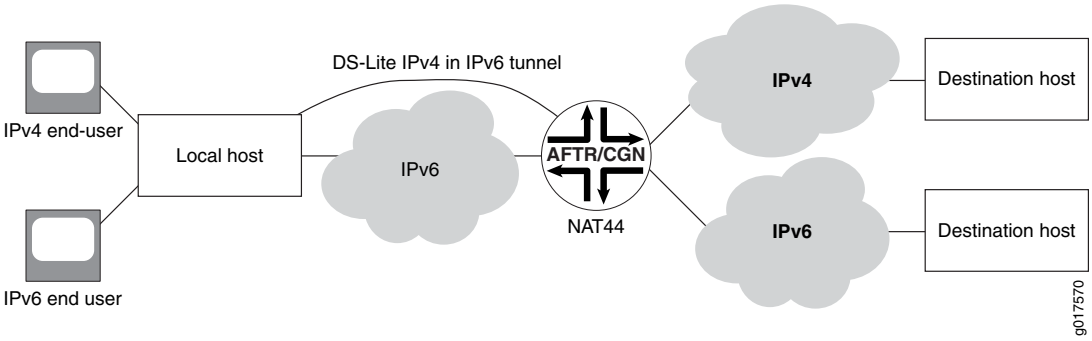
Figure 8: 464XLAT Wireless Flow



Dual-Stack Lite

Dual-stack lite (DS-Lite) flow is shown in Figure 9 on page 85.

Figure 9: DS-Lite Flow



DS-Lite employs IPv4-over-IPv6 tunnels to cross an IPv6 access network to reach a carrier-grade IPv4-IPv4 NAT. This facilitates the phased introduction of IPv6 on the Internet by providing backward compatibility with IPv4.

DS-Lite is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

Junos Address Aware Network Addressing Line Card Support

Junos Address Aware Network Addressing technologies are available on the following line cards:

- MultiServices Dense Port Concentrator (MS-DPC)
- MS-100, MS-400, and MS-500 MultiServices PICS
- MultiServices Modular Port Concentrator (MS-MPC) and MultiServices Modular Interface Card (MS-MIC)
- Modular Port Concentrators (inline NAT).

For a listing of the specific NAT types supported on each type of card, see “Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card” on page 87.

Release History Table

Release	Description
19.2R1	Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
17.4R1	Starting in Junos OS Release 17.4R1, deterministic NAPT64 is supported on the MS-MPC and MS-MIC.
17.4R1	Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.
17.1R1	Starting in Junos OS Release 17.1R1, you can configure a 464XLAT Provider-Side Translater (PLAT).

RELATED DOCUMENTATION

Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card | **87**

ALGs Available for Junos OS Address Aware NAT | **208**

Junos OS Carrier-Grade NAT Implementation Overview

Junos OS enables you to implement and scale a Carrier-Grade Network Address Translation (CGNAT) solution based on the type of services interfaces used for your implementation:

- MultiServices Denser Port Concentrator (MS-DPC)—The layer 3 services package is used to configure NAT for MS-DPC adaptive services PICs. This solution provides the NAT functionality described in "Junos Address Aware Network Addressing Overview" on page 78.
- MS-100, MS-400, and MS-500 MultiServices PICS—The layer 3 services package is used to configure NAT for multiservices PICs. This solution provides the NAT functionality described in "Junos Address Aware Network Addressing Overview" on page 78.
- MultiServices Modular Port Concentrator (MS-MPC) and MultiServices Modular Interface Card (MS-MIC)—MS-MPCs and MS-MICs are pre-configured to enable configuration of carrier-grade NAT. This solution provides the NAT functionality described in "Junos Address Aware Network Addressing Overview" on page 78.
- Inline NAT for Modular Port Concentrator (MPC) Line Cards)—Inline NAT leverages the services capabilities of MPC line cards, allowing a cost-effective implementation of NAT functionality on the data plane, as described in "Inline Network Address Translation Overview" on page 308.

RELATED DOCUMENTATION

Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card | 87

Carrier-Grade NAT Implementation: Best Practices | 120

Example: Configuring Basic NAT44 | 154

Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card

Table 9 on page 87 summarizes feature differences among the Junos OS carrier-grade NAT implementations.

Starting in Junos OS release 17.2R1, inline NAT is supported on the MPC5E and MPC6E.

Starting in Junos OS release 17.4R1, inline NAT is supported on the MPC7E, MPC8E, and MPC9E.

Table 9: Carrier-Grade NAT—Feature Comparison by Platform

Feature	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
Static Source NAT	yes	yes	yes
Dynamic Source NAT - Address Only	yes	yes	no
Dynamic Source NAT - NAPT Port Translation with Secured Port Block Allocation	yes	yes (Dynamic Source NAT - NAPT Port Translation with Secured Port Block Allocation supported for MS-MPC and MS-MIC starting in Junos OS Release 14.2R2)	no

Table 9: Carrier-Grade NAT—Feature Comparison by Platform *(continued)*

Feature	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
Dynamic Source NAT - NAPT44 Port Translation with Deterministic Port Block Allocation	yes	yes (Dynamic Source NAT - NAPT44 Port Translation with Deterministic Port Block Allocation supported for MS-MPC and MS-MIC starting in Junos OS release 17.3R1, in Junos OS release 14.2R7 and later 14.2 releases, in 15.1R3 and later 15.1 releases, and in 16.1R5 and later 16.1 releases)	no
Dynamic Source NAT - NAPT64 Port Translation with Deterministic Port Block Allocation	No	yes (Dynamic Source NAT - NAPT64 Port Translation with Deterministic Port Block Allocation supported for MS-MPC and MS-MIC starting in Junos OS release 17.4R1)	No
Static Destination NAT	yes	yes	yes **NOTE:** Destination NAT can be implemented indirectly. See "Inline Network Address Translation Overview" on page 308
Twice NAT	yes	yes (Twice NAT supported for MS-MPC and MS-MIC starting in Junos OS Release 15.1R1)	yes **NOTE:** Twice NAT can be implemented indirectly. See "Inline Network Address Translation Overview" on page 308

Table 9: Carrier-Grade NAT—Feature Comparison by Platform *(continued)*

Feature	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
NAPT - Preserve Parity and Range	yes	yes (NAPT - Preserve Parity and Range supported for MS-MPC and MS-MIC starting in Junos OS release 15.1R1)	no
NAPT - APP/EIF/EIM	yes	yes	no
IKE ALG	no	yes (Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1)	no
Stateful NAT64	yes	yes	no
Stateful NAT64 with APP/EIM/EIF	no	yes	no
Stateful NAT64 with ALGs • FTP • IKE • TFTP • SIP • RTSP • PPPT	no	yes	no
DS-Lite	yes	yes (DS-Lite supported for MS-MPC and MS-MIC starting in Junos OS release 17.4R1)	no
6rd	yes	no	no
6to4	yes	no	no
Inline 6rd	Need inputs	Need inputs	Need inputs

Table 9: Carrier-Grade NAT—Feature Comparison by Platform *(continued)*

Feature	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
Inline 6to4	Need inputs	Need inputs	Need inputs
464XLAT	no	yes (starting in Junos OS Release 17.1R1)	no
Overlap Address Across NAT Pool	yes	yes	no
Port Control Protocol	yes	yes (Port Control Protocol with NAPT44 is supported for MS-MPC and MS-MIC starting in Junos OS Release 17.4R1. PCP with DS-Lite is not supported.)	no
CGN-PIC	yes	no	no
AMS Support	no	yes	no
Port forwarding	yes	yes (Port forwarding is supported for MS-MPC and MS-MIC starting in Junos OS Release 17.4R1.)	no
No translation	yes	yes (No translation supported for MS-MPC and MS-MIC starting in Junos OS Release 15.1R1)	yes

Table 10 on page 91 summarizes availability of translation types by type of line card.

Table 10: Carrier-Grade NAT Translation Types

Translation Type	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
basic-nat44	yes	yes	yes
basic-nat66	yes	no	no
basic-nat-pt	yes	no	no
deterministic-napt44	yes	yes (**deterministic-napt44** supported for MS-MPC and MS-MIC starting in Junos OS release 17.3R1, in Junos OS release 14.2R7 and later 14.2 releases, in 15.1R3 and later 15.1 releases, and in 16.1R5 and later 16.1 releases)	no
deterministic-napt64	no	yes (**deterministic-napt64** supported for MS-MPC and MS-MIC starting in Junos OS release 17.4R1)	no
dnat-44	yes	yes	no
dynamic-nat44	yes	yes	no
napt-44	yes	yes	no
napt-66	yes	no	no
napt-pt	yes	no	no
stateful-nat464	no	yes (starting in Junos OS Release 17.1R1)	no
stateful-nat64	yes	yes	no

Table 10: Carrier-Grade NAT Translation Types *(continued)*

Translation Type	MS-DPC MS-100 MS-400 MS-500	MS-MPC MS-MIC	MPC1, MPC2, MPC3, MPC5E, MPC6E, MPC7E, MPC8E, and MPC9E *Inline NAT*
twice-basic-nat-44	yes	yes (**twice-dynamic-nat-44** supported for MS-MPC and MS-MIC starting in Junos OS Release 15.1R1)	yes (**twice-basic-nat-44** supported for inline NAT starting in Junos OS Release 15.1R1)
twice-dynamic-nat-44	yes	yes (**twice-dynamic-nat-44** supported for MS-MPC and MS-MIC starting in Junos OS Release 15.1R1)	no
twice-dynamic-napt-44	yes	yes (**twice-dynamic-napt-44** supported for MS-MPC and MS-MIC starting in Junos OS Release 15.1R1)	no

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1, inline NAT is supported on the MPC7E, MPC8E, and MPC9E.
17.4R1	Dynamic Source NAT - NAPT64 Port Translation with Deterministic Port Block Allocation supported for MS-MPC and MS-MIC
17.4R1	DS-Lite supported for MS-MPC and MS-MIC
17.4R1	**deterministic-napt64** supported for MS-MPC and MS-MIC
17.4.R1	Port forwarding is supported for MS-MPC and MS-MIC
17.2R1	Starting in Junos OS release 17.2R1, inline NAT is supported on the MPC5E and MPC6E.
17.1R4	Port Control Protocol with NAPT44 is supported for MS-MPC and MS-MIC
17.1R1	464XLAT
17.1R1	**stateful-nat464**
15.1R1	Twice NAT supported for MS-MPC and MS-MIC
15.1R1	NAPT - Preserve Parity and Range supported for MS-MPC and MS-MIC
15.1R1	No translation supported for MS-MPC and MS-MIC
15.1R1	**twice-dynamic-nat-44** supported for MS-MPC and MS-MIC
15.1R1	**twice-basic-nat-44** supported for inline NAT
15.1R1	**twice-dynamic-nat-44** supported for MS-MPC and MS-MIC
15.1R1	**twice-dynamic-napt-44** supported for MS-MPC and MS-MIC
14.2R7	Dynamic Source NAT - NAPT44 Port Translation with Deterministic Port Block Allocation supported for MS-MPC and MS-MIC
14.2R7	IKE ALG
14.2R7	**deterministic-napt44** supported for MS-MPC and MS-MIC

14.2R2	Dynamic Source NAT - NAPT Port Translation with Secured Port Block Allocation supported for MS-MPC and MS-MIC

RELATED DOCUMENTATION

- Junos OS Carrier-Grade NAT Implementation Overview | 86

CHAPTER 5

NAT Configuration Overview

IN THIS CHAPTER

Network Address Translation Overview on ACX Series

Network Address Translation (NAT) is a method for modifying or translating network address information in packet headers. Either or both source and destination addresses in a packet may be translated. NAT can include the translation of port numbers as well as IP addresses.

NAT is described in RFC 1631 to solve IP (version 4) address depletion problems. NAT has been found to be a useful tool for firewalls, traffic redirect, load sharing, network migrations, and so on.

NOTE: In ACX Series routers, NAT is supported only on the ACX1100 AC-powered router and ACX500 routers for inline NAT and inline IPsec services. ACX1100 AC-powered router supports only source NAT for IPv4 packets. Static and dynamic NAT types are currently not supported. Service chaining (GRE, NAT, and IPSec) on ACX1100-AC and ACX500 routers is not supported.

A license is required for enabling inline services on ACX500 routers.

NOTE: ACX5048 and ACX5096 routers do not support NAT configurations.

Source NAT is the translation of the source IP address of a packet leaving the router. Source NAT is used to allow hosts with private IP addresses to access a public network.

Source NAT allows connections to be initiated only for outgoing network connections—for example, from a private network to the Internet. Source NAT is commonly used to:

- Translate a single IP address to another address (for example, to provide a single device in a private network with access to the Internet).
- Translate a contiguous block of addresses to another block of addresses of the same size.
- Translate a contiguous block of addresses to another block of addresses of smaller size.
- Translate a contiguous block of addresses to a single IP address or a smaller block of addresses using port translation.
- Translate a contiguous block of addresses to the address of the egress interface.

RELATED DOCUMENTATION

Network Address Port Translation Overview | **98**

Enabling Inline Services Interface on ACX Series | **116**

Understanding Service Sets

Service Filters in ACX Series | **14**

Guidelines for Applying Service Filters | **15**

Service Filter Match Conditions for IPv4 Traffic | **17**

Service Filter Actions | **18**

Network Address Translation Address Overload in ACX Series | **98**

CoS for NAT Services on ACX Series Routers

Network Address Translation Constraints on ACX | **100**

Configuring Address Pools for Network Address Port Translation (NAPT) Overview | **115**

Configuring Service Sets to Be Applied to Services Interfaces

Configuring Queuing and Scheduling on Inline Services Interface | **20**

Network Address Port Translation Overview

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP ports are translated into a single network address and its TCP/UDP ports. This translation can be configured in both IPv4 and IPv6 networks.

In ACX Series routers, you can have up to 4096 network address translations at a time.

RELATED DOCUMENTATION

- Network Address Translation Overview on ACX Series | **96**
- Enabling Inline Services Interface on ACX Series | **116**
- *Understanding Service Sets*
- Service Filters in ACX Series | **14**
- Guidelines for Applying Service Filters | **15**
- Service Filter Match Conditions for IPv4 Traffic | **17**
- Service Filter Actions | **18**
- Network Address Translation Address Overload in ACX Series | **98**
- *CoS for NAT Services on ACX Series Routers*
- Network Address Translation Constraints on ACX | **100**
- Configuring Address Pools for Network Address Port Translation (NAPT) Overview | **115**
- *Configuring Service Sets to Be Applied to Services Interfaces*
- Configuring Queuing and Scheduling on Inline Services Interface | **20**

Network Address Translation Address Overload in ACX Series

The NAT services on ACX Series routers allows Junos OS interface addresses to be shared with a NAPT pool. This feature of sharing the same address/port between the NAPT pool and Junos OS is termed as address overloading.

To achieve address overloading, the available IPv4 address or port range of 1 to 65,536 addresses is partitioned between Junos OS and NAT as shown below:

- Junos OS—1 to 49,159 addresses.
- NAPT pool—49,160 through 53,255 addresses.
- Junos OS—53,255 through 65,535 addresses.

The number of ports reserved for NAPT pool with address overload feature is 4096.

To enable address-overloading, include the **address-overload** statement and the **interface** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level.

The **address-overload** statement enables sharing of IPv4 address between Junos OS and the NAT pool. Along with the **address-overload** statement, you must also specify the **interface** statement so that the first available IPv4 address or port of the interface is picked up for the NAT pool.

You can configure the address overload feature the following ways:

- Configure an interface along with the **address-overload** statement as shown in the following example.

```
pool p3 {
   address-overload;
   interface ge-0/0/1.0;
   port {
      range low 49160 high 53255;
   }
}
```

  In this case, the primary address on the interface is picked for the NAT pool.

- Directly configure a /32 address as shown in the following example:

```
pool p4 {
   address-overload;
   address 45.0.0.1/32;
   port {
      range low 49160 high 53255;
   }
}
```

The **interface** statement enables sharing of IPv4 interface address with the NAT pool along with the port range specified in the pool.

RELATED DOCUMENTATION

Network Address Translation Overview on ACX Series | **96**

Network Address Port Translation Overview | **98**

Enabling Inline Services Interface on ACX Series | **116**

Understanding Service Sets

Service Filters in ACX Series | **14**

Network Address Translation Constraints on ACX

You should consider the following constraints while configuring Network Address Translation (NAT) on ACX Series routers:

- When a port is defined in a NAT pool, you can configure only one address or one address range in the pool.
- ACX Series routers support **nat-rules** with **match-direction** as *input*. **match-direction** as *output* is not supported.
- When you specify an address range or an address prefix in a NAT pool, the maximum number of addresses supported is 65,535. ACX Series routers supports up to 4096 network address translations at a time.
- The maximum number of service sets that can be configured is 2.
- In a NAT rule term, the **from** clause can contain a maximum of 4 matching addresses.
- The maximum terms per NAT rule allowed is 4.
- The maximum NAT rules per service set allowed is 2.

RELATED DOCUMENTATION

Network Address Translation Configuration Overview

To configure network address translation (NAT), complete the following high-level steps:

1. Configure the source and destination addresses. For more information, see "Configuring Source and Destination Addresses Network Address Translation Overview" on page 101.

2. Define the addresses or prefixes, address ranges, and ports used for NAT. For more information, see "Configuring Pools of Addresses and Ports for Network Address Translation Overview" on page 103

3. If applicable, configure the address pools for network address port translation (NAPT). For more information, see "Configuring Address Pools for Network Address Port Translation (NAPT) Overview" on page 170.

4. Configure the NAT rules. Within the rules, include match directions, match conditions, actions, and translation types. For more information, see "Network Address Translation Rules Overview" on page 106.

5. Configure service sets for NAT processing. Within each service set, define the interfaces for handling inbound and outbound traffic and a NAT rule or ruleset. For more information, see "Configuring Service Sets for Network Address Translation" on page 117.

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview

You must configure a specific address, a prefix, or the address-range boundaries:

- 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)

The addresses that are specified as valid in the **inet.0** routing table and not supported for NAT translation are **orlonger** match filter types. You cannot specify any regions within such address prefixes in a NAT pool.

- On MX Series routers with MS-MPCs and MS-MICs, if you configure a NAT address pool with a prefix length that is equal to or greater than /16, the PIC does not contain sufficient memory to provision the configured pool. Also, memory utilization problems might occur if you attempt to configure many pools whose combined total IP addresses exceed /16. In such circumstances, a system logging message is generated stating that the NAT pool name is failed to be created and that the service set is not activated. On MS-MPCs and MS-MICs, you must not configure NAT pools with prefix lengths greater than or equal to /16.
- 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. For more information, see *Examples: Configuring NAT Rules*.
- 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 or IPv6 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.
- When you configure a NAT address pool prefix size with the **address** statement at the [**edit services nat pool *nat-pool-name***] hierarchy level, the subnet and broadcast addresses are not included in the list of usable IP addresses. For example, if you use **address 10.11.12.0/28** in a NAT pool, the addresses 10.11.12.0 (subnet address) and 10.11.12.15 (broadcast address) are not available.

NOTE: When you include a NAT configuration that changes IP addresses, it 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 protocol operation, because the protocol peering, neighbor, and interface addresses can be altered when routing protocols packets transit the Adaptive Services (AS) or Multiservices PIC.

RELATED DOCUMENTATION

Junos Address Aware Network Addressing Overview | 78

Configuring Pools of Addresses and Ports for Network Address Translation Overview

IN THIS SECTION

Configuring NAT Pools

You can use the **pool** statement to define the addresses (or prefixes), address ranges, and ports used for Network Address Translation (NAT). To configure the information, include the **pool** statement at the **[edit services nat]** hierarchy level.

Starting in Junos OS Release 14.2, configure the NAT pool as follows. Starting in Junos OS Release 16.1, the **limit-ports-per-address** statement is supported.

```
[edit services nat]
```

```
pool nat-pool-name {
    address ip-prefix</prefix-length>;
    address-range low minimum-value high maximum-value;
    limit-ports-per-address number;
    port {
        automatic (sequential | random-allocation);
        range low minimum-value high maximum-value random-allocation;
        preserve-parity;
        preserve-range {
    }
}
```

In Junos OS Release 14.1 and earlier, configure the NAT pool as follows:

```
[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 {
    }
}
```

To configure pools for traditional NAT, specify either a destination pool or a source pool.

With 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.

With static destination NAT, you can also 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 than or equal to the netmask or range for the destination pool address. If you define the pool to be larger than required, some addresses will not be 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.

For constraints on specific translation types, see "Network Address Translation Rules Overview" on page 106.

With source static NAT, the prefixes and address ranges cannot overlap between separate pools.

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.

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.

Preserve Range and Preserve Parity

You can configure your carrier-grade NAT (CGN) to preserve the range or parity of the packet source port when it allocates a source port for an outbound connection. You can configure the preserve parity and preserve range options under the NAT pool definition by including the **preserve-range** and **preserve-parity** configuration statements at the **[edit services nat pool *poolname* port]** hierarchy level.

Preserving range and preserving parity are supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Preserving range and preserving parity are supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 15.1R1.

- Preserve range—RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*, defines two ranges: 0 through 1023, and 1024 through 65,535. When the **preserve-range** knob is configured and the incoming port falls into one of these ranges, CGN allocates a port from that range only. However, if there is no available port in the range, the port allocation request fails and that session is not created. The failure is reflected on counters and system logging, but no Internet Control Message Protocol (ICMP) message is generated. If this knob is not configured, allocation is based on the configured port range without regard to the port range that contains the incoming port. The exception is some application-level gateways (ALGs), such as hello, that have special zones.
- Preserve parity—When the **preserve-parity** knob is configured, CGN allocates a port with the same even or odd parity as the incoming port. If the incoming port number is odd or even, the outgoing port number should correspondingly be odd or even. If a port number of the desired parity is not available, the port allocation request fails, the session is not created, and the packet is dropped.

Specifying Destination and Source Prefixes Without Configuring a Pool

You can directly specify the destination or source prefix used in NAT 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;
            }
        }
    }
```

```
}
```

Release History Table

Release	Description
16.1	Starting in Junos OS Release 16.1, the **limit-ports-per-address** statement is supported.
14.2	Starting in Junos OS Release 14.2, configure the NAT pool as follows.

Network Address Translation Rules Overview

IN THIS SECTION

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

```
[edit services nat]
allow-overlapping-nat-pools ;
   apply-groups;
   apply-groups-except;
   pool pool-name;
port-forwarding port-forwarding-name;
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 {
                address-pooling paired;
                clat-prefix clat-prefix;
                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-name;
                overload-prefix overload-prefix;
                source-pool nat-pool-name;
                source-prefix source-prefix;
                translation-type {
                    (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44 | napt-44 | napt-66 | napt-pt |
                        stateful-nat464 | stateful-nat64 | twice-basic-nat-44 | twice-dynamic-nat-44 | twice-napt-44);
                }
            }
            syslog;
        }
    }
}
```

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

> **NOTE:** ACX Series routers support only *input* as the match direction.

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 the components of NAT rules:

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 DPC and Multiservices PICs. When a packet is sent to the PIC, direction information is carried along with it. The packet direction is determined based on the following criteria:

- 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 DPC or 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 or DPC, the packet direction is output. For more information about inside and outside interfaces, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.
- On the Multiservices DPC and 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 *Routing Policies, Firewall Filters, and Traffic Policers User 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. For an example, see "Examples: Configuring Stateful Firewall Rules" on page 553.

If the **translation-type** statement in the **then** statement of the NAT rule is set to **stateful-nat-64**, the range specified by the **destination-address-range** or the **destination-prefix-list** in the **from** statement must be within the range specified by the **destination-prefix** statement in the **then** statement.

If at least one NAT term within a NAT rule has the address pooling paired (APP) functionality enabled (by including the **address-pooling** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level, all the other terms in the NAT rule that use the same NAT address pool as the address pool for the term with APP enabled must have APP enabled. Otherwise, if you add a NAT rule term without enabling APP to a rule that contains other terms with APP enabled, all the terms with APP enabled in a NAT rule drop traffic flows that match the specified criteria in the NAT rule.

For MX Series routers with MS-MICs and MS-MPCs, although the address pooling paired (APP) functionality is enabled within a NAT rule (by including the **address-pooling** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level), it is a characteristic of a NAT pool. Such a NAT pool for which APP is enabled cannot be shared with NAT rules that do not have APP configured.

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

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 {
        from {
            destination-address-range low minimum-value high maximum-value <except>;
            destination-prefix-list list-name <except>;
        }
```

```
        then {
            destination-prefix destination-prefix;
        }
```

```
[edit services nat rule rule-name term term-name]
then {
    no-translation;
    syslog;
    translated {
        clat-prefix clat-prefix;
        destination-pool nat-pool-name;
        destination-prefix destination-prefix;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | dynamic-nat44 | napt-44 | napt-66 |
            napt-pt | stateful-nat464 | stateful-nat64 | twice-basic-nat-44 | twice-dynamic-nat-44 | twice-napt-44);
        }
    }
}
```

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

  The **no-translation** statement is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. The **no-translation** statement is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 15.1R1.

- The **system log** 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 Pools of Addresses and Ports for Network Address Translation Overview" on page 103.

- The **translation-type** statement specifies the type of NAT used for source or destination traffic. The options are **basic-nat-pt**, **basic-nat44**, **basic-nat66**, **dnat-44**, **dynamic-nat44**, **napt-44**, **napt-66**, **napt-pt**, **stateful-nat464**, **stateful-nat64**, **twice-basic-nat-44**, **twice-dynamic-nat-44**, and **twice-napt-44**.

  NOTE: In Junos OS Release 13.2 and earlier, the following restriction was not enforced by the CLI: if the **translation-type** statement in the **then** statement of a NAT rule was set to **stateful-nat-64**, the range specified by the **destination-address-range** or the **destination-prefix-list** in the **from** statement needed to be within the range specified by the **destination-prefix** statement in the **then** statement. Starting in Junos OS Release 13.3R1, this restriction is enforced.

Configuring Translation Types

The implementation details of the nine options of the **translation-type** statement are as follows:

- **basic-nat44**—This option implements the static translation of source IP addresses without port mapping. You must configure the **from source-address** statement in the match condition for the rule. The size of the address range specified in the statement must be the same as or smaller than the source pool. You must specify either a source pool or a destination prefix. The referenced pool can contain multiple addresses but you cannot specify ports for translation.

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

  > **NOTE:** Prior to Junos OS Release 11.4R3, you could only use a source NAT pool in a single service set. As of Junos OS Release 11.4R3 and subsequent releases, you can reuse a source NAT pool in multiple service sets.

- **basic-nat66**—This option implements the static translation of source IP addresses without port mapping in IPv6 networks. The configuration is similar to the **basic-nat44** implementation, but with IPv6 addresses.

  The **basic-nat66** option is not available if you are using MS-MPCs or MS-MICs.

- **basic-nat-pt**—This option implements translation of addresses of IPv6 hosts, as they originate sessions to the IPv4 hosts in an external domain and vice versa. This option is always implemented with DNS ALG. You must define the source and destination pools of IPv4 addresses. You must configure one rule and define two terms. Configure the IPv6 addresses in the **from** statement in both **term** statements. In the **then** statement of the first term within the rule, reference both the source and destination pools and configure **dns-alg-prefix**. Configure the source prefix in the **then** statement of the second term within the same rule.

  The **basic-nat-pt** option is not available if you are using MS-MPCs or MS-MICs.

- **deterministic-napt44**—This option implements algorithm-based allocation of blocks of destination ports and IP address. This ensures that an incoming (source) IP address and port always map to the same destination IP address and port, thus eliminating the need for the address translation logging. When you use **deterministic-napt44**, you must also use **deterministic-port-block-allocation** at the **[edit services nat pool *poolname* port]** hierarchy level.

  The **deterministic-napt44** option is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. The **deterministic-napt44** option if you are using MX Series routers with MS-MPCs or MS-MICs is supported only in Junos OS release 14.2R7 and later 14.2 releases and in release 15.1R3 and later 15.1 releases.

- **dnat-44**—This option implements static translation of destination IP addresses without port mapping. 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. 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 destination addresses in the **from** statement. You must include exactly one **destination-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 value remain unused, because a pool cannot be shared among multiple terms or rules.

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

  The **dynamic-nat44** address-only option supports translating up to 16,777,216 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. Because all the private hosts might not simultaneously create sessions, they can share a few public IP addresses.

- **napt-44**—This option implements dynamic translation of source IP addresses with port mapping. You must specify a name for the **source-pool** statement. The referenced pool must include a **port** configuration. If the port is configured as automatic or a port range is specified, then it implies that Network Address Port Translation (NAPT) is used.

- **napt-66**—This option implements dynamic address translation of source IP addresses with port mapping for IPv6 addresses. The configuration is similar to the **napt-44** implementation, but with IPv6 addresses.

  The **napt-66** option is not available if you are using MS-MPCs or MS-MICs.

- **napt-pt**—This option implements dynamic address and port translation for source and static translation of destination IP address. You must specify a name for the **source-pool** statement. The referenced pool must include a port configuration (for NAPT). Additionally, you must configure two rules, one for the DNS traffic and the other for the rest of the traffic. The rule meant for the DNS traffic should be DNS ALG enabled and the **dns-alg-prefix** statement should be configured. Moreover, the prefix configured in the **dns-alg-prefix** statement must be used in the second rule to translate the destination IPv6 addresses to IPv4 addresses.

  The **napt-pt** option is not available if you are using MS-MPCs or MS-MICs.

- **stateful-nat464**—This option implements 464XLAT Provider-Side Translater (PLAT) address translation for source IP addresses and IPv6 prefix removal translation for destination IPv4 addresses. You must specify the IPv4 addresses used for translation at the [edit services nat pool] hierarchy level. This pool must be referenced in the rule that translates the IPv6 addresses to IPv4.

  The **stateful-nat464** option is available only if you are using MS-MPCs or MS-MICs, and is supported starting in Junos OS Release 17.1R1.

- **stateful-nat64**—This option implements dynamic address and port translation for source IP addresses and prefix removal translation for destination IP addresses. You must specify the IPv4 addresses used for translation at the **[edit services nat pool]** hierarchy level. This pool must be referenced in the rule that translates the IPv6 addresses to IPv4.
- **twice-basic-nat-44**—This option implements static source and static destination translation for IPv4 addresses, thus combining **basic-nat44** for source and **dnat-44** for destination addresses.

  The **twice-basic-nat-44** option is supported on MS-DPCs and MS-100, MS-400, and MS-500 MultiServices PICS. The **twice-basic-nat-44** option is supported on MS-MPCs and MS-MICs starting in Junos OS Release 15.1R1.
- **twice-dynamic-nat-44**—This option implements source dynamic and destination static translation for IPv4 addresses, combining **dynamic-nat44** for source and **dnat-44** for destination addresses.

  The **twice-dynamic-nat-44** option is supported on MS-DPCs and MS-100, MS-400, and MS-500 MultiServices PICS. The **twice-dynamic-nat-44** option is supported on MS-MPCs and MS-MICs starting in Junos OS Release 15.1R1.
- **twice-napt-44**—This option implements source NAPT and destination static translation for IPv4 addresses, combining **napt-44** for source and **dnat-44** for destination addresses.

  The **twice-napt-44** option is supported on MS-DPCs and MS-100, MS-400, and MS-500 MultiServices PICS. The **twice-napt-44** option is supported on MS-MPCs and MS-MICs starting in Junos OS Release 15.1R1.

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

Configuring NAT Rules for IPsec Passthrough for Non-NAT-T Peers

Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers. Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, you can pass IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant. Only ESP tunnel mode is supported. This feature is supported only on MS-MPCs and MS-MICs.

To configure NAT rules for IPsec passthrough for NAPT-44 or NAT64:

1. Configure an IKE ALG application. See "Configuring Application Properties" on page 502.

2. Add the application to an application set. See "Configuring Application Sets" on page 501.

3. Configure a NAT pool. See "Configuring Pools of Addresses and Ports for Network Address Translation Overview" on page 103.

4. Configure the NAT rule:

   a. Configure a match direction for the rule. See "Configuring Match Direction for NAT Rules" on page 108.

   b. Configure one of the matching conditions to be the application set for IKE and IPsec passthrough that you configured in Step 2.

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

   c. Configure other match conditions. See "Configuring Match Conditions in NAT Rules" on page 108.

   d. Configure the translation type as NAPT-44 or NAT64.

      ```
      [edit services nat rule rule-name term term-name then translated]
      user@host# set translation-type (napt-44 | stateful-nat64)
      ```

   e. Configure other NAT actions. See "Configuring Actions in NAT Rules" on page 109.

5. Assign the NAT rule to a service set.

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

Release History Table

Release	Description
17.1R1	Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, you can pass IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant.

RELATED DOCUMENTATION

Junos Address Aware Network Addressing Overview | 78

Configuring Address Pools for Network Address Port Translation (NAPT) Overview

IN THIS SECTION

With Network Address Port Translation (NAPT), you can have up to 4096 network address or port translations.

The **port** statement specifies port assignment for the translated addresses. 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.

Junos OS for ACX Series routers allocates ports sequentially—that is, ACX Series routers allocate the first available address or port from the NAT pool.

The NAT pool called **napt** in the following configuration example uses the sequential implementation:

```
pool napt {
   address-range low 100.0.0.1 high 100.0.0.3;
   port {
      range low 49160 high 53255;
   }
}
```

Endpoint Independent Flow for NAPT

Endpoint independent flow ensures the assignment of the same external address *and* port for all connections from a given host or port to any destination. This means if the address or port are from a different source, you are free to assign a different external address.

RELATED DOCUMENTATION

- Network Address Translation Overview on ACX Series | 96
- Network Address Port Translation Overview | 98
- Enabling Inline Services Interface on ACX Series | 116

Enabling Inline Services Interface on ACX Series

The inline services interface is a virtual interface that resides on the Packet Forwarding Engine. The **si-** interface makes it possible to provide NAT and IPsec services without using a special services PIC.

To configure inline services interface, you define the service interface as type **si-** (service-inline) interface. You must also reserve adequate bandwidth for the inline services interface. This enables you to configure both interface or next-hop service sets used for NAT and IPsec services.

> **NOTE:** In ACX Series routers, you can configure only one inline services interface as an anchor interface for NAT and IPsec sessions: si-0/0/0.

> **NOTE:** In ACX Series routers, only ACX1100-AC and ACX500 routers support IPsec services. ACX Series routers support only basic NAT.

To enable inline services interface:

1. Access an FPC-managed slot and the PIC where the interface is to be enabled.

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

2. Enable the interface and specify the amount of bandwidth reserved on each Packet Forwarding Engine for tunnel traffic that uses inline services.

```
[edit chassis fpc slot-number pic number]
user@host# set inline-services bandwidth 1g
```

RELATED DOCUMENTATION

- Network Address Translation Overview on ACX Series | 96
- Network Address Port Translation Overview | 98
- IPsec for ACX Series Overview | 635
- *Understanding Service Sets*
- Service Filters in ACX Series | 14
- Guidelines for Applying Service Filters | 15
- Service Filter Match Conditions for IPv4 Traffic | 17
- Service Filter Actions | 18
- Network Address Translation Address Overload in ACX Series | 98
- *CoS for NAT Services on ACX Series Routers*
- Network Address Translation Constraints on ACX | 100
- Configuring Address Pools for Network Address Port Translation (NAPT) Overview | 115
- *Configuring Service Sets to Be Applied to Services Interfaces*
- Configuring Queuing and Scheduling on Inline Services Interface | 20

Configuring Service Sets for Network Address Translation

When configuring a service set for NAT processing, make sure you have defined:

- Service interface(s) for handling inbound and outbound traffic

NOTE: Prior to Junos OS Release 11.4R3, you could only use a source NAT pool in a single service set. As of Junos OS Release 11.4R3 and subsequent releases, you can reuse a source or destination NAT pool in multiple service sets, provided that the service interfaces associated with the service sets are in different virtual routing and forwarding (VRF) instances.

- For interface style service sets, when a NAT pool is reused in multiple service sets, the service interfaces used in the **interface-service service-interface** option of each service set must be in different VRFs.
- For next-hop style service sets, when a NAT pool is reused in multiple service sets, the service interfaces used in the **outside-interface** option of each service set must be in different VRFs.

  Not adhering to these service interface restrictions will cause multiple routes to be installed in the same VRF for the same NAT addresses, causing reverse traffic to be processed incorrectly.

To enable sharing of source NAT pools, include the **allow-overlapping-nat-pools** statement at the **[edit services nat]** hierarchy level.

- A NAT rule or ruleset

NOTE: To configure an MS-DPC interface to be used exclusively for carrier-grade NAT (CGN) or related services (intrusion detection, stateful firewall, and softwire), include the **cgn-pic** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level. This allows CGN to access all of the available memory on the MS-DPC.

To configure a NAT service set:

1. At the **[edit services]** hierarchy level, define the service set.

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

2. Configure either an interface service, which requires a single service interface, or a next-hop service, which requires an inside and outside service interface.

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

   Or

```
[edit services service-set service-set-name]
user@host# set next-hop-service inside-service-interface interface-name outside-service-interface
    interface-name
```

NOTE: On ACX series routers, or if you have a Trio-based line card (MPC/MIC), you can use an inline-services interface that was configured on that card, as shown in this example:

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

For more information on interface service and next-hop service, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.

3. Configure a reference to the NAT rules or ruleset to be used with the service set.

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

4. (Optional) For NAT64, specify that the don't fragment (DF) bit for IPv4 packet headers is cleared when packet length is less than 1280 bytes.

```
[edit services service-set service-set-name]
user@host# set nat-options stateful-nat64 clear-dont-fragment-bit
```

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

Carrier-Grade NAT Implementation: Best Practices

IN THIS SECTION

The following topics present the best practices for carrier-grade NAT implementation:

Use Round-Robin Address-Allocation When Using APP with the MS-DPC

BEST PRACTICE: If you are using an MS-DPC and you configure address-pooling paired (APP) in a NAT rule, you should use round-robin address allocation for the NAT pool.

The APP feature maps a private IP address to the same public IP address in a NAT pool for all the NAT sessions for that private IP address.

Sequential address allocation for NAT pools is the default on the MS-DPC, and allocates all the ports for a public IP address before assigning the next IP address. Sequential allocation, together with APP, might result in mapping multiple private hosts to the same public IP address, resulting in fast port exhaustion for a public IP address while other ports are still available from the remaining IP addresses in the NAT pool.

Round-robin allocation, on the other hand, assigns the next IP address in the NAT pool to the next private IP address needing translation, reducing the chance that all the ports for one public IP address are depleted.

For more information about APP and round-robin address allocation, see “Configuring Address Pools for Network Address Port Translation (NAPT) Overview” on page 170.

NOTE: The MS-MPC and MS-MIC only use round-robin allocation.

The following example shows round-robin address allocation.

```
[edit services]
nat pool natpool-1 {
    port {
        automatic;
    }
    address-allocation round-robin;
    mapping-timeout 120;
}
```

Use the EIM Feature Only When Needed

BEST PRACTICE: Do not use endpoint-independent mapping (EIM) in NAT rule terms that include Junos ALGs. EIM assigns the same external NAT address and port for a specific session from a private host, but adds processing overhead. EIM provides no benefit for any of the Junos ALGs, which already employ the functionality used by EIM.

BEST PRACTICE: Enable EIM for applications that do reuse the source ports and rely on a CGNAT device to maintain the same address and port mapping for all traffic sent to different destinations. For example, use EIM for console gaming applications such as Xbox and PS4 or applications that use unilateral self-address fixing methods (UNSAF). See (*IETF RFC 3424 IAB Considerations for Unilateral Self-Address Fixing (UNSAF) Across Network Address Translation*).

For more information about EIM, see "Configuring Address Pools for Network Address Port Translation (NAPT) Overview" on page 170.

The following example uses the Junos SIP ALG in the NAT rule, so EIM is *not* used.

```
[edit services nat]
rule natrule-1 {
    match-direction input;
    term1 {
        from {
```

```
            applications junos-sip;
        }
    }
        then {
            translated {
                source-pool natpool-3;
                translation-type {
                    napt-44;
                }
                address-pooling paired;
            }
        }
}
```

Define Port Block Allocation Block Sizes Based on Expected Number of User Sessions

BEST PRACTICE: For secure port block allocation and deterministic port block allocation, define a port block allocation block size that is 2 to 4 times larger than the expected average number of active sessions for a user. For example, if the user is expected to have an average of approximately 200 to 250 NAT sessions active, configuring the block size to 512 or 1024 provides a liberal allocation.

BEST PRACTICE: If you are rolling out secure port block allocation using the MX Series as a NAT device and are not sure of your subscriber user profile and traffic profile, set the port block size to 1024 if you have enough NAT IP addresses to handle the estimated peak number of private subscribers. The number of NAT IP addresses times 62 gives you the number of private subscribers that can be handled with a port block size of 1024 (there are 62 blocks per IP address). Then, closely monitor the MX Series router by using the **show services nat pool detail** command to determine whether the block size needs to be changed.

BEST PRACTICE: Be careful not to make the block size too large if the number of IP addresses you can allocate to the NAT pool is limited. Making a port block size that is large enough to efficiently assign the blocks to your subscribers might cause all the port blocks to be tied up.

Secure port block allocation allocates blocks of ports to a particular user for NAT44 or NAT64. Secure port block allocation limits the number of syslog messages by generating only one syslog per block of ports.

However, configuring the block size incorrectly can lead to inefficient use of NAT resources or to performance issues. For example, when a user connects to a website that requires the establishment of a significant number of sockets for a single HTML page, a corresponding number of new ports must be allocated. The port block size should be large enough to prevent continual allocation of new blocks. If the number of concurrent sessions for a private subscriber exceeds the number of ports available in the active port block, the other port blocks allocated to the subscriber are scanned for available ports to use or a new block is allocated from the free block pool for the subscriber. The scanning of allocated port blocks and allocation of additional blocks can result in delays in setting up new sessions and loading web pages.

For more information about port block allocation, see "Configuring Secured Port Block Allocation" on page 282 and "Configuring Deterministic NAPT" on page 202.

The following example sets the port block size to 1024.

```
[edit services nat]
pool natpool-1 {
    address-range low 192.0.2.0 high 192.0.2.10;
    port {
        automatic;
        secure-port-block-allocation {
            block-size 1024;
            max-blocks-per-user 8;
            active-block-timeout 300;
        }
    }
    mapping-timeout 300;
}
```

Considerations When Changing Port Block Allocation Configuration on Running Systems

BEST PRACTICE: Before changing the secure port block allocation or deterministic port block configuration on a running system when using an MS-MPC or MS-MIC, plan for a quick disruption in the NAT sessions. The change in configuration results in the re-creation of all the current NAT sessions.

BEST PRACTICE: Before changing the port block allocation configuration on a running system when using an MS-DPC, plan for a disruption of services. After changing the configuration, you must reboot the MS-DPC, or if this is not possible, you must deactivate and reactivate the service set.

Changes to port block allocation configuration include:

- Changing any NAT pool PBA configuration.
- Changing a PBA NAT pool to a non-PBA NAT pool.
- Changing a non-PBA NAT pool to a PBA NAT pool.

For more information about configuring port block allocation, see "Configuring Secured Port Block Allocation" on page 282 and "Configuring Deterministic NAPT" on page 202.

Do Not Allocate NAT Pools That Are Larger Than Needed

MS-MPC and MS-MIC

BEST PRACTICE: When using NAPT44 as your translation type with the MS-MIC or MS-MPC, do not configure NAT pools that are larger than needed for the peak session rate, which would tie up valuable IPv4 resources. Each conversation, also known as a session, includes two flows — an ingress and egress flow. Each conversation requires one port and each IP address in the pool has a 1024-65535 port range (64K), so the NAT pool size does not need to be larger than:

peak number of conversations /64K

BEST PRACTICE: When using NAPT44 as your translation type with the MS-MIC, we recommend a maximum NAT pool size of 128 addresses (a /25 network).

BEST PRACTICE: When using NAPT44 as your translation type with the MS-MPC, we recommend a maximum NAT pool size of 256 addresses (a /24 network).

The maximum recommended NAT pool size when using NAPT-44 for an MS-MIC is 128 IP addresses because the MS-MIC supports a maximum of 14 million flows, or 7 million conversations, which require 7 million ports. A total of 7 million ports are available with 128 IP addresses, with each IP address having a port range of 1024-65535.

The maximum recommended NAT pool size for each slot on an MS-MPC when using NAPT-44 is 256 IP addresses because each slot supports a maximum of 30 million flows, or 15 million conversations, which require 15 million ports. A total of 15 million ports are available with 256 IP addresses, with each IP address having a port range of 1024-65535.

You can use larger pools than the recommended values, and you can expect that configurations that use the port block allocation (PBA) feature require larger pools. This is because PBA assigns blocks of ports to private IP addresses, which changes the pool efficiency model.

For more information about configuring NAT pools, see "Configuring Pools of Addresses and Ports for Network Address Translation Overview" on page 103.

MS-DPC

BEST PRACTICE: When using NAPT44 as your translation type with the MS-DPC, do not configure NAT pools that are larger than needed for the peak flow rate, which would tie up valuable IPv4 resources. Each conversation includes two flows (1 reverse flow for each forward flow). Each conversation requires one port and each IP address in the pool has a 1024-65535 port range (64K), so the NAT pool size does not need to be larger than:

peak number of conversations /64K

BEST PRACTICE: When using NAPT44 as your translation type with the MS-DPC, do not configure NAT pools with more than 64 addresses (a /26 network).

The maximum NAT pool size for an MS-DPC is 64 IP addresses because the MS-DPC supports a maximum of 8 million flows, or 4 million conversations, which requires a maximum of 4 million ports. A total of 4 million ports are available with 64 IP addresses, with each IP address having a port range of 1024-65535. If APP, EIM, and EIF are enabled, the MS-DPC supports a maximum of 5.8 million flows, or 2.9 million conversations, so the maximum NAT pool size would be less.

For more information about configuring NAT pools, see "Configuring Pools of Addresses and Ports for Network Address Translation Overview" on page 103.

Configure System Logging for NAT Only When Needed

BEST PRACTICE: Do not enable system logging per session for secure port block allocation configurations.

BEST PRACTICE: Do not enable system logging for deterministic NAT configurations.

BEST PRACTICE: Enable system logging at the service-set level rather than at the services interface level when possible.

BEST PRACTICE: In production networks, always send the log messages to an external system log server. This avoids adding CPU load to the Routing Engine, which occurs when messages are logged locally.

BEST PRACTICE: Specify the system log class to restrict logging to the class of applications in which you are interested.

BEST PRACTICE: If you configure system logging within a NAT rule term, use a stateful firewall rule to restrict the traffic that reaches the NAT rule term.

System log messages can negatively affect the performance of the services card, depending on the frequency of creation and deletion of sessions. All system log messages created by the services card require CPU processing at the services card, and the system log messages themselves constitute traffic that is sent across the MX Series router and competes with user traffic to reach the external log server.

Secure port block allocation removes the need to configure logs per session, because you know the block and block size and can derive the ports allocated to each user.

Deterministic NAT removes the need to log at all, because all information on port allocation can be deduced mathematically.

The following example restricts logging to NAT events and sends log messages to the external log server 203.0.113.4

```
[edit services service-set S-SET-1]
class {
    nat-logs;
}
```

```
syslog {
    host 203.0.113.4;
}
```

When you configure system logging within a NAT rule term, all traffic that enters the NAT rule term generates a log, which can cause excessive logging. This might result in the logging rate limit being reached, and you would lose logs that you do need.

For more information about configuring system logging for NAT, see "Configuring NAT Session Logs" on page 361.

Limit the Impact of Missing IP Fragments

BEST PRACTICE: For the services interface that is configured for NAT, limit the impact of missing or delayed fragments by configuring the following:

- Maximum number of fragments for a packet
- Maximum wait time for a missing fragment

IP fragments received by the services card configured for NAT are buffered as they arrive. This allows an integrity check of the completely reassembled packet before the packet is processed by NAT. Missing or delayed fragments can cause the already received fragments to be held until the internal buffer is full and they are flushed out, resulting in CPU usage overhead and reduced traffic forwarding.

Configuring the maximum number of fragments a packet can have and limiting the wait time for a missing fragment reduces the chance of the internal buffer becoming full.

The following example sets the maximum number of fragments to 10 and the maximum wait time to 3 seconds.

```
[edit interfaces ms-0/0/0]
services-options {
    fragment-limit 10;
    reassembly-timeout 3;
}
```

Do Not Use Configurations Prone to Packet Routing Loops

BEST PRACTICE: Prevent packet routing loops by ensuring that only the intended traffic is allowed to reach the services card and be processed by the service set NAT rule. You can do this by:

- Configuring a source-address range under the NAT rule when possible.
- Configuring a firewall filter that accepts only the traffic meant to be serviced by the NAT rule in a next-hop style service set.

Packet looping between the Packet Forwarding Engine and the services card results in persistent high CPU usage on the services card. Packet looping can be caused by the services card receiving traffic from an unexpected private source network. When unexpected traffic is processed by NAT, a pinhole is created, and in the case of EIF many pinholes might be created. These pinholes cause routing loops if the return traffic routes back through the services card.

The following example shows a firewall filter that only allows traffic from 198.51.100.0/24 to reach services interface ms-1/0/0, which is the inside interface for a next-hop service set.

```
[edit firewall filter to_be_serviced]
term 1 {
   from }
      address {
      }
      198.51.100.0/24;
   }
   then accept;
}
term 2 {
   then disard;
   }
[edit interfaces ms-1/0/0]
   unit 1 {
      family intet {
         filter {
            output to_be_serviced;
         }
      }
      service-domain inside;
   }
```

For more information about configuring firewall filters, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The following example shows a NAT rule that only processes traffic from 198.51.100.0/24 (other traffic reaches the services interface, but is not processed).

```
[edit services nat]
rule rule_1 {
    match-direction input;
    term t1 {
        from {
            source-address {
                198.51.100.0/24;
            }
        }
        then {
            translated {
                source-pool pool1;
                translation-type {
                    napt-44;
                }
            }
        }
    }
}
```

For more information about configuring NAT rules, see "Network Address Translation Rules Overview" on page 106.

Inactivity Timeouts

BEST PRACTICE: Set the inactivity timeout only for user-defined applications that could require the NAT session mapping to remain in memory for longer than the default NAT inactivity timeout of 30 seconds. For example, an HTTP or HTTPS banking application may require more than 30 seconds of inactivity because the user must enter data.

BEST PRACTICE: Before making changes to the existing inactivity timeouts, run the following commands several times during peak hours. Then run the commands after making the changes, and verify that the changes are not starving the MX Series router of NAT resources or the services card of memory.

- **show services sessions** count
- **show services nat pool** detail
- **show services service-sets summary**

The following example shows the inactivity timeout being set to 1800 seconds for HTTPS and HTTP applications.

```
[edit applications]
application https {
    inactivity-timeout 1800;
    destination-port 443;
    protocol tcp;
}
application http {
    inactivity-timeout 1800;
    destination-port 443;
    protocol tcp;
}
```

For more information about configuring user-defined applications, see "Configuring Application Properties" on page 502.

You need to weigh the risks of setting high inactivity timeouts for all traffic. While the default NAT inactivity timeout of 30 seconds may be too low for some user-defined applications, setting a timeout value too high can tie up NAT resources. For example, setting high inactivity timeout values can tie up any TCP session that is inactive just minutes after it was created. If the TCP session is not cleanly closed by a FIN or RST by the client or server, the session will sit in memory and tie up the NAT resources assigned to it until the timeout value expires.

Setting higher inactivity timeouts that impact every UDP and TCP port can be dangerous, especially with UDP traffic like DNS. Unlike TCP, UDP has no way to end a session other than timing out, so all UDP sessions would stay active for the full inactivity timeout value.

The following example is *not* a recommended configuration because it sets high inactivity timeout values for all TCP and UDP traffic.

```
[edit applications]
application UDP-All {
    protocol UDP;
    source-port 1-65535;
    inactivity-timeout 3600;
}
application TCP-All {
    protocol TCP;
    source-port 1-65535;
    inactivity-timeout 3600;
}
```

We do not have specific recommended inactivity timeout values. The proper inactivity timeout values depend on several factors, including:

- What applications are used on an end user's network

  For example, Apple has stated that an inactivity timeout of 60 minutes is required for the following Apple services, which require a long connection lifetime:

  - Apple Push Services: inbound TCP port 5223
  - Exchange Active Sync: inbound TCP port 443
  - MobileMe: inbound TCP ports 5222 and 5223
- How the NAT solution is being used, for example as a Gi NAT device or as an Enterprise edge router
- How large your NAT pools are
- How much traffic each services card receives during peak loads
- How much memory you have available

Enable Dump on Flow Control

BEST PRACTICE: Enable the dump-on-flow-control option for any services card that is processing NAT traffic in a production network. This option detects when a services card is locked up, writes a core dump that Juniper Networks can analyze to determine why the card locked up, and recovers the services card by restarting it.

For the MS-MIC and MS-MPC, set the dump-on-flow-control option under the pc- interface, which is used to send control traffic from the Routing Engine to the services card. The following example shows the configuration if the services interface is ms-2/1/0.

```
[edit interfaces pc-2/1/0]
multiservice-options {
    flow-control-options {
        dump-on-flow-control;
    }
}
```

For the MS-DPC, set the dump-on-flow control option under the sp- interface. The following example shows the configuration if the services interface is sp-2/1/0.

```
[edit interfaces sp-2/1/0]
multiservice-options {
    flow-control-options {
        dump-on-flow-control;
    }
}
```

RELATED DOCUMENTATION

Network Address Translation Configuration Overview | **101**

CHAPTER 6

Avoiding IPv4 Exhaustion Using Junos Address Aware Network Addressing and Stateful NAT64

IN THIS CHAPTER

Sample IPv6 Transition Scenarios

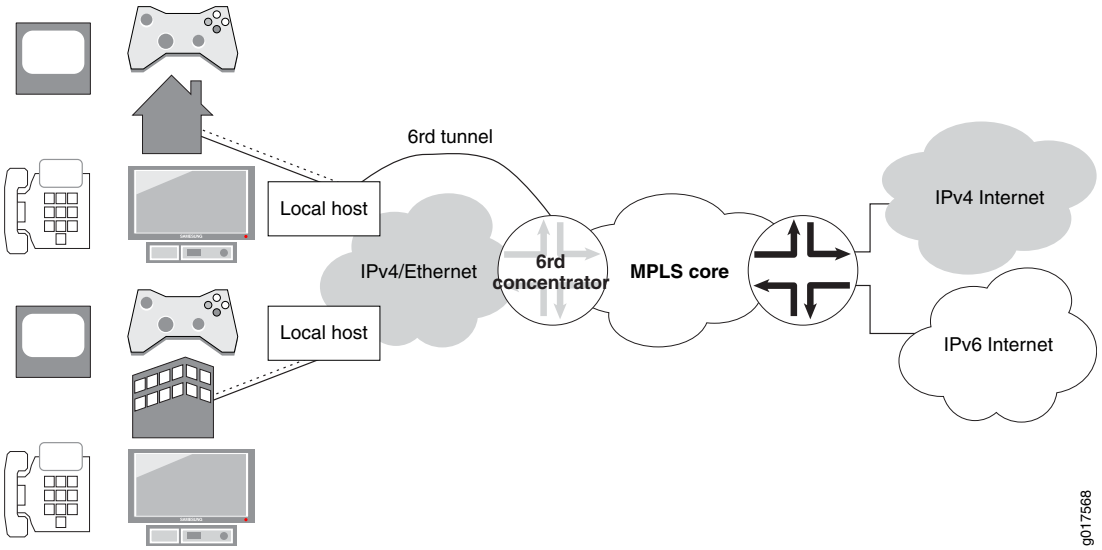
IN THIS SECTION

The Junos OS supports many IPv6 transition scenarios required by Junos OS customers. The following are selected examples:

Example 1: IPv4 Depletion with a Non-IPv6 Access Network

Figure 10 on page 134 depicts a scenario in which the Internet service provider (ISP) has not significantly changed its IPv4 network. This approach enables IPv4 hosts to access the IPv4 Internet and IPv6 hosts to access the IPv6 Internet. A dual-stack host can be treated as an IPv4 host when it uses the IPv4 access service, and as an IPv6 host when it uses the IPv6 access service.

Figure 10: IPv4 Depletion Solution - IPv4 Access Network

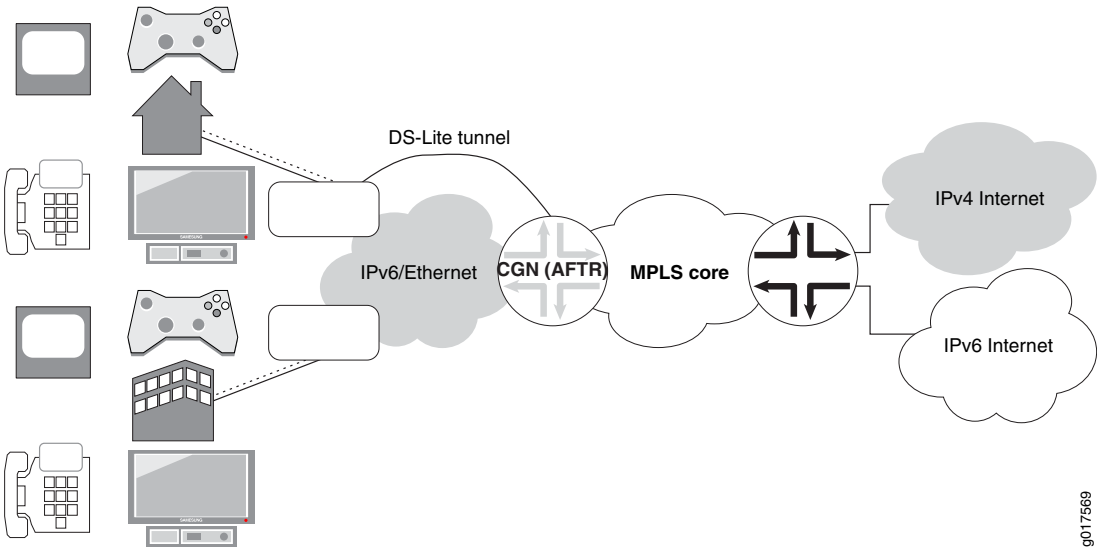


Two new types of devices must be deployed in this approach: a dual-stack home gateway and a dual-stack carrier-grade Network Address Translation (NAT). The dual-stack home gateway integrates IPv4 forwarding and v6-over-v4 tunneling functions. It can also integrate a v4-v4 NAT function. The dual-stack carrier-grade NAT (CGN) integrates v6-over-v4 tunneling and carrier-grade v4-v4 NAT functions.

Example 2: IPv4 Depletion with an IPv6 Access Network

In the scenario shown in Figure 11 on page 134, the ISP network is IPv6-only.

Figure 11: IPv4 Depletion Solution - IPv6 Access Network



The dual-stack lite (DS-Lite) solution accommodates IPv6-only ISPs. The best business model for this approach is that the customer premises equipment (CPE) has integrated the functions for tunneling IPv6 to an IPv4 backbone, tunneling IPv4 to an IPv6 backbone, and can automatically detect which solution is required.

Not all customers of a given ISP must switch from IPv4 access to IPv6 access simultaneously; in fact, transition can be managed better by switching groups of customers (for example, all those connected to a single point of presence) on an incremental basis. Such an incremental approach should prove easier to plan, schedule, and execute than an across-the-board conversion.

Example 3: IPv4 Depletion for Mobile Networks

The complexity of mobile networks necessitates a flexible migration approach to ensure minimal disruption and maximum backward compatibility during transition. NAT64 can be used to enable IPv6 devices to communicate to IPv4 hosts without modifying the clients.

Configuring Stateful NAT64

To configure stateful NAT64, you must configure a rule at the **[edit services nat]** hierarchy level for translating the source address dynamically and the destination address statically.

> **BEST PRACTICE:** When you configure the service set that includes your NAT rule, include the **set stateful-nat64 clear-dont-fragment-bit** at the **[edit services service-set *service-set-name*]** hierarchy level.This clears the DF (don't fragment) bit in order to prevent unnecessary creation of an IPv6 fragmentation header when translating IPv4 packets that are less than 1280 bytes. RFC 6145, *IP/ICMP Translation Algorithm*, provides a full discussion of the use of the DF flag to control generation of fragmentation headers. For more information on service sets for NAT, see "Configuring Service Sets for Network Address Translation" on page 117.

To configure stateful NAT64:

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

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

2. Define the pool of source addresses to be used for dynamic translation.

```
[edit services nat]
user@host# set pool pool name address source addresses
user@host# set pool pool name port source ports
```

For example:

```
[edit services nat]
user@host#  set pool src-pool-nat64 address 203.0.113.0/24
user@host#  set pool src-pool-nat64 port automatic
```

NOTE: Starting in Junos OS release 14.2, the **sequential** option is introduced to enable you to configure sequential allocation of ports. The **sequential** and **random-allocation** options available with the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level are mutually exclusive. You can include the **sequential** option for sequential allocation and the **random-allocation** option for random delegation of ports. By default, sequential allocation of ports takes place if you include only the **port automatic** statement at the **[edit services nat pool *nat-pool- name*]** hierarchy level. The **auto** option is hidden and is deprecated in Junos OS Release 14.2 and later, and is only maintained for backward compatibility. It might be removed completely in a future software release.

3. Define a NAT rule for translating the source addresses. Set the **match-direction** statement of the rule as **input**. Then define a term that uses **stateful-nat64** as the translation type for translating the addresses of the pool defined in the previous step.

```
[edit services nat]
user@host# set rule rule name match-direction input
user@host# set rule rule name term term name from source-address source address
user@host# set rule rule name term term name from destination-address destination address
user@host# set rule rule name term term name then translated source-pool pool name
user@host# set rule rule name term term name then translated destination-prefix destination prefix
user@host# set rule rule name term term name then translated translation-type stateful-nat64
```

For example:

```
[edit services nat]
user@host# set rule stateful-nat64 match-direction input
user@host# set rule stateful-nat64 term t1 from source-address 2001:DB8::0/96
user@host# set rule stateful-nat64 term t1 from destination-address 64:FF9B::/96
user@host# set rule stateful-nat64 term t1 then translated source-pool src-pool-nat64
user@host# set rule stateful-nat64 term t1 then translated destination-prefix 64:FF9B::/96
```

```
user@host# set rule stateful-nat64 term t1 then translated translation-type stateful-nat64
```

The following example configures dynamic source address (IPv6-to-IPv4) and static destination address (IPv6-to-IPv4) translation.

```
[edit services]
user@host# show
nat {
    pool src-pool-nat64 {
        address 203.0.113.0/24;
        port {
            automatic;
        }
    }
    rule stateful-nat64 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    2001:db8::0/96;
                }
                destination-address {
                    64:ff9b::/96;
                }
            }
            then {
                translated {
                    source-pool src-pool-nat64;
                    destination-prefix 64:ff9b::/96;
                    translation-type {
                        stateful-nat64;
                    }
                }
            }
        }
    }
}
service-set sset-nat64 {
    nat-options {
        stateful-nat64 {
            clear-dont-fragment-bit;
        }
    }
```

```
    service-set-options;
    nat-rules stateful-nat64;
    interface-service {
        service-interface ms-0/1/0;
    }
}
```

NOTE: If you configure two NAT64 rules and associate them with the same service set, along with stateful firewall rules, and apply the service set on two VLAN-tagged interfaces, for traffic that is transmitted matching both the NAT rules, the traffic that is destined to the second NAT rule is dropped. In such a scenario, traffic flows are not dropped on the Routing Engine. This behavior of traffic drop by the second NAT rule is expected. With Junos OS Extension-Provider packages installed on a device, because endpoint-independent mapping (EIM) is not supported, EIM per VLAN or per NAT rule term. The second session, which is dropped by the second NAT rule in the configuration scenario described here, is not created owing to the following sequence of events:

1. The first packet matching either rule creates an EIM and a session.
2. The second packet matches the EIM entry because the second packet is sent with the same source IP address and port as the first packet (but with a different destination address).

This condition causes allocation (reuse) of the same public IP address and port to the second packet as the first packet. The reverse flow for this session has the same 5-tuple data as the reverse flow of the first session. This behavior causes flow addition failure because a duplicate flow in the same service set is not permitted.

To work around this problem, disable EIM in both the NAT rules, which causes both the sessions to be established and processed correctly. Alternatively, to avoid this problem, specify the NAT rules on different service-sets configured on different units of the media interface with EIM enabled to successfully establish both the sessions.

Release History Table

Release	Description
14.2	Starting in Junos OS release 14.2, the **sequential** option is introduced to enable you to configure sequential allocation of ports.

CHAPTER 7

Hiding Private Networks Using Static Source NAT

IN THIS CHAPTER

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:

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 source-address address
```

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 nat]** 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;
                    }
                }
            }
        }
    }
}
```

NOTE: If you don't configure a stateful firewall (SFW) rule for your traffic, then each packet is subjected to the following default stateful firewall rule:

- Allow any valid packets from inside to outside.
- Create forward and return flow based on packets 5-tuple.
- Allow only valid packets matching return flows from outside to inside.

The stateful firewall's packet validity checks are described in the *Stateful Firewall Anomaly Checking* in "Junos Network Secure Overview" on page 542. When a packets pass stateful firewall validity checking but are not matched by a NAT rule, they are not translated and may be forwarded if the NAT node has a valid route to the packets' destination IP addresses.

NOTE: When you add or delete a parameter in the **from** statement (NAT rule term match condition) at the **[edit services service-set service-set-name nat-rules *rule-name* term *term-name*]** hierarchy level, this configuration change triggers a deletion and addition of the NAT policy (which is equivalent to the deactivation and activation of a service set) that causes all existing NAT mappings to be deleted. Because the sessions are not closed owing to the change in the NAT policy, this behavior causes the mappings to timeout immediately after the sessions are closed. This behavior is expected and is applicable only with Junos OS Extension-Provider packages installed on a device. When a NAT policy is deleted and readded, only EIM mappings are deleted. This NAT policy change does not deactivate and activate the service set. We recommend that you deactivate and reactivate the service set in such scenarios in Junos OS Release 14.2 and earlier.

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
```

NOTE: If you have a Trio-based line card, you can configure an inline-services interface on that card:

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

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;
    }
}
```

6. Associate the NAT service set with an **xe-** interface:

```
user@host# set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
user@host# set interfaces xe-1/1/0 unit 0 family inet service input service-set s1
user@host# set interfaces xe-1/1/0 unit 0 family inet service output service-set s1
```

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

```
[edit interfaces]
user@host# show
xe-1/1/0 {
    unit 0 {
        family inet {
            service {
                input {
                    service-set s1;
                }
                output {
                    service-set s1;
                }
             }
            address 10.255.247.2/24;
        }
    }
}
```

Configuring Trace Options

To configure the trace options:

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;
    }                                   }
```

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

Sample Configuration - Static Source NAT Using a Static Pool With An Address Prefix And An Address Range

```
[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 t1 {
      from {
         source-address {
            10.10.10.252/30;
         }
      }
      then {
         translated {
            source-pool p1;
            translation-type basic-nat44;
         }
```

```
     }
   }
 }
```

Sample Configuration - Static Source Nat for One-To-One Mapping Between a Private Subnet and a Public Subnet

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

```
    }
}
```

```
[edit interfaces]
user@host# show
xe-1/1/0 {
    unit 0 {
        family inet {
            service {
                input {
                    service-set s1;
                }
                output {
                    service-set s1;
                }
             }
            address 10.255.247.2/24;
        }
    }
}
```

Release History Table

Release	Description
14.2	We recommend that you deactivate and reactivate the service set in such scenarios in Junos OS Release 14.2 and earlier.

Configuring Static Source Translation in IPv6 Networks

To configure the translation type as **basic-nat66**, you must configure the NAT pool and rule, service set with service interface, and trace options. The **basic-nat66** translation type is not available if you are using MS-MPCs or MS-MICs.

This topic includes the following tasks:

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 rule name is **rule-basic-nat66** and the match direction is **input**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 match-direction input
```

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

```
[edit services nat]
user@host# set rule rule-basic-nat66 term term-name from from source-address address
```

In the following, the term name is **t1** and the input condition is **source-address 2001:db8:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 from source-address 2001:db8:10::0/96
```

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

```
[edit services nat]
user@host# set rule rule-basic-nat66 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-nat66 term t1 then translated source-pool src_pool
```

6. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then translated translation-type translation-type
```

In the following example, the translation type is **basic-nat66**.

```
[edit services nat]
user@host# set rule rule-basic-nat66 term t1 then translated translation-type basic-nat66
```

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-nat66 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    2001:db8:10::0/96;
                }
            }
            then {
                translated {
                    source-pool src_pool;
                    translation-type {
                        basic-nat66;
                    }
```

```
                }
            }
        }
    }
}
```

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-nat66**.

   ```
   [edit services service-set s1]
   user@host# set nat-rules rule-basic-nat66
   ```

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 **sp-1/2/0**.

```
[edit services service-set s1]
user@host# set interface-service service-interface sp-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-nat66;
    interface-service {
        service-interface sp-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;
    }
}
```

The following example configures the translation type as **basic-nat66**.

```
[edit]
user@host# show services
service-set s1 {
    nat-rules rule-basic-nat66;
    interface-service {
        service-interface sp-1/2/0;
    }
}
nat {
    pool src_pool {
        address 10.10.10.2/32;
    }
    rule rule-basic-nat66 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    2001:db8:10::0/96/96;
                }
            }
            then {
                translated {
                    source-pool src_pool;
                    translation-type {
                        basic-nat66;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
```

```
    traceoptions {
        flag all;
    }
}
```

Example: Configuring Basic NAT44

IN THIS SECTION

This example describes how to implement a basic NAT44 configuration.

Requirements

This example uses the following hardware and software components:

- An MX Series 5G Universal Routing Platform with a Services DPC or an M Series Multiservice Edge router with a services PIC
- A domain name server (DNS)
- Junos OS Release 11.4 or higher

Overview

This example shows a complete CGN NAT44 configuration and advanced options.

Configuring Basic NAT44

Chassis Configuration

Step-by-Step Procedure

To configure the service PIC (FPC 5 Slot 0) with the Layer 3 service package:

1. Go to the **[edit chassis]** hierarchy level.

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

2. Configure the Layer 3 service package.

```
[edit chassis]
user@host# set fpc 5 pic 0 adaptive-services service-package layer-3
```

Interfaces Configuration

Step-by-Step Procedure

To configure interfaces to the private network and the public Internet:

1. Define the interface to the private network.

```
user@host# edit interfaces ge-1/3/5
[edit interfaces ge-1/3/5]
user@host# set description “Private”
user@host# edit unit 0 family inet
[edit interfaces ge-1/3/5 unit 0 family inet]
user@host# set service input service-set ss2
user@host# set service output service-set ss2
user@host# set address 9.0.0.1/24
```

2. Define the interface to the public Internet.

```
user@host# edit interfaces ge-1/3/6
[edit interfaces ge-1/3/6]
user@host# set description “Public”
user@host# set unit 0 family inet address 128.0.0.1/24
```

3. Define the service interface for NAT processing.

```
user@host# edit interfaces sp-5/0/0
[edit interfaces sp-5/0/0]
user@host# set unit 0 family inet
```

Results

user@host# show interfaces ge-1/3/5

```
description Private;
unit 0 {
    family inet {
        service {
            input {
                 service-set sset2;
            }
            output {
                service-set sset2;
            }
        }
        address 9.0.0.1/24;
    }
}
}
```

user@host# show interfaces ge-1/3/6

```
description Public:;
unit 0 {
    family inet {
        address 128.0.0.1/24;
    }
}
```

user@host# show interfaces sp-5/0/0

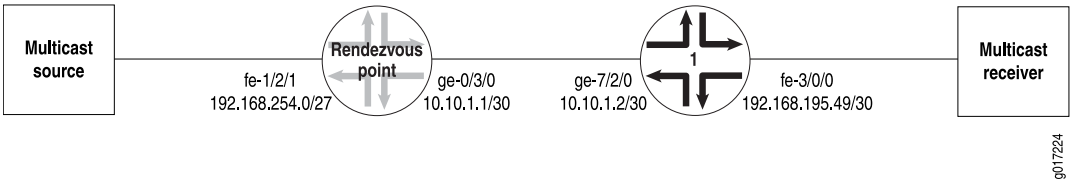
```
unit 0 {
family inet;
}
```

Example: Configuring NAT for Multicast Traffic

IN THIS SECTION

Figure 12 on page 157 illustrates the network setup for the following configuration, which allows IP multicast traffic to be sent to the Multiservices PIC.

Figure 12: Configuring NAT for Multicast Traffic



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 Multiservices DPC or Multiservices PIC. The inside interface on the PIC is **ms-1/1/0.1** and the outside interface is **ms-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 basic-nat44;
        }
        syslog;
    }
  }
}
service-set nat_ss {
  allow-multicast;
  nat-rules nat_rule_1;
  next-hop-service {
    inside-service-interface ms-1/1/0.1;
    outside-service-interface ms-1/1/0.2;
  }
}
```

The Gigabit Ethernet interface **ge-0/3/0** carries traffic out of the RP to Router 1. The multiservices interface **ms-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;
    }
  }
}
ms-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 Multiservices DPC or the Multiservices PIC using a next-hop service set. In the case of NAT, you must also configure a VPN routing and forwarding instance (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 **ms-1/1/0.1** on the Multiservices DPC or Multiservices PIC:

```
[edit]
routing-instances stage {
    instance-type forwarding;
    routing-options {
        static {
            route 224.0.0.0/4 next-hop ms-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 (**ms-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 ms-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;
}
```

CHAPTER 8

Making Private Servers Available Using Static Destination NAT

IN THIS CHAPTER

Configuring Static Destination Address Translation in IPv4 Networks

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 editservices 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;
    }
  }
```

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;
    }
  }
```

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 napt-44; # dynamic NAT with port translation
            }
        }
    }
    }
    rule my-nat-rule2 {
    match-direction input;
    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 dnat-44; # static destination NAT
            }
        }
    }
}
}
```

The following configuration performs NAT 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 dnat44;
                destination-prefix 20.20.10.0/24;
            }
        }
    }
}
```

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101

CHAPTER 9

Allowing Components of a Private Network to Share a Single Address Using NAPT

IN THIS CHAPTER

Configuring Address Pools for Network Address Port Translation (NAPT) Overview

IN THIS SECTION

With Network Address Port Translation (NAPT), you can configure up to 32 address ranges with up to 65,536 addresses each.

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. By default, sequential allocation of ports occurs.

Starting with Junos OS Release 14.2, you can include the **sequential** option with the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level for sequenced allocation of ports from the specified range. 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.

> **NOTE:** When 99% of the total available ports in pool for napt-44 , no new flows are allowed on that NAT pool.
>
> Starting with Junos OS Release 14.2, the **auto** option is hidden and is deprecated, and is only maintained for backward compatibility. It might be removed completely in a future software release.

The Junos OS provides several alternatives for allocating ports:

Round-Robin Allocation for NAPT

To configure round-robin allocation for NAT pools, include the **address-allocation round-robin** configuration statement at the **[edit services nat pool *pool-name*]** hierarchy level. 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.

- The first connection is allocated to the address:port 100.0.0.1:3333.
- The second connection is allocated to the address:port 100.0.0.2:3333.
- The third connection is allocated to the address:port 100.0.0.3:3333.
- The fourth connection is allocated to the address:port 100.0.0.4:3333.
- The fifth connection is allocated to the address:port 100.0.0.5:3333.
- The sixth connection is allocated to the address:port 100.0.0.6:3333.
- The seventh connection is allocated to the address:port 100.0.0.7:3333.
- The eighth connection is allocated to the address:port 100.0.0.8:3333.
- The ninth connection is allocated to the address:port 100.0.0.9:3333.
- The tenth connection is allocated to the address:port 100.0.0.10:3333.
- The eleventh connection is allocated to the address:port 100.0.0.11:3333.

- The twelfth connection is allocated to the address:port 100.0.0.12:3333.
- Wraparound occurs and the thirteenth connection is allocated to the address:port 100.0.0.1:3334.

Sequential Allocation for NAPT

With sequential allocation, the next available address in the NAT pool is selected only when all the ports available from an address are exhausted.

Sequential Allocation can be configured only for the MS-DPC and the MS-100, MS-400, and MS-500 MultiServices PICS. The MS-MPC and MS-MIC cards use only the round-robin allocation approach.

> **NOTE:**
> - This legacy implementation provides backward compatibility and is no longer a recommended approach.

The NAT pool called **napt** in the following configuration example uses the sequential implementation:

```
pool napt {
    address-range low 100.0.0.1 high 100.0.0.3;
    address-range low 100.0.0.4 high 100.0.0.6;
    address-range low 100.0.0.8 high 100.0.0.10;
    address-range low 100.0.0.12 high 100.0.0.13;
    port {
        range low 3333 high 3334;
    }
}
```

In this example, the ports are allocated starting from the first address in the first address-range, and allocation continues from this address until all available ports have been used. When all available ports have been used, the next address (in the same address-range or in the following address-range) is allocated and all its ports are selected as needed. In the case of the example **napt** pool, the tuple address, port 100.0.0.4:3333, is allocated only when all ports for all the addresses in the first range have been used.

- The first connection is allocated to the address:port 100.0.0.1:3333.
- The second connection is allocated to the address:port 100.0.0.1:3334.
- The third connection is allocated to the address:port 100.0.0.2:3333.
- The fourth connection is allocated to the address:port 100.0.0.2:3334, and so on.

Preserve Parity and Preserve Range for NAPT

Preserve parity and preserve range options are available for NAPT, and are supported on MS-DPCs and MS-100, MS-400, and MS-500 MultiServices PICS. Support for MS-MPCs and MS-MICs starts in Junos OS Release 15.1R1. The following options are available for NAPT:

- Preserving parity—Use the **preserve-parity** command to allocate even ports for packets with even source ports and odd ports for packets with odd source ports.
- Preserving range—Use the **preserve-range** command to allocate ports within a range from 0 to 1023, assuming the original packet contains a source port in the reserved range. This applies to control sessions, not data sessions.

Address Pooling and Endpoint Independent Mapping for NAPT

IN THIS SECTION

Address Pooling

Address pooling, or address pooling paired (APP) ensures assignment of the same external IP address for all sessions originating from the same internal host. You can use this feature when assigning external IP addresses from a pool. This option does not affect port utilization

Address pooling solves the problems of an application opening multiple connections. For example, when Session Initiation Protocol (SIP) client sends Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) packets, the SIP generally server requires that they come from the same IP address, even if they have been subject to NAT. If RTP and RTCP IP addresses are different, the receiving endpoint might drop packets. Any point-to-point (P2P) protocol that negotiates ports (assuming address stability) benefits from address pooling paired.

The following are use cases for address pooling:

- A site that offers instant messaging services requires that chat and their control sessions come from the same public source address. When the user signs on to chat, a control session authenticates the user. A different session begins when the user starts a chat session. If the chat session originates from a source address that is different from the authentication session, the instant messaging server rejects the chat session, because it originates from an unauthorized address.

- Certain websites such as online banking sites require that all connections from a given host come from the same IP address.

> **NOTE:** Starting with Junos OS Release 14.1, when you deactivate a service-set that contains address pooling paired (APP) for that service-set, messages are displayed on the PIC console and the mappings are cleared for that service-set. These messages are triggered when the deletion of a service-set commences and again generated when the deletion of the service-set is completed. The following sample messages are displayed when deletion starts and ends:
>
> - Nov 15 08:33:13.974 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion initiated
> - Nov 15 08:33:14.674 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion completed
>
> In a scaled environment that contains a large number of APP in a service set, a heavy volume of messages is generated and this process takes some amount of time. We recommend that you wait until the console messages indicating the completion of deletion of the service set are completed before you reactivate the service-set again.

Endpoint Independent Mapping and Endpoint Independent Filtering

Endpoint independent mapping (EIM) ensures the assignment of the same external address *and* port for all connections from a given host if they use the same internal port. This means if they come from a different source port, you are free to assign a different external address.

EIM and APP differ as follows:

- APP ensures assigning the same external IP address.
- EIM provides a stable external IP address and port (for a period of time) to which external hosts can connect. Endpoint independent filtering (EIF) controls which external hosts can connect to an internal host.

NOTE: Starting with Junos OS Release 14.1, when you deactivate a service-set that contains endpoint independent mapping (EIM) mapping for that service-set, messages are displayed on the PIC console and the mappings are cleared for that service-set. These messages are triggered when the deletion of a service-set commences and again generated when the deletion of the service-set is completed. The following sample messages are displayed when deletion starts and ends:

- Nov 15 08:33:13.974 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion initiated
- Nov 15 08:33:14.674 LOG: Critical] SVC-SET ss1 (iid 5) deactivate/delete: NAT Mappings and flows deletion completed

In a scaled environment that contains a large number of EIM mappings in a service set, a heavy volume of messages is generated and this process takes some amount of time. We recommend that you wait until the console messages indicating the completion of deletion of the service set are completed before you reactivate the service-set again.

Secured Port Block Allocation for NAPT

IN THIS SECTION

Port block allocation is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Port block allocation is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 14.2R2.

Carriers track subscribers using the IP address (RADIUS or DHCP) log. If they use NAPT, an IP address is shared by multiple subscribers, and the carrier must track the IP address and port, which are part of the NAT log. Because ports are used and reused at a very high rate, tracking subscribers using the log becomes difficult due to the large number of messages, which are difficult to archive and correlate. By enabling the allocation of ports in blocks, port block allocation can significantly reduce the number of logs, making it easier to track subscribers.

Secured Port Block Allocation for NAPT

Secured port block allocation can be used for translation types **napt-44** and **stateful-nat64**.

When allocating blocks of ports, the most recently allocated block is the current active block. New requests for NAT ports are served from the active block. Ports are allocated randomly from the current active block.

When you configure secured port block allocation, you can specify the following:

- **block-size**
- **max-blocks-per-address**
- **active-block-timeout**

Interim Logging for Port Block Allocation

With port block allocation we generate one syslog log per set of ports allocated for a subscriber. These logs are UDP based and can be lost in the network, particularly for long-running flows. Interim logging triggers re-sending the above logs at a configured interval for active blocks that have traffic on at least one of the ports of the block.

Interim logging is activated by including the **pba-interim-logging-interval** statement under **services-options** for sp- interfaces.

SEE ALSO

Configuring Secured Port Block Allocation | 282

Configuring NAT Session Logs | 361

Secured Port Block Allocation for NAPT44 and NAT64 Overview | 275

Comparison of NAPT Implementation Methods

Table 11 on page 176 provides a feature comparison of available NAPT implementation methods.

Table 11: Comparison of NAPT Implementation Methods

Feature/Function	Dynamic Port Allocation	Secured Port Block Allocation	Deterministic Port Block Allocation
Users per IP	High	Medium	Low
Security Risk	Low	Medium	Medium
Log Utilization	High	Low	None (no logs necessary)
Security Risk Reduction	Random allocation	**active-block-timeout** feature	n/a

Table 11: Comparison of NAPT Implementation Methods *(continued)*

Feature/Function	Dynamic Port Allocation	Secured Port Block Allocation	Deterministic Port Block Allocation
Increasing Users per IP	n/a	Configure multiples of smaller port blocks to maximize users/ public IP	Algorithm-based port allocation

Configuring NAPT in IPv4 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP 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 must 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 **sequential** or **auto**.

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

> **NOTE:** Starting in Junos OS Release 14.2, the **sequential** option is introduced to enable you to configure sequential allocation of ports. The **sequential** and **random-allocation** options available with the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level are mutually exclusive. You can include the **sequential** option for sequential allocation and the **random-allocation** option for random delegation of ports. By default, sequential allocation of ports takes place if you include only the **port automatic** statement at the **[edit services nat pool *nat-pool- name*]** hierarchy level. The **auto** option is hidden and is deprecated in Junos OS Release 14.2 and later, and is only maintained for backward compatibility. It might be removed completely in a future software release.

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 napt-44
```

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;
    }
}
```

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 auto;
        }
    }
    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;
    }
}
```

Dynamic Address Translation to a Small Pool with Fallback to NAT

The following configuration shows dynamic address translation from a large prefix to a small pool, translating a **/24** subnet to a pool of 10 addresses. When the addresses in the source pool (**src-pool**) are exhausted, NAT is provided by the NAPT overload pool (**pat-pool)**.

```
[edit services nat]
pool src-pool {
   address-range low 192.16.2.1 high 192.16.2.10;
}
pool pat-pool {
   address-range low 192.16.2.11 high 192.16.2.12;
   port automatic auto;
   rule myrule {
   match-direction input;
   term myterm {
      from {
         source-address 10.150.1.0/24;
      }
      then {
         translated {
            source-pool src-pool;
            overload-pool pat-pool;
            translation-type napt-44;
         }
      }
   }
}
```

Dynamic Address Translation with Small Pool

The following configuration shows dynamic address translation from a large prefix to a small pool, translating a **/24** subnet to a pool of 10 addresses. Sessions from the first 10 host sessions are assigned an address from the pool on a first-come, first-served basis, and any additional requests are rejected. Each host with an assigned NAT can participate in multiple sessions.

```
[edit services nat]
pool my-pool {
   address-range low 10.10.10.1 high 10.10.10.10;
}
rule src-nat {
   match-direction input;
```

```
    term t1 {
      from {
        source-address 192.168.1.0/24;
      }
      then {
        translated {
          translation-type dynamic-nat44;
          source-pool my-pool;
        }
      }
    }
}
```

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, the **sequential** option is introduced to enable you to configure sequential allocation of ports.

Configuring NAPT in IPv6 Networks

Network Address Port Translation (NAPT) is a method by which many network addresses and their TCP/UDP 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 IPv6 networks. Configuring NAPT in IPv6 networks is not supported if you are using MS-MPCs or MS-MICs. For information about configuring NAPT in IPv4 networks, see "Configuring NAPT in IPv4 Networks" on page 177.

To configure NAPT, you must configure a rule at the **[edit services nat]** hierarchy level for dynamically translating the source IPv6 addresses.

To configure NAPT in IPv6 networks:

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

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

2. Define the pool of IPv6 source addresses that must be used for dynamic translation. For NAPT, also specify port numbers when configuring the source pool.

```
[edit services nat]
user@host# set pool pool name address IPv6 source addresses
user@host# set pool pool name port source ports
```

For example:

```
[edit services nat]
user@host#  set pool IPV6-NAPT-Pool address 2002::1/96
user@host#  set pool IPV6-NAPT-Pool port automatic sequential
```

3. Define a NAT rule for translating the source addresses. To do this, set the **match-direction** statement of the rule as **input**. In addition, define a term that uses **napt-66** as the translation type for translating the addresses of the pool defined in the previous step. Note that the **napt-66** translation type is supported only on the MS-DPC, MS-100, MS-400, and MS-500 line cards.

```
[edit services nat]
user@host# set rule rule name match-direction input
user@host# set rule rule name term term name then translated source-pool pool name
user@host# set rule rule name term term name then translated translation-type napt-66
```

For example:

```
[edit services nat]
user@host# set rule IPV6-NAPT-Rule match-direction input
user@host# set rule IPV6-NAPT-Rule term t1 then translated source-pool IPV6-NAPT-Pool
user@host# set rule IPV6-NAPT-Rule term t1 then translated translation-type napt-66
```

4. Enter the **up** command to navigate to the **[edit services]** hierarchy level.

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

5. Define a service set to specify the services interface that must be used, and reference the NAT rule implemented for NAPT translation.

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

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

For example:

```
[edit services]
user@host# set service-set IPV6-NAPT-ServiceSet interface-service service-interface sp-0/1/0
user@host# set service-set IPV6-NAPT-ServiceSet nat-rules IPV6-NAPT-Rule
```

6. Define the trace options for the adaptive services PIC.

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

For example:

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

The following example configures dynamic source (address and port) translation or NAPT for an IPv6 network.

```
[edit services]
user@host# show
    service-set IPV6-NAPT-ServiceSet {
        nat-rules IPV6-NAPT-Rule;
        interface-service {
            service-interface sp-0/1/0;
        }
    }
    nat {
        pool IPV6-NAPT-Pool {
            address 2002::1/96;
            port automatic sequential;
        }
        rule IPV6-NAPT-Rule {
            match-direction input;
            term term1 {
                then {
                    translated {
                        source-pool IPV6-NAPT-Pool;
                        translation-type {
```

```
                        napt-66;
                    }
                }
            }
        }
    }
    adaptive-services-pics {
        traceoptions {
            flag all;
        }
    }
}
```

Example: Configuring NAT with Port Translation

IN THIS SECTION

This example shows how to configure NAT with port translation.

Requirements

This example uses the following hardware and software components:

- An MX Series 5G Universal Routing Platform with a Services DPC or an M Series Multiservice Edge router with a services PIC
- A domain name server (DNS)
- Junos OS Release 11.4 or higher

Overview

This example shows a complete CGN NAT44 configuration and advanced options.

Configuring NAT with Port Translation

Step-by-Step Procedure

To configure the service set:

1. Configure a service set.

```
user@host# edit services service-set ss2
```

2. Specify the NAT rule to be used.

```
[edit services service-set ss2]
host# set nat-rules r1
```

3. Specify the interface service.

```
[edit services service-set ss2]
host# set interface-service service-interface sp-5/0/0
```

Results

user@host# show services service-sets sset2

```
nat-rules r1;
interface-service {
    service-interface sp-5/0/0;
}
```

RELATED DOCUMENTATION

Example: NAPT Configuration on the MS-MPC With an Interface Service Set

IN THIS SECTION

This example shows how to configure network address translation with port translation (NAPT) on an MX series router using a MultiServices Modular Port Concentrator (MS-MPC) as a services interface card.

Requirements

This example uses the following hardware and software components:

- MX-series router
- MultiServices Modular Port Concentrator (MS-MPC)
- Junos OS Release 13.2R1 or higher

Overview

A service provider has chosen an MS-MPC as a platform to provide NAT services to accommodate new subscribers.

Configuration

IN THIS SECTION

To configure NAPT44 using the MS-MPC as a services interface card, perform these tasks:

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-0/2/0 unit 0 family inet address 10.255.248.2/24
set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1
set interfaces ms-3/0/0 unit 0 family inet
set applications application-set accept-algs application junos-http
set applications application-set accept-algs application junos-ftp
set applications application-set accept-algs application junos-tftp
set applications application-set accept-algs application junos-telnet
set applications application-set accept-algs application junos-sip
set applications application-set accept-algs application junos-rtcp
set services stateful-firewall rule sf-rule1 match-direction input-output
set services stateful-firewall rule sf-rule1 term sf-term1 from source-address 10.255.247.0/24
set services stateful-firewall rule sf-rule1 term sf-term1 from application-sets accept-algs
set services stateful-firewall rule sf-rule1 term sf-term1 then accept
set services nat pool napt-pool address 1.1.1.0/24
set services nat pool napt-pool port automatic
* nat rule for napt
set services nat rule nat-rule1 match-direction input
set services nat rule nat-rule1 term nat-term1 from source-address 10.255.247.0/24
set services nat rule nat-rule1 term nat-term1 from application-sets accept-algs
set services nat rule nat-rule1 term nat-term1 then translated source-pool napt-pool
set services nat rule nat-rule1 term nat-term1 then translated translation-type napt-44
* nat rule for basic nat
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0
```

Configuring Interfaces

Step-by-Step Procedure

Configure the interfaces required for NAT processing. You will need the following interfaces:

- A customer-facing interface that handles traffic from and to the customer.
- An internet-facing interface.
- A services interface that provides NAT and stateful firewall services to the customer-facing interface

1. Configure the interface for the customer-facing interface.

```
user@host# edit
[edit ]
user@host# set interfaces xe-1/1/0 unit 0 family inet address 10.255.247.2/24
user@host# set interfaces xe-1/1/0 unit 0 family inet service input service-set sset1
user@host# set interfaces xe-1/1/0 unit 0 family inet service output service-set sset1
```

2. Configure the interface for the Internet-facing interface.

```
[edit ]
set interfaces ge-0/2/0 unit 0 family inet address 10.255.248.2/24
```

3. Configure the interface for the service set that will connect services to the customer-facing interface. In our example, the interface resides on an MS-MPC.

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

Configure an Application Set of Acceptable Application Traffic

Step-by-Step Procedure

Identify the acceptable applications for incoming traffic.

1. Specify an application set that contains acceptable incoming application traffic.

```
user@host# set applications application-set accept-algs application junos-http
user@host# set applications application-set accept-algs application junos-ftp
user@host# set applications application-set accept-algs application junos-tftp
user@host# set applications application-set accept-algs application junos-telnet
user@host# set applications application-set accept-algs application junos-sip
user@host# set applications application-set accept-algs application junos-rtcp
```

Results

`user@host#`**edit services applications application-set accept-algs**

`user@host#`**show**

```
application junos-http;
application junos-ftp;
application junos-tftp;
```

```
application junos-telnet;
application junos-sip;
application junos-
```

Configuring a Stateful Firewall Rule

Step-by-Step Procedure

Configure a stateful firewall rule that will accept all incoming traffic.

1. Specify firewall matching for all input and output

```
user@hos#t set services stateful-firewall rule sf-rule1 match-direction input-output
```

2. Identify source-address and acceptable application traffic from the customer-facing interface.

```
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from source-address 10.255.247.0/24
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 from application-sets accept-algs
user@host# set services stateful-firewall rule sf-rule1 term sf-term1 then accept
```

Results

```
user@host# edit services stateful-firewall
```

```
user@host# show
```

```
rule sf-rule1 {
    match-direction input-output;
    term sf-term1 {
        from {
            source-address {
                10.255.247.0/24;
            }
            application-sets accept-algs;
        }
        then {
            accept;
        }
    }
}
```

Configuring NAT Pool and Rule

Step-by-Step Procedure

Configure a NAT pool and rule for address translation with automatic port assignment.

1. Configure the NAT pool with automatic port assignment.

```
user@host# set services nat pool napt-pool address 1.1.1.0/24
user@host# set services nat pool napt-pool port automatic auto
```

2. Configure a NAT rule that applies translation type **napt-44** using the defined NAT pool.

```
user@host# set services nat rule nat-rule1 term nat-term1 from application-sets accept-algs
user@host# set services nat rule nat-rule1 term nat-term1 then translated source-pool napt-pool
user@host# set services nat rule nat-rule1 term nat-term1 then translated translation-type napt-44
```

Results

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

`user@host#`**show**

```
pool napt-pool {
    address 1.1.1.0/24;
    port {
        automatic;
    }
}
rule nat-rule1 {
    match-direction input;
    term nat-term1 {
        from {
            source-address {
                10.255.247.0/24;
            }
            application-sets accept-algs;
        }
        then {
            translated {
                source-pool napt-pool;
                translation-type {
                    napt-44;
```

```
                }
            }
        }
    }
}
```

Configuring the Service Set

Step-by-Step Procedure

Configure an interface type service set.

1. Specify the NAT and stateful firewall rules that apply to customer traffic.

   ```
   user@host set services service-set sset1 stateful-firewall-rules sf-rule1
   user@host set services service-set sset1 nat-rules bat-rule1
   ```

2. Specify the services interface that applies the rules to customer traffic.

   ```
   set services service-set sset1 interface-service service-interface ms-3/0/0
   ```

Results

```
user@host# edit services service-set sset1

user@host# show
```

```
set services service-set sset1 stateful-firewall-rules sf-rule1
set services service-set sset1 nat-rules nat-rule1
set services service-set sset1 interface-service service-interface ms-3/0/0
```

RELATED DOCUMENTATION

Junos Address Aware Network Addressing Overview | 78

Example: Dynamic Source NAT as a Next-Hop Service

The following example shows dynamic-source NAT applied as a next-hop service:

```
[edit interfaces]
ge-0/2/0 {
    unit 0 {
        family mpls;
    }
}
sp-1/3/0 {
    unit 0 {
        family inet;
    }
    unit 20 {
        family inet;
    }
    unit 32 {
        family inet;
    }
}
[edit routing-instances]
protected-domain {
    interface ge-0/2/0.0;
    interface sp-1/3/0.20;
    instance-type vrf;
    route-distinguisher 10.58.255.17:37;
    vrf-import protected-domain-policy;
    vrf-export protected-domain-policy;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop sp-1/3/0.20;
        }
    }
}
[edit policy-options]
policy-statement protected-domain-policy {
    term t1 {
        then reject;
    }
}
[edit services]
stateful-firewall {
    rule allow-all {
        match-direction input;
        term t1 {
            then {
                accept;
```

```
            }
        }
    }
}
nat {
    pool my-pool {
        address 10.58.16.100;
        port automatic;
    }
    rule hide-all {
        match-direction input;
        term t1 {
            then {
                translated {
                    source-pool my-pool;
                    translation-type napt-44;
                }
            }
        }
    }
}
service-set null-sfw-with-nat {
    stateful-firewall-rules allow-all;
    nat-rules hide-all;
    next-hop-service {
        inside-service-interface sp-1/3/0.20;
        outside-service-interface sp-1/3/0.32;
    }
}
```

CHAPTER 10

Mapping Addresses and Ports With Deterministic NAT

IN THIS CHAPTER

Deterministic NAPT Overview

You can configure deterministic NAPT44 to ensure that the original source IPv4 address and port always map to the same post-NAT IPv4 address and port range, and that the reverse mapping of a given translated external IPv4 address and port are always mapped to the same internal IPv4 address. You can configure deterministic NAPT64 to ensure that the original source IPv6 address and port always map to the same post-NAT IPv4 address and port range, and that the reverse mapping of a given translated external IPv4 address and port are always mapped to the same internal IPv6 address. Deterministic NAPT uses an algorithm-based allocation of blocks of destination ports.

Deterministic NAPT44 is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Deterministic NAPT 44 is supported for MS-MPCs and MS-MICs starting in Junos OS release 17.3R1, in Junos OS release 14.2R7 and later 14.2 releases, and in Junos OS release 15.1R3 and later 15.1 releases. Starting in Junos OS Release 17.4R1, deterministic NAPT64 is supported on the MS-MPC and MS-MIC.

If the source address in the **from** clause of a deterministic NAPT rule does not have a prefix of /32, the network and broadcast addresses in the source address range are not translated unless you configure **include-boundary-addresses**.

For detailed information on how to configure deterministic NAPT, see "Configuring Deterministic NAPT" on page 202.

Benefits of Deterministic NAPT

- Eliminates the need for address translation logging because an IP address is always mapped to the same external IP address and port range, and the reverse mapping of a given translated external IP address and port are always mapped to the same internal IP address.

Understanding Deterministic NAPT Algorithms

The effectiveness of your implementation of deterministic NAPT depends on your analysis of your subscriber requirements. The block size you provide indicates how many ports will be made available for each incoming subscriber address from the range in the **from** clause specified in the applicable NAT rule. The allocation algorithm computes an offset value to determine the outgoing IP address and port. A reverse algorithm is used to derive the originating subscriber address.

> **NOTE:** In order to track subscribers without using logs, an ISP must use a reverse algorithm to derive a subscriber (source) addresses from a translated address.

The following variables are used in forward calculation (private subscriber IP address to public IP address) and reverse calculation (public IP address to private subscriber IP address):

- Pr_Prefix—Any pre-NAT IPv4 subscriber address.
- Pr_Port—Any pre-NAT protocol port.
- Block_Size—Number of ports configured to be available for each Pr_Prefix.

  If **block-size** is configured as zero, the method for computing the block size is computed as follows:

  block-size = int(64512/ceil[(Nr_Addr_PR_Prefix/Nr_Addr_PU_Prefix)])

  where 64512 is the maximum available port range per public IP address.
- Base_PR_Prefix—First usable pre-NAT IPv4 subscriber address in a **from** clause of the NAT rule.
- Base_PU_Prefix—First usable post-NAT IPv4 subscriber address configured in the NAT pool.
- Pu_Port_Range_Start—First usable post-NAT port. This is 1024.
- Pr_Offset—The offset of the pre-NAT IP address that is being translated from the first usable pre-NAT IPv4 subscriber address in a **from** clause of the NAT rule. PR_Offset = Pr_Prefix – Base_Pr_Prefix.
- PR_Port_Offset—Offset of the pre-NAT IP address multiplied by the block size. PR_Port_Offset = Pr_Offset * Block_Size.
- Pu_Prefix—Post-NAT address for a given Pr_Prefix.
- Pu_Start_Port—Post-NAT start port for a flow from a given Pr_Prefix
- Pu_Actual_Port—Post-NAT port seen on a reverse flow.
- Nr_Addr_PR_Prefix — Number of usable pre-NAT IPv4 subscriber addresses in a **from** clause clause of the NAT rule.
- Nr_Addr_PU_Prefix — Number of usable post-NAT IPv4 addresses configured in the NAT pool.
- Rounded_Port_Range_Per_IP — Number of ports available for each post-NAT IP address. Rounded_Port_Range_Per_IP = ceil[(Nr_Addr_PR_Prefix/Nr_Addr_PU_Prefix)] * Block_Size.
- Pu_Offset—Offset of the post-NAT IP address from the first usable post-NAT address. Pu_Offset = Pu_Prefix – Base_Pu_Prefix.
- Pu_Port_Offset— Offset of the post-NAT port from 1024 added to the product of the offset of the post-NAT IP address and the number of ports available for each post-NAT IP address. Pu_Port_Offset = (Pu_Offset * Rounded_Port_Range_Per_IP) + (Pu_Actual_Port – Pu_Port_Range_Start).

Algorithm Usage–Assume the following configuration:

```
services {
    nat {
        pool src-pool {
            address-range low 32.32.32.1 high 32.32.32.254;
```

```
            port {
                automatic {
                    random-allocation;
                }
                deterministic-block-allocation {
                    block-size 249;
                }
            }
        }
    rule det-nat {
    match-direction input;
        term t1 {
            from {
                source-address {
                    10.1.0.0/16;
                }
            }
            then {
                translated {
                    source-pool src-pool;
                    translation-type {
                        deterministic-napt44;
                    }
                }
            }
        }
```

Forward Translation

1. Pr_Offset = Pr_Prefix – Base_Pr_Prefix

2. Pr_Port_Offset = Pr_Offset * Block_Size

3. Rounded_Port_Range_Per_IP = ceil[(Nr_Addr_PR_Prefix/Nr_Addr_PU_Prefix)] * Block_Size

4. Pu_Prefix = Base_Public_Prefix + floor(Pr_Port_Offset / Rounded_Port_Range_Per_IP)

5. Pu_Start_Port = Pu_Port_Range_Start + (Pr_Port_Offset % Rounded_Port_Range_Per_IP)

Using the sample configuration and assuming a subscriber flow sourced from 10.1.1.250:5000:

1. Pr_Offset = 10.1.1.250 – 10.1.0.1 = 505

2. Pr_Port_Offset = 505 * 249 = 125,745

3. Rounded_Port_Range_Per_IP = ceil[(65, 533/254)] * 249 = 259 * 249 = 64,491

4. Pu_Prefix = 32.32.32.1 + floor(125,745 /64,491) = 32.32.32.1 +1 =32.32.32.2

5. Pu_Start_Port = 1,024 + (125,745 % 64,491) = 62278

   - 10.1.1.250 is translated to 32.32.32.2.
   - The starting port is 62278. There are 249 ports available to the subscriber based on the configured block size. The available port range spans ports 62278 through 62526 (inclusive).
   - The specific flow 10.1.1.250:5000 randomly assigns any of the ports in its range because random allocation was specified.

Reverse Translation

1. Pu_Offset = Pu_Prefix – Base_Pu_Prefix

2. Pu_Port_Offset = (Pu_Offset * Rounded_Port_Range_Per_IP) + (Pu_Actual_Port – Pu_Port_Range_Start)

3. Subscriber_IP = Base_Pr_Prefix + floor(Pu_Port_Offset / Block_Size)

The reverse translation is determined as follows. Assume a flow returning to 32.32.32.2:62278.

1. Pu_Offset = 32.32.32.2 – 32.32.32.1 = 1

2. Pu_Port_Offset = (1 * 64,491) + (62,280 - 1024) = 125,747

3. Subscriber_IP = 10.1.0.1 + floor(125,747 / 249) = 10.1.0.1 + 505 = 10.1.1.250

> **NOTE:** In reverse translation, only the original private IP address can be derived, and not the original port in use. This is sufficiently granular for law enforcement requirements.

When you have configured deterministic NAPT, you can use the **show services nat deterministic-nat internal-host** and **show services nat deterministic-nat nat-port-block** commands to show forward and reverse mapping. However, mappings will change if you reconfigure your deterministic port block allocation block size or the **from** clause for your NAT rule. In order to provide historical information on mappings, we recommend that you write scripts that can show specific mappings for prior configurations.

Deterministic NAPT Restrictions

When you configure deterministic NAPT, you must be aware of the following restrictions. Violation of any restriction results in a commit error. The restrictions and their error messages are shown in Table 12 on page 201.

Table 12: Deterministic NAPT Commit Constraints

Restriction	Error Message
The total number of deterministic NAT blocks must be greater than or equal to the **from** clause addresses configured. This means that the Rounded_Port_Range_Per_IP value must be less than or equal to 64,512.	Number of addresses and port blocks combination in the NAT pool is less than number of addresses in 'from' clause
IPv6 addresses should not be used in deterministic NAT pool/from clause.	Invalid IP address in pool p1 with translation type deterministic-napt44 OR There is already a range configured with v4 address range
The **from** clause addresses should be same if the same deterministic NAT pool is used across multiple terms/rules. Only one **from** clause address/range should be specified if the same deterministic NAT pool is used across multiple terms/rules.	With translation-type deterministic-napt44, same 'from' address/range should be configured if pool is shared by multiple rules or terms
The **from** clause must have at least one source address.	With translation-type deterministic-napt44, at least one non-except 'from' address/range should be configured. error: configuration check-out failed
There should not be address overlap between **except** entries in the **from** clause addresses.	overlapping address, in the 'from' clause between 'except' entries
Addresses in a NAT pool used for deterministic NAPT should not overlap with the addresses in any other NAT pool.	NAT pool det-nat-pool1 overlaps with det-nat-pool used by service set sset_det-nat error: configuration check-out failed
A deterministic NAT pool cannot be used with other translation types. In addition, a deterministic NAT pool cannot be used in both deterministic NAPT44 and deterministic NAPT64 NAT rules.	Deterministic NAT pool cannot be used with other translation-types

Table 12: Deterministic NAPT Commit Constraints *(continued)*

Restriction	Error Message
Deterministic NAPT44 must use a source pool with deterministic-port-block-allocation configuration.	Deterministic NAPT44 must use a source pool with deterministic-port-block-allocation configuration
If **address-allocation round-robin** is configured, a commit results in display of a warning indicating that this technique is not needed with translation-type deterministic-napt44 and is ignored.	Address allocation round-robin is not needed with translation-type deterministic-napt44
The total number of IP addresses assigned to a deterministic NAT pool should be less than or equal to 2^{24} (16777216).	Number of addresses in pool with deterministic-napt44 translation are limited to at most 16777216(2^24)

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, deterministic NAPT64 is supported on the MS-MPC and MS-MIC.
17.3R1	Deterministic NAPT 44 is supported for MS-MPCs and MS-MICs starting in Junos OS release 17.3R1

RELATED DOCUMENTATION

Configuring Deterministic NAPT | 202

Configuring Deterministic NAPT

IN THIS SECTION

Deterministic NAPT44 is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Deterministic NAPT44 is supported for MS-MPCs and MS-MICs starting in Junos OS release 17.3R1, in Junos OS release 14.2R7 and later 14.2 releases, and in Junos OS release 15.1R3 and later 15.1 releases. Starting in Junos OS Release 17.4R1, deterministic NAPT64 is supported on the MS-MPC and MS-MIC.

To configure deterministic NAPT, perform the following:

Configuring the NAT Pool for Deterministic NAPT

To configure the NAT pool for deterministic NAPT:

1. At the **[edit services nat pool *poolname*]** hierarchy level, create a pool.

   ```
   user@host# edit services nat pool poolname
   ```

2. Define the range of addresses to be translated, specifying the upper and lower limits of the range or an address prefix that describes the range.

   ```
   [edit services nat pool pba-pool1]
   user@host# set address-range low address high address
   ```

   Or

   ```
   user@host# set address address-prefix
   ```

3. To configure automatic port assignment, specify either sequential or random allocation.

   ```
   [edit services nat pool pba-pool1]
   user@host# set port automatic (sequential | random-allocation)
   ```

> **NOTE:** Starting in Junos OS Release 14.2R1, the **sequential** option is introduced to enable you to configure sequential allocation of ports. The **sequential** and **random-allocation** options available with the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level are mutually exclusive. You can include the **sequential** option for sequential allocation and the **random-allocation** option for random delegation of ports. By default, sequential allocation of ports takes place if you include only the **port automatic** statement at the **[edit services nat pool *nat-pool- name*]** hierarchy level.
>
> For releases earlier than Junos OS Release 14.2R1, configure automatic sequential port assignment by using the **auto** option at the **[edit services nat pool *nat-pool-name* port automatic]** hierarchy level.

4. To configure a range of ports to assign, specify the low and high values for the port. If you do not configure automatic port assignment, you must configure a range of ports.

   > **NOTE:** If you specify a range of ports to assign, the **automatic** statement is ignored.

   ```
   [edit services nat pool pba-pool1]
   user@host# set port range low minimum-value high maximum-value
   ```

5. Configure deterministic port block allocation. Specify **block-size** or accept the default value of 512.

   You can also specify **include-boundary-addresses** if you want the lowest and highest addresses (the network and broadcast addresses) in the source address range of a NAT rule to be translated when the NAT pool is used. If the source address has a prefix of /32, the lowest and highest address are automatically translated.

   ```
   [edit services nat pool pba-pool1]
   user@host# set port deterministic-port-block-allocation block-size block-size include-boundary-addresses
   ```

   For example:

   ```
   [edit services nat pool pba-pool1]
   user@host# set port deterministic-port-block-allocation block-size 256
   ```

NOTE: In order for **deterministic-port-block-allocation** configuration changes to take effect, you must reboot the services PIC whenever you change any of the following **nat pool** options:

- **address** or **address-range**
- **port range**
- **port deterministic-port-block-allocation block-size**

SEE ALSO

Network Address Translation Configuration Overview | **101**

Configuring the NAT Rule for Deterministic NAPT

To configure the NAT rule for deterministic NAPT:

1. Configure the NAT rule name.

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

2. Configure the NAT rule match direction as input.

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

3. Specify the addresses that are translated by the NAT rule.

   To specify one address:

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

   To specify a range of addresses:

```
[edit services nat]
```

```
user@host# set rule rule-name term term-name from source-address-range low minimum-value high
    maximum-value
```

4. Specify the NAT pool that contains the addresses for translated traffic.

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

5. Configure the translation type as deterministic NAPT44 or deterministic NAPT64.

```
[edit services nat]
user@host# set rule rule-name term term-name then translation-type (deterministic-napt44 |
    deterministic-napt64)
```

Configuring the Service Set for Deterministic NAT

To configure the service set for deterministic NAPT:

1. Define the service set.

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

2. Configure either an interface service, which requires a single service interface, or a next-hop service, which requires an inside and outside service interface.

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

or

```
[edit services service-set service-set-name]
user@host# set next-hop-service inside-service-interface interface-name outside-service-interface
    interface-name
```

3. Specify the NAT rules or ruleset to be used with the service set.

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

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

CHAPTER 11

Securing Traffic Using NAT-PT and ALGs

IN THIS CHAPTER

ALGs Available for Junos OS Address Aware NAT

The following Application Level Gateways (ALGs) listed in Table 13 on page 209 are supported for NAT processing on the listed platforms.

To view the implementation details (port, protocol, and so on) for these Junos OS default applications, locate the Junos OS Default ALG Name in the table and then look up the listed name in the **groups**. For example, for details about TFTP, look up **junos-tftp** as shown.

TIP: The Junos OS provides the **junos-alg**, which enables other ALGs to function by handling ALG registrations, causing slow path packets to flow through registered ALGs, and transferring ALG events to the ALG plug-ins. The **junos-alg** ALG is automatically available on the MS-MPC and MS-MIC platforms and does not require further configuration.

NOTE: The remote shell (RSH) and remote login (rlogin) application layer gateways (ALGs) are not supported with network address port translation (NAPT) on MX Series routers with MS-MICs and MS-MPCs.

```
user@host# show groups junos-defaults applications application junos-tftp
```

```
application-protocol tftp;
protocol udp;
destination-port 69;
```

Table 13 on page 209 summarizes the ALGs available for Junos OS Address Aware NAT for services interfaces cards.

Table 13: ALGs Available for NAT by Type of Interface Card

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Basic TCP ALG	yes	yes	**NOTE:** Specific Junos OS ALGs are not supported. However, a feature called TCP tracker, available by default, performs segment ordering and retransmit and connection tracking, validations for TCP connections.
Basic UDP ALG	yes	yes	**NOTE:** TCP tracker performs limited integrity and validation checks for UDP.
BOOTP	yes	no	• **junos-bootpc** • **junos-bootps**
DCE RPC Services	yes	yes	• **junos-dce-rpc-portmap** • **junos-dcerpc-endpoint-mapper-service** • **junos-dcerpc-msexchange-directory-nsp** • **junos-dcerpc-msexchange-directory-rfr** • **junos-dcerpc-msexchange-information-store**
DNS	yes	yes	• **junos-dns-udp**
DNS	no	no	• **junos-dns-tcp**
FTP	yes	yes	• **junos-ftp**

Table 13: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Gatekeeper RAS (Starting in Junos OS Release 17.1R1)	no	yes	• **junos-h323-ras**
H323	no	yes	• **junos-h323**
ICMP	yes	yes **NOTE:** In Junos OS Release 14.1 and earlier, ICMP messages are handled by default, but PING ALG support is not provided. Starting In Junos OS 14.2, ICMP messages are handled by default and PING ALG support is provided.	• **junos-icmp-all** • **junos-icmp-ping**
IIOP	yes	no	• **junos-iiop-java** • **junos-iiop-orbix**
IKE ALG	no	yes **NOTE:** Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG ALG is supported on MS-MPCs and MS-MICs.	• **junos-ike**
IP	yes	The TCP tracker, available by default on these platforms, performs limited integrity and validation checks.	• **junos-ip**

Table 13: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
NETBIOS	yes	no	• **junos-netbios-datagram** • **junos-netbios-name-tcp** • **junos-netbios-name-udp** • **junos-netbios-session**
NETSHOW	yes	no	• **junos-netshow**
PPTP	yes	yes	• **junos-pptp**
REALAUDIO	yes	no	• **junos-realaudio**
Sun RPC and RPC Port Map Services	yes	yes	• **junos-rpc-portmap-tcp** • **junos-rpc-portmap-udp**
RTSP	yes	yes	• **junos-rtsp**
SIP	yes	Yes	• **junos-sip** The SIP **callid** is *not* translated in **register** messages. **NOTE:** SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. SIP sessions on the MS-DPC have no time limits.
SNMP	yes	No	• **junos-snmp-get** • **junos-snmp-get-next** • **junos-snmp-response** • **junos-snmp-trap**
SQLNET	yes	yes	• **junos-sqlnet**
TFTP	yes	yes	• **junos-tftp**

Table 13: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Traceroute	yes	yes	• **junos-traceroute**
Unix Remote Shell Service	yes	yes **NOTE:** Remote Shell (RSH) ALG is not supported for network address port translation (NAPT).	• **junos-rsh**
WINFrame	yes	No	• **junos-citrix-winframe** • **junos-citrix-winframe-udp**
TALK-UDP	No	Yes	• **junos-talk-udp**
MS RPC	No	Yes	• **junos-rpc-portmap-tcp** • **junos-rpc-portmap-udp** • **junos-rpc-services-tcp** • **junos-rpc-services-udp**

Release History Table

Release	Description
17.1R1	Gatekeeper RAS (Starting in Junos OS Release 17.1R1)
14.2R7	Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG ALG is supported on MS-MPCs and MS-MICs.
14.2	Starting In Junos OS 14.2, ICMP messages are handled by default and PING ALG support is provided.

RELATED DOCUMENTATION

ALG Descriptions | 466

ALGs Available by Default for Junos OS Address Aware NAT on ACX500 Router

The following Application Level Gateways (ALGs) listed in Table 13 on page 209 are supported for NAT processing on ACX500 routers.

To view the implementation details (port, protocol, and so on) for these Junos OS default applications, locate the Junos OS Default ALG Name in the table and then look up the listed name in the **groups**. For example, for details about TFTP, look up **junos-tftp** as shown.

NOTE: The ALG for NAT is supported only on the ACX500 indoor routers.

TIP: The Junos OS provides the **junos-alg**, which enables other ALGs to function by handling ALG registrations, causing slow path packets to flow through registered ALGs, and transferring ALG events to the ALG plug-ins. The **junos-alg** ALG is automatically available on the ACX500 router and does not require further configuration.

NOTE: The remote login (rlogin) application layer gateways (ALGs) are not supported with network address port translation (NAPT) on ACX500 router.

Table 14: ALGs Available by Default

ALG	ACX500 Router	Junos OS Default ALG Name
Basic TCP ALG	yes	**NOTE:** Specific Junos OS ALGs are not supported. However, a feature called TCP tracker, available by default, performs segment ordering and retransmit and connection tracking, validations for TCP connections.
Basic UDP ALG	yes	**NOTE:** TCP tracker performs limited integrity and validation checks for UDP.
DNS	yes	• **junos-dns-tcp** • **junos-dns-udp**
FTP	yes	• **junos-ftp**

Table 14: ALGs Available by Default *(continued)*

ALG	ACX500 Router	Junos OS Default ALG Name
ICMP	yes **NOTE:** ICMP messages are handled by default, but PING ALG support is not provided.	• **junos-icmp-all**
TFTP	yes	• **junos-tftp**
Unix Remote Shell Service	yes **NOTE:** Remote Shell (RSH) ALG is not supported for network address port translation (NAPT).	• **junos-rsh**

ALG Support Details

IN THIS SECTION

This section includes details about the ALGs. It includes the following:

Basic TCP

This ALG performs basic sanity checking on TCP packets. If it finds errors, it generates the following anomaly events and system log messages:

- TCP source or destination port zero
- TCP header length check failed
- TCP sequence number zero and no flags are set

- TCP sequence number zero and FIN/PSH/RST flags are set
- TCP FIN/RST or SYN(URG|FIN|RST) flags are set

The TCP ALG performs the following steps:

1. When the router receives a SYN packet, the ALG creates TCP forward and reverse flows and groups them in a *conversation*. It tracks the TCP three-way handshake.
2. The SYN-defense mechanism tracks the TCP connection establishment state. It expects the TCP session to be established within a small time interval (currently 4 seconds). If the TCP three-way handshake is not established in that period, the session is terminated.
3. A keepalive mechanism detects TCP sessions with nonresponsive endpoints.
4. ICMP errors are allowed only when a flow matches the selector information specified in the ICMP data.

Basic UDP

This ALG performs basic sanity checking on UDP headers. If it finds errors, it generates the following anomaly events and system log messages:

- UDP source or destination port 0
- UDP header length check failed

The UDP ALG performs the following steps:

1. When it receives the first packet, the ALG creates bidirectional flows to accept forward and reverse UDP session traffic.
2. If the session is idle for more than the maximum allowed idle time (the default is 30 seconds), the flows are deleted.
3. ICMP errors are allowed only when a flow matches the selector information specified in the ICMP data.

DNS

The Domain Name System (DNS) ALG handles data associated with locating and translating domain names into IP addresses. The ALG typically runs on port 53. The ALG monitors DNS query and reply packets and supports only UDP traffic. The ALG does not support payload translations. The DNS ALG closes the session only when a reply is received or an idle timeout is reached.

The following is an example for configuring DNS ALG:

1. Creating NAT interface.

```
[edit]
services {
    service-set set-dns {
        nat-rules nat-dns;
```

```
        interface-service {
            service-interface ms-0/2/0;
        }
    }
```

2. Configuring NAT pool.

```
[edit]
services {
    nat {
        pool p-napt {
            address 1.1.1.1/32;
        }
    }
}
```

3. Defining NAT rules for DNS ALG.

```
[edit]
services {
    nat {
        rule nat-dns {
            match-direction input;
            term term1 {
                from {
                    source-address {
                        50.50.50.2/32;
                    }
                    applications junos-dns-udp;;
                }
                then {
                    translated {
                        source-pool p-napt;
                            translation-type {
                            basic-nat44;
                        }
                    }
                }
        }
    }
}
```

4. Binding service sets to the interface.

```
[edit]
interfaces {
    ge-0/1/0 {
        media-type copper;
        unit 0 {
            family inet {
                service {
                    input {
                    service-set set-dns;
                    }
                    output {
                    service-set set-dns;
                }
            }
            address 50.50.50.1/24;
        }
    }
    }
    ge-0/1/1 {
        media-type copper;
        unit 0 {
            family inet {
            address 60.60.60.1/24;
        }
    }
    }
    ms-0/2/0 {
        unit 0 {
            family inet;
        }
    }
}
```

FTP

FTP is the File Transfer Protocol, specified in RFC 959. In addition to the main control connection, data connections are also made for any data transfer between the client and the server; and the host, port, and direction are negotiated through the control channel.

For non-passive-mode FTP, Junos OS stateful firewall service scans the client-to-server application data for the PORT command, which provides the IP address and port number to which the server connects. For passive-mode FTP, Junos OS stateful firewall service scans the client-to-server application data for

the PASV command and then scans the server-to-client responses for the 227 response, which contains the IP address and port number to which the client connects.

There is an additional complication: FTP represents these addresses and port numbers in ASCII. As a result, when addresses and ports are rewritten, the TCP sequence number might be changed, and thereafter the NAT service needs to maintain this delta in SEQ and ACK numbers by performing sequence NAT on all subsequent packets.

Support for stateful firewall and NAT services requires that you configure the FTP ALG on TCP port 21 to enable the FTP control protocol. The ALG performs the following tasks:

- Automatically allocates data ports and firewall permissions for dynamic data connection
- Creates flows for the dynamically negotiated data connection
- Monitors the control connection in both active and passive modes
- Rewrites the control packets with the appropriate NAT address and port information

On ACX500, for passive FTP to work properly without FTP application layer gateway (ALG) enabled (by not specifying the **application junos-ftp** statement at the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy level), you must enable the address pooling paired (APP) functionality enabled (by including the **address-pooling** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level). Such a configuration causes the data and control FTP sessions to receive the same NAT address.

The following is an example for configuring FTP ALG:

1. Creating NAT interface.

```
[edit]
services {
   service-set set-ftp {
      nat-rules nat-ftp;
      interface-service {
         service-interface ms-0/2/0;
      }
   }
```

2. Configuring NAT pool.

```
[edit]
services {
   nat {
      pool p-napt {
         address 30.30.30.0/24;
```

```
        port {
        range low 9000 high 9010;
      }
    }
}
```

3. Defining NAT rules for FTP ALG.

```
[edit]
services {
    nat {
        rule nat-ftp {
            match-direction input;
            term term1 {
                from {
                    source-address {
                        10.10.10.0/24;
                    }
                    applications junos-ftp;
                }
                then {
                    translated {
                        source-pool p-napt;
                            translation-type {
                            napt-44;
                        }
                    }
                }
        }
    }
}
```

4. Binding service sets to the interface.

```
[edit]
interfaces {
    ge-0/1/0 {
        media-type copper;
        unit 0 {
            family inet {
                service {
                    input {
```

```
                service-set set-ftp;
                }
                output {
                service-set set-ftp;
            }
          }
          address 10.10.10.1/24;
        }
      }
      }
      ge-0/1/1 {
        media-type copper;
        unit 0 {
          family inet {
          address 10.10.10.1/24;
        }
      }
      }
      ms-0/2/0 {
        unit 0 {
          family inet;
        }
      }
  }
```

ICMP

The Internet Control Message Protocol (ICMP) is defined in RFC 792. The Junos OS allows ICMP messages to be filtered by specific type or specific type code value. ICMP error packets that lack a specifically configured type and code are matched against any existing flow in the opposite direction to check for the legitimacy of the error packet. ICMP error packets that pass the filter matching are subject to NAT translation.

The ICMP ALG always tracks ping traffic statefully using the ICMP sequence number. Each echo reply is forwarded only if there is an echo request with the corresponding sequence number. For any ping flow, only 20 echo requests can be forwarded without receiving an echo reply. When you configure dynamic NAT, the PING packet identifier is translated to allow additional hosts in the NAT pool to use the same identifier.

Support for NAT services requires that you configure the ICMP ALG if the protocol is needed. You can configure the ICMP type and code for additional filtering.

TFTP

The Trivial File Transfer Protocol (TFTP) is specified in RFC 1350. The initial TFTP requests are sent to UDP destination port 69. Additional flows can be created to **get** or **put** individual files. Support of NAT services requires that you configure the TFTP ALG for UDP destination port 69.

The following is an example for configuring TFTP ALG:

1. Creating NAT interface.

```
[edit]
services {
   service-set set-tftp {
      nat-rules nat-tftp;
      interface-service {
         service-interface ms-0/2/0;
      }
   }
```

2. Configuring NAT pool.

```
[edit]
services {
   nat {
      pool p-napt {
         address 1.1.1.1/32;
      }
   }
}
```

3. Defining NAT rules for TFTP ALG.

```
[edit]
services {
   nat {
      rule nat-tftp {
         match-direction input;
         term term1 {
            from {
               source-address {
                  50.50.50.2/32;
               }
               applications junos-tftp;
            }
```

```
            then {
               translated {
                  source-pool p-napt;
                     translation-type {
                     dynamic-nat44;
                  }
               }
            }
      }
   }
}
```

4. Binding service sets to the interface.

```
[edit]
interfaces {
   ge-0/1/0 {
      media-type copper;
      unit 0 {
         family inet {
            service {
               input {
               service-set set-tftp;
               }
               output {
               service-set set-tftp;
            }
         }
         address 50.50.50.1/24;
      }
   }
   }
   ge-0/1/1 {
      media-type copper;
      unit 0 {
         family inet {
         address 60.60.60.1/24;
      }
   }
   }
   ms-0/2/0 {
      unit 0 {
         family inet;
```

```
        }
    }
}
```

UNIX Remote-Shell Services

Three protocols form the basis for UNIX remote-shell services:

- Exec—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 512. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.
- Login—Better known as **rlogin**; uses well-known TCP port 513. For details, see RFC 1282. No special firewall processing is required.
- Shell—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 514. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.

NAT remote-shell services require that any dynamic source port assigned be within the port range 512 to 1023. If you configure a NAT pool, this port range is reserved exclusively for remote shell applications.

The following is an example for configuring RSH ALG:

1. Creating NAT interface.

```
[edit]
services {
    service-set set-rsh {
        nat-rules nat-rsh;
        interface-service {
            service-interface ms-0/2/0;
        }
    }
```

2. Configuring NAT pool.

```
[edit]
services {
    nat {
        pool p-napt {
            address 1.1.1.1/32;
        }
```

```
    }
}
```

3. Defining NAT rules for RSH ALG.

```
[edit]
services {
    nat {
        rule nat-rsh {
            match-direction input;
            term term1 {
                from {
                    source-address {
                        50.50.50.2/32;
                    }
                    applications junos-rsh;
                }
                then {
                    translated {
                        source-pool p-napt;
                            translation-type {
                            dynamic-nat44;
                        }
                    }
                }
        }
    }
}
```

4. Binding service sets to the interface.

```
[edit]
interfaces {
    ge-0/1/0 {
        media-type copper;
        unit 0 {
            family inet {
                service {
                    input {
                    service-set set-rsh;
                    }
                    output {
```

```
                service-set set-rsh;
              }
            }
            address 50.50.50.1/24;
          }
        }
        }
        ge-0/1/1 {
          media-type copper;
          unit 0 {
            family inet {
            address 60.60.60.1/24;
          }
        }
        }
        ms-0/2/0 {
          unit 0 {
            family inet;
          }
        }
    }
```

RELATED DOCUMENTATION

Junos Network Secure Overview | 542

Configuring Stateful Firewall Rules | 546

Understanding Service Sets

Configuring Service Sets to Be Applied to Services Interfaces

Configuring NAT-PT

To configure the translation type as **basic-nat-pt**, you must configure the DNS ALG application, the NAT pools and rules, a service set with a service interface, and trace options. Configuring NAT-PT is not supported if you are using MS-MPCs or MS-MICs. This topic includes the following tasks:

- Configuring the DNS ALG Application | 226
- Configuring the NAT Pool and NAT Rule | 226

Configuring the DNS ALG Application

To configure the DNS ALG application:

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

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

2. Configure the ALG to which the DNS traffic is destined at the **[edit applications]** hierarchy level. Define the application name and specify the application protocol to use in match conditions in the first NAT rule or term.

   ```
   [edit applications]
   user@host# set application application-name application-protocol application-protocol
   ```

   In the following example, the application name is **dns-alg** and application protocol is **dns**.

   ```
   [edit applications]
   user@host# set application dns-alg application-protocol dns
   ```

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

   ```
   [edit applications]
   user@host# show
   application dns-alg {
       application-protocol dns;
   }
   ```

Configuring the NAT Pool and NAT Rule

To configure the NAT pool and NAT rule:

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

   ```
   [edit]
   ```

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

2. Configure the NAT pool and its address.

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

In the following example, the name of the NAT pool is **p1** and the address is **10.10.10.2/32**.

```
[edit services nat]
user@host# set pool p1 address 10.10.10.2/32
```

3. Configure the source pool and its address.

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

In the following example, the name of the source pool is **src_pool0** and the source pool address is **20.1.1.1/32**.

```
[edit services nat]
user@host# set pool src_pool0 address 20.1.1.1/32
```

4. Configure the destination pool and its address.

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

In the following example, the name of the destination pool is **dst_pool0** and the destination pool address is **50.1.1.2/32**.

```
[edit services nat]
user@host# set pool dst_pool0 address 50.1.1.2/32
```

5. 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 rule name is **rule-basic-nat-pt** and the match direction is **input**.

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

6. Configure the term and the input conditions for the NAT term.

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

In the following example, the term is **t1** and the input conditions are **source-address 2000::2/128**, **destination-address 4000::2/128**, and **applications dns_alg**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from source-address 2000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from destination-address 4000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 from applications dns_alg
```

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

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

In the following example, the term action is **translated** and the properties of the translated traffic are **source-pool src_pool0**, **destination-pool dst_pool0**, and **dns-alg-prefix 2001:db8:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated source-pool src_pool0
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated destination-pool dst_pool0
[edit services nat]
user@host# set rule rule-basic-nat-pt term t1 then translated dns-alg-prefix 2001:db8:10::0/96
```

8. Configure the translation type.

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

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

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

9. Configure another term and the input conditions for the NAT term.

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

In the following example, the term name is **t2** and the input conditions are **source-address 2000::2/128** and **destination-address 2001:db8:10::0/96**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 from source-address 2000::2/128
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 from destination-address 2001:db8:10::0/96
```

10. Configure the NAT term action and the property of the translated traffic.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then term-action translated-property
```

In the following example, the term action is **translated** and the property of the translated traffic is **source-prefix 19.19.19.1/32**.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then translated source-prefix 19.19.19.1/32
```

11. Configure the translation type.

```
[edit services nat]
user@host# set rule rule-basic-nat-pt term t2 then translated translation-type translation-type
```

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

```
[edit services nat]
```

```
user@host# set rule rule-basic-nat-pt term t2 then translated translation-type basic-nat-pt
```

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

```
[edit services nat]
user@host# show
pool p1 {
    address 10.10.10.2/32;
}
pool src_pool0 {
    address 20.1.1.1/32;
}
pool dst_pool0 {
    address 50.1.1.2/32;
}
rule rule-basic-nat-pt {
    match-direction input;
    term t1 {
        from {
            source-address {
                2000::2/128;
            }
            destination-address {
                4000::2/128;
            }
            applications dns_alg;
        }
        then {
            translated {
                source-pool src_pool0;
                destination-pool dst_pool0;
                dns-alg-prefix 2001:db8:10::0/96;
                translation-type {
                    basic-nat-pt;
                }
            }
        }
    }
    term t2 {
        from {
            source-address {
                2000::2/128;
            }
```

```
            destination-address {
                2001:db8:10::0/96;
            }
        }
        then {
            translated {
                source-prefix 19.19.19.1/32;
                translation-type {
                    basic-nat-pt;
                }
            }
        }
    }
}
```

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 name of the service set is **ss_dns**.

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

3. Configure the service set with NAT rules.

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

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

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

4. Configure the service interface.

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

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

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

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

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

Configuring Trace Options

To configure the trace options:

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;
    }
}
```

The following example configures the translation type as **basic-nat-pt**.

```
[edit]
user@host# show services
service-set ss_dns {
    nat-rules rule-basic-nat-pt;
    interface-service {
        service-interface sp-1/2/0;
    }
}
nat {
    pool p1 {
        address 10.10.10.2/32;
    }
    pool src_pool0 {
        address 20.1.1.1/32;
    }
    pool dst_pool0 {
        address 50.1.1.2/32;
    }
    rule rule-basic-nat-pt {
        match-direction input;
        term t1 {
            from {
                source-address {
                    2000::2/128;
```

```
                }
                destination-address {
                    4000::2/128;
                }
                applications dns_alg;
            }
            then {
                translated {
                    source-pool src_pool0;
                    destination-pool dst_pool0;
                    dns-alg-prefix 2001:db8:10::0/96;
                    translation-type {
                        basic-nat-pt;
                    }
                }
            }
        }
        term t2 {
            from {
                source-address {
                    2000::2/128;
                }
                destination-address {
                    2001:db8:10::0/96;
                }
            }
            then {
                translated {
                    source-prefix 19.19.19.1/32;
                    translation-type {
                        basic-nat-pt;
                    }
                }
            }
        }
    }
}
adaptive-services-pics {
    traceoptions {
        flag all;
    }
}
```

Example: Configuring NAT-PT

IN THIS SECTION

A Domain Name System application-level gateway (DNS ALG) is used with Network Address Translation-Protocol Translation (NAT-PT) to facilitate name-to-address mapping. You can configure the DNS ALG to map addresses returned in the DNS response to an IPv6 address. Configuring NAT-PT is not supported if you are using MS-MPCs or MS-MICs.

When you configure NAT-PT with DNS ALG support, you must configure two NAT rules or one rule with two terms. In this example, you configure two rules. The first NAT rule ensures that the DNS query and response packets are translated correctly. For this rule to work, you must configure a DNS ALG application and reference it in the rule. The second rule is required to ensure that NAT sessions are destined to the address mapped by the DNS ALG.

Then, you must configure a service set, and then apply the service set to the interfaces.

This example describes how to configure NAT-PT with DNS ALG:

Requirements

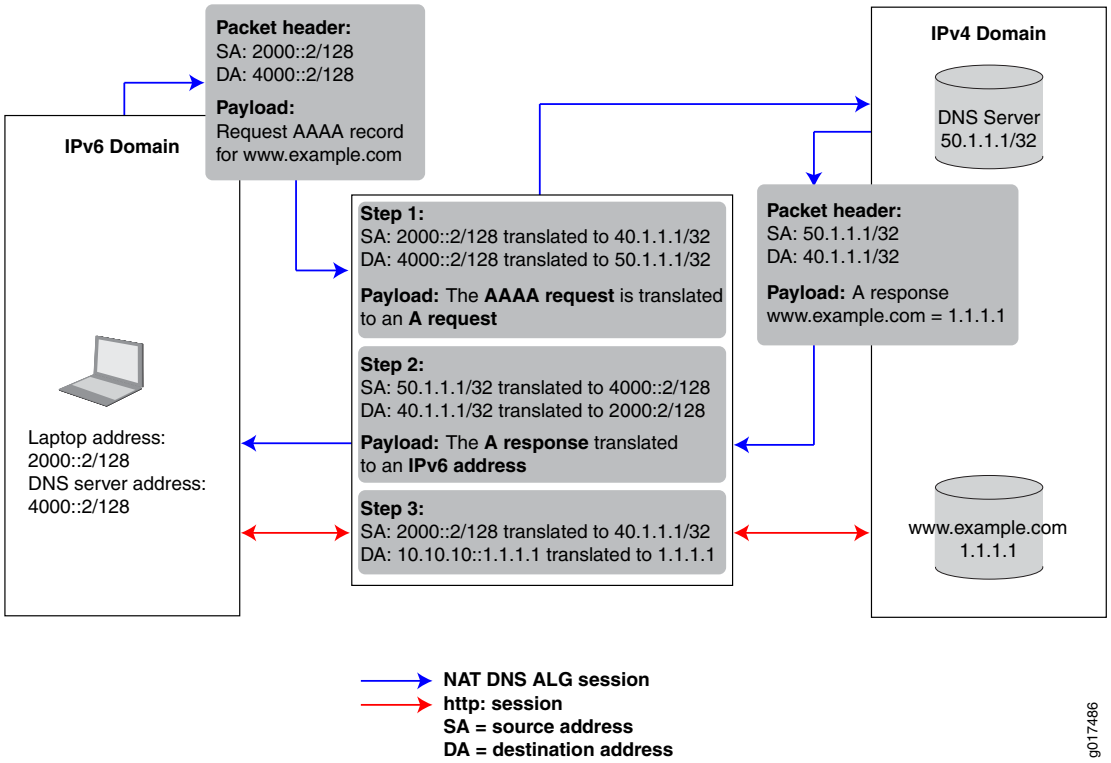
This example uses the following hardware and software components:

- Junos OS Release 11.2
- A multiservices interface (**ms-**)

Overview and Topology

The following scenario shows the process of NAT-PT with DNS ALG when a laptop in an IPv6-only domain requests access to a server in an IPv4-only domain.

Figure 13: Configuring DNS ALGs with NAT-PT Network Topology



The Juniper Networks router in the center of the illustration performs address translation in two steps. When the laptop requests a session with the **www.example.com** server that is in an IPv4-only domain, the Juniper Networks router performs the following:

- Translates the IPv6 laptop and DNS server addresses into IPv4 addresses.
- Translates the AAAA request from the laptop into an A request so that the DNS server can provide the IPv4 address.

When the DNS server responds with the A request, the Juniper Networks router performs the following:

- Translates the IPv4 DNS server address back into an IPv6 address.
- Translates the A request back into a AAAA request so that the laptop now has the 96-bit IPv6 address of the **www.example.com** server.

After the laptop receives the IPv6 version of the **www.example.com** server address, the laptop initiates a second session using the 96-bit IPv6 address to access that server. The Juniper Networks router performs the following:

- Translates the laptop IPv4 address directly into its IPv4 address.
- Translates the 96-bit IPv6 **www.example.com** server address into its IPv4 address.

Configuration of NAT-PT with DNS ALGs

IN THIS SECTION

To configure NAT-PT with DNS ALG , perform the following tasks:

Configuring the Application-Level Gateway

Step-by-Step Procedure

Configure the DNS application as the ALG to which the DNS traffic is destined. The DNS application protocol closes the DNS flow as soon as the DNS response is received. When you configure the DNS application protocol, you must specify the UDP protocol as the network protocol to match in the application definition.

To configure the DNS application:

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

```
user@host# edit applications
```

2. Define the application name and specify the application protocol to use in match conditions in the first NAT rule.

```
[edit applications]
user@host#  set application application-name application-protocol protocol-name
```

For example:

```
[edit applications]
user@host#  set application dns_alg application-protocol dns
```

3. Specify the protocol to match, in this case UDP.

```
[edit applications]
user@host#  set application application-name protocol type
```

For example:

```
[edit applications]
user@host# set application dns_alg protocol udp
```

4. Define the UDP destination port for additional packet matching, in this case the domain port.

```
[edit applications]
user@host#  set application application-name destination-port value
```

For example:

```
[edit applications]
user@host# set application dns_alg destination-port 53
```

Results

```
[edit applications]
user@host# show
application dns_alg {
    application-protocol dns;
    protocol udp;
    destination-port 53;
}
```

Configuring the NAT Pools

Step-by-Step Procedure

In this configuration, you configure two pools that define the addresses (or prefixes) used for NAT. These pools define the IPv4 addresses that are translated into IPv6 addresses. The first pool includes the IPv4 address of the source. The second pool defines the IPv4 address of the DNS server. To configure NAT pools:

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

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

2. Specify the name of the first pool and the IPv4 source address (laptop).

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

For example:

```
[edit services nat]
user@host# set pool pool1 address 40.1.1.1/32
```

3. Specify the name of the second pool and the IPv4 address of the DNS server.

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

For example:

```
[edit services nat]
user@host# set pool pool2 address 50.1.1.1/32
```

Results

The following sample output shows the configuration of NAT pools.

```
[edit services nat]
user@host# show
pool pool1 {
    address 40.1.1.1/32;
}
pool pool2 {
    address 50.1.1.1/32;
}
```

Configuring the DNS Server Session: First NAT Rule

Step-by-Step Procedure

The first NAT rule is applied to DNS traffic going to the DNS server. This rule ensures that the DNS query and response packets are translated correctly. For this rule to work, you must configure a DNS ALG application and reference it in the rule. The DNS application was configured in "Configuring the DNS ALG Application" on page 226. In addition, you must specify the direction in which traffic is matched, the source address of the laptop, the destination address of the DNS server, and the actions to take when the match conditions are met.

To configure the first NAT rule:

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

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

2. Specify the name of the NAT rule.

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

   For example:

   ```
   [edit services nat]
   user@host# edit rule rule1
   ```

3. Specify the name of the NAT term.

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

   For example:

   ```
   [edit services nat rule rule1]
   user@host# edit term term1
   ```

4. Define the match conditions for this rule.

   a. Specify the IPv6 source address of the device (laptop) attempting to access an IPv4 address.

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

      For example:

```
[edit services nat rule rule1 term term1]
user@host# set from source-address 2000::2/128
```

b. Specify the IPv6 destination address of the DNS server.

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

For example:

```
[edit services nat rule rule1 term term1]
user@host# set from destination-address 4000::2/128
```

c. Reference the DNS application to which the DNS traffic destined for port 53 is applied.

```
[edit services nat rule rule1 term term1]
user@host# set from applications application-name
```

In this example, the application name configured in the *Configuring the DNS Application* step is **dns_alg**:

```
[edit services nat rule rule1 term term1]
user@host# set from applications dns_alg
```

5. Define the actions to take when the match conditions are met. The source and destination pools you configured in "Configuring the NAT Pools" on page 238 are applied here.

a. Apply the NAT pool configured for source translation.

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

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated source-pool pool1
```

b. Apply the NAT pool configured for destination translation.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated destination-pool nat-pool-name
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated source-pool pool2
```

6. Define the DNS ALG 96-bit prefix for IPv4-to-IPv6 address mapping.

```
[edit services nat rule rule-name term term-name]
user@host# set then translated dns-alg-prefix dns-alg-prefix
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated dns-alg-prefix 10:10:10::0/96
```

7. Specify the type of NAT used for source and destination traffic.

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

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then translated translation-type basic-nat-pt
```

NOTE: In this example, since NAT is achieved using address-only translation, the **basic-nat-pt** translation type is used. To achieve NAT using address and port translation (NAPT), use the **napt-pt** translation type.

8. Specify the direction in which to match traffic that meets the rule conditions.

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

For example:

```
[edit services nat rule rule1]
user@host# set match-direction input
```

9. Configure system logging to record information from the services interface to the /var/log directory.

```
[edit services nat rule rule-name term term-name]
user@host# set then syslog
```

For example:

```
[edit services nat rule rule1 term term1]
user@host# set then syslog
```

Results

The following sample output shows the configuration of the first NAT rule that goes to the DNS server.

```
[edit services nat]
user@host# show
rule rule1 {
    match-direction input;
    term term1 {
        from {
            source-address {
                2000::2/128;
            }
            destination-address {
                4000::2/128;
            }
            applications dns_alg;
        }
        then {
            translated {
                source-pool pool1;
                destination-pool pool2;
                dns-alg-prefix 10:10:10::0/96;
                translation-type {
                    basic-nat-pt;

                }
            }
            syslog;
        }
    }
}
```

Configuring the HTTP Session: Second NAT Rule

Step-by-Step Procedure

The second NAT rule is applied to destination traffic going to the IPv4 server (**www.example.com**). This rule ensures that NAT sessions are destined to the address mapped by the DNS ALG. For this rule to work, you must configure the DNS ALG address map that correlates the DNS query or response processing done by the first rule with the actual data sessions processed by the second rule. In addition, you must specify the direction in which traffic is matched: the IPv4 address for the IPv6 source address (laptop), the 96-bit prefix to prepend to the IPv4 destination address (www.example.com), and the translation type.

To configure the second NAT rule:

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

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

2. Specify the name of the NAT rule and term.

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

   For example:

   ```
   [edit services nat]
   user@host# edit rule rule2 term term1
   ```

3. Define the match conditions for this rule:

   a. Specify the IPv6 address of the device attempting to access the IPv4 server.

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

      For example:

      ```
      [edit services nat rule rule2 term term1]
      user@host# set from source-address 2000::2/128
      ```

   b. Specify the 96-bit IPv6 prefix to prepend to the IPv4 server address.

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

For example:

```
[edit services nat rule rule2 term term1]
user@host# set from destination-address 10:10:10::c0a8:108/128
```

4. Define the actions to take when the match conditions are met.

   - Specify the prefix for the translation of the IPv6 source address.

     ```
     [edit services nat rule rule-name term term-name]
     user@host# set then translated source-prefix source-prefix
     ```

     For example:

     ```
     [edit services nat rule rule2 term term1]
     user@host# set then translated source-prefix 19.19.19.1/32
     ```

5. Specify the type of NAT used for source and destination traffic.

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

   For example:

   ```
   [edit services nat rule rule2 term term1]
   user@host# set then translated translation-type basic-nat-pt
   ```

   NOTE: In this example, since NAT is achieved using address-only translation, the **basic-nat-pt** translation type is used. To achieve NAT using address and port translation (NAPT), you must use the **napt-pt** translation type.

6. Specify the direction in which to match traffic that meets the conditions in the rule.

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

   For example:

   ```
   [edit services nat rule rule2]
   user@host# set match-direction input
   ```

Results

The following sample output shows the configuration of the second NAT rule.

```
[edit services nat]
user@host# show
rule rule2 {
    match-direction input;
    term term1 {
        from {
            source-address {
                2000::2/128;
            }
            destination-address {
                10:10:10::c0a8:108/128;
            }
        }
        then {
            translated {
                source-prefix 19.19.19.1/32;
                translation-type {
                    basic-nat-pt;
                }
            }
        }
    }
}
```

Configuring the Service Set

Step-by-Step Procedure

This service set is an interface service set used as an action modifier across the entire services (**ms-**) interface. Stateful firewall and NAT rule sets are applied to traffic processed by the services interface.

To configure the service set:

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

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

2. Define a service set.

   ```
   [edit services]
   ```

```
user@host# edit service-set service-set-name
```

For example:

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

3. Specify properties that control how system log messages are generated for the service set.

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

The example below includes all severity levels.

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

4. Specify the stateful firewall rule included in this service set.

```
[edit services service-set ss]
user@host# set stateful-firewall-rules rule1 severity-level
```

The example below references the stateful firewall rule defined in “Configuring the Stateful Firewall Rule” on page 248.

```
[edit services service-set ss]
user@host# set stateful-firewall-rules rule1
```

5. Define the NAT rules included in this service set.

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

The example below references the two rules defined in this configuration example.

```
[edit services service-set ss
user@host# set nat-rules rule1
user@host# set nat-rules rule2
```

6. Configure an adaptive services interface on which the service is to be performed.

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

For example:

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

Only the device name is needed, because the router software manages logical unit numbers automatically. The services interface must be an adaptive services interface for which you have configured **unit 0 family inet** at the **[edit interfaces *interface-name*]** hierarchy level in "Configuring Interfaces" on page 250.

Results

The following sample output shows the configuration of the service set.

```
[edit services]
user@host# show
service-set ss {
    syslog {
        host local {
            services any;
        }
    }
    stateful-firewall-rules rule1;
    nat-rules rule1;
    nat-rules rule2;
    interface-service {
        service-interface ms-2/0/0;
    }
}
```

Configuring the Stateful Firewall Rule

Step-by-Step Procedure

This example uses a stateful firewall to inspect packets for state information derived from past communications and other applications. The NAT-PT router checks the traffic flow matching the direction specified by the rule, in this case both input and output. When a packet is sent to the services (**ms-**) interface, direction information is carried along with it.

To configure the stateful firewall rule:

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

   ```
   user@host# edit services stateful firewall
   ```

2. Specify the name of the stateful firewall rule.

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

   For example:

   ```
   [edit services stateful-firewall]
   user@host# edit rule rule1
   ```

3. Specify the direction in which traffic is to be matched.

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

   For example:

   ```
   [edit services stateful-firewall rule rule1]
   user@host# set match-direction input-output
   ```

4. Specify the name of the stateful firewall term.

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

   For example:

   ```
   [edit services stateful-firewall rule rule1]
   user@host# edit term term1
   ```

5. Define the terms that make up this rule.

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

For example:

```
[edit services stateful-firewall rule rule1 term term1]
user@host# set then accept
```

Results

The following sample output shows the configuration of the services stateful firewall.

```
[edit services]
user@host# show
stateful-firewall {
    rule rule1 {
        match-direction input-output;
        term term1 {
            then {
                accept;
            }
        }
    }
}
```

Configuring Interfaces

Step-by-Step Procedure

After you have defined the service set, you must apply services to one or more interfaces installed on the router. In this example, you configure one interface on which you apply the service set for input and output traffic. When you apply the service set to an interface, it automatically ensures that packets are directed to the services (**ms-**) interface.

To configure the interfaces:

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

```
user@host# edit interfaces
```

2. Configure the interface on which the service set is applied to automatically ensure that packets are directed to the services (**ms-**) interface.

   a. For IPv4 traffic, specify the IPv4 address.

   ```
   [edit interfaces]
   user@host# set ge-1/0/9 unit 0 family inet address 30.1.1.1/24
   ```

   b. Apply the service set defined in “Configuring Interfaces” on page 250.

   ```
   [edit interfaces]
   user@host# set ge-1/0/9 unit 0 family inet6 service input service-set ss
   user@host# set ge-1/0/9 unit 0 family inet6 service output service-set ss
   ```

   c. For IPv6 traffic, specify the IPv6 address.

   ```
   [edit interfaces]
   user@host# set ge-1/0/9 unit 0 family inet6 address 2000::1/64
   ```

3. Specify the interface properties for the services interface that performs the service.

   ```
   [edit interfaces]
   user@host# set ms-2/0/0 services-options syslog host local services any
   user@host# set ms-2/0/0 unit 0 family inet
   user@host# set ms-2/0/0 unit 0 family inet6
   ```

Results

The following sample output shows the configuration of the interfaces for this example.

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

ge-1/0/9 {
    unit 0 {
        family inet {
            address 30.1.1.1/24;
        }
        family inet6 {
            service {
```

```
                input {
                    service-set ss;
                }
                output {
                    service-set ss;
                }
            }
            address 2000::1/64;
        }
    }
}

ms-2/0/0 {
    services-options {
        syslog {
            host local {
                services any;
            }
        }
    }
    unit 0 {
        family inet;
        family inet6;
    }
}
```

RELATED DOCUMENTATION

- Junos Address Aware Network Addressing Overview | **78**
- Configuring NAT-PT | **225**
- Configuring Service Sets to be Applied to Services Interfaces | **9**
- Example: Configuring Layer 3 Services and the Services SDK on Two PICs | **558**
- dns-alg-prefix | **1177**
- dns-alg-pool | **1176**

CHAPTER 12

Providing IPv4 Connectivity Across IPv6-Only Network Using 464XLAT

IN THIS CHAPTER

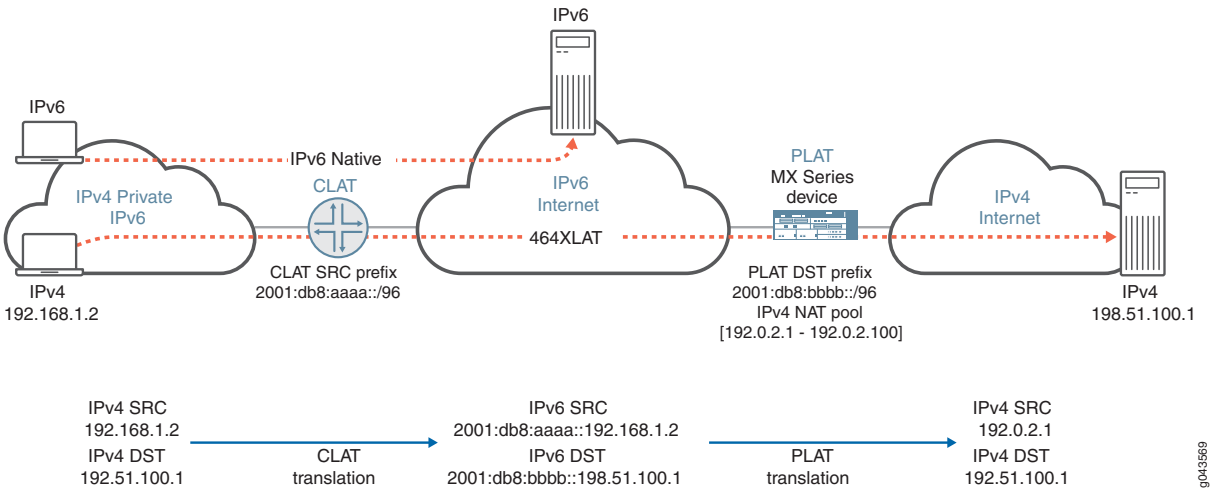
464XLAT Overview

Starting in Junos OS Release 17.1R1, you can configure a 464XLAT Provider-Side Tranlator (PLAT). This is supported only on MS-MICs and MS-MPCs. 464XLAT provides a simple and scalable technique for an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. 464XLAT only suports IPv4 in the client-server model, so it does not support IPv4 peer-to-peer communication or inbound IPv4 connections.

XLAT464 provides the advantages of not having to maintain an IPv4 network for this IPv4 traffic and not having to assign additional public IPv4 addresses.

A customer-side translator (CLAT), which is not a Juniper Networks product, translates the IPv4 packet to IPv6 by embedding the IPv4 source and destination addresses in IPv6 /96 prefixes, and sends the packet over an IPv6 network to the PLAT. The PLAT translates the packet to IPv4, and sends the packet to the IPv4 host over an IPv4 network (see Figure 14 on page 254).

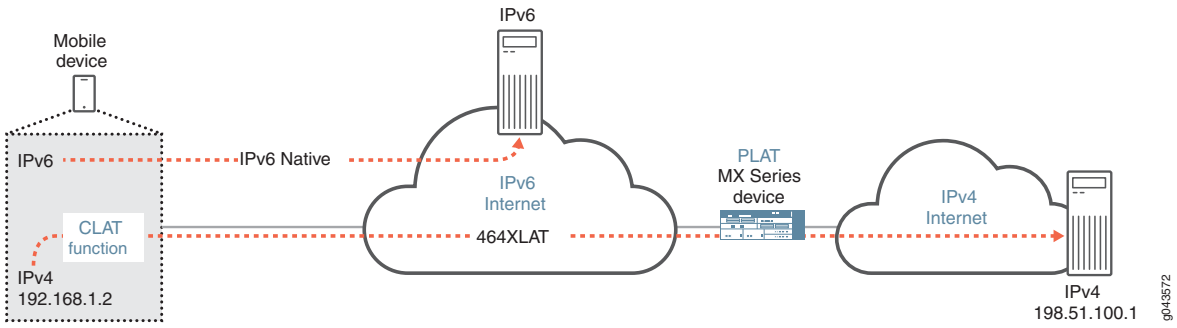
Figure 14: 464XLAT Wireline Flow



The CLAT uses a unique source IPv6 prefix for each end user, and translates the IPv4 source address by embedding it in the IPv6 /96prefix. In Figure 14 on page 254, the CLAT source IPv6 prefix is 2001:db8:aaaa::/96, and the IPv4 source address 192.168.1.2 is translated to 2001:db8:aaaa::192.168.1.2. The CLAT translates the IPv4 destination address by embedding it in the IPv6 /96 prefix of the PLAT (MX Series router). In Figure 14 on page 254, the PLAT destination IPv6 prefix is 2001:db8:bbbb::/96, so the CLAT translates the IPv4 destination address 198.51.100.1 to 2001:db8:bbbb::198.51.100.

The CLAT can reside on the end user mobile device in an IPv6-only mobile network, allowing mobile network providers to roll out IPv6 for their users *and* support IPv4-only applications on mobile devices (see Figure 15 on page 254).

Figure 15: 464XLAT Wireless Flow



To configure the PLAT on the MX Series router, you create a NAT rule that uses the PLAT IPv6 prefix for the destination address and destination prefix and uses the NAT translation type **stateful-nat464**. For the source address and CLAT prefix in the NAT rule, identify the IPv6 prefix for the CLAT. The NAT rule must specify a NAT pool that the PLAT uses for converting the private IPv4 source address to a public IPv4 address.

Benefits of 464XLAT

- No need to maintain an IPv4 transit network
- No need to assign additional public IPv4 addresses

RELATED DOCUMENTATION

Configuring 464XLAT Provider-Side Translater for IPv4 Connectivity Across IPv6-Only Network | 255

Configuring 464XLAT Provider-Side Translater for IPv4 Connectivity Across IPv6-Only Network

Starting in Junos OS Release 17.1R1, you can configure a 464XLAT Provider-Side Tranlator (PLAT). This is supported only on MS-MICs and MS-MPCs. 464XLAT provides a simple and scalable technique for an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. 464XLAT only suports IPv4 in the client-server model, so it does not support IPv4 peer-to-peer communication or inbound IPv4 connections.

The following restrictions apply when configuring the PLAT:

- An **overload-pool** cannot be configured in the NAT rule.
- Different terms in the NAT rule cannot have the same **destination-prefix**.

To configure the PLAT:

1. Configure a NAT pool NAT pool that the PLAT uses for converting the private IPv4 source address to a public IPv4 address. See "Configuring Pools of Addresses and Ports for Network Address Translation Overview" on page 103.

2. Configure a name for a NAT rule.

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

3. Configure a match direction for the rule. See "Configuring Match Direction for NAT Rules" on page 108.

4. Configure the IPv6 source address prefix. This must be the CLAT IPv6 prefix or contain the CLAT IPv6 prefix.

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

5. Configure the IPv6 destination address prefix, which must have a length of /96. This is the PLAT destination IPv6 IP prefix.

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

6. Specify the NAT pool that the PLAT uses for converting the private IPv4 source address to a public IPv4 address.

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

7. Specify the CLAT IPv6 source prefix.

```
[edit services nat rule rule-name term term-name then translated]
user@host# set clat-prefix clat-prefix
```

8. Configure the IPv6 destination prefix, which must have a length of /96. This is the PLAT destination IPv6 IP prefix.

```
[edit services nat rule rule-name term term-name then translated]
user@host# set destination-prefix destination-prefix
```

9. Configure the translation type as stateful NAT464.

```
[edit services nat rule rule-name term term-name then translated]
user@host# set translation-type stateful-nat464
```

10. Enable address pooling paired (APP).

```
[edit services nat rule rule-name term term-name then translated]
user@host# set address-pooling paired.
```

11. Assign the NAT rule to a service set.

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

RELATED DOCUMENTATION

- 464XLAT Overview | 253

CHAPTER 13

Reducing Traffic and Bandwidth Requirements Using Port Control Protocol

IN THIS CHAPTER

Port Control Protocol Overview

Port Control Protocol (PCP) provides a way to control the forwarding of incoming packets by upstream devices, such as NAT44 and firewall devices, and a way to reduce application keepalive traffic. PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICs. Starting in Junos OS Release 17.4R1, PCP for NAPT44 is also supported on the MS-MPC and MS-MIC. Starting in Junos 20.2R1, PCP for CGNAT DS-Lite services are supported for Next Gen Services.Starting in Junos OS Release 18.2R1, PCP on the MS-MPC and MS-MIC supports DS-Lite. In Junos OS Release 18.1 and earlier releases, PCP on the MS-MPC and MS-MIC does not support DS-Lite.

PCP is designed to be implemented in the context of both Carrier-Grade NATs (CGNs) and small NATs (for example, residential NATs). PCP enables hosts to operate servers for a long time (as in the case of a webcam) or a short time (for example, while playing a game or on a phone call) when behind a NAT device, including when behind a CGN operated by their ISP. PCP enables applications to create mappings from an external IP address and port to an internal IP address and port. These mappings are required for successful inbound communications destined to machines located behind a NAT or a firewall. After a mapping for incoming connections is created, remote computers must be informed about the IP address and port for the incoming connection. This is usually done in an application-specific manner.

Junos OS supports PCP version 2 and version 1.

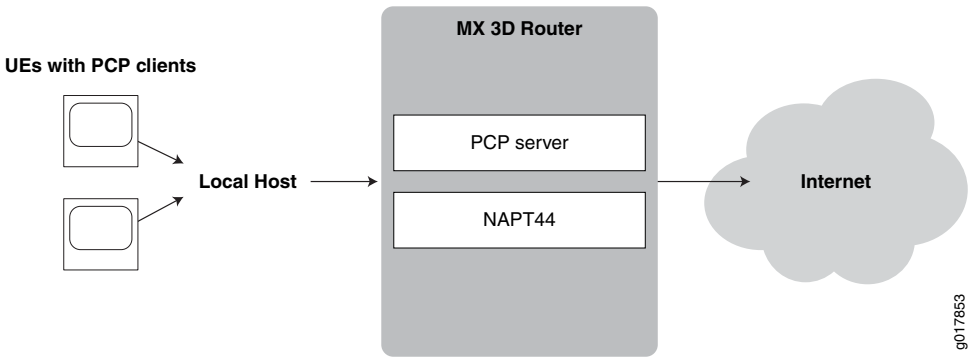
PCP consists of the following components:

- PCP client—A host or gateway that issues PCP requests to a PCP server in order to obtain and control resources.
- PCP server—Typically a CGN gateway or co-located server that receives and processes PCP requests

Junos OS enables configuring PCP servers for mapping flows using NAPT44 capabilities such as port forwarding and port block allocation. Flows can be processed from these sources:

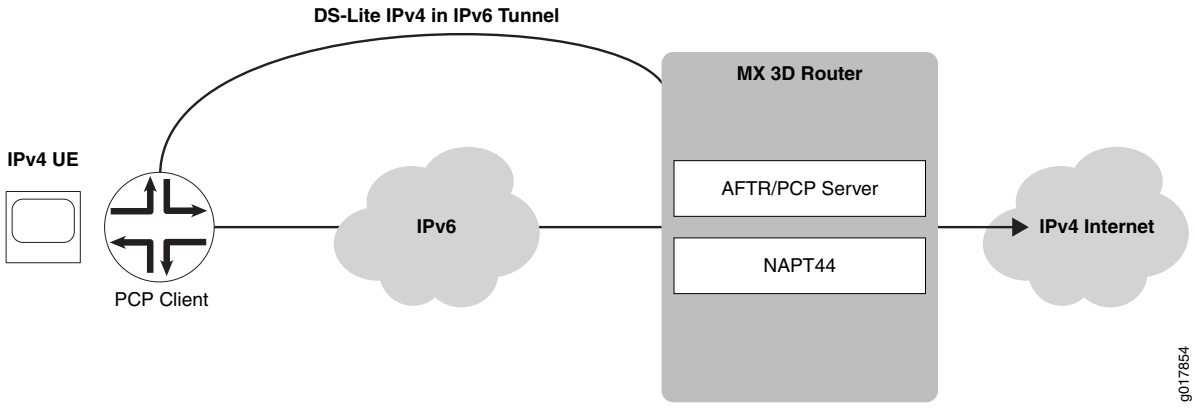
- Traffic containing PCP requests received directly from user equipment, as shown in Figure 16 on page 259.

Figure 16: Basic PCP NAPT44 Topology



- Mapping of traffic containing PCP requests added by a router functioning as a DS-Lite softwire initiator (B4). This mode, known as *DS-Lite plain mode*, is shown in Figure 17 on page 259.

Figure 17: PCP with DS-Lite Plain Mode



NOTE: Junos OS does not support deterministic port block allocation for PCP-originated traffic.

Benefits of Port Control Protocol

Many NAT-friendly applications send frequent application-level messages to ensure their sessions are not being timed out by a NAT device. PCP is used to:

- Reduce the frequency of these NAT keepalive messages
- Reduce bandwidth on the subscriber's access network
- Reduce traffic to the server
- Reduce battery consumption on mobile devices

Port Control Protocol Version 2

Starting with Junos OS Release 15.1, Port Control Protocol (PCP) version 2 is supported, which is in compliance with RFC 6887. PCP provides a way to control the forwarding of incoming packets by upstream devices, such as NAT44, and firewall devices, and a way to reduce application keep-alive traffic. PCP version 2 supports nonce authentication. PCP allows applications to create mappings from an external IP address and port to an internal IP address and port. A nonce payload prevents a replay attack and it is sent by default unless it is explicitly disabled.

Client nonce verification for version 2 map requests (for refresh or delete) requires that the nonce received in the original map request that causes the PCP mapping to be created is preserved. The version of the initial request that enables the mapping to be created is also preserved. This behavior of saving the nonce and version parameters denotes that 13 bytes per PCP mapping are used. This slight increase in storage space is not significant when matched with the current memory usage of a system for a single requested mapping (taking into account the endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF) that are created along with it). In a customer deployment, PCP causes EIM and EIF mappings to represent a fraction of all such mappings.

Until Junos Release 15.1, services PICs support PCP servers on Juniper Networks routers in accordance with PCP draft version 22 with version 1 message encoding. With PCP being refined from the draft version as defined in *Port Control Protocol (PCP) draft-ietf-pcp-base-22 (July 2012 expiration)* to a finalized, standard version as defined in RFC 6887 -- Port Control Protocol (PCP), the message encoding changed to version 2 with the addition of a random nonce payload to authenticate peer and map requests as necessary. Version 1 does not decode messages compliant with version 2 format and nonce authentication is not supported. In a real-word network environment, with customer premises equipment (CPE) devices increasingly supporting version 2 only, it is required to parse and send version 2 messages. Backward compatibility with version 1-supporting CPE devices is maintained (version negotiation is part of the standard) and authenticates request nonce payload packets when v2 messages are in use.

The output of the **show services pcp statistics** command contains the PCP unsupported version field, which is incremented to indicate whenever the version is not 1 or 2. A new field, PCP request nonce does not match existing mapping, is introduced to indicate the number of PCP version 2 requests that were ignored because the nonce payload did not match the one recorded in the mapping (authentication failed). If version 2 is in use, the client nonce is used for authentication.

Release History Table

Release	Description
20.2R1	Starting in Junos 20.2R1, PCP for CGNAT DS-Lite services are supported for Next Gen Services.
18.2R1	Starting in Junos OS Release 18.2R1, PCP on the MS-MPC and MS-MIC supports DS-Lite.
17.4R1	Starting in Junos OS Release 17.4R1, PCP for NAPT44 is also supported on the MS-MPC and MS-MIC.
15.1	Starting with Junos OS Release 15.1, Port Control Protocol (PCP) version 2 is supported, which is in compliance with RFC 6887.

RELATED DOCUMENTATION

Configuring Port Control Protocol | **261**

Configuring Port Control Protocol

IN THIS SECTION

This topic describes how to configure port control protocol (PCP). PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICs. Starting in Junos OS Release 17.4R1, PCP for NAPT44 is also supported on the MS-MPC and MS-MIC. Starting in Junos OS Release 18.2R1, PCP on the MS-MPC and MS-MIC supports DS-Lite. In Junos OS Release 18.1 and earlier releases, PCP on the MS-MPC and MS-MIC does not support DS-Lite. Starting in Junos OS release 20.2R1 PCP is supported on the MX-SPC3 security services card for CGNAT services.

Perform the following configuration tasks:

Configuring PCP Server Options

1. Specify a PCP server name.

```
user @host# edit services pcp server server-name
```

2. Set the IPv4 or IPv6 addresses of the server. For PCP DS-Lite, the **ipv6-address** must match the address of the AFTR (Address Family Transition Router or softwire concentrator).

> **NOTE:** Starting in Junos OS Release 18.2R1, PCP on the MS-MPC and MS-MIC supports DS-Lite. In Junos OS Release 18.1 and earlier releases, PCP on the MS-MPC and MS-MIC does not support DS-Lite.

```
[edit services pcp server server-name]
user @host# set ipv6-address ipv6-address
```

or

```
[edit services pcp server server-name]
user @host# set ipv4-address ipv4-address
```

3. For PCP DS-Lite, provide the name of the DS-Lite softwire concentrator configuration.

```
[edit services pcp server server-name]
user @host# set softwire-concentrator softwire-concentrator-name
```

4. Specify the minimum and maximum mapping lifetimes for the server.

```
[edit services pcp server server-name]
user @host# set mapping-lifetime-minimum mapping-lifetime-min
user @host# set mapping-lifetime-maximum mapping-lifetime-max
```

5. Specify the time limits for generating short lifetime or long lifetime errors.

```
[edit services pcp server server-name]
```

```
user @host# set short-lifetime-error short-lifetime-error
user @host# set long-lifetime-error long-lifetime-error
```

6. (Optional)—Enable PCP options on the specified PCP server. The following options are available—**third-party** and **prefer-failure**. The third-party option is required to enable third-party requests by the PCP client. DS-Lite requires the **third-party** option. The **prefer-failure** option requests generation of an error message when the PCP client requests a specific IP address/port that is not available, rather than assigning another available address from the NAT pool. If **prefer-failure** is not specified NAPT44 assigns an available address/port from the NAT pool based on the configured NAT options.

```
[edit services pcp server server-name]
user @host# set pcp-options third-party
user @host# set pcp-options prefer-failure
```

7. (Optional)—Specify which NAT pool to use for mapping.

```
[edit services pcp server server-name]
user @host# set nat-options pool-name1 <poolname2...>
```

NOTE: When you do not explicitly specify a NAT pool for mapping, the Junos OS performs a partial rule match based on source IP, source port, and protocol, and the Junos OS uses the NAT pool configured for the first matching rule to allocate mappings for PCP.

You *must* use explicit configuration in order to use multiple NAT pools.

For the MX-SPC3 security services card and Next Gen Services, the **nat-options** statement supports only one pool name to attach to a PCP server.

8. (Optional)—Configure the maximum number of mappings per client. The default is 32 and maximum is 128.

```
[edit services pcp server server-name]
user @host# set max-mappings-per-client max-mappings-per-client
```

Configuring a PCP Rule

A PCP rule has the same basic options as all service set rules:

- A **term** option that allows a single rule to have multiple applications.

  A term is not required when running the MX-SPC3 security services card for Next Gen Services.
- A **from** option that identifies the traffic that is subject to the rule.
- A **then** option that identifies what action is to be taken. In the case of a PCP rule, this option Identifies the pcp server that handles selected traffic

1. Go to the **[edit services pcp rule *rule-name*]** hierarchy level and specify **match-direction** input.

   ```
   user @host# edit services pcp rule rule-name
   user @host# set match-direction input
   ```

2. Go to the **[edit services pcp rule *rule-name* term *term-name*]** hierarchy level and provide a term name.

   ```
   user @host# edit term term-name
   ```

   This step is not required when running the MX-SPC3 security services card for Next Gen Services.

3. (Optional)—Provide a **from** option to filter the traffic to be selected for processing by the rule. When you omit the **from** option, all traffic handled by the service set's service interface is subject to the rule. The following options are available at the **[edit services pcp rule *rule-name* term *term-name* from]** hierarchy level:

   application-sets *set-name* —Traffic for the application set is processed by the PCP rule.

   This step is not required when running the MX-SPC3 security services card for Next Gen Services.

   applications [*application-name*]—Traffic for the application is processed by the PCP rule.

   This option is not required when running the MX-SPC3 security services card for Next Gen Services.

   destination-address *address* <except>—Traffic for the destination address or prefix is processed by the PCP rule. If you include the **except** option, traffic for the destination address or prefix is *not* processed by the PCP rule.

   destination-address-range high *maximum-value* low *minimum-value* <except>—Traffic for the destination address range is processed by the PCP rule. If you include the **except** option, traffic for the destination address range is *not* processed by the PCP rule.

   destination-port high *maximum-value* low *minimum-value*—Traffic for the destination port range is processed by the PCP rule.

destination-prefix-list ***list-name*** **<except>**—Traffic for a destination address in the prefix list is processed by the PCP rule. If you include the **except** option, traffic for a destination address in the prefix list is *not* processed by the PCP rule.

source-address ***address*** **<except>**—Traffic from the source address or prefix is processed by the PCP rule. If you include the **except** option, traffic from the source address or prefix is *not* processed by the PCP rule.

source-address-range high ***maximum-value*** **low** ***minimum-value*** **<except>**—Traffic from the source address range is processed by the PCP rule. If you include the **except** option, traffic from the source address range is *not* processed by the PCP rule.

source-prefix-list ***list-name*** **<except>**—Traffic from a source address in the prefix list is processed by the PCP rule. If you include the **except** option, traffic from a source address in the prefix list is *not* processed by the PCP rule.

4. Set the **then** option to identify the target PCP server.

```
[edit services pcp rule rule-name term term-name]
user @host# set then pcp-server server-name
```

Configuring a NAT Rule

To configure a NAT rule:

1. Configure the NAT rule name and the match direction.

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

2. Specify the NAT pool to use:

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

3. Configure the translation type.

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

4. If you are using PCP with IPv4-to-IPv4 NAT or with DS-Lite, configure endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF).

```
[edit services nat rule-name term term-name then translated]
user@host# set mapping-type endpoint-independent
user@host# set filtering-type endpoint-independent
```

> **NOTE:** The PCP mappings are not created if you do not configure EIM and EIF with PCP for IPv4-to-IPv4 NAT or for DS-Lite.

Configuring a Service Set to Apply PCP

To use PCP, you must provide the rule name (or name of a list of rule names) in the **pcp-rule *rule-name*** option.

1. Go to the **[edit services service-set *service-set-name*** hierarchy level.

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

2. If this is a new service set, provide basic service set information, including interface information and any other rules that may apply.

3. Specify the name of the PCP rule or rule list used to send traffic to the specified PCP server.

```
[edit services service-set service-set-name ]
user @host# set pcp-rule rule-name | rule-listname
```

> **NOTE:** Your service set must also identify any required **nat-rule** and **softwire-rule**.

SYSLOG Message Configuration

A new syslog class, configuration option, **pcp-logs**, has been provided to control PCP log generation. It provides the following levels of logging:

- **protocol**—All logs related to mapping creation, deletion are included at this level of logging.

- **protocol-error**—-All protocol error related logs (such as mapping refresh failed, PCP look up failed, mapping creation failed). are included in this level of logging.
- **system-error**—Memory and infrastructure errors are included in this level of logging.

SEE ALSO

Port Control Protocol Overview | 258

Example: Configuring Port Control Protocol with NAPT44

IN THIS SECTION

NOTE: PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP for NATP44 is also supported on the MS-MPC and MS-MIC.

Requirements

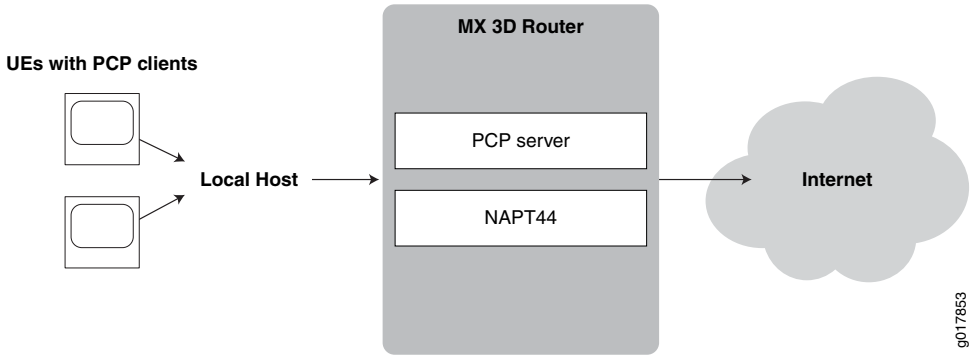
Hardware Requirements

- UEs with PCP clients.
- An MX 3D Router with an MS-DPC services PIC.
- Software Requirements
- Junos OS 13.2
- Layer-3 Services Package

Overview

An ISP wants to enable UEs with PCP clients to maintain connections to servers without timing out. The PCP clients generate PCP requests for the type and duration of the connection they require. Connections may be of a long duration, such as applications using a webcam, or a shorter duration, such as online games. An MX 3D router provides a PCP server to interpret PCP client requests, and NAPT44. Figure 18 on page 268 shows the basic topology for this example.

Figure 18: PCP with NAPT44



PCP 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 chassis fpc 2 pic 0 adaptive-services service-package layer-3
set interfaces sp-2/0/0 services-options inactivity-timeout 180 cgn-pic
set interfaces sp-2/0/0 unit 0 family inet
set interfaces xe-3/2/0 unit 0 family inet service input service-set sset_0
set interfaces xe-3/2/0 unit 0 family inet service output service-set sset_0
set interfaces xe-3/2/0 unit 0 family inet address 30.0.0.1/24
set interfaces xe-5/0/0 unit 0 family inet address 25.0.0.1/24
set services nat pool pcp-pool address 44.0.0.0/16
set services nat pool pcp-pool port automatic random-allocation address-allocation round-robin
set services nat pool pcp-pool address-allocation round-robin
set services nat rule pcp-rule match-direction input
set services nat rule pcp-rule term t0 then translated source-pool pcp-pool translation-type napt-44
set services nat rule pcp-rule term t0 then translated mapping-type endpoint-independent filtering-type
    endpoint-independent
set services nat rule pcp-rule term t0 then translated mapping-type endpoint-independent filtering-type
    endpoint-independent
```

```
set services pcp server pcp-s1 ipv4-address 124.124.124.122
set services pcp server pcp-s1 mapping-lifetime-minimum 600 mapping-lifetime-maximum 86500
set services pcp server pcp-s1 short-lifetime-error 120 long-lifetime-error 1200
set services pcp server pcp-s1 max-mappings-per-client 128 pcp-options third-party prefer-failure
set services service-set sset_0 pcp-rules r1
set services service-set sset_0 nat-rules pcp-rule
set services service-set sset_0 interface-service service-interface sp-2/0/0.0
```

Chassis Configuration

Step-by-Step Procedure

To configure the service PIC (FPC 2 Slot 0) with the Layer 3 service package:

1. Go to the [edit chassis] hierarchy level.

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

2. Configure the Layer 3 service package.

```
[edit chassis]
user@host# set fpc 2 pic 0 adaptive-services service-package layer-3
```

Results

`user@host#` **show chassis fpc 2 pic 0**

```
pcp-rules pcp-napt44-rule;
nat-rules pcp-rule;
interface-service {
    service-interface sp-2/0/0.0;
}
```

Interface Configuration

Step-by-Step Procedure

1. Configure the services MS-DPC.

```
user@host# set interfaces sp-2/0/0 services-options inactivity-timeout 180 cgn-pic
user@host# set interfaces sp-2/0/0 unit 0 family inet
```

2. Configure the customer-facing interface used for NAT and PCP services.

```
user@host# set interfaces xe-3/2/0 unit 0 family inet service input service-set sset_0
user@host# set interfaces xe-3/2/0 unit 0 family inet service output service-set sset_0
user@host# set interfaces xe-3/2/0 unit 0 family inet address 30.0.0.1/24
```

3. Configure the Internet-facing interface.

```
user@host# set interfaces xe-5/0/0 unit 0 family inet address 25.0.0.1/24
```

Results

`user@host#`

```
sp-2/0/0 {
    services-options {
        inactivity-timeout 180;
        cgn-pic;
    }
    unit 0 {
        family inet;
    }
}
xe-3/2/0 {
    unit 0 {
        family inet {
            service {
                input {
                    service-set sset_0;
                }
                output {
                    service-set sset_0;
                }
            }
            address 30.0.0.1/24;
        }
    }
}
xe-5/0/0 {
    unit 0 {
        family inet {
            address 25.0.0.1/24;
        }
```

```
    }
}
```

NAT Configuration

Step-by-Step Procedure

1. Go the **[edit services nat]** hierarchy.

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

2. Configure a NAT pool called **pcp-pool**.

   ```
   [edit services nat]
   user@host# set pool pcp-pool address 44.0.0.0/16
   user@host# set pool pcp-pool port automatic random-allocation
   user@host# set pool pcp-pool address-allocation round-robin
   ```

3. Configure a NAT rule called **pcp-rule**.

   ```
   [edit services nat]
   user@host# set rule pcp-rule term t0 then translated source-pool pcp-pool translation-type napt-44
   user@host# set rule pcp-rule term t0 then translated mapping-type endpoint-independent filtering-type
     endpoint-independent
   ```

Results

`user@host#` **show services nat**

```
pool pcp-pool {
    address 44.0.0.0/16;
    port {
        automatic {
            random-allocation;
        }
    }
    address-allocation round-robin;
}
rule pcp-rule {
    match-direction input;
    term t0 {
```

```
        then {
            translated {
                source-pool pcp-pool;
                translation-type {
                    napt-44;
                }
                mapping-type endpoint-independent;
                filtering-type {
                    endpoint-independent;
                }
            }
        }
    }
}
```

PCP Configuration

Step-by-Step Procedure

To configure the PCP server and PCP rule options.

1. Go to the **edit services pcp** hierarchy level for server **pcp-s1**

   ```
   user@host# edit services pcp server pcp-s1
   ```

2. Configure the PCP server options.

   ```
   [edit services pcp server pcp-s1]
   user@host# set ipv4-address 124.124.124.122
   user@host# set mapping-lifetime-minimum 600
   user@host# set mapping-lifetime-maximum 86500
   user@host# set short-lifetime-error 120
   user@host# set long-lifetime-error 1200
   user@host# set max-mappings-per-client 128
   user@host# set pcp-options third-party prefer-failure
   ```

3. Create the PCP rule.

   ```
   [edit services pcp rule pcp-napt44-rule
   user@host# edit rule pcp-napt44-rule
   ```

4. Configure the PCP rule options.

```
[edit services pcp rule pcp-napt44-rule]
user@host# set match-direction input
user@host# set term t0 then pcp-server pcp-s1
```

Results

`user@host#` **show services pcp**

```
server pcp-s1 {
    ipv4-address 124.124.124.122;
    mapping-lifetime-minimum 600;
    mapping-lifetime-maximum 86500;
    short-lifetime-error 120;
    long-lifetime-error 1200;
    max-mappings-per-client 128;
    pcp-options third-party prefer-failure;
}
rule pcp-napt44-rule {
    match-direction input;
    term t0 {
        then {
            pcp-server pcp-s1;
        }
    }
}
```

Service Set Configuration

Step-by-Step Procedure

1. Create a service set, **sset_0**, at the **edit services service-set** hierarchy level.

```
user@host# edit services service-set sset_0
```

```
service-set sset_0 {
    pcp-rules pcp-napt44-rule;
    nat-rules pcp-rule;
    interface-service {
        service-interface sp-2/0/0.0;
    }
}
```

2. Identify the NAT rule associated with the service set.

```
[edit services service-set sset_0]
user@host# set nat-rules pcp-rule
```

3. Identify the PCP rule associated with the service set.

```
[edit services service-set sset_0]
user@host# set pcp-rules r1
```

4. Identify the service interface associated with the service set.

```
[edit services service-set sset_0]
user@host# set interface-service service-interface sp-2/0/0.0
```

Results

`user@host# show`

```
pcp-rules pcp-napt44-rule;
nat-rules pcp-rule;
interface-service {
    service-interface sp-2/0/0.0;
}
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, PCP for NATP44 is also supported on the MS-MPC and MS-MIC.

CHAPTER 14

Automatically Assigning Ports Using Secured Port Block Allocation

IN THIS CHAPTER

Secured Port Block Allocation for NAPT44 and NAT64 Overview

Secured port block allocation ensures that when a subscriber requires a port to be assigned for the first time, a block of ports are allocated to the particular user. Here, a subscriber is defined uniquely as a private IP address and service set ID. Because the subscriber has a block of ports assigned to it, all subsequent requests from this subscriber use ports from the assigned block. A new port block is allocated when the current active block is exhausted, or after the active port block timeout interval has expired. You can configure the maximum number of blocks allocated to a user. This behavior of allocation of NAT ports in blocks is different from the traditional NAT utility where the request for a port allocates a single port and not a group of ports in a block.

You can use the secured port block allocation mechanism to allocate ports in blocks for NAPT44 (translation of an IPv4 address to an IPv4 address) and NAT64 (translation of an IPv6 address to an IPv4 address) types. By using secured port block allocation, the port usage might be a little inefficient, depending on traffic patterns. Secured port block allocation is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS release 14.2R2, secured port block allocation is supported on MX series routers with MS-MPCs and MS-MICs.

Starting with Junos OS Release 15.1, in an environment in which Junos Address Aware (carrier-grade NAT) is employed, service providers or carrier operators can monitor and track the consumption of resources and types of services being utilized by subscribers or users in an easier and effective manner by using system logging messages recorded for the allocation of ports to clients. By using IP addresses in RADIUS or DHCP logs, evaluation of the logs is performed to analyze an determine the services usage and bandwidth

consumption by subscribers. With carrier-grade NAT, because IP addresses are shared by multiple subscribers, examining logs to track the IP addresses and ports that are part of the system logs might be time-consuming and difficult. Also, because ports are allocated and released at frequent intervals depending on the logging-in and closure of subscriber sessions, a large number of logs are triggered for every port allocation and deallocation. As a result, excessive syslogs render it cumbersome to archive and correlate the logs to identify a subscriber. You can now allocate ports in blocks, which reduces the amount of syslogs considerably.

Benefits of Secured Port Block Allocation

- Reduces the effort to correlate logs to a subscriber
- Reduces the number of logs

Release History Table

Release	Description
14.2R2	Starting in Junos OS release 14.2R2, secured port block allocation is supported on MX series routers with MS-MPCs and MS-MICs.

Interim Logging for Secured Port Block Allocation

With port block allocation we generate one syslog log per set of ports allocated for a subscriber. These logs are UDP based and can be lost in the network, particularly for long-running flows. Interim logging triggers re-sending the above logs at a configured interval for active blocks that have traffic on at least one of the ports of the block. Depending on your network topology, you can set the interval for the port block allocation logs based on the period of the archive so that at least one log per port block (for an active flow) in each archive is present.

To configure the interim logging interval at the services interface level, which applies to all the NAT pools on that ms- interface, include the **pba-interim-logging-interval *seconds*** statement at the **[edit interfaces ms-fpc/pic/port services-options]** hierarchy level. The **pba-interim-logging-interval** option is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. The **pba-interim-logging-interval** option is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 14.2R2.

Starting in Junos OS Release 15.1R1, you can also configure the interim logging interval at a NAT pool level. This capability is supported only on MX Series routers with MS-MPCs and MS-MICs. To configure the interim logging interval at a NAT pool level, include the **interim-logging-interval *seconds*** statement at the **[edit services nat pool *pool-name* port secured-port-block-allocation]** hierarchy level. You can specify a value from 0 through 86400 seconds for the interim logging frequency.

Benefits of Iterim Logging

- Enables you to identify the currently used port blocks
- Eliminates the need to search and analyze archived logs to identify the internal host that is using the external IP address and port

Release History Table

Release	Description
15.1R1	Starting in Junos OS Release 15.1R1, you can also configure the interim logging interval at a NAT pool level.

RELATED DOCUMENTATION

Configuring NAT Session Logs | 361

Secured Port Block Allocation for NAPT44 and NAT64 Overview | 275

Guidelines for Configuring Interim Logging for Secured Port Block Allocation

Observe the following guidelines when you configure the interim logging interval for secured port block allocation:

- Interim logging is enabled only when the interim logging functionality is configured. The **pba-interim-logging-interval** statement that you can configure at the **[edit interfaces *ms-fpc/pic/port* services-options]** hierarchy level of an ms-interface is provided for backward compatibility. The **pba-interim-logging-interval** option is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. The **pba-interim-logging-interval** option is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 14.2R2.

  The **interim-logging-interval** statement that is available for configuration on the MS-MPC and MS-MIC starting in Junos OS release 15.1R1 provides interim logging for a specific NAT pool.

- If you configure the interim logging capability to be applicable to all PBA pools residing on that particular services interface and the interim logging capability for a specific PBA pool, the NAT pool-specific interval takes precedence over the services interface specific interval. For port blocks allocated from other PBA pools for which interim logging interval at the NAT pool-level is not configured, the logging interval value as configured at the ms- interface-level applies.
- The default value is zero, which denotes no interim logging message is generated.

- Interim logs are sent any time after the configured period of time in seconds. The time-difference is not fixed between the logging intervals of two logs.
- Interim logs are generated for port blocks (both active and inactive) that contain at least one port in use by a flow which has traffic. No timer controls run on the port blocks to generate the logs. When a packet is received on a flow, the validation is performed to generate an interim log. If the conditions are satisfied, an interim log is generated for that port block. Interim logs are not generated for deleted port blocks.
- The interim log contains the timestamp of the port block creation in hexadecimal format (when local time is set, the hexadecimal value provides the time in UTC format).
- The conversion of the timestamp to UTC format can be performed in the external syslog server as necessary.
- In certain scenarios, it is possible that the timestamp in hexadecimal value and the actual timestamp in ALLOC messages differ by a couple of seconds. This behavior occurs because the syslog mechanism contains a slight difference when it reads the time (as seen in PORT_BLOCK_ALLOC syslog) and the time at which NAT application reads the time (to update the ALLOC time in the subscriber context). The interim system log displays the ALLOC time retrieved from the subscriber context.
- Because these logs are generated on CPU computation and in the fast path, a slight impact might be observed with fast path performance only when a generation of the log occurs.
- Port block creation timestamp in hexadecimal is saved in the JSERVICES_NAT_PORT_BLOCK_RELEASE message, even if interim logging is not present.
- If you define the logging interval when traffic flow is in progress, this functionality takes effect on existing and new flows. You need not reboot the MIC or activate and deactivate the service set.
- If the flows or subscribers are timing out, it denotes that no new packets or traffic flows are seen for this 5-tuple data or for that particular subscriber. In such a case, interim logs are not generated.
- If the interim-logging interval is lower than the inactivity-timeout of the flow, interim logs are not observed when the flow is timing out and the interim-logging interval has elapsed. If the interim-logging interval is lower than the subscriber-timeout value, interim logs are not observed when the subscriber is timing out and the interim-logging interval has elapsed. For example, if the inactivity-timeout is configured to 2500 seconds and the interim-logging is configured as 1800 seconds, when the flow is timing out, there is a point in time when 1800 seconds has elapsed since the last packet was seen on this flow and no interim log is generated in this case.
- The interim logs are recorded for those pools that have PBA configured. If pools exist without the PBA configuration present on the service network processing unit (NPU), interim logs are not saved even if you enable the interim logging functionality.
- You can configure only a range of values for the interval at which the logs need to be generated, such as 0, [1800, 86400].
- You can enable the generation of syslogs by using the *syslog* statement at the **[edit system]** and **[edit services service-sets *service-set name* nat rule *rule-name* term *term-name* then]** hierarchy levels that

contain the NAT rules with PBA pools. Interim logs are not triggered if the recording of syslogs are not enabled on the system.

- We recommend that you configure the interim-logging interval to be higher than the inactivity timeout period for established flows. Also, we recommend that you configure the interim-logging interval to be higher than the subscriber-timeout value. When endpoint-independent mapping (EIM) is configured, the interim-logging interval must be higher than the sum of the address pooling paired (APP) timeout and EIM timeout values.
- Transmission of logs occurs in clear-text format similar to other log messages that the services PICs do not encrypt. It is assumed that the transport of logs and the positioning of the log collector are within a secured realm. Because the messages do not contain sensitive details such as username or passwords, the messages do not cause any security or reliability risks. Increased generation of log messages does not cause a possibility of a flood of logs because the frequency of logging can be configured, depending on the network topology, traffic levels, and your monitoring needs.
- The logs for PBA in the microkernel start with the prefix of ASP_*. These logs have been modified to start with the prefix of JSERVICES_*. The following are examples of system logs for PBA in the microkernel and with the Junos OS Extension-Provider packages installed and configured on the device.

  Microkernel: 1970-01-01 00:32:36 {nat64}[FWNAT]:ASP_NAT_PORT_BLOCK_ACTIVE: 2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f

  Junos OS Extension-Provider (eJunos): 1970-01-01 00:32:36 {nat64}[FWNAT]:JSERVICES_NAT_PORT_BLOCK_ACTIVE: 2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f

- Also, you can specify the interim logging interval per NAT pool instead of a global configuration per MS-PIC, based on whether you want the syslog settings to apply to all the NAT pools on a device or for a particular NAT pool. For NAT, the member interfaces must have the jservices-nat package configured. The JSERVICES_NAT_PORT_BLOCK_ACTIVE system logging message is generated when you configure interim logging for PBA. The following sample logs denote the log messages generated with the interim interval set as 1800 seconds. You can notice that the timestamp between consecutive interim logs is more than 1800 seconds.

```
1970-01-01 00:01:51 [FWNAT]:JSERVICES_NAT_PORT_BLOCK_ALLOC: 2001:0:0:0:0:0:0:2
-> 1.1.1.1:1050-1091
1970-01-01 00:32:36 {nat64}[FWNAT]:JSERVICES_NAT_PORT_BLOCK_ACTIVE:
2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f
1970-01-01 01:03:20 {nat64}[FWNAT]:JSERVICES_NAT_PORT_BLOCK_ACTIVE:
2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f
1970-01-01 01:34:04 {nat64}[FWNAT]:JSERVICES_NAT_PORT_BLOCK_ACTIVE:
2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f
```

```
1970-01-01 02:04:48 {nat64}[FWNAT]:JSERVICES_NAT_PORT_BLOCK_ACTIVE:
2001:0:0:0:0:0:0:2 -> 1.1.1.1:1050-1091 0x6f
```

- Starting in Junos OS release 19.3R1, when you configure a softwire prefix other than 128, all the JSERVICES_NAT_PORT_BLOCK logs now displays the prefixed B4 address. The following JSERVICES_NAT_PORT_BLOCK are modified:
  - JSERVICES_NAT_PORT_BLOCK_ALLOC
  - JSERVICES_NAT_PORT_BLOCK_RELEASE
  - JSERVICES_NAT_PORT_BLOCK_ACTIVE

  In earlier Junos OS releases, when a softwire prefix was configured, some of the B4 addresses displayed in the JSERVICES_NAT_PORT_BLOCK log were /128 addresses. For example, when a /56 prefix was configured, the port block syslog displayed the following B4 addresses:
  - The JSERVICES_NAT_PORT_BLOCK_ALLOC displayed the /128 B4 address of the first B4 which was allocated a port from a particular port block
  - The JSERVICES_NAT_PORT_BLOCK_RELEASE displayed the /128 B4 address of the last B4 which released its port back to the port block

RELATED DOCUMENTATION

Configuring NAT Session Logs | 361

Secured Port Block Allocation for NAPT44 and NAT64 Overview | 275

Guidelines for Configuring Secured Port Block Allocation

Keep the following points in mind when you configure secured PBA:

- Block size is not configurable at the NAT rule level.
- Increase in setup rate of sessions is not impacted when you configure secured PBA.
- If a block of a particular size is not available, an out-of-ports message is displayed and smaller-sized blocks are not allocated alternatively in such a scenario.
- Addresses in the pool using port-block-allocation method cannot be used in any other pool.
- Port range in the NAT pool must be contiguous.
- Preserve parity (Allocate ports with same parity as the original port) is not supported with block-allocation of ports.

- The limitation on the number of open sessions when the specified threshold is reached (for intrusion detection services) and the maximum number of blocks that can be allocated to a user address that is configured for secured PBA are independent functionalities.
- The functionality to preserve privileged port range after translation is not supported. The blocks are assigned from unprivileged port range (1024-65535). For ports in privileged range, port block allocation method is not applicable.
- Port usage efficiency is lower when port-block allocation is enabled. PBA does not use ports from 0-1023 of a NAT IP address.
- If you configure the automatic port assignment method, which enables sequential assignment of ports, the port range from 1024 through 65535 is available for allocation to users.
- Port blocks can start at any start port that you can configure.
- The number of ports used is dependent on the block size and the rest of the ports are not be used.
- An overloaded pool, which indicates an address pool that can be used if the source pool becomes exhausted, is not supported with secured PBA.
- NAT IP addresses of PBA pool must not overlap with any other pool. Although a validation is not performed to identify whether any overlapping pools exist, you must ensure that the addresses of a pool that is used for PBA are not used in other pools. This condition is because some of the users require the overload pool to use the same IP addresses as that of NAT IP addresses, but a different port range of PBA pool to support the address pooling paired (APP) functionality.
- The block-size is fixed per NAT pool and is configurable at the NAT pool level. Multiple port blocks can be allocated to a private IP address.
- You can configure the maximum number of blocks per pool per subscriber by including the **max-blocks-per-user *max-blocks*** statement at the **[edit services nat pool pool-name port secured-port-block-allocation]** hierarchy level. If a subscriber matches two pools, that particular user can be allocated a maximum of port blocks that equals the sum of the maximum number of port blocks for each pool for that subscriber. New requests for NAT ports arrive from the current active block only.
- Ports can be allocated randomly from the current active block, which specifies whether ports should be allocated sequentially or randomly within the port block.
- A block is active for a timeout interval that you can define by including the **active-block-timeout *timeout-seconds*** at the **[edit services nat pool pool-name port secured-port-block-allocation]** hierarchy level. After the timeout period, a new block is allocated even if ports are available in the active block. The default timeout of an active block is 120 seconds. When you configure it as 0 (infinite), the active block transitions to inactive only when it runs out of ports and a new block is allocated.
- If the maximum number of blocks of blocks is exceeded, and a new request is received, the active block is moved to a block that contains available ports. Any non-active block without any ports in use is freed to NAT pool.
- In addition to tracking port blocks assigned to each private IP address, actual ports in use are also computed and maintained. This metric is used to calculate port usage efficiency.

- A syslog message is generated for each block allocation and release. The format of the message is similar to the messages recorded for individual port allocation and release.
- Session setup rate is the same or slightly improved than the existing non-block allocation setup rate. NAT pool using block-port allocation method can have partial port ranges. If the address is used for port forwarding, those ports can be removed from the pool port range. You can configure partial port ranges by using the **port range low *minimum-value* high *maximum-value* random-allocation** statement at the **[edit services nat pool nat-pool-name]** hierarchy level. Port block allocation works in the same manner as NAPT44 for TCP, UDP, and ICMP traffic.
- Randomness can be achieved by allocating ports randomly within the block and changing active block periodically. The block of ports do not contain random ports (ports within the block are sequential). This capability is supported with aggregated multiservices (ams) interfaces.
- The starting port number is calculated differently in the microkernel and in Junos OS Extension-Provider packages. In the microkernel, the starting or first port is the nearest multiple of the block size after 1023. In that implementation, more ports are wasted because ports are wasted at the beginning and the end of the port range depending on the block size. In Junos OS Extension-Provider packages, the start port of a block is not restricted to a multiple of the block size. The start port can start at the lower boundary of the range of the port configured.

RELATED DOCUMENTATION

Configuring NAT Session Logs | 361

Secured Port Block Allocation for NAPT44 and NAT64 Overview | 275

Configuring Secured Port Block Allocation

Secured port block allocation is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Secured port block allocation is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 14.2R2. To configure secured port block allocation:

1. At the **[edit services nat pool *nat-pool-name*]** hierarchy level, create a pool.

   ```
   user@host# edit services nat pool poolname
   ```

   For example:

   ```
   user@host# edit services nat pool pba-pool1
   ```

2. Define the range of addresses to be translated, specifying the upper and lower limits of the range or an address prefix that describes the range.

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

Or

```
user@host# set address address-prefix
```

For example:

```
[edit services nat pool pba-pool1]
user@host# set address 203.0.113.0/24
```

3. Define the range of ports to be used in the translation, or use automatic port assignment by the Junos OS. You can optionally specify random assignment of ports; sequential assignment is the default.

```
[edit services nat pool nat-pool-name]
user@host# set port range low address high address random
```

Or

```
user@host# set port automatic random-allocation
```

For example:

```
[edit services nat pool pba-pool1]
user@host# set port range low 256 high 511 random
```

Or

```
[edit services nat pool pba-pool1]
user@host# set port automatic random-allocation
```

NOTE: When you configure a port range, the range should be a multiple of the port block-size value (see Step 4). When the **nat pool port range** is *not* a multiple of the port **block-size** value, the number of ports or port-blocks that are effectively available for use is less than the configured number of ports and port-blocks.

When you configure automatic assignment of ports, the available port range for allocation is 1024 through 65535. Automatic allocation can result in no ports being available for use. Use the **show services nat pool** command on the Routing Engine after you configure the port block allocation method to determine the number of ports and port blocks available for allocation to users.

4. Configure secured port block allocation. Specify **active-block-timeout**, **block-size**, and **max-blocks-per-address**, or accept the default values for those options.

```
[edit services nat pool nat-pool-name]
user@host# set secured-port-block-allocation active-block-timeout active-block-timeout block-size block-size
    max-blocks-per-address max-blocks-per-address
```

For example:

```
[edit services nat pool pba-pool1]
user@host# set secured-port-block-allocation active-block-timeout 120 block-size 256
    max-blocks-per-address 12
```

NOTE: In order for **secured-port-block-allocation** configuration changes to take effect, you must reboot the services PIC whenever you change any of the following **nat pool** options:

- ***nat-pool-name***
- **address** or **address-range**
- **port range**
- **port secured-port-block-allocation block-size**
- **port secured-port-block-allocation max-blocks-per-address**.
- **port secured-port-block-allocation active-block-timeout**.
- **from** hierarchy in the **nat rule**

NOTE: If you make any configuration changes related to a NAT pool that has secured port block allocation configured, you must delete the existing NAT address pool, wait at least 5 seconds, and then configure a new NAT address pool. We also strongly recommend that you perform this procedure if you make any changes to the NAT pool configuration, even when secured port block allocation is not configured.

NOTE: MS-MICs and MS-MPCs support up to a maximum of nine million port blocks per NPU. If your configuration exceeds this maximum supported number, one or more service sets might not be activated on that NPU.

RELATED DOCUMENTATION

Network Address Translation Configuration Overview | 101

CHAPTER 15

Connecting Specific Ports and Addresses Using Port Forwarding

IN THIS CHAPTER

Port Forwarding Overview

You can map an external IP address and port with an IP address and port in a private network. This mapping, called port forwarding, is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

Port forwarding allows the destination address and port of a packet to be changed to reach the correct host in a Network Address Translation (NAT) gateway. The translation facilitates reaching a host within a masqueraded, typically private, network, based on the port number on which the packet was received from the originating host. An example of this type of destination is the host of a public HTTP server within a private network. You can also configure port forwarding without translating a destination address. Port forwarding supports endpoint-independent mapping (EIM), endpoint-independent filltering (EIF), and address pooling paired (APP).

Port forwarding works only with the FTP application-level gateway (ALG), and has no support for technologies that offer IPv6 services over IPv4 infrastructure, such as IPv6 rapid deployment (6rd) and dual-stack lite (DS-Lite). Port forwarding supports only **dnat-44** and **twice-napt-44** on IPv4 networks.

Benefits of Port Forwarding

- Allows remote computers, such as public machines on the Internet, to connect to a non-standard port of a specific computer that is hidden within a private network.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Configuring Port Forwarding Without Destination Address Translation | 291

Configuring Port Forwarding for Static Destination Address Translation

You can configure destination address translation with port forwarding. Port forwarding allows the destination address and port of a packet to be changed to reach the correct host in a Network Address Translation (NAT) gateway. Port forwarding is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

To configure destination address translation with port forwarding:

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, **dest-pool** is used as the pool name and **192.0.2.2** as the address.

```
user@host# set pool dest-pool address 192.0.2.2
```

3. 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 **198.51.100.20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from destination-address 198.51.100.20
```

4. Configure the destination port range.

```
[edit services nat]
user@host# set rule rule-name match-direction match-direction term term-name from destination-port range
    high maximum-value low minimum-value
```

In the following example, the upper port range is **50** and the lower port range is **20**.

```
[edit services nat]
user@host# set rule rule-dnat44 match-direction input term t1 from destination-port range high 50 low 20
```

5. Go to the **[edit services nat rule *rule-name* term *term-name*]** hierarchy level.

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

6. Configure the destination pool.

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

In the following example, the destination pool name is **dest-pool**.

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

7. Specify the name of the mapping for port forwarding and configure the translation type. You can only configure one mapping within a NAT rule term.

```
[edit services nat rule rule-name term term-name]
user@host# set then port-forwarding-mappings  map-name
user@host# set then translated translation-type translation-type
```

In the following example, the port forwarding mapping name is **map1**, and the translation type is **dnat-44**.

```
[edit services nat rule rule-dnat44 term t1]
user@host# set then port-forwarding-mappings map1
user@host# set then translated translation-type dnat-44
```

8. Go to the **[edit services nat port-forwarding *map-name*]** hierarchy level.

```
[edit services nat]
user@host# edit port-forwarding map-name
```

9. Configure the mapping for port forwarding.

```
[edit port-forwarding map-name]
user@host# set destined-port port-id
user@host# set translated-port port-id
```

In the following example, the destination port number that needs to be translated is **23** and the port to which traffic is mapped is **45**.

```
[edit port-forwarding map1]
user@host# set destined-port 23
user@host# set translated-port 45
```

NOTE:

- Multiple port mappings are supported with port forwarding. Up to 32 port maps can be configured for port forwarding.
- The destination port should not overlap the port range configured for NAT.

10. Apply the NAT rule to the service set that performs the port mapping.

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

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

```
[edit services]
user@host# show
nat {
 pool dest-pool {
     address 192.0.2.2/32;
 }
 rule rule-dnat44 {
     match-direction input;
     term t1
          from {
             destination-address {
             198.51.100.20/32
             }
             destination-port {
             range low 20 high 50;
         }
  }
          then {
             port-forwarding-mappings map1;
             translated {
                  destination-pool dest-pool;
                  translation-type {
                     dnat-44;
                }
         }
     }
    }
 }
 port-forwarding map1 {
       destined-port 45;
       translated-port 23;
     }
}
service-set ss1 {
     nat-rules rule-dnat44;
     interface-service {
        service-interface sp-10/0/0.0;
```

```
        }
    }
```

NOTE:

- A similar configuration is possible with twice NAT for IPv4. See "Example: Configuring Port Forwarding with Twice NAT" on page 294.
- Port forwarding and stateful firewall can be configured together. Stateful firewall has precedence over port forwarding.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

RELATED DOCUMENTATION

Configuring Port Forwarding Without Destination Address Translation | 291

Configuring Port Forwarding Without Destination Address Translation

You can configure port forwarding without translating a destination address. Port forwarding allows the destination port to be changed to reach the correct port in a Network Address Translation (NAT) gateway. Port forwarding is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

To configure port forwarding without destination address translation in IPv4 networks:

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

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

2. Configure the rule, match direction, term name, and any conditions that the traffic must match before the rule is applied.

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

In the following example, the name of the rule is **rule-port-forwarding**, the match direction is **input**, the name of the term is **t1**, and the destination address that must be matched is **198.51.100.20**.

```
[edit services nat]
user@host# set rule rule-port-forwarding match-direction input term t1 from destination-address
  198.51.100.20
```

3. Go to the **[edit services nat rule *rule-name* term *term-name*]** hierarchy level.

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

4. Specify that there is no address translation for this rule.

```
[edit services nat rule rule-name term term-name]
user@host# set then no-translation
```

5. Specify the name of the mapping for port forwarding. You can only configure one mapping within a NAT rule term.

```
[edit services nat rule rule-name term term-name]
user@host# set then port-forwarding-mappings map-name
```

In the following example, the port forwarding mapping name is **map1**.

```
[edit services nat rule rule-port-forwarding term t1]
user@host# set then port-forwarding-mappings map1
```

6. Go to the **[edit services nat port-forwarding *map-name*]** hierarchy level.

```
[edit services nat]
user@host# edit port-forwarding map-name
```

7. Configure the mapping for port forwarding.

```
[edit port-forwarding map-name]
user@host# set destined-port port-id
user@host# set translated-port port-id
```

In the following example, the destination port number that needs to be translated is **23** and the port to which traffic is mapped is **45**.

```
[edit port-forwarding map1]
user@host# set destined-port 23
user@host# set translated-port 45
```

NOTE:

- Multiple port mappings are supported with port forwarding. Up to 32 port maps can be configured for port forwarding.
- The destination port should not overlap the port range configured for NAPT.

8. Apply the NAT rule to the service set that performs the port mapping.

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

NOTE: On the MS-MPC and MS-MIC, you cannot apply port forwarding NAT rules to an AMS interface.

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

```
[edit services]
user@host# show
nat {
 rule rule-port-forwarding {
     match-direction input;
     term t1 {
      then {
         port-forwarding-mappings map1;
         no-translation          }
     }
```

```
    }
 }
 port-forwarding map1 {
     destined-port 45;
       translated-port 23;
     }
}
service-set ss2 {
     nat-rules rule-port-forwarding;
     interface-service {
        service-interface sp-10/0/0.0;
        }
     }
```

NOTE: Port forwarding and stateful firewall can be configured together. Stateful firewall has precedence over port forwarding.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Example: Configuring Port Forwarding with Twice NAT

The following example configures port forwarding with **twice-napt-44** as the translation type. The example also has stateful firewall and multiple port maps configured.

Port forwarding is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

```
[edit services]
user@host# show
service-set in {
    syslog {
        host local {
            services any;
        }
    }
    stateful-firewall-rules r;
    nat-rules r;
    interface-service {
        service-interface sp-10/0/0.0;
    }
}
stateful-firewall {
    rule r {
        match-direction input;
        term t {
            from {
                destination-port {
                    range low 20 high 5000;
                }
            }
            then {
                reject;
            }
        }
    }
}
nat {
    pool x {
        address 203.0.113.2/32;
    }
    rule r {
        match-direction input;
        term t {
            from {
                destination-address {
                    198.51.100.2/32;
                }
                destination-port {
```

```
                    range low 10 high 20000;
                }
            }
            then {
                port-forwarding-mappings y;
                translated {
                   destination-pool x;
                   translation-type {
                      twice-napt-44;
                    }
                }
            }
        }
    }
    port-forwarding y {
        destined-port 45;
        translated-port 23;
        destined-port 55;
        translated-port 33;
        destined-port 65;
        translated-port 43;
   }
}
adaptive-services-pics {
    traceoptions {
        file sp-trace;
        flag all;
    }
}
```

NOTE:

- Stateful firewall has precedence over port forwarding. In this example, for instance, no traffic destined to any port between 20 and 5000 will be translated.
- Up to 32 port maps can be configured.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, port forwarding is also supported on the MS-MPC and MS-MIC.

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

CHAPTER 16

Allocating a Few Public Addresses to Many Private Hosts Using Dynamic NAT

IN THIS CHAPTER

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, 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-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 editservices 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 term 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 editservices 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;
    }
  }
```

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;
    }
  }
```

The following configuration specifies that NAT is not performed on incoming traffic from the source address **192.168.20.24/32** by providing a NAT rule term **t0** that configures **no-translation**. Dynamic NAT is performed on all other incoming traffic, as configured by term **t1** of the NAT rule. The **no-translation** option is supported on MX Series routers with MS-DPCs and on M Series routers with MS-100, MS-400,

and MS-500 MultiServices PICS. The **no-translation** option is supported on MX Series routers with MS-MPCs and MS-MICs starting in Junos OS release 15.1R1.

```
[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 dynamic-nat44;
                source-pool my-pool;
            }
        }
    }
}
```

The following configuration performs NAT 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 dynamic-nat44;
            source-prefix 20.20.10.0/24;
        }
    }
}
```

The following configuration performs NAT 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 dnat44;
                destination-prefix 20.20.10.0/24;
            }
        }
    }
}
```

Example: Dynamic Source NAT as a Next-Hop Service

The following example shows dynamic-source NAT applied as a next-hop service:

```
[edit interfaces]
ge-0/2/0 {
    unit 0 {
        family mpls;
    }
}
sp-1/3/0 {
    unit 0 {
        family inet;
    }
    unit 20 {
        family inet;
    }
    unit 32 {
        family inet;
    }
}
[edit routing-instances]
protected-domain {
    interface ge-0/2/0.0;
    interface sp-1/3/0.20;
    instance-type vrf;
    route-distinguisher 10.58.255.17:37;
```

```
    vrf-import protected-domain-policy;
    vrf-export protected-domain-policy;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop sp-1/3/0.20;
        }
    }
}
[edit policy-options]
policy-statement protected-domain-policy {
    term t1 {
        then reject;
    }
}
[edit services]
stateful-firewall {
    rule allow-all {
        match-direction input;
        term t1 {
            then {
                accept;
            }
        }
    }
}
nat {
    pool my-pool {
        address 10.58.16.100;
        port automatic;
    }
    rule hide-all {
        match-direction input;
        term t1 {
            then {
                translated {
                    source-pool my-pool;
                    translation-type napt-44;
                }
            }
        }
    }
}
service-set null-sfw-with-nat {
    stateful-firewall-rules allow-all;
```

```
    nat-rules hide-all;
    next-hop-service {
        inside-service-interface sp-1/3/0.20;
        outside-service-interface sp-1/3/0.32;
    }
}
```

Example: Assigning Addresses from a Dynamic Pool for Static Use

The following configuration statically assigns a subset of addresses that are configured as part of a dynamic pool (**dynamic-pool**) to two separate static pools (**static-pool** and **static-pool2**).

```
[edit services nat]
pool dynamic-pool {
    address 20.20.10.0/24;
}
pool static-pool {
    address-range low 20.20.10.10 high 10.20.10.12;
}
pool static-pool2 {
    address 20.20.10.15/32;
}
rule src-nat {
    match-direction input;
    term t1 {
        from {
            source-address 30.30.30.0/24;
        }
        then {
            translation-type dynamic-nat44;
            source-pool dynamic-pool;
        }
    }
    term t2 {
        from {
            source-address 10.10.10.2;
        }
        then {
            translation-type basic-nat44;
            source-pool static-pool;
        }
```

```
    }
    term t3 {
        from {
            source-address 10.10.10.10;
        }
        then {
            translation-type basic-nat44;
            source-pool static-pool2;
        }
    }
}
```

CHAPTER 17

Achieving Line-Rate, Low-Latency Translations Using Inline NAT

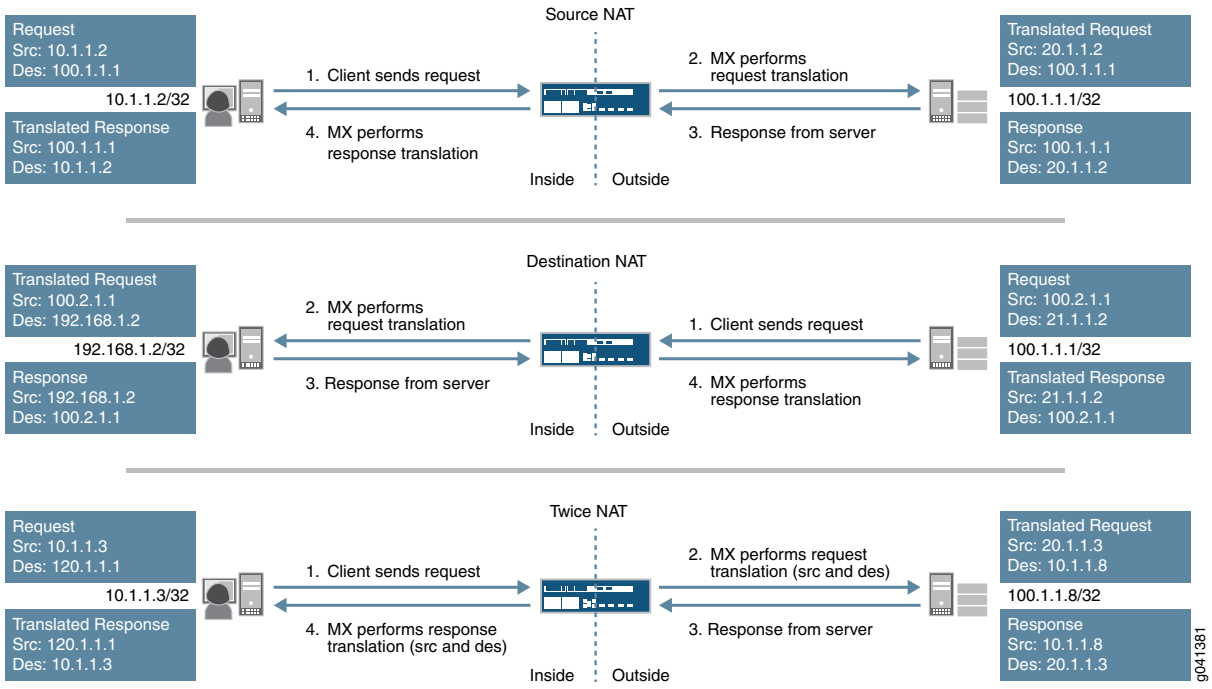
IN THIS CHAPTER

Inline Network Address Translation Overview

Inline NAT uses the capabilities of the MPC line card, eliminating the need for a services card for NAT. Consequently, you can achieve line-rate, low-latency address translations (up to 120 Gbps per slot). The current implementation provides:

- 1:1 static address mapping.
- Bidirectional mapping - source NAT for outbound traffic and destination NAT for inbound traffic.
- No limit on number of flows.
- Support for Source, destination, and twice NAT, as shown in Figure 19 on page 309. Inline NAT supports the translation type **basic-nat44**. Starting in Junos OS Release 15.1R1, inline NAT also supports **twice-basic-nat-44**.
- Support for hairpinning.

Figure 19: Supported Inline NAT Types



To configure inline NAT, you define your service interface as type **si-** (service-inline) interface. You must also reserve adequate bandwidth for the inline interface. This enables you to configure both interface or next-hop service-sets used for NAT. The **si-** interface serves as a “virtual service PIC”.

NOTE:

- Only static NAT is supported. Port translation, dynamic NAT, and ALGs are not supported. Hence, applications such as SIP or FTP Active Mode which require advanced processing for NAT do not function. An MS-MPC, MS-MIC, MS-DPC, or MS-PIC is still needed for any stateful-firewall processing, ALG support, and dynamic port translation.
- Inline NAT does not support sampling or logging of packets.

Benefits of Inline NAT

- Eliminates the need for a services card
- Supports more NAT flows than a services card

Release History Table

Release	Description
15.1R1	Starting in Junos OS Release 15.1R1, inline NAT also supports **twice-basic-nat-44**

RELATED DOCUMENTATION

- Network Address Translation Configuration Overview | **101**
- Example: Configuring Inline Network Address Translation—Interface-Based Method | **310**
- Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card | **87**

Example: Configuring Inline Network Address Translation—Interface-Based Method

IN THIS SECTION

This configuration example illustrates how to configure interface-based inline network address translation (NAT) on MX Series devices using **si-** (service-inline) interfaces with interface-style service-sets.

This topic covers:

Requirements

This example uses the following hardware and software components:

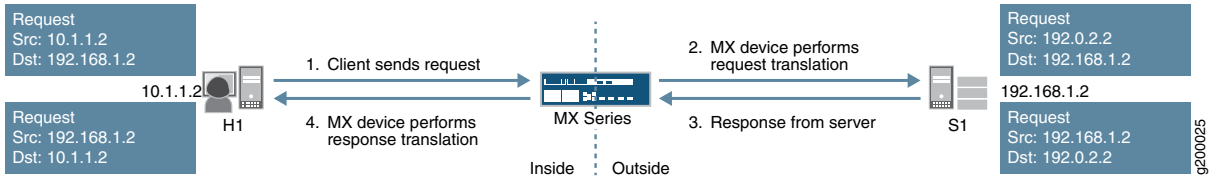
- MX Series router with a Modular Port Concentrator (MPC) line card
- Junos OS Release 11.4R1 or higher

Overview and Topology

As of Junos OS Release 11.4R1, MPC line cards can perform some services without the need of a dedicated services card, such as an MS-MPC. Inline services generally provide better performance than using a services card, however their functionality tends to be more basic. For example, inline NAT supports only static NAT.

In this example, an MX Series device with an MPC line card provides inline source NAT services to traffic flowing between two end hosts. The topology for this scenario is shown in Figure 20 on page 311

Figure 20: Inline Source NAT Using an MX Series Device with an MPC



As shown in the figure, host H1 sends traffic towards server S1. The MX Series device performs source NAT to translate H1's source IP address from 10.1.1.2 to 192.0.2.2. Server S1 then sends return traffic to host H1 using the destination IP address 192.0.2.2, and the MX Series device reverts H1's IP address back to 10.1.1.2.

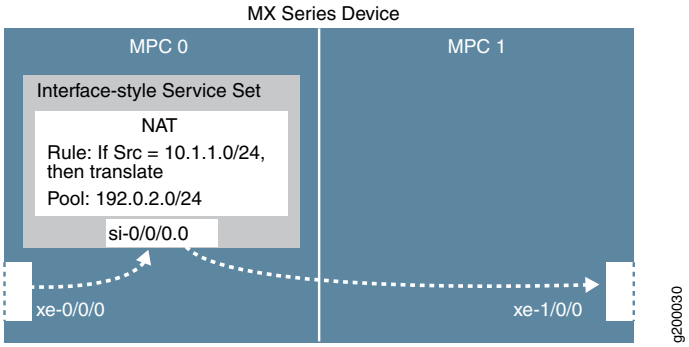
The following configuration elements are used in this scenario:

- Inline service interface—a virtual interface that resides on the Packet Forwarding Engine of the MPC. To access services, traffic flows in and out of these **si-** (service-inline) interfaces.
- Service set—defines the service(s) to be performed, and identifies which inline interface(s) will feed traffic into and out of the service set. There are two ways to implement service sets:
  - Interface-style—an interface-based method, where packets arriving at an interface are forwarded through the inline service.
  - Next-hop-style—a route-based method, where static routes are used to forward packets destined for a specific destination through the inline service.

  This example uses the interface-style service set.
- NAT rule—uses an if-then structure (similar to firewall filters) to define matching conditions and then apply address translation to the matching traffic.
- NAT pool—a user-defined set of IP addresses that are used by the NAT rule for translation.

These elements come together as shown in Figure 21 on page 312

Figure 21: Interface-Based Inline Source NAT



Configuration

IN THIS SECTION

To configure inline NAT using an interface-style service set, perform these tasks:

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.

```
## Enable inline services, create an si- interface, reserve bandwidth ##
set chassis fpc 0 pic 0 inline-services bandwidth 1g
set interfaces si-0/0/0 unit 0 family inet
## Configure a NAT rule and pool ##
set services nat rule SRC-NAT1 match-direction input
set services nat rule SRC-NAT1 term r1 from source-address 10.1.1.0/24
set services nat rule SRC-NAT1 term r1 then translated translation-type basic-nat44
set services nat rule SRC-NAT1 term r1 then translated source-pool p1
set services nat pool p1 address 192.0.2.0/24
## Configure the (interface-style) service set ##
```

```
set services service-set INT-STYLE-SS-NAT1 nat-rules SRC-NAT1
set services service-set INT-STYLE-SS-NAT1 interface-service service-interface si-0/0/0.0
## Configure interfaces ##
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces xe-0/0/0 description INSIDE
set interfaces xe-1/0/0 unit 0 family inet address 192.168.1.1/24
set interfaces xe-1/0/0 description OUTSIDE
set interfaces xe-0/0/0 unit 0 family inet service input service-set INT-STYLE-SS-NAT1
set interfaces xe-0/0/0 unit 0 family inet service output service-set INT-STYLE-SS-NAT1
```

Enable Inline Services and Create an Inline Interface

Step-by-Step Procedure

1. Enable inline services for the relevant FPC slot and PIC slot, and define the amount of bandwidth to dedicate for inline services.

   The FPC and PIC settings here will create and map to an **si-** interface.

   ```
   [edit chassis fpc 0 pic 0]
   user@MX# set inline-services bandwidth 1g
   ```

2. On the **si-** interface, specify the protocol family (or families) that will need NAT services.

   NOTE: The FPC and PIC settings here must match the settings defined above.

   ```
   [edit interfaces si-0/0/0]
   user@MX# set unit 0 family inet
   ```

Configure NAT Rule and Pool

Step-by-Step Procedure

1. Configure a NAT rule that matches on traffic arriving at the MX device from H1's subnet (10.1.1.0/24), translates it using basic IPv4 NAT, and uses an IP address from pool **p1**.

   ```
   [edit services nat]
   user@MX# set rule SRC-NAT1 match-direction input
   user@MX# set rule SRC-NAT1 term r1 from source-address 10.1.1.0/24
   user@MX# set rule SRC-NAT1 term r1 then translated translation-type basic-nat44
   user@MX# set rule SRC-NAT1 term r1 then translated source-pool p1
   ```

2. Configure the NAT pool.

```
[edit services nat]
user@MX# set pool p1 address 192.0.2.0/24
```

Configure the (Interface-style) Service Set

Step-by-Step Procedure

1. Configure a service set that uses the inline NAT service (**nat-rules**), and the inline interface defined above. Use the **interface-service** parameter to specify that this is an interface-style service set.

   Traffic will flow into and out of the **si-** interface to access the inline NAT service.

```
[edit services]
user@MX# set service-set INT-STYLE-SS-NAT1 nat-rules SRC-NAT1
user@MX# set service-set INT-STYLE-SS-NAT1 interface-service service-interface si-0/0/0.0
```

Configure Physical Interfaces

Step-by-Step Procedure

1. Configure the physical interfaces.

```
[edit interfaces]
user@MX# set xe-0/0/0 unit 0 family inet address 10.1.1.1/24
user@MX# set xe-0/0/0 description INSIDE
user@MX# set xe-1/0/0 unit 0 family inet address 192.168.1.1/24
user@MX# set xe-1/0/0 description OUTSIDE
```

2. On the 'inside' interface, specify that traffic will be sent through the service set defined above.

```
[edit interfaces xe-0/0/0 unit 0]
user@MX# set family inet service input service-set INT-STYLE-SS-NAT1
user@MX# set family inet service output service-set INT-STYLE-SS-NAT1
```

Results

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 1g;
```

```
            }
        }
    }
}

services {
    service-set INT-STYLE-SS-NAT1 {
        nat-rules SRC-NAT1;
        interface-service {
            service-interface si-0/0/0.0;
        }
    }
    nat {
        pool p1 {
            address 192.0.2.0/24;
        }
        rule SRC-NAT1 {
            match-direction input;
            term r1 {
                from {
                    source-address {
                        10.1.1.0/24;
                    }
                }
                then {
                    translated {
                        source-pool p1;
                        translation-type {
                            basic-nat44;
                        }
                    }
                }
            }
        }
    }
}

interfaces {
    si-0/0/0 {
        unit 0 {
            family inet;
        }
    }
    xe-0/0/0 {
```

```
        description INSIDE;
        unit 0 {
            family inet {
                service {
                    input {
                        service-set INT-STYLE-SS-NAT1;
                    }
                    output {
                        service-set INT-STYLE-SS-NAT1;
                    }
                }
                address 10.1.1.1/24;
            }
        }
    }
    xe-1/0/0 {
        description OUTSIDE;
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
}
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying Reachability from Host H1 to Server S1

Purpose

Verify reachability between H1 and S1.

Action

On host H1, verify that the host can ping server S1.

```
user@H1> ping 192.168.1.2 count 5
```

```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=63 time=0.991 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=14.186 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=3.016 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=3.742 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=4.748 ms

--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.991/5.337/14.186/4.593 ms
```

Meaning

H1 can successfully reach S1.

Verifying Address Translation

Purpose

Verify that address translation is working correctly.

Action

1. On the MX device, verify that the inline NAT configuration details have been applied correctly.

   ```
   user@MX> show services inline nat pool
   ```

   ```
   Interface: si-0/0/0, Service set: INT-STYLE-SS-NAT1
     NAT pool: p1, Translation type: BASIC NAT44
       Address range: 192.0.2.0-192.0.2.255
       NATed packets: 5, deNATed packets: 5, Errors: 0
   ```

2. On server S1, verify that the server is receiving the pings from H1's NAT-translated source IP address (192.0.2.2).

   Issue the command below, and send pings again from H1.

   NOTE: For this setup, another MX device is used to represent server S1 to enable monitoring of the inbound traffic.

   ```
   user@S1> monitor traffic interface xe-1/1/1 no-resolve
   ```

```
verbose output suppressed, use <detail> or <extensive> for full protocol decode
Address resolution is OFF.
Listening on xe-1/1/1, capture size 96 bytes

23:28:28.577377  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 3293, seq
 0, length 64
23:28:28.577405 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 3293, seq
0, length 64
23:28:29.579253  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 3293, seq
 1, length 64
23:28:29.579278 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 3293, seq
1, length 64
23:28:30.579275  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 3293, seq
 2, length 64
23:28:30.579302 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 3293, seq
2, length 64
23:28:31.580279  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 3293, seq
 3, length 64
23:28:31.580305 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 3293, seq
3, length 64
23:28:32.581266  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 3293, seq
 4, length 64
23:28:32.581293 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 3293, seq
4, length 64
^C
10 packets received by filter
0 packets dropped by kernel
```

Meaning

Step 1 above confirms that the inline NAT service parameters and interface-style service set are correctly implemented. Step 2 above confirms that server S1 is correctly receiving H1's pings from its NAT-translated source IP address.

RELATED DOCUMENTATION

- Inline Network Address Translation Overview | 308
- Understanding Service Sets | 6
- Example: Configuring Inline Network Address Translation—Route-Based Method | 319
- Day One: CGNAT Up and Running on the MX Series

Example: Configuring Inline Network Address Translation—Route-Based Method

IN THIS SECTION

This configuration example illustrates how to configure route-based inline network address translation (NAT) on MX Series devices using **si-** (service-inline) interfaces with next-hop style service-sets.

This topic covers:

Requirements

This example uses the following hardware and software components:

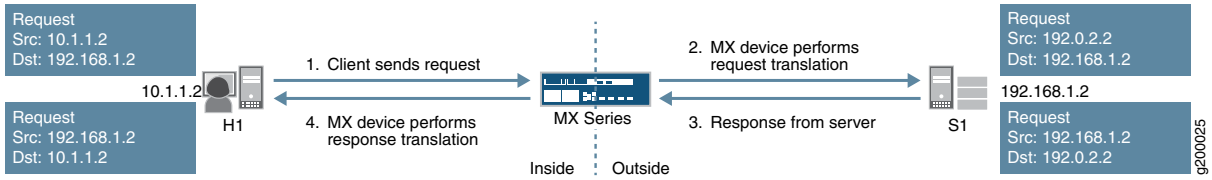
- MX Series router with a Modular Port Concentrator (MPC) line card
- Junos OS Release 11.4R1 or higher

Overview and Topology

As of Junos OS Release 11.4R1, MPC line cards can perform some services without the need of a dedicated services card, such as an MS-MPC. Inline services generally provide better performance than using a services card, however their functionality tends to be more basic. For example, inline NAT supports only static NAT.

In this example, an MX Series device with an MPC line card provides inline source NAT services to traffic flowing between two end hosts. The topology for this scenario is shown in Figure 20 on page 311

Figure 22: Inline Source NAT Using an MX Series Device with an MPC



As shown in the figure, host H1 sends traffic towards server S1. The MX Series device performs source NAT to translate H1's source IP address from 10.1.1.2 to 192.0.2.2. Server S1 then sends return traffic to host H1 using the destination IP address 192.0.2.2, and the MX Series device reverts H1's IP address back to 10.1.1.2.

The following configuration elements are used in this scenario:

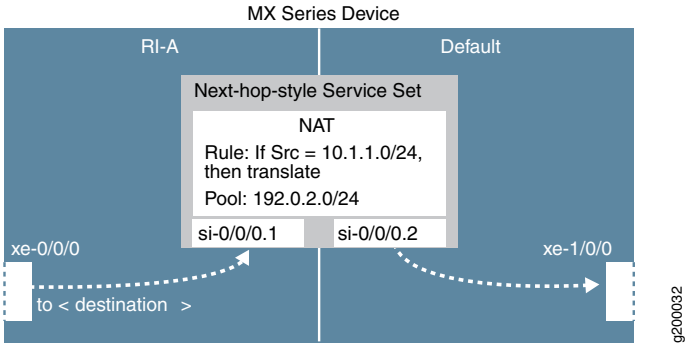
- Inline service interface—a virtual interface that resides on the Packet Forwarding Engine of the MPC. To access services, traffic flows in and out of these **si-** (service-inline) interfaces.
- Service set—defines the service(s) to be performed, and identifies which inline interface(s) will feed traffic into and out of the service set. There are two ways to implement service sets:
  - Interface-style—an interface-based method, where packets arriving at an interface are forwarded through the inline service.
  - Next-hop-style—a route-based method, where static routes are used to forward packets destined for a specific destination through the inline service.

  This example uses the next-hop-style service set.
- NAT rule—uses an if-then structure (similar to firewall filters) to define matching conditions and then apply address translation to the matching traffic.
- NAT pool—a user-defined set of IP addresses that are used by the NAT rule for translation.
- Routing instance—a collection of routing tables, interfaces, and routing protocol parameters that run separate from the main (default) routing instance.

  Route-based inline NAT is typically used in scenarios that involve routing instances.

These elements come together as shown in Figure 21 on page 312.

Figure 23: Route-Based Inline Source NAT



Configuration

IN THIS SECTION

To configure inline NAT using a next-hop-style service set, perform these tasks:

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.

```
## Configure interfaces ##
set interfaces xe-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces xe-0/0/0 description INSIDE
set interfaces xe-1/0/0 unit 0 family inet address 192.168.1.1/24
set interfaces xe-1/0/0 description OUTSIDE
## Enable inline services, create an si- interface, reserve bandwidth ##
set chassis fpc 0 pic 0 inline-services bandwidth 1g
set interfaces si-0/0/0 unit 1 family inet
set interfaces si-0/0/0 unit 1 service-domain inside
```

```
set interfaces si-0/0/0 unit 2 family inet
set interfaces si-0/0/0 unit 2 service-domain outside
## Configure routing instance, feed traffic into the inline NAT service ##
set routing-instances RI-A instance-type virtual-router
set routing-instances RI-A interface xe-0/0/0.0
set routing-instances RI-A interface si-0/0/0.1
set routing-instances RI-A routing-options static route 192.168.1.2/32 next-hop si-0/0/0.1
## Configure a NAT rule and pool ##
set services nat rule SRC-NAT1 match-direction input
set services nat rule SRC-NAT1 term r1 from source-address 10.1.1.0/24
set services nat rule SRC-NAT1 term r1 then translated translation-type basic-nat44
set services nat rule SRC-NAT1 term r1 then translated source-pool p1
set services nat pool p1 address 192.0.2.0/24
## Configure the (next-hop-style) service set ##
set services service-set NH-STYLE-SS-NAT1 nat-rules SRC-NAT1
set services service-set NH-STYLE-SS-NAT1 next-hop-service inside-service-interface si-0/0/0.1
set services service-set NH-STYLE-SS-NAT1 next-hop-service outside-service-interface si-0/0/0.2
```

Configure Physical Interfaces

Step-by-Step Procedure

1. Configure the physical interfaces.

```
[edit interfaces]
user@MX# set xe-0/0/0 unit 0 family inet address 10.1.1.1/24
user@MX# set xe-0/0/0 description INSIDE
user@MX# set xe-1/0/0 unit 0 family inet address 192.168.1.1/24
user@MX# set xe-1/0/0 description OUTSIDE
```

Enable Inline Services and Create an Inline Interface

Step-by-Step Procedure

1. Enable inline services for the relevant FPC slot and PIC slot, and define the amount of bandwidth to dedicate for inline services.

   The FPC and PIC settings here will create and map to an **si-** interface.

```
[edit chassis fpc 0 pic 0]
user@MX# set inline-services bandwidth 1g
```

2. On the **si-** interface, create two logical units. For each unit, specify the protocol family (or families) that will need NAT services, and the 'inside' or 'outside' interfaces for the service domain.

NOTE: The FPC and PIC settings here must match the settings defined above.

```
[edit interfaces si-0/0/0]
user@MX# set unit 1 family inet
user@MX# set unit 1 service-domain inside
user@MX# set unit 2 family inet
user@MX# set unit 2 service-domain outside
```

Configure Routing Instance and Identify Traffic to Send Through Inline NAT Service

Step-by-Step Procedure

1. Configure a routing instance that includes the 'ínside' physical and **si-** interfaces, as well as a static route that identifies traffic to forward into the inline NAT service through the **si-** interface.

   For simplicity, the static route used here simply identifies server S1.

```
[edit routing-instances]
user@MX# set RI-A instance-type virtual-router
user@MX# set RI-A interface xe-0/0/0.0
user@MX# set RI-A interface si-0/0/0.1
user@MX# set RI-A routing-options static route 192.168.1.2/32 next-hop si-0/0/0.1
```

Configure NAT Rule and Pool

Step-by-Step Procedure

1. Configure a NAT rule that matches on traffic arriving at the MX device from H1's subnet (10.1.1.0/24), translates it using basic IPv4 NAT, and uses an IP address from pool **p1**.

```
[edit services nat]
user@MX# set rule SRC-NAT1 match-direction input
user@MX# set rule SRC-NAT1 term r1 from source-address 10.1.1.0/24
user@MX# set rule SRC-NAT1 term r1 then translated translation-type basic-nat44
user@MX# set rule SRC-NAT1 term r1 then translated source-pool p1
```

2. Configure the NAT pool.

```
[edit services nat]
user@MX# set pool p1 address 192.0.2.0/24
```

Configure the (Next-hop-style) Service Set

Step-by-Step Procedure

1. Configure a service set that uses the inline NAT service (**nat-rules**), and the inline interfaces defined above. Use the **next-hop-service** parameter to specify that this is a next-hop-style service set, and assign the **si-** interfaces as 'inside' and 'outside' based on their settings above.

   Traffic will flow into and out of the **si-** interfaces to access the inline NAT service.

   ```
   [edit services]
   user@MX# set service-set NH-STYLE-SS-NAT1 nat-rules SRC-NAT1
   user@MX# set service-set NH-STYLE-SS-NAT1 next-hop-service inside-service-interface si-0/0/0.1
   user@MX# set service-set NH-STYLE-SS-NAT1 next-hop-service outside-service-interface si-0/0/0.2
   ```

Results

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 1g;
            }
        }
    }
}

services {
    service-set NH-STYLE-SS-NAT1 {
        nat-rules SRC-NAT1;
        next-hop-service {
            inside-service-interface si-0/0/0.1;
            outside-service-interface si-0/0/0.2;
        }
    }
    nat {
        pool p1 {
            address 192.0.2.0/24;
        }
        rule SRC-NAT1 {
            match-direction input;
            term r1 {
                from {
                    source-address {
                        10.1.1.0/24;
```

```
                    }
                }
                then {
                    translated {
                        source-pool p1;
                        translation-type {
                            basic-nat44;
                        }
                    }
                }
            }
        }
    }
}

interfaces {
    si-0/0/0 {
       unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
    }
    xe-0/0/0 {
        description INSIDE;
        unit 0 {
            family inet {
                  address 10.1.1.1/24;
            }
        }
    }
    xe-1/0/0 {
        description OUTSIDE;
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
}
```

```
routing-instances {
    RI-A {
        instance-type virtual-router;
        interface xe-0/0/0.0;
        interface si-0/0/0.1;
        routing-options {
            static {
                route 192.168.1.2/32 next-hop si-0/0/0.1;
            }
        }
    }
}
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying Reachability from Host H1 to Server S1

Purpose

Verify reachability between H1 and S1.

Action

On host H1, verify that the host can ping server S1.

`user@H1>` **ping 192.168.1.2 count 5**

```
PING 192.168.1.2 (192.168.1.2): 56 data bytes
64 bytes from 192.168.1.2: icmp_seq=0 ttl=63 time=0.926 ms
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.859 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=63 time=0.853 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=63 time=0.825 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=63 time=0.930 ms
```

```
--- 192.168.1.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.825/0.879/0.930/0.042 ms
```

Meaning

H1 can successfully reach S1.

Verifying Address Translation

Purpose

Verify that address translation is working correctly.

Action

1. On the MX device, verify that the inline NAT configuration details have been applied correctly.

   `user@MX>` **show services inline nat pool**

   ```
   Interface: si-0/0/0, Service set: NH-STYLE-SS-NAT1
     NAT pool: p1, Translation type: BASIC NAT44
       Address range: 192.0.2.0-192.0.2.255
       NATed packets: 5, deNATed packets: 5, Errors: 0, Skipped packets: 0
   ```

2. On server S1, verify that the server is receiving the pings from H1's NAT-translated source IP address (192.0.2.2).

   Issue the command below, and send pings again from H1.

   > **NOTE:** For this setup, another MX device is used to represent server S1 to enable monitoring of the inbound traffic.

   `user@S1>` **monitor traffic interface xe-1/1/1 no-resolve**

   ```
   verbose output suppressed, use <detail> or <extensive> for full protocol decode
   Address resolution is OFF.
   Listening on xe-1/1/1, capture size 96 bytes

   20:19:36.182690  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 4436, seq
    0, length 64
   20:19:36.182719 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 4436, seq
   0, length 64
   20:19:37.182918  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 4436, seq
   ```

```
 1, length 64
20:19:37.182945 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 4436, seq
1, length 64
20:19:38.183914  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 4436, seq
 2, length 64
20:19:38.183940 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 4436, seq
2, length 64
20:19:39.184872  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 4436, seq
 3, length 64
20:19:39.184896 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 4436, seq
3, length 64
20:19:40.185882  In IP 192.0.2.2 > 192.168.1.2: ICMP echo request, id 4436, seq
 4, length 64
20:19:40.185907 Out IP 192.168.1.2 > 192.0.2.2: ICMP echo reply, id 4436, seq
4, length 64
^C
10 packets received by filter
0 packets dropped by kernel
```

Meaning

Step 1 above confirms that the inline NAT service parameters and next-hop-style service set are correctly implemented. Step 2 above confirms that server S1 is correctly receiving H1's pings from its NAT-translated source IP address.

RELATED DOCUMENTATION

- Inline Network Address Translation Overview | 308
- Understanding Service Sets | 6
- Example: Configuring Inline Network Address Translation—Interface-Based Method | 310
- Day One: CGNAT Up and Running on the MX Series

Example: Configuring Inline Network Address Translation Hairpinning

IN THIS SECTION

This configuration example illustrates how to configure inline network address translation (NAT) hairpinning on MX Series devices using **si-** (service-inline) interfaces with a next-hop style service set.

This topic covers:

Requirements

This example uses the following hardware and software components:

- MX Series router with a Modular Port Concentrator (MPC) line card

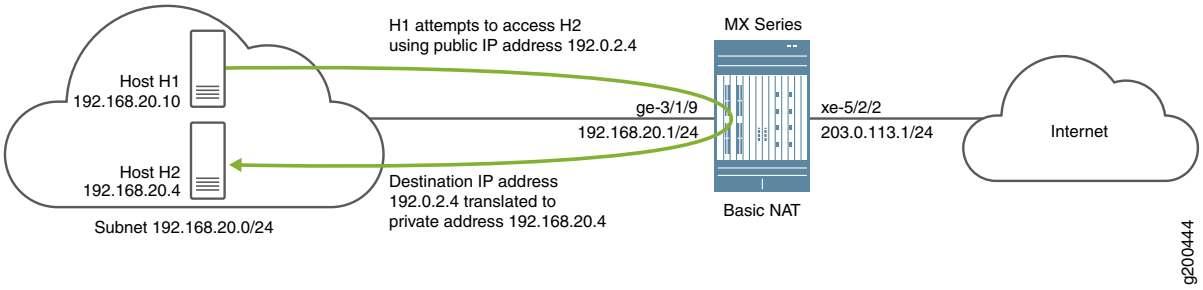
Overview and Topology

MPC line cards can perform some services without the need of a dedicated services card, such as an MS-MPC. Inline services generally provide better performance than using a services card.

This example shows hairpinning for inline basic NAT44. Generally, a source host in a subnetwork might not recognize that traffic is intended for a destination host within the same subnetwork because the source host identifies the destination host only by its public IP address. NAT hairpinning analyzes the IP packets and routes the traffic back to the correct destination host instead of passing the traffic through to the public network.

The topology for this scenario is shown in Figure 24 on page 329.

Figure 24: Inline NAT Hairpinning With MX Series



As shown in Figure 24 on page 329, host H1 and H2 are in the subnet 192.168.20.0/24. H1 sends traffic towards the public address of host H2, 192.0.2.4. The MX Series device performs NAT to translate the

destination address of 192.0.2.4 to 192.168.20.4, the private IP address of H2, and sends the traffic to host H2.

The following configuration elements are used in this scenario:

- Inline service interface—a virtual interface that resides on the Packet Forwarding Engine of the MPC. To access services, traffic flows in and out of these **si-** (service-inline) interfaces.
- Service set—defines the service(s) to be performed, and identifies which si- inline interfaces will feed traffic into and out of the service set. This example uses a next-hop-style service set, where static routes are used to forward packets with a specific destination through the inline service. In this example, the 0.0.0.0/0 destination is used, so all traffic from the subnet is forwarded to the inline service.
- NAT rule—uses an if-then structure to define matching conditions and then apply address translation to the matching traffic.
- NAT pool—a user-defined set of IP addresses that are used by the NAT rule for translation.
- Routing instance—a collection of routing tables, interfaces, and routing protocol parameters that run separate from the main (default) routing instance.

Configuration

IN THIS SECTION

To configure inline NAT using a next-hop-style service set, perform these tasks:

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.

```
## Configure interfaces ##
set interfaces ge-3/1/9 unit 0 family inet address 192.168.20.1/24
set interfaces xe-5/2/2 unit 0 family inet address 203.0.113.1/24
```

```
## Enable inline services, create an si-interface, reserve bandwidth
set chassis fpc 5 pic 1 inline-services bandwidth 10g
set interfaces si-5/1/0 unit 0 family inet
set interfaces si-5/1/0 unit 1 family inet
set interfaces si-5/1/0 unit 1 service-domain inside
set interfaces si-5/1/0 unit 2 family inet
set interfaces si-5/1/0 unit 2 service-domain outside
## Configure routing instance, feed traffic into the inline NAT service ##
set routing-instances vr-1 instance-type virtual-router
set routing-instances vr-1 interface ge-3/1/9.0
set routing-instances vr-1 interface si-5/1/0.1
set routing-instances vr-1 routing-options static route 0.0.0.0/0 next-hop si-5/1/0.1
## Configure a NAT rule and pool ##
set services nat rule nat_rule1 match-direction input
set services nat rule nat_rule1 term t1 from source-address 192.168.20.0/24
set services nat rule nat_rule1 term t1 then translated source-pool source_pool_1
set services nat rule nat_rule1 term t1 then translated translation-type basic-nat44
set services nat pool source_pool_1 address 192.0.2.0/24
## Configure the (next-hop-style) service set ##
set services service-set inline_nat_ss1 nat-rules nat_rule1
set services service-set inline_nat_ss1 next-hop-service inside-service-interface si-5/1/0.1
set services service-set inline_nat_ss1 next-hop-service outside-service-interface si-5/1/0.2
```

Configure Physical Interfaces

Step-by-Step Procedure

1. Configure the physical interfaces.

```
[edit interfaces]
user@host# set interfaces ge-3/1/9 unit 0 family inet address 192.168.20.1/24
user@host# set interfaces xe-5/2/2 unit 0 family inet address 203.0.113.1/24
```

Enable Inline Services and Create an Inline Interface

Step-by-Step Procedure

1. Enable inline services for the relevant FPC slot and PIC slot, and define the amount of bandwidth to dedicate for inline services.

   The FPC and PIC settings here will create and map to an si- interface.

```
[edit chassis fpc 5 pic 1]
user@host# set inline-services bandwidth 10g
```

2. On the si- interface, create two logical units. For each unit, specify the protocol family (or families) that will need NAT services, and the ’inside’ or ’outside’ interfaces for the service domain.

```
[edit interfaces si-5/1/0]
user@host# set unit 0 family inet
user@host# set unit 1 family inet
user@host# set unit 1 service-domain inside
user@host# set unit 2 family inet
user@host# set unit 2 service-domain outside
```

Configure Routing Instance and Identify Traffic to Send Through Inline NAT Service

Step-by-Step Procedure

1. Configure a routing instance that includes the 'ínside' physical and **si-** interfaces, as well as a static route that forwards all traffic into the inline NAT service through the **si-** interface.

```
[edit routing-instances]
user@host# set vr-1 instance-type virtual-router
user@host# set vr-1 interface ge-3/1/9.0
user@host# set vr-1 interface si-5/1/0.1
user@host# set vr-1 routing-options static route 0.0.0.0/0 next-hop si-5/1/0.1
```

Configure NAT Rule and Pool

Step-by-Step Procedure

1. Configure a NAT rule that matches on traffic arriving at the MX device from subnet 192.168.20.0/24, translates it using basic IPv4 NAT, and uses an IP address from pool **source_pool_1**.

```
[edit services nat]
user@host# set rule nat_rule1 match-direction input
user@host# set rule nat_rule1 term t1 from source-address 192.168.20.0/24
user@host# set rule nat_rule1 term t1 then translated source_pool_1
user@host# set rule nat_rule1 term t1 then translated translation-type basic-nat44
```

2. Configure the NAT pool.

```
[edit services nat]
user@host# set pool source_pool_1 address 192.0.2.0/24
```

Configure the (Next-hop-style) Service Set

Step-by-Step Procedure

- Configure a service set that uses the inline NAT service (**nat-rules**), and the inline interfaces defined above. Use the **next-hop-service** parameter to specify that this is a next-hop-style service set, and assign the **si-** interfaces as 'inside' and 'outside' based on their settings above.

  Traffic will flow into and out of the **si-** interfaces to access the inline NAT service.

```
[edit services]
user@host# set service-set inline_nat_ss1 nat-rules nat_rule1
user@host# set service-set inline_nat_ss1 next-hop-service inside-service-interface si-5/1/0.1
user@host# set service-set inline_nat_ss1 next-hop-service outside-service-interface si-5/1/0.2
```

Verification

IN THIS SECTION

Verifying That si Interface Comes Up

Purpose

Verify that the si interface comes up.

Action

On the MX Series router, verify that the si interface and logical units that you configured come up.

`user@host>` **show interfaces terse si-5/1/0**

```
Aug 10 02:30:39
Interface               Admin Link Proto    Local         Remote
si-5/1/0                up    up
si-5/1/0.0              up    up   inet
si-5/1/0.1              up    up   inet
si-5/1/0.2              up    up   inet
```

Verifying NAT Pools Are Configured on the si Interface

Purpose

Verify that the NAT pools are configured on the si interface.

Action

On the MX Series router, verify that the NAT pools are configured correctly on the si interface.

`user@host>` **show services inline nat pool**

```
Aug 10 02:31:15
Interface: si-5/1/0, Service set: inline_nat_ss1
  NAT pool: source_pool_1, Translation type: BASIC NAT44
    Address range: 192.0.2.0-192.0.2.255
    NATed packets: 9, deNATed packets: 9, Errors: 0, Skipped packets: 0
```

Verifying Address Translation

Purpose

Verify that the si interface is properly translating IP addresses.

Action

On the MX Series router, verify that IP addresses are being translated.

`user@host>` **show services inline nat statistics**

```
Aug 10 02:32:27

 Service PIC Name                                    si-5/1/0

 Control Plane Statistics
     Received IPv4 packets                             0
     ICMPv4 error packets pass through                 0
     ICMPv4 error packets locally generate             0
     Dropped IPv4 packets                              0
     Received IPv6 packets                             0
     ICMPv6 error packets pass through for NPTv6       0
     ICMPv6 error packets locally generated for NPTv6  0
     Dropped IPv6 packets                              0

 Data Plane Statistics          Packets                Bytes
     IPv4 NATed packets           18                    1512
     IPv4 deNATed packets         18                    1512
     IPv4 error packets           0                     0
     IPv4 skipped packets         0                     0
     IPv6 NATed packets           0                     0
```

```
    IPv6 deNATed packets          0                    0
    IPv6 error packets            0                    0
    IPv6 skipped packets          0                    0
```

RELATED DOCUMENTATION

- Inline Network Address Translation Overview | 308
- Understanding Service Sets | 6
- Example: Configuring Inline Network Address Translation—Interface-Based Method | 310
- Day One: CGNAT Up and Running on the MX Series

CHAPTER 18

Removing Address Dependency Using Network Prefix Translation for IPv6 Traffic

IN THIS CHAPTER

Stateless Source Network Prefix Translation for IPv6 Overview

Starting with Junos OS Release 15.1, you can configure stateless translation of source address prefixes in IPv6 networks (IPv6 to IPv6). This capability is supported on MX Series routers with MPCs where inline NAT is supported. To configure stateless network prefix translation for IPv6 packets (NPTv6), include the **translation-type nptv6** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level. The NPTv6 translator translates the source address prefix in such a way that the transport layer checksum of the packet does not need to be recomputed. NPTv6 defines a stateless method of IPv6 network prefix translation between internal and external networks. NPTv6 does not maintain the state for each node or each flow in the translator. You can use the **show services nat mappings nptv6 (internal | external)** command to view the NAT mappings for NPTv6 for internal and external addresses respectively. You can also use the **show services inline nat statistics** and **show services inline nat pool** commands to display information about inline NAT with NPTv6 configured.

Benefits of Stateless Source Network Prefix Translation

- For edge networks, you do not need to renumber the IPv6 addresses used inside the local network for interfaces, access lists, and system logging messages if:
  - The global prefixes used by the edge network are changed.

  - The IPv6 addresses are used inside the edge network or within other upstream networks (such as multihomed devices) when a site adds, drops, or changes upstream networks.
- IPv6 addresses used by the edge network do not need ingress filtering in upstream networks and do not need their customer-specific prefixes advertised to upstream networks.
- Connections that traverse the translation function are not disrupted by a reset or brief outage of an NPTv6 translator.

NPTv6

Network prefix translation for IPv6 (NPTv6) defines a stateless way of IPv6 address prefix translation between internal and external networks. NPTv6 does not maintain the state for each node or each flow in the translator. Maintenance of mapping state is not required for the address mapping of inbound or outbound packets. A stateless, transport-agnostic IPv6-to-IPv6 NPTv6 function offers the advantage of address-independence associated with IPv4-to-IPv4 NAT (NAPT44) and provides a 1:1 relationship between addresses in the *inside* and *outside* prefixes, thereby preserving end-to-end reachability at the network layer. In upstream networks, IPv6 addresses used by the edge network always contain a provider-allocated prefix.

NPTv6 is designed to provide address independence to the edge networks to achieve internal address stability, regardless of its upstream service provider networks. However, using provider-independent addresses without translation might be very expensive because the routing table enumerates the edge networks, instead of enumerating the transit domain that provides the service to the edge networks. This phenomenon can cause a massive and unmanageable route table. NPTv6 is a mechanism that effectively and cohesively provides address independence without advertising an internal network prefix to external networks. In contrast, the main objective of network address port translation (NAPT) for IPv4 (NAPT44) is to solve IPv4 address depletion, although it brings the same benefit of address independence. NAPT for IPv6, specifically NAPT66, is already supported in microkernel. However, similar to NAPT44, NAPT66 requires flow-state information to be preserved. NPTv6 provides a simple and streamlined technique to avoid as many of the limitations associated with NAPT66 as possible. It is defined to include a two-way, checksum-neutral, and an algorithmic translation function.

NPTv6 does not maintain state information for a node, flow, or a connection in the translator. Internal to external and external to internal packets are translated algorithmically using information present in the IPv6 header. As a result of its stateless nature, if multiple NPTv6 translators exist between the same two networks, the load can shift or be dynamically shared among them. Also, unlike NAPT44, because the mapping can be done in either direction, the translator does not interfere with the inbound connection establishment. Instead, a firewall can be used in conjunction with an NPTv6 translator. This behavior offers the network administrator more flexibility to specify security policy than that can be achieved with a traditional NAT.

Another advantage of NPTv6 is checksum-neutral translations. The translator does not need to rewrite the transport header for updating the checksum and does not perform port mapping. As a result, to deploy

new transport layer protocols, you do not need to modify the translator. Because the transport layer is not modified, the algorithm does not interfere with encryption of the IP payload. Although NPTv6 compares favorably to NAPT44 or NAPT66 in several ways, it does not eliminate all of the architectural problems. Because NPTv6 modifies the IP headers of packets, it is not compatible with security mechanisms such as the IPsec authentication header. The use of separate internal and external prefixes creates complexity for Domain Name System (DNS) deployment. Also, those applications that require application layer gateways (ALGs) to work correctly through NAPT44 or NAPT66 devices might require similar ALGs to work through NPTv6 translators. Because NPTv6 does not maintain connection states, the failure of the translator does not impact the non-transmit power control (TPC) traffic through the server. TCP connections can be interrupted because of the change in the source IP address of a connection. Connections might be timed out and then reestablished in this case.

NPTv6 uses inline NAT. Inline NAT uses the capabilites of the Modular Port Concentrator (MPC) line card, eliminating the need for a MultiServices DPC (MS-DPC) for NAT. To configure inline NAT, you define your service interface as type **si-** (service-inline) interface. You must also reserve adequate bandwidth for the inline interface. This enables you to configure both interface service sets and next-hop service sets used for NAT. The **si-** interface serves as a *virtual service PIC*.

Guidelines for Configuring Stateless Source Network Prefix Translation

Keep the following points in mind when you configure stateless translation of source IPv6 prefixes:

This topic contains the following sections that describe the working behavior of different functionalities with stateless source IPv6 prefix translation and the various system conditions:

- Graceful Routing Engine switchover (GRES) support is the same as for NAT44.
- Unified ISSU and nonstop software upgrade (NSSU) are not supported.
- NPTv6 deployment enables direct inbound connections to internal nodes from external networks. This mechanism causes slight vulnerability because it opens the internal nodes to attacks from outside. The stateless translation of NPTv6 makes it difficult to trace external connection requests, based on connection states. This behavior enables NAT44 networks to be well-protected against external attacks. The best option to secure an NPTv6 translator is to add a firewall above the NPTv6 translator.
- A 6rd softwire concentrator interoperates with NPTv6. All other mechanisms that do not require the application layer gateway (ALG) to change the source IP address in the payload are supported. TCP, UDP, ICMP, SSH, and Telnet are supported by the NPTv6 translator. FTP and Session Initiation Protocol (SIP) that require the ALG to change the source IP address in the payload are not supported.
- The NPTv6 pools are allocated in the external data memory. The pool data structure consists of the address prefix, prefix length, and the checksum. The size of each record is of 192 bits. For every pool, a denat pool is allocated automatically. The size of the denat pool is 192 bits. There is a total allocation

of 8000 64-bit entries for NAT-processed and untranslated NPTv6 pools. This allocation comes from the 64,000 entries allocated for the inline services (JNH_APP_INLINE_SVCS).

- Chaining of inline services for interoperation of 6rd with NPTv6 is not supported.
- You need to configure a source pool and specify the **from** (source) address, while configuring NPTv6.
- The external and internal prefix lengths must be greater than or equal to /16 subnet mask and less than or equal to /112 subnet mask.
- Two different internal prefixes cannot be translated to the same external prefix.
- NPTv6 cannot be applied to IPSec and Internet Key Exchange (IKE) packets. The NPTv6 translator is bypassed in this case.
- Because the translation is of one IPv6 address prefix, there is only one address in the pool. If more than one address is configured by the user, the system does not raise any error, instead only the first address prefix of the pool is chosen for translation.
- For packets going from internal network to external network, if the internal subnet is not mapped or is set to 0xFFFF, then the datagram is discarded and an ICMP destination unreachable error is generated.
- For packets going from internal network to external network, if the 16-bit word has the adjustment added to it using the 1's complement method and is equal to 0xFFFF, then the value is written as zero.
- For packets coming from the external network to internal network, if the 16-bit word has the adjustment subtracted from it using 1's complement method and is equal to 0xFFFF, the 16-bit word is overwritten as zero.
- For translation of prefixes /48 or shorter, the adjustment must be added or subtracted from the first 16 bits after the /48 subnet mask, the values of which are not 0xFFFF. If the prefix is /49 or longer, then the adjustment must be added or subtracted from the first 16 bits (from 64 to 123), the values of which are not 0xFFFF.

Interoperation of Functionalities with Network Prefix Translation for IPv6

This topic contains the following sections that describe the working behavior of different functionalities with stateless source IPv6 prefix translation and the various system conditions:

Address Mapping Algorithm

The NPTv6 translator filters the packets going out of the network and, if the source address of the packet matches with the source address defined in the rule (the **from** or source address in configuration), the source address is replaced with an address prefix from the pool defined for the rule. The next 16 bits after the prefix of the source address are replaced with the checksum-adjusted value to ensure that the checksum remains the same in the outgoing packet even though the source address is changed. During the definition

of the configuration rule and pool for the packets going outside the network, a denat rule and pool are created for the translation of the destination address for the packets coming into the network.

Internal to External Translation

When a packet is going from the internal network to the external network, the IPv6 prefix in the source address of the packet (coming from inside node) is mapped to the external prefix. After checksum adjustment, the packet is routed toward the external network.

External to Internal Translation

When a packet is coming from external network to internal network, the IPv6 prefix in the destination address of the packet (coming from outside host) is mapped to the internal prefix. After checksum adjustment, the packet is routed to internal network.

Checksum-Neutral Translation

The NPTv6 translator translates the source address prefix in such a way that the transport layer checksum of the packet does not need to be recomputed. A checksum change caused by modifying part of the area covered by the checksum can be corrected by making an additional change to a different 16-bit field covered by the same checksum. This checksum neutral method first computes 1's complement checksum of the **internal-prefix** and the **external-prefix**.

For packets coming from the internal network, the adjustment is calculated as 1’s complement and it is computed as follows:

Adjustment = Internal prefix checksum – External prefix checksum.

The adjustment value is added to the 16-bit word of the source address after the prefix.

For packets coming from external network, the adjustment is 1’s complement and it is calculated as follows:

Adjustment = External prefix checksum – Internal prefix checksum.

The adjustment is added to the 16-bit word of the destination address after the translated prefix.

Multihoming

If there are two NPTv6 translators with different external IPv6 prefix configurations for the same internal IPv6 prefix, then these two NPTV6 translators will translate the same internal IPv6 network prefix to two different external IPv6 network prefixes, depending on the translator the packet traverses.

Hairpinning

When an internal node has knowledge of only the external (that is, the global address) of another internal node, it uses that address to send packet to that internal node. If such a packet is received by an NPTv6 translator, that packet is routed toward the internal network again after it undergoes source address and destination address translation.

Load Balancing

Load sharing is achieved when two translators have the same internal to external mapping configuration and packet load is shared between them. How the load balancing is achieved is beyond the scope of NPTv6.

The balancing could be implemented based on subnet ID portion of the IPv6 address. There can be two si- logical interfaces with the same mapping of the internal prefix to the external prefix. Packets are routed to one of the si- logical interfaces based on the subnet ID.

ICMPv6 for NPTv6

Any host in the internal network should be able to ping a host in the external network through an NPTv6 translator. All ICMP error messages should be forwarded to the host in the internal network. During internal to external translation if there is no mapping possible for a prefix, then packet is dropped and the ICMP Destination Unreachable message is sent back. An ICMPv6 Destination Unreachable error is returned by the translator if the ICMP error is enabled in the following cases:

- If source address prefix lengths are less than or equal to /48 and the 48-63 bits are equal to 0xFFFF
- If prefix lengths are greater than /48 and all the 16-bit blocks in the interface ID (IID) (bits 64-127) are equal to 0xFFFF

Otherwise the packet is discarded.

For prefix lengths less than or equal to /48, the bits 48-63 are used as the 16-bit word adjusted for checksum. For prefix lengths greater than /48, the first 16-bit block in the IID that does not have the value 0xFFFF is the 16-bit word adjusted for checksum.

If the interface ID (IID) part of the address to be translated contains all zeros, ICMPv6 Parameter Problem error is returned by the translator if the ICMP error option is enabled. Otherwise the packet is discarded. ICMPv6 errors are generated by the control plane. The source address of the ICMPv6 pakcket is the IP address of the ingress interface.

RELATED DOCUMENTATION

Working of NPTv6 with Interface-Style and Next Hop-Style Service Sets

The objective is to add network prefix translation for IPv6 (NPTv6) inline service that performs stateless translation of the source IPv6 address. Consider a sample topology in which NPTv6 is implemented between an internal network with the prefix of FD01:0203:0405:/48 and an external network with the prefix of 2001:0DB8:0001:/48.

The source addresses FD01:0203:0405:/48 in the packets from a single administrative domain (internal network) destined to hosts in global network (external network) will be translated to 2001:0DB8:0001:/48. Packets destined to internal network coming from external network will have their destination address as 2001:0DB8:0001:/48. This destination address will be mapped to internal network address FD01:0203:0405:/48 and will be forwarded to the internal network host. The lengths of both the subnets are assumed to be the same for this case. If they differ the shorter one would be extended to the prefix length of the longer one by suffixing zeros.

Address mapping algorithm used for NPTv6 is checksum-neutral. The translated IP headers will generate the same IPv6 pseudo-header checksum. Checksum is calculated using the standard Internet checksum algorithm. Changes that are made during translation of the IPv6 prefix are offset by the calculated changes made to the other parts of the IPv6 address. This results in transport layers that use the Internet checksum (such as TCP and UDP) calculating the same IPv6 pseudo-header checksum for both the internal and external forms of the same datagram and avoids the need to modify transport layer headers to correct the checksum value. The algorithm can map the addresses for inbound packets and outbound packets.

The NPTv6 translator works for both fragmented packets and packets with IP options enabled. The configuration changes required for NPTv6 are covered in the next sections.

The configuration of a router to handle services is through the definition of logical service interface, service sets and service set rules. These define how the service is applied to the packets.

The inline services logical interface, si-ifl, implementation available for static v4-v4 source-address inline-NAT can be reused for inline NPTv6. The configuration for the NPTv6 implemented for MS-DPC can be modified for inline NPTv6 implementation. There are two types of service set configurations—interface style and next hop style.

For the next hop-style service, a route entry is configured to steer packets to an inline service interface. There the packet would go through the service rules. If the packet matches the service rules, it is processed as per the service rules. For the interface-style service, the service set is configured directly on the media interface affecting traffic as it leaves and enters the interface. The packets are steered to the inline service interface by the service filter applied to the media interface.

Example: Achieving Address Independence By Configuring Stateless Network Prefix Translation in IPv6 Networks by Using Interface-Style Service Sets

IN THIS SECTION

You can configure stateless translation of source address prefixes in IPv6 networks (IPv6 to IPv6) on MX Series routers with MPCs that support inline NAT. The NPTv6 translator translates the source address prefix in such a way that the transport layer checksum of the packet does not need to be recomputed. NPTv6 defines a stateless method of IPv6 network prefix translation between internal and external networks. NPTv6 does not maintain the state for each node or each flow in the translator. You can use the **show services nat mappings nptv6 (internal | external)** command to view the NAT mappings for NPTv6 for internal and external addresses respectively. You can also use the **show services inline nat statistics** and **show services inline nat pool** commands to display information about inline NAT with NPTv6 configured.

NOTE: This functionality is supported on MX Series routers with Trio-based FPCs (MPCs).

This example describes how to configure stateless source prefix translation for IPv6 packets using interface-style service sets on MX Series routers with MPCs, and contains the following sections:

Requirements

This example uses the following hardware and software components:

- One MX Series router with an MPC.
- Junos OS Release 15.1R1 or later for MX Series routers

Overview and Topology for Stateless Network Prefix Translation in IPv6 Networks Using Interface-Style Service Sets

For the interface style service, the service set is configured directly on the media interface affecting traffic as it leaves and enters the interface. The packets are steered to the inline service interface by the service filter applied to the media interface.

When you have defined and grouped the service rules by configuring the service-set definition, you can apply services to one or more interfaces installed on the router. When you apply the service set to an interface, it automatically ensures that packets are directed to the PIC.

Consider a sample configuration scenario in which NPTv6 is configured using interface-style service sets. An inline services interface, si-0/1/0, is configured with a bandwidth reserved for 10 gigabits per second. The si-0/1/0 interface is defined with inet6 family. A NAT address pool, nptv6_pool, is configured with the address of abcd:ef12:3456::/48. A NAT rule is applied in the input direction to perform NPTv6 translation on packets that arrive from the source address of 1234:5678:9abc::/48. For packets from the source address of 1234:5678:9abc::/48 that match the NAT rule criterion, the address from the NAT address pool is allocated. A service set, ss_nptv6, is specified with the NAT rule. A gigabit Ethernet interface, ge-5/0/0, is configured and the service set is applied to this interface.

Configuration

To configure stateless network prefix translation for IPv6 using interface-style service sets, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in 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:

Configuring Interfaces

```
set interfaces si-0/1/0 unit 0 family inet6
```

Configuring Interfaces for Traffic to Be Handled By the Service Set

```
set interfaces ge-5/0/0 unit 0 family inet6 service input service-set nptv6-service-set
set interfaces ge-5/0/0 unit 0 family inet6 service output service-set nptv6-service-set
set interfaces ge-5/0/0 unit 0 family inet6 address 1234:5678:9abc::1/64
```

Configuring Bandwidth for the Service Inline (si-) Interface

```
set chassis fpc 0 pic 1 inline-services bandwidth 10g
```

Configuring NAT Pool and Rules

```
set services nat pool ss_nptv6_pool address abcd:ef12:3456::/48
set services nat rule ss_nptv6_rule match-direction input term t0 from source-address
  1234:5678:9abc::/48
set services nat rule ss_nptv6_rule match-direction input term t0 then translated source-pool
  ss_nptv6_pool
set services nat rule ss_nptv6_rule match-direction input term t0 then translated translation-type
  nptv6
```

Configuring the Service Set

```
set services service-set ss_nptv6 nat-rules ss_nptv6_rule
set services service-set ss_nptv6 nat-options nptv6 icmpv6-error-messages
set services service-set ss_nptv6 interface-service service-interface si-0/1/0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure stateless network prefix translation for IPv6 using interface-style service sets:

1. Configure an inline services (si-) interface.

   ```
   [edit]
   user@host# set interfaces si-0/1/0 unit 0 family inet6
   ```

2. Configure the interfaces for traffic to be handled by the service set.

   ```
   [edit]
   user@host# set interfaces ge-5/0/0 unit 0 family inet6 service input service-set nptv6-service-set
   ```

```
user@host# set interfaces ge-5/0/0 unit 0 family inet6 service output service-set nptv6-service-set
user@host# set interfaces ge-5/0/0 unit 0 family inet6 address 1234:5678:9abc::1/64
```

3. Configure the bandwidth for the service inline (si-) interface.

```
[edit]
user@host# set chassis fpc 0 pic 1 inline-services bandwidth 10g
```

4. Configure a NAT pool and rule.

```
[edit]
user@host# set services nat pool ss_nptv6_pool address abcd:ef12:3456::/48
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 from source-address
   1234:5678:9abc::/48
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 then translated source-pool
   ss_nptv6_pool
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 then translated translation-type
   nptv6
```

5. Configure the service set

```
[edit]
user@host# set services service-set ss_nptv6 nat-rules ss_nptv6_rule
user@host# set services service-set ss_nptv6 nat-options nptv6 icmpv6-error-messages
user@host# set services service-set ss_nptv6 interface-service service-interface si-0/1/0.0
```

Results

From the configuration mode, confirm your configuration by entering the **show chassis**, **show interfaces**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show chassis
chassis {
   fpc 0 {
      pic 1 {
         inline-services {
            bandwidth 10g;
         }
```

```
      }
   }
}
```

```
user@host# show interfaces
interfaces {
   si-0/1/0 {
       unit 0 {
          family inet6;
       }
   }
   ge-5/0/0 {
       unit 0 {
          family inet6 {
             service {
                input {
                   service-set nptv6-service-set;
                }
                output {
                   service-set nptv6-service-set;
                }
             }
             address 1234:5678:9abc::1/64;
          }
       }
   }
}
```

```
user@host# show services
services {
    service-set ss_nptv6 {
       nat-rules ss_nptv6_rule;
       nat-options {
          nptv6 {
             icmpv6-error-messages;
          }
       }
       interface-service {
          service-interface si-0/1/0.0;
       }
    }
```

```
    nat {
       pool ss_nptv6_pool {
          address abcd:ef12:3456::/48;
       }
       rule ss_nptv6_rule {
          match-direction input;
          term t0 {
             from {
                source-address {
                   1234:5678:9abc::/48;
                }
             }
             then {
                translated {
                   source-pool ss_nptv6_pool;
                   translation-type {
                      nptv6;
                   }
                }
             }
          }
       }
    }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform the following:

Verifying the NAT Pool Mappings

Purpose

Verify the existing NAT address pools and mappings for IPv6 network prefix translation.

Action

From operational mode, use the **show services nat mappings nptv6** command:

```
user@host> show services nat mappings nptv6 internal 1111:2222:3333:aaaa:bbbb::1
```

```
 Interface       Service-set     NAT-Pool           Address Mapping
 si-0/1/0        ss_nptv6         ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1 ->
aaaa:bbbb:cccc:dddd:bbbb::1
```

```
user@host> show services nat mappings nptv6 external aaaa:bbbb:cccc:dddd:bbbb::1
```

```
 Interface       Service-set     NAT-Pool              Address Mapping
 si-0/1/0        ss_nptv6            ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1
-> aaaa:bbbb:cccc:dddd:bbbb::1
```

Meaning

The output shows the mapping between NAT addresses and ports for IPv6 stateless network prefix translation of external and internal addresses. The address and port details that are originally sent and converted using NAT are displayed.

Verifying the Inline NAT Pools and Statistics

Purpose

Verify the inline NAT pools and statistics for IPv6 network prefix translation.

Action

From operational mode, use the **show services inline nat** command:

```
user@host> show services inline nat statistics interface si-4/0/0
```

```
Service PIC Name: si-4/0/0

 Control Plane Statistics
     ICMPv4 errors packets pass through                :0
     ICMPv4 errors packets locally generated           :0
     ICMPv6 errors packets pass through                :0
     ICMPv6 errors packets locally generated           :0
     Dropped packets                                   :0
```

```
  Data Plane Statistics
     NATed packets                                    :0
     deNATed packets                                  :0
     Errors                                           :0
```

user@host> **show services inline nat pool**

```
Interface: si-4/0/0, Service set: ss_nptv6
   NAT pool: ss_nptv6_pool1, Translation type: NPTV6
        Address range: abcd:ef12:3456::/48
        NATed packets: 0, deNATed packets: 0, Errors: 0

   NAT pool: ss_nptv6_pool2, Translation type: NPTV6
         Address range: 1111:2222:3333::/48
         NATed packets: 0, deNATed packets: 0, Errors: 0
```

user@host> **show services inline nat pool ss_nptv6_pool1**

```
Interface: si-4/0/0, Service set: ss_nptv6
    NAT pool: ss_nptv6_pool1, Translation type: NPTV6
         Address range: abcd:ef12:3456::/48
         NATed packets: 0, deNATed packets: 0, Errors: 0
```

Meaning

The output shows the information about inline NAT address translations, such as the number of packets that are subject to NAT processing, the packets that are not translated, and the packets with translation errors for a specified service set and an si- interface.

RELATED DOCUMENTATION

Example: Achieving Address Independence By Configuring Stateless Network Prefix Translation in IPv6 Networks by Using Next-Hop -Style Service Sets

IN THIS SECTION

You can configure stateless translation of source address prefixes in IPv6 networks (IPv6 to IPv6) on MX Series routers with MPCs where inline NAT is supported. The NPTv6 translator translates the source address prefix in such a way that the transport layer checksum of the packet does not need to be recomputed. NPTv6 defines a stateless method of IPv6 network prefix translation between internal and external networks. NPTv6 does not maintain per node or per flow state in the translator. You can use the show services nat mappings nptv6 (internal | external) command to view the NAT mappings for NPTv6 for internal and external addresses respectively. You can also use the show services inline nat statistics and show services inline nat pool commands to display information about inline NAT with NPTv6 configured.

NOTE: This functionality is supported on MX Series routers with Trio-based FPCs (MPCs).

This example describes how to configure stateless source prefix translation for IPv6 packets using next-hop style service sets on MX Series routers with MPCs, and contains the following sections:

Requirements

This example uses the following hardware and software components:

- One MX Series router with an MPC.
- Junos OS Release 15.1R1 or later for MX Series routers

Overview and Topology of Stateless Network Prefix Translation in IPv6 Networks Using Next-Hop Style Service Sets

A next-hop service set is a route-based method of applying a particular service. Only packets destined for a specific next hop are serviced by the creation of explicit static routes. This configuration is useful when services need to be applied to an entire virtual private network (VPN) routing and forwarding (VRF) table, or when routing decisions determine that services need to be performed.

For the next hop style service, a route entry is configured to steer packets to an inline service interface. The packet is validated through the service rules. If the packet matches the service rules, it would be processed according to the service rules.

Consider a sample configuration scenario in which NPTv6 is configured using next-hop style service sets. An inline services interface, si-0/1/0, is configured with a bandwidth reserved for 10 gigabits per second. The si-0/1/0 interface is defined with inet6 family. A NAT address pool, nptv6_pool, is configured with the address of abcd:ef12:3456::/48. A NAT rule is applied in the input direction to perform NPTv6 translation on packets that arrive from the source address of 1234:5678:9abc::/48. For packets from the source address of 1234:5678:9abc::/48 that match the NAT rule criterion, the address from the NAT address pool is allocated. The service set is configured for forwarding next-hops with the service interface of si-0/1/0.1 associated with the service set applied inside the network. with parameters for next hop service interfaces for the inside network and si-/1/0.2 associated with the service set applied outside the network. A service set, ss_nptv6, is specified with the NAT rule. The service interface domain is specified for the si- interface with the inside service-domain configured for si-0/1/0.1 and outside service domain configured for si-0/1/0.2. A routing instance, inst1, is configured with the instance type as a VRF instance. interface si-0/1/0.1 and interface ge-5/0/0 are associated with inst1. The inside and outside interface domain matches that specified with the inside-service-interface and outside-service-interface statements. A policy is configured for NAT events with the action to reject all packets.

Configuration

To configure stateless network prefix translation for IPv6 using next-hop style service sets, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in 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:

Configuring Inline Interfaces

```
set interfaces si-0/1/0 unit 0 family inet6
```

```
set interfaces si-0/1/0 unit 1 family inet6
set interfacessi-0/1/0 unit 1 service-domain inside
set interfaces si-0/1/0 unit 2 family inet6
set interfaces si-0/1/0 unit 2 service-domain outside
set interfaces ge-5/0/0 unit 0 family inet6 address 1234:5678:9abc::1/64
```

Configuring Bandwidth for Inline Services

```
set chassis fpc 0 pic 1 inline-services bandwidth 10g
```

Configuring NAT Pool and Rule

```
set services nat pool ss_nptv6_pool address abcd:ef12:3456::/48
set services nat rule ss_nptv6_rule match-direction input term t0 from source-address
   1234:5678:9abc::/48
set services nat rule ss_nptv6_rule match-direction input term t0 then translated source-pool
   ss_nptv6_pool
set services nat rule ss_nptv6_rule match-direction input term t0 then translated translation-type
   nptv6
```

Configuring a Service Set

```
set services service-set ss_nptv6 nat-rules ss_nptv6_rule
set services service-set ss_nptv6 nat-options nptv6 icmpv6-error-messages
set services service-set ss_nptv6 nexthop-service inside-service-interface si-0/1/0.1
set services service-set ss_nptv6 nexthop-service outside-service-interface si-0/1/0.2
```

Configuring Routing Instances

```
set routing-instances inst1 instance-type vrf
set routing-instances inst1 interface si-0/1/0.1
set routing-instances inst1 interface ge-5/0/0.0
```

```
set routing-instances inst1 route-distinguisher 1234:5678
set routing-instances inst1 vrf-import reject-all
set routing-instances inst1 vrf-export reject-all
set routing-instances inst1 routing-options rib inst1.inet6.0 static route ::0/0 next-hop si-0/1/0.1
```

Configuring the Policy and Action Modifier

```
set policy-options policy-statement reject-all then reject
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure stateless network prefix translation for IPv6 using next-hop style service sets:

1. Configure the inline interface for NAT services.

```
[edit]
user@host# set interfaces si-0/1/0 unit 0 family inet6
user@host# set interfaces si-0/1/0 unit 1 family inet6
user@host# set interfacessi-0/1/0 unit 1 service-domain inside
user@host# set interfaces si-0/1/0 unit 2 family inet6
user@host# set interfaces si-0/1/0 unit 2 service-domain outside
user@host# set interfaces ge-5/0/0 unit 0 family inet6 address 1234:5678:9abc::1/64
```

2. Set the bandwidth for inline services.

```
[edit]
user@host# set chassis fpc 0 pic 1 inline-services bandwidth 10g
```

3. Configure the NAT pool and rule.

```
[edit]
user@host# set services nat pool ss_nptv6_pool address abcd:ef12:3456::/48
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 from source-address
   1234:5678:9abc::/48
```

```
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 then translated source-pool
  ss_nptv6_pool
user@host# set services nat rule ss_nptv6_rule match-direction input term t0 then translated translation-type
  nptv6
```

4. Configure a service set using the NAT rule associated with the NAT pool.

```
[edit]
user@host# set services service-set ss_nptv6 nat-rules ss_nptv6_rule
user@host# set services service-set ss_nptv6 nat-options nptv6 icmpv6-error-messages
user@host# set services service-set ss_nptv6 nexthop-service inside-service-interface si-0/1/0.1
user@host# set services service-set ss_nptv6 nexthop-service outside-service-interface si-0/1/0.2
```

5. Configure routing instances that use the si- interfaces configured.

```
[edit]
user@host# set routing-instances inst1 instance-type vrf
user@host# set routing-instances inst1 interface si-0/1/0.1
user@host# set routing-instances inst1 interface ge-5/0/0.0
user@host# set routing-instances inst1 route-distinguisher 1234:5678
user@host# set routing-instances inst1 vrf-import reject-all
user@host# set routing-instances inst1 vrf-export reject-all
user@host# set routing-instances inst1 routing-options rib inst1.inet6.0 static route ::0/0 next-hop si-0/1/0.1
```

6. Configure the policy and the action modifier for NAT packets.

```
[edit]
user@host# set policy-options policy-statement reject-all then reject
```

Results

From the configuration mode, confirm your configuration by entering the **show chassis**, **show interfaces**, **show policy-options**, **show routing-instances**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show chassis
chassis {
      fpc 0 {
           pic 1 {
```

```
                inline-services {
                    bandwidth 10g;
                }
            }
      }
}
```

```
user@host# show interfaces

chassis {
      fpc 0 {
           pic 1 {
                inline-services {
                    bandwidth 10g;
                }
           }
      }
}

interfaces {
  si-0/1/0 {
          unit 0 {
               family inet6;
          }
             unit 1 {
                  family inet6;
                  service-domain inside;
          }
             unit 2 {
                  family inet6;
                  service-domain outside;
             }
       }
 ge-5/0/0 {
            unit 0 {
                 family inet6 {
                           address 1234:5678:9abc::1/64;
                             }
                   }
            }

 }
```

```
user@host# show policy-options
policy-options {
      policy-statement reject-all {
           then reject;
      }
}
```

```
user@host# show routing-instances
routing-instances {
      inst1 {
           instance-type vrf;
          interface si-0/1/0.1;
           interface ge-5/0/0.0;
           route-distinguisher 1234:5678;
           vrf-import reject-all;
           vrf-export reject-all;
           routing-options {
                rib inst1.inet6.0 {
                    static {
                         route ::0/0 next-hop si-0/1/0.1;
                    }
                }
           }
      }
}
```

```
user@host# show services
 services {
  service-set ss_nptv6 {
   nat-rules ss_nptv6_rule;
   nat-options {
    nptv6 {
     icmpv6-error-messages;
    }
   }
   nexthop-service {
    inside-service-interface si-0/1/0.1;
```

```
    outside-service-interface si-0/1/0.2;
   }
  }
  nat {
   pool ss_nptv6_pool {
    address abcd:ef12:3456::/48;
   }
   rule ss_nptv6_rule {
    match-direction input;
    term t0 {
     from {
      source-address {
       1234:5678:9abc::/48;
      }
                         }
     then {
      translated {
       source-pool ss_nptv6_pool;
       translation-type {
        nptv6;
       }
      }
     }
    }
   }
  }
}
```

Verification

IN THIS SECTION

To confirm that the configuration is working properly, perform the following:

Verifying the NAT Pool Mappings

Purpose

Verify the existing NAT address pools and mappings for IPv6 network prefix translation.

Action

From operational mode, use the **show services nat mappings nptv6** command:

```
user@host> show services nat mappings nptv6 internal 1111:2222:3333:aaaa:bbbb::1
```

```
 Interface       Service-set     NAT-Pool           Address Mapping
 si-0/1/0        ss_nptv6         ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1 ->
aaaa:bbbb:cccc:dddd:bbbb::1
```

```
user@host> show services nat mappings nptv6 external aaaa:bbbb:cccc:dddd:bbbb::1
```

```
 Interface       Service-set     NAT-Pool              Address Mapping
 si-0/1/0        ss_nptv6            ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1
-> aaaa:bbbb:cccc:dddd:bbbb::1
```

Meaning

The output shows the information about inline NAT address translations, such as the number of packets that are subject to NAT processing, the packets that are not translated, and the packets with translation errors for a specified service set and an si- interface.

Verifying the Inline NAT Pools and Statistics

Purpose

Verify the inline NAT pools and statistics for IPv6 network prefix translation.

Action

From operational mode, use the **show services inline nat** command:

```
user@host> show services inline nat statistics interface si-4/0/0
```

```
Service PIC Name
      :si-4/0/0

 Control Plane Statistics
     ICMPv4 errors packets pass through                                  :0
     ICMPv4 errors packets locally generated                            :0
```

```
    ICMPv6 errors packets pass through                                    :0
    ICMPv6 errors packets locally generated                              :0
    Dropped packets
     :0

Data Plane Statistics
   NATed packets
    :0
   deNATed packets
  :0
   Errors
             :0
```

`user@host>` **show services inline nat pool**

```
      Interface: si-0/1/0, Service set: ss_nptv6
          NAT pool: ss_nptv6_pool1, Translation type: NPTV6
               Address range: abcd:ef12:3456::/48
               NATed packets: 0, deNATed packets: 0, Errors: 0

         NAT pool: ss_nptv6_pool2, Translation type: NPTV6
               Address range: 1111:2222:3333::/48
               NATed packets: 0, deNATed packets: 0, Errors: 0
```

`user@host>` **show services inline nat pool ss_nptv6_pool1**

```
    Interface: si-0/1/0, Service set: ss_nptv6
          NAT pool: ss_nptv6_pool1, Translation type: NPTV6
               Address range: abcd:ef12:3456::/48
               NATed packets: 0, deNATed packets: 0, Errors: 0
```

Meaning

The output shows the mapping between NAT addresses and ports for IPv6 stateless network prefix translation of external and internal addresses. The address and port details that are originally sent and converted using NAT are displayed.

CHAPTER 19

Monitoring NAT

IN THIS CHAPTER

Configuring NAT Session Logs

You can configure session logs for NAT from the CLI. By default, session open and close logs are produced. However, you can request that only one type of log be produced.

To configure NAT session logs:

1. Go to the **[edit services service-set *service-set-name* syslog host class *classname*]** hierarchy level.

   ```
   user@host# edit services service-set service-set-name syslog host class classname
   ```

2. Configure NAT logging using the **nat-logs** configuration statement.

   ```
   [edit services service-set service-set-name syslog host class classname]
   user@host# set nat-logs
   ```

3. Configure session logging using the **session-logs** statement. Open and close logs are produced by default. Specify **open** or **close** to produce only one type of log.

   ```
   [edit services service-set service-set-name syslog host class classname]
   user@host# set session-logs
   ```

   Or

   ```
   [edit services service-set service-set-name syslog host class classname]
   ```

```
user@host# set session-logs open
```

Or

```
[edit services service-set service-set-name syslog host class classname]
user@host# set session-logs close
```

4. For NAT sessions that use secured port block allocation (PBA), enter the **pba-interim-logging interval** option.

```
[edit services service-set service-set-name syslog host class classname]
user@host# top
[edit]
user@host# set interfaces interface-name service-options pba-interim-logging-interval
```

5. Configure a /32 IP address under unit 0 of the service interface that is assigned to the service set. This is the source IP address for all syslog messages generated by the service set for the NAT session logs. If you do not configure the IP address, syslog messages are not generated.

```
[edit]
user@host# set interfaces interface-name unit 0 family inet address address
```

> **NOTE:** If you use anything other than a /32 IP address, unwanted traffic might be sent to the service interface, which can eat up valuable CPU time on the service PIC.

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

Interim Logging for Secured Port Block Allocation | 276

Monitoring NAT Pool Usage

Purpose

Use the **show services nat pool detail** command to find global NAT statistics related to pool usage. This command is frequently used in conjunction with the **show services stateful-firewall statistics** command.

Action

`user@host#` **show services nat pool detail**

```
Interface: ms-1/0/0, Service set: s1
  NAT pool: dest-pool, Translation type: DNAT-44
    Address range: 10.10.10.2-10.10.10.2
  NAT pool: napt-pool, Translation type: NAPT-44
    Address range: 50.50.50.1-50.50.50.254
    Port range: 1024-63487, Ports in use: 0, Out of port errors: 0, Max ports used:
 0
  NAT pool: source-dynamic-pool, Translation type: DYNAMIC NAT44
    Address range: 40.40.40.1-40.40.40.254
    Out of address errors: 0, Addresses in use: 0
  NAT pool: source-static-pool, Translation type: BASIC NAT44
    Address range: 30.30.30.1-30.30.30.254
```

RELATED DOCUMENTATION

Configuring Pools of Addresses and Ports for Network Address Translation Overview | 103

Using the Enterprise-Specific Utility MIB

IN THIS SECTION

Using the Enterprise-Specific Utility MIB

The enterprise-specific Utility MIB enables you to add SNMP-compliant applications information to the enterprise-specific Utility MIB. The application information includes:

- NAT mappings
- Carrier-grade NAT (CGNAT) pools
- Service set CPU utilization
- Service set memory usage
- Service set summary information
- Service set packet drop information
- Service set memory zone information
- Multiservices PIC CPU and memory utilization
- Stateful firewall flow counters
- Session application connection information
- Session analysis information
- Subscriber analysis information
- Traffic Load Balancer information

You use a delivered Stylesheet Language Alternative Syntax (SLAX) script to place applications information into the enterprise-specific Utility MIB. The script is invoked based on event policies (such as reboot of the router or switchover of Routing Engines) defined in an event script. The script can also be invoked from the command line as an op script. The script only runs on the master Routing Engine. After the script is invoked, it polls data from the specified components at regular intervals using the XML-RPC API and writes the converted data to the Utility MIB as SNMP variables. The script automatically restarts after a configured polling cycle elapses.

SEE ALSO

Populating the Enterprise-Specific Utility MIB with Information | 364

Populating the Enterprise-Specific Utility MIB with Information

To use a SLAX script to populate the enterprise-specific Utility MIB with information:

1. Enable the **services-oids-slax** script.

```
user@host# set system scripts op file services-oids.slax
```

2. Configure the maximum amount of memory for the data segment during the execution of the script.

```
user@host# set event-options event-script max-database 512m
```

3. Enable the script.

```
user@host# set event-options event-script file services-oids-ev-policy.slax
```

4. (Optional) Enable the **log-stats** argument to allow sys logging of stateful firewall rate statistics when the event-script is run.

   a. Display the event policies and the arguments that can be used.

```
user@host> show event-options event-scripts polices
```

```
event-options {
    policy services-oids-done {
        events system;
        attributes-match {
          system.message matches "Completed polling cycle normally. Exiting";

        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
    policy system-started {
        events system;
        attributes-match {
            system.message matches "Starting of initial processes complete";

        }
        then {
```

```
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
}
event-options {
    policy services-oids-done {
        events system;
        attributes-match {
           system.message matches "Completed polling cycle normally. Exiting";

        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
    policy system-started {
        events system;
        attributes-match {
            system.message matches "Starting of initial processes complete";

        }
        then {
            event-script services-oids.slax {
                arguments {
                    max-polls 30;
                    interval 120;
                }
            }
        }
    }
}
```

The **log-stats** argument does not appear, so you must enable it.

b. Start the Linux shell.

```
user@host> start shell
```

```
%
```

c. Open the **/var/db/scripts/event/services-oids-eve-policy.slax** file for editing.

```
<event-options> {
        /*
         * This policy detects when the services-oids.slax script ends, then
 restarts it.
         */
        <policy> {
            <name> "services-oids-done";
            <events> "system";
            <attributes-match> {
                <from-event-attribute> "system.message";
                <condition> "matches";
               <to-event-attribute-value> "Completed polling cycle normally.
 Exiting";
            }
            <then> {
                <event-script> {
                    <name> "services-oids.slax";
                    <arguments> {
                        <name>"max-polls";
                        <value>"30";
                    }
                    <arguments> {
                        <name>"interval";
                        <value>"120";
                    }
                    /*
                    <arguments> {
                        <name>"log-stats";
                        <value>"yes";
                    }
                    */
                }
            }
        }

        /*
```

```
         * This policy detects when the system has booted and kicks off the
services-oids.slax script.
         * This policy hooks the 'system started' event
         */
        <policy> {
            <name> "system-started";
            <events> "system";
            <attributes-match> {
                <from-event-attribute> "system.message";
                <condition> "matches";
                <to-event-attribute-value> "Starting of initial processes
complete";
            }
            <then> {
                <event-script> {
                    <name> "services-oids.slax";
                    <arguments> {
                        <name>"max-polls";
                        <value>"30";
                    }
                    <arguments> {
                        <name>"interval";
                        <value>"120";
                    }
                    /*
                    <arguments> {
                        <name>"log-stats";
                        <value>"yes";
                    }
                    */
                }
            }
        }

}
```

d. Remove the comment enclosures (/* and */) surrounding the **<arguments>** tags containing **“log-stats”**.

e. Exit the Linux shell and return to the CLI.

```
% exit
```

f. Load the changes you made to the event script file.

```
user@host>request system scripts event-scripts reload
```

The **log-stats** argument is available the next time the event script restarts.

5. Set up the script logging file **services-oids.log**.

```
user@host# set system syslog file services-oids.log any info
user@host# set system syslog file services-oids.log match cscript
```

6. Synchronize scripts between Routing Engines so that when a switchover of Routing Engine occurs, the event policy starts on the new master.

   - To synchronize on a per-commit basis:

```
user@host# commit synchronize scripts
```

   - To synchronize scripts every time you execute a **commit synchronize**:

```
[edit system scripts]
user@host# set synchronize
user@host# commit synchronize
```

7. The script starts automatically at system boot, but you can manually start it with the CLI.

```
user@host> op services-oids arguments
```

Table 15 on page 369 describes the arguments that you can use.

Table 15: Arguments for services-oids.slax Script

Argument	Description
clean	A value of **1** clears all Utility MIB OIDs. Use this only to clean OID tables.
clear-semaphore	A value of **1** resets the semaphore in the Utility MIB to recover from an abnormal script exit or from a manual script exit.
debug	Prints debug messages on console.
detail	Displays detailed output.
interval	Sets the number of seconds between poll cycles (default is 120).

Table 15: Arguments for services-oids.slax Script *(continued)*

Argument	Description
invoke-debugger	Invokes script in debugger mode.
log-stats	**Yes** value enables sys logging of stateful firewall rate statistics (default is no).
max-polls	Sets the number of poll cycles before exiting the script (default is 30).
one-cycle-only	Value of **1** quits after one cycle of polling. Event policy does not restart the script. Use this option for testing only. The default is **0**.
signal-stop	A value of **1** stops the script and sets the semaphore, which causes the next iteration to exit.
silent	Prints trace messages on console if it is unset. Set it to zero-length string (“ ”) to unset it. Default is 1.
|	Pipes through a command.

8. Check the status of the script from the log file.

```
router> show /var/log/services-oids.log | no-more
```

```
Jun 27 19:51:47  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
Beginning polling cycle.
Jun 27 19:51:47  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing traffic load-balance statistics
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing cgnat pool detail
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing cgnat mappings summary
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets summary
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets cpu-usage
Jun 27 19:51:48  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-sets mem-usage
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall statistics
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall flow-analysis
```

```
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing stateful firewall flows counts
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing FW policy connections/second
Jun 27 19:51:49  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing FW/NAT app connections
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set packet-drops
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set memory-usage zone
Jun 27 19:51:51  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing service-set policy throughput stats
Jun 27 19:51:52  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info]
processing ms-pic CPU amd Memory utilization stats
Jun 27 19:51:52  wf-cheesypoofs cscript: services-oids.slax(v0.14):[info] 1/30
 Sleeping for 110 seconds.
```

9. Verify that you are getting Utility MIB OID updates.

```
router> show snmp mib walk jnxUtil ascii
```

```
. . .
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-1" = 0
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-2" = 0
jnxUtilCounter64Value."services10tcp-errors09CGN-SET-3" = 0
jnxUtilCounter64Value."services10udp-errors09CGN-SET-1" = 1119
jnxUtilCounter64Value."services10udp-errors09CGN-SET-2" = 0
. . .
```

To exclude the timestamp information, use

```
router> show snmp mib walk jnxUtil ascii | match Value
```

SEE ALSO

Using the Enterprise-Specific Utility MIB | 364

Stopping the SLAX Script with the CLI

To stop the SLAX script from the CLI:

- Issue the stop argument.

```
user@host> op services-oids signal-stop 1
```

SEE ALSO

Populating the Enterprise-Specific Utility MIB with Information | 364
Using the Enterprise-Specific Utility MIB | 364

Clearing the Utility MIB

To clear all the utility MIB OIDs:

- Issue the clean argument.

```
user@host> op services-oids clean 1
```

SEE ALSO

Populating the Enterprise-Specific Utility MIB with Information | 364
Using the Enterprise-Specific Utility MIB | 364

Recovering from an Abnormal SLAX Script Exit or a SLAX Script Exit with the CLI

To recover from an abnormal SLAX script exit or an SLAX script exit with the CLI:

- Issue the clear semaphore argument.

```
user@host> op services-oids clear-semaphore 1
```

SEE ALSO

RELATED DOCUMENTATION

SLAX Overview

3

PART

Transitioning to IPv6 Using Softwires

CHAPTER 20

Softwires Overview

IN THIS CHAPTER

Tunneling Services for IPv4-to-IPv6 Transition Overview

IN THIS SECTION

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 requires 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 the packet 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. The number of established softwires does not affect throughput, and scalability is independent of the number of interfaces. Scalability is only limited to the number of flows that the services DPC or PIC can support.

This topic contains the following sections:

6to4 Overview

IN THIS SECTION

Basic 6to4

6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that enables 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, because IPv6 is not required on nodes between the host and the destination. 6to4 is intended only as a transition mechanism and is not meant to be used permanently.

6to4 is supported on Multiservices 100, 400, and 500 PICs on M Series routers and on MX Series routers equipped with Multiservices DPCs and on MX240, MX480, and MX960 routers with the MX-SPC3 services card. 6rd is not supported on MX Series routers with MS-MPCs or MS-MICs.

6to4 can be used by an individual host or by a local IPv6 network. When used by a host, 6to4 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, the host's IPv6 default gateway must be set to a 6to4 address that 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. When processed by 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. We recommend that providers who want to provide 6to4 service to their clients or peers advertise the Anycast prefix like any other IP prefix, and route the prefix to the provider's 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 the embedding of IPv4 routes into the routing tables of IPv6 routers. From the 6to4 relay router the packets can then be sent over the IPv4 Internet to the destination.

6to4 Anycast

Router 6to4 requires 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. Removing this configuration makes the solution available for small or domestic users, even those with a single host or simple home gateway instead of a border router. Removing this configuration 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, *6to 4 Provider-Managed Tunnels (PMT)*. That document, a work in progress, proposes a solution that providers can implement 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 *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 that translates the source 6to4 prefix to a provider assigned prefix that 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 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 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 MS-DPCs and MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS release 20.2R1, DS-Lite is supported Next Gen Services on MX240, Mx480 and MX960 routers with the MX-SPC3.Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs. Starting in Junos OS release 18.2R1, DS-lite is supported on AMS interfaces.Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

> **NOTE:** IPv6 Provider Edge , 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.

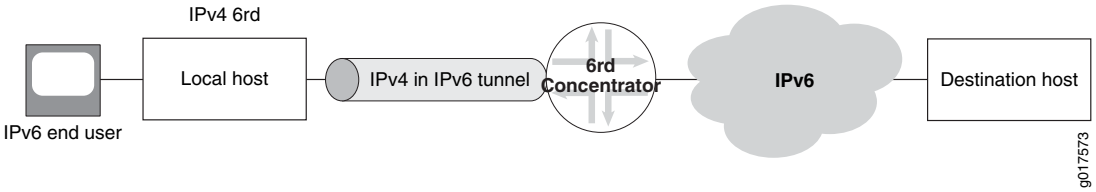
For more information on DS-Lite softwires, see the IETF draft *Dual Stack Lite Broadband Deployments Following IPv4 Exhaustion*.

> **NOTE:** The most recent IETF draft documentation for DS-Lite uses new terminology:
>
> - The term *softwire initiator* has been replaced by *B4*.
> - The term *softwire 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 softwire flow is shown in Figure 25 on page 379.

Figure 25: 6rd Softwire Flow



Junos OS supports a 6rd softwire concentrator on a services DPC or PIC to facilitate rapid deployment of IPv6 service to subscribers on native IPv4 customer edge WANs. IPv6 packets are encapsulated in IPv4 packets by a softwire initiator at the customer edge WAN. These packets are tunneled to a softwire concentrator residing on an MS-DPC or MX-SPC3 (branch relay). A softwire is created when IPv4 packets containing IPv6 destination information are received at the softwire 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 softwire and sent to the customer edge WAN.

The softwire concentrator creates softwires as the IPv4 packets are received from the customer edge WAN side or IPv6 packets are received from the Internet. A 6rd softwire on the Services DPC is identified by the 3-tuple containing the service set ID, customer edge softwire initiator IPv4 address, and softwire concentrator IPv4 address. IPv6 flows are also created for the encapsulated IPv6 payload, and are associated with the specific softwire 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 routers, and on MX Series routers equipped with Multiservices DPCs. 6rd is not supported on MX Series routers with MS-MPCs or MS-MICs.

Junos OS supports inline 6rd and 6to4 on Modular Port Concentrator (MPC) line cards.

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

Release History Table

Release	Description
20.2R1	Starting in Junos OS release 20.2R1, DS-Lite is supported Next Gen Services on MX240, Mx480 and MX960 routers with the MX-SPC3.
19.2R1	Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
18.2R1	Starting in Junos OS release 18.2R1, DS-lite is supported on AMS interfaces.
17.4R1	Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

- Junos Address Aware Network Addressing Overview | 78
- Configuring a 6rd Softwire Concentrator | 414
- Configuring a DS-Lite Softwire Concentrator | 389
- Configuring Softwire Rules | 381
- Configuring Service Sets for Softwire | 383
- Configuring Inline 6rd | 431

CHAPTER 21

Softwires Configuration Overview

IN THIS CHAPTER

Configuring Softwire Rules

You configure softwire rules to instruct the router how to direct traffic to the addresses specified for 6rd or DS-Lite softwire concentrators. Softwire 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 softwire concentrator.

Softwire rules are supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, softwire rules for DS-Lite are supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

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

To configure a softwire rule:

1. Assign a name to the rule.

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

2. Specify the match direction.

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

3. Assign a name for the first term.

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

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

```
[edit services softwire rule rule-name term term-name]
user@host# set then ds-lite name
```

Or

```
user@host# set then v6rd v6rd-softwire-concentator
```

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

Release History Table

Release	Description
19.2R1	Starting in Junos OS release 19.2R1, softwire rules for DS-Lite are supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
17.4R1	Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | 375
- Configuring a 6rd Softwire Concentrator | 414
- Configuring a DS-Lite Softwire Concentrator | 389
- Configuring IPv6 Multicast Interfaces | 391
- Configuring Service Sets for Softwire | 383

Configuring Service Sets for Softwire

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

Softwire rules are supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. Starting in Junos OS release 20.2R1, softwire rules for DS-Lite are supported supported for CGNAT Next Gen Services on MX240, MX480 and MX960 routers.Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, softwire rules for DS-Lite are supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

To configure service sets for softwire:

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

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

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

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

NOTE: With a DS-Lite softwire concentrator, if you configure stateful firewall rules without configuring NAT rules, using an interface service set causes the ICMP echo reply messages to be not sent correctly to DS-Lite. This behavior occurs if you apply a service set to both inet and inet6 families. In such a scenario, the traffic that is not destined to the DS-Lite softwire concentrator is also processed by the service set and the packets might be dropped, although the service set must not process such packets.

To prevent the problem to incorrect processing of traffic applicable for DS-Lite, you must configure a next-hop style service set and not an interface style service set. This problem does not occur when you configure NAT rules with interface service sets for DS-Lite.

For further information, see ""Configuring Service Rules" on page 21."

Release History Table

Release	Description
20.2R1	Starting in Junos OS release 20.2R1, softwire rules for DS-Lite are supported supported for CGNAT Next Gen Services on MX240, MX480 and MX960 routers.
19.2R1	Starting in Junos OS release 19.2R1, softwire rules for DS-Lite are supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
17.4R1	Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

Tunneling Services for IPv4-to-IPv6 Transition Overview | 375

Configuring Softwire Rules | 381

Example: Configuring DS-Lite and 6rd in the Same Service Set | 400

CHAPTER 22

Transitioning to IPv6 Using 6to4 Softwires

IN THIS CHAPTER

Configuring a 6to4 Provider-Managed Tunnel

When configuring a 6to4 provider-managed tunnel (PMT), replace the Anycast destination with the address of a managed relay in the provider network.

6to4 tunnels are supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. 6to4 tunnels are not supported on MX Series routers with MS-MPCs or MS-MICs.

To configure a 6to4 PMT:

1. Configure the ingress interface for 6to4 traffic. Include the name of the service set that identifies the rules for input and output service on this interface.

```
[edit interfaces ge-0/2/1]
user@host# set unit logical-unit-number family family service input service-set-name
user@host# set unit logical-unit-number family family service output service-set-name
user@host# set unit logical-unit-number family family address addres
```

   For example:

```
[edit interfaces ge-0/2/1]
user@host# set unit 0 family inet service input service-set v6to4-pmt
user@host# set unit 0 family inet service output service-set v6to4-pmt
user@host# set unit 0 family inet address 130.130.130.1/24
```

2. Configure the egress interface.

```
[edit interfaces ge-0/2/2]
```

```
user@host# set unit logical-unit-number family family address address
```

For example:

```
[edit interfaces ge-0/2/2]
user@host# set unit 0 family inet6 address 4ABC::1/16
```

3. Configure the service interface that contains the rules for processing incoming traffic. Include a syslog option and associate a logical unit.

```
[edit interfaces sp-2/0/0]
user@host# edit services-options syslog host host-name services any
user@host# edit unit logical-unit-number family family
user@host# edit unit 0 family family
```

For example:

```
[edit interfaces sp-2/0/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
```

4. Configure the softwire concentrator and softwire rule for 6to4. In the Junos OS, 6to4 PMT configuration uses the same options as 6rd.

```
[edit services softwire softwire-concentrator v6rd v6to4]
user@host# set softwire-address softwire-addres
user@host# set ipv4-prefix ipv4-prefix
user@host# set v6rd-prefix v6rd-prefix
user@host# set mtu-v4 mtu-v4
```

For example:

```
[edit services softwire softwire-concentrator v6rd v6to4]
user@host# set softwire-address 192.88.99.1
user@host# set ipv4-prefix 130.130.130.2/32
user@host# set v6rd-prefix 2002::0/16
user@host# set mtu-v4 9192
```

5. Define the softwire rule that will process traffic on the ingress interface.

```
[edit services softwire rule v6to4-r1]
user@host# set match-direction input
user@host# set term term-name then v6rd softwire-concentrator
```

For example:

```
[edit services softwire rule v6to4-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd v6to4
```

6. Define a stateful firewall rule that will accept all incoming traffic on the ingress interface.

```
[edit services stateful-firewall rule sfw-r1]
user@host# set match-direction direction
user@host# set term term-name then accept
user@host# set term term-name then syslog
```

For example:

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

7. Define the NAT pool to be used for IPv6 NAT translation. This pool supports translation of the Anycast 6to4 relay addresses to addresses at the provider-managed relay.

```
[edit services nat pool v6to4-pmt]
user@host# set address address
user@host# port automatic
```

For example:

```
[edit services nat pool v6to4-pmt]
user@host# set address 3ABC::1/128
user@host# set port automatic
```

8. Define the NAT rule for translation.

```
[edit services nat rule rule-name]
```

```
user@host# set match-direction input
user@host# set term term-name then translated source-pool pool-name
user@host# set term t1 then translated translation-type translation-type
```

For example:

```
[edit services nat rule v6to4-pmt-r1]
user@host# set match-direction input
user@host# set term t1 then translated source-pool v6to4-pmt
user@host# set term t1 then translated translation-type napt-66
```

9. Define the service set that specifies the softwire rule and NAT rule.

```
[edit services service-set v6to4-pmt]
user@host# set softwire-rules rule-name
user@host# set stateful-firewall-rules rule-name
user@host# set nat-rules rule-name
user@host# set interface-service service-interface interface-name
```

For example:

```
[edit services service-set v6to4-pmt]
user@host# set softwire-rules v6to4-r1
user@host# set stateful-firewall-rules sfw-r1
user@host# set nat-rules v6to4-pmt-r1
user@host# set interface-service service-interface sp-2/0/0
```

CHAPTER 23

Transitioning to IPv6 Using DS-Lite Softwires

IN THIS CHAPTER

Configuring a DS-Lite Softwire Concentrator

DS-Lite is supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

To configure a DS-Lite softwire concentrator:

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

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

2. Specify the address of the softwire tunnel.

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

3. Specify the MTU for the softwire tunnel.

```
[edit services softwire softwire-concentrator ds-lite ds-lite-softwire-concentrator]
```

```
user@host# set mtu-v6 bytes
```

NOTE: The **mtu-v6** option is supported on MX Series routers equipped with MS-DPCs. Starting in Junos OS release 18.1R1, the **mtu-v6** option is supported on MX Series routers with MS-MICs or MS-MICs.

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. This statement is not supported on MS-MPCs and MS-MICs.

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

5. Specify the maximum number of flows for the softwire.

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

Release History Table

Release	Description
19.2R1	Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
18.1R1	Starting in Junos OS release 18.1R1, the **mtu-v6** option is supported on MX Series routers with MS-MPCs or MS-MICs.
17.4R1	Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

Tunneling Services for IPv4-to-IPv6 Transition Overview | 375

Configuring IPv6 Multicast Interfaces

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

To configure IPv6 multicast interfaces:

1. Access the softwire hierarchy.

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

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

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

Or configure all softwire interfaces as IPv6 multicast.

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

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | 375
- Configuring a 6rd Softwire Concentrator | 414
- Configuring a DS-Lite Softwire Concentrator | 389
- Configuring Softwire Rules | 381

Example: Basic DS-Lite Configuration

IN THIS SECTION

DS-Lite employs IPv4-over-IPv6 tunnels to cross an IPv6 access network to reach a carrier-grade IPv4-IPv4 NAT. This facilitates the phased introduction of IPv6 on the Internet by providing backward compatibility with IPv4. See *Understanding IPv6 Dual-Stack Lite*.

Requirements

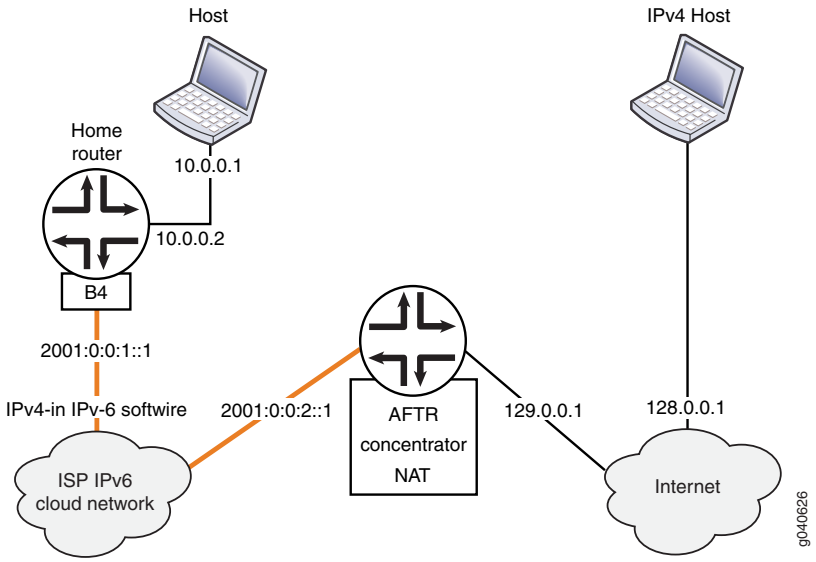
The following hardware components can perform DS-Lite:

- M Series Multiservice Edge routers with Multiservices PICs.
- T Series Core routers with Multiservices PICs.
- MX Series 5G Universal Routing Platforms with Multiservices DPCs. Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.

Configuration Overview and Topology

This example describes how configure an MX Series router with an MS-DPC as an AFTR to facilitate the flow shown in Figure 26 on page 392.

Figure 26: 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

IN THIS SECTION

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

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

1. Go the **[edit interfaces]** edit hierachy 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]** hierachy 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:

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

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

2. Define a NAT pool p1.

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

3. Define a NAT rule, beginning with the match direction.

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

4. 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
```

5. 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
```

6. (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;
        }
    }
```

Softwire Configuration

Step-by-Step Procedure

To configure the DS-Lite softwire concentrator and associated rules:

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

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

2. Define the DS-Lite softwire concentrator.

   ```
   [edit services softwire]
   user@host# set softwire-concentrator ds-lite ds-1 softwire-address 1001::1 mtu-v6 1460
   ```

3. Define the softwire rule.

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

Results

user@host# show services softwire

```
softwire-concentrator {
    ds-lite ds1 {
        softwire-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 softwire 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 softwire rule to define the softwire tunnel.

   ```
   [edit services service-set sset]
   user@host# set softwire-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;
    }
}
softwire-rules r1;
nat-rules r1;
interface-service {
    service-interface sp-0/0/0;
}
}
```

Release History Table

Release	Description
19.2R1	Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
17.4R1	Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | 375
- Configuring a DS-Lite Softwire Concentrator | 389
- Configuring Softwire Rules | 381
- Configuring Service Sets for Softwire | 383
- Example: Basic 6rd Configuration | 417
- Example: Configuring DS-Lite and 6rd in the Same Service Set | 400

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

IN THIS SECTION

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 5G Universal Routing Platforms with Multiservices DPCs. Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.Starting in Junos OS release 20.2R1, DS-Lite is supported for CGNAT Next Gen Services on MX240, MX480 and MX960 routers.

Overview

This example describes a softwire 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;
    }
}
```

Softwire Concentrator, Softwire Rule, Stateful Firewall Rule Configuration

Step-by-Step Procedure

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

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

```
user@host# edit services softwire softwire-concentrator ds-lite ds1
[edit services softwire softwire-concentrator ds-lite ds1]
user@host# set softwire-address 1001::1
user@host# mtu-v6 9192
usert@host# up 1
usert@host# edit v6rd v6rd-dom1
[edit services softwire softwire-concentrator v6rd v6rd-dom1]
```

```
user@host# set softwire-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 softwire rules.

```
user@host# edit services softwire rule v6rd-r1]
[edit services softwire 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 softwire]
[edit services softwire]
user@host# edit rule dslite-r1
[edit services softwire 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@host# 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@host# 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@host# 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 softwire]

user@host# show
```

```
softwire-concentrator {
    ds-lite ds1 {
        softwire-address 1001::1;
        mtu-v6 9192;
    }
    v6rd v6rd-dom1 {
        softwire-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@host# 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 softwire 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 softwire-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 {
    softwire-rules v6rd-r1;
    softwire-rules dslite-r1;
    stateful-firewall-rules r1;
    nat-rules dslite-nat-r1;
    interface-service {
        service-interface sp-3/0/0;
    }
```

Release History Table

Release	Description
20.2R1	Starting in Junos OS release 20.2R1, DS-Lite is supported for CGNAT Next Gen Services on MX240, MX480 and MX960 routers.
19.2R1	Starting in Junos OS release 19.2R1, DS-Lite is supported on MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers.
17.4R1	Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | 375
- Configuring Service Sets for Softwire | 383
- Example: Basic DS-Lite Configuration | 391
- Example: Basic 6rd Configuration | 417

Protecting CGN Devices Against Denial of Service (DOS) Attacks

IN THIS SECTION

You can now choose configuration options that help prevent or minimize the effect of attempted denial of service (DOS) attacks.

Mapping Refresh Behavior

Prior to the implementation of the new options for configuring NAT mapping refresh behavior, described in this topic, a conversation was kept alive when either inbound or outbound flows were active. This remains the default behavior. You can now also specify mapping refresh for only inbound flows or only outbound flows. To configure mapping refresh behavior, include the **mapping-refresh (inbound | outbound | inbound-outbound)** statement at the **[edit services nat rule *rule-name* term *term-name* then translated secure-nat-mapping]** hierarchy level.

EIF Inbound Flow Limit

Previously. the number of inbound connections on an EIF mapping was limited only by the maximum flows allowed on the system. You can now configure the number of inbound flows allowed for an EIF. To limit the number of inbound connections on an EIF mapping, include the **eif-flow-limit *number-of-flows*** statement at the **[edit services nat rule *rule-name* term *term-name* then translated secure-nat-mapping]** hierarchy level.

DS-Lite Subnet Limitation

IN THIS SECTION

DS-Lite Per Subnet Limitation Overview

Junos OS enables you to limit the number of softwire flows from a subscriber's basic bridging broadband (B4) device at a given point in time, preventing subscribers from excessive use of addresses within the subnet. This limitation reduces the risk of denial-of-service (DoS) attacks. This limitation is supported on MX Series routers equipped with MS-DPCs. Starting in Junos OS Release 18.2R1, MS-MPCs and MS-MICs also support the subnet limitation feature.Starting in Junos OS Release 19.2R1, MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers also support the subnet limitation feature.Starting in Junos OS release 20.2R1, DS-Lite is supported for CGNAT Next Gen Services on MX240, MX480 and MX960 routers.

A household using IPv6 with DS-Lite is a subnet, not just an individual IP address. The subnet limitation feature associates a subscriber and mapping with an IPv6 prefix instead of an IPv6 address. A subscriber can use any IPv6 addresses in that prefix as a DS-Lite B4 address and potentially exhaust carrier-grade NAT resources. The subnet limitation feature enables greater control of resource utilization by identifying a subscriber with a prefix instead of a specific address.

The subnet limit provides the following features:

- Flows utilize the complete B4 address.
- Prefix length can be configured per service set under softwire-options for the individual service-set.
- Port blocks are allocated per prefix of the subscriber B4 device, and not on each B4 address (if the prefix length is less than 128). If the prefix length is 128, then each IPv6 address is treated as a B4. Port blocks are allocated per 128-bit IPv6 address.
- Session limit, defined under the DS-Lite softwire concentrator configuration, limits the number of IPv4 sessions for the prefix.
- EIM, EIF, and PCP mappings are created per softwire tunnel (full 128 bit IPv6 address). Stale mappings time out based on timeout values.
- If prefix length is configured , then PCP **max-mappings-per-subscriber** (configurable under **pcp-server**) is based on the prefix only, and not the full B4 address.
- SYSLOGS for PBA allocation and release contain the prefix portion of the address completed with all zeros. SYSLOGS for PCP allocate and release, flow creation and deletion will still contain the complete IPv6 address.

The **show services nat mappings address-pooling-paired** operational command output now shows the mapping for the prefix. The mapping shows the address of the active B4.

The **show services softwire statistics ds-lite** output includes a new field that displays the number of times the session limit was exceeded for the MPC.

For Next Gen Services on MX240, MX480, and MX960 routers, the subnet limit statistic is displayed in the **Softwire session limit exceeded** field.

show services softwire statistics (MX-SPC3)

```
user@host> show services softwire statistics
vms-2/0/0
    Total Session Interest events       :3
    Total Session Destroy events                            :2
    Total Session Public Request events                     :0
    Total Session Accepts                                   :1
    Total Session Discards                                  :0
    Total Session Ignores                                   :0
    Total Session extension alloc failures                  :0
    Total Session extension set failures                    :0
Softwire statistics
    Total Softwire sessions created                         :1
    Total Softwire sessions deleted                         :2
    Total Softwire sessions created for reverse packets     :1
    Total Softwire session create failed for reverse pkts   :0
    Total Softwire rule match success                       :1
    Total Softwire rule match failed                        :0
    Softwire session limit exceeded                         :0
Softwire packet statistics
    Total Packets processed                                 :1
    Total packets encapsulated                              :1
    Total packets decapsulated                              :1
    Encapsulation errors                                    :0
    Decapsulation errors                                    :0
    Encapsulated pkts re-inject failures                    :0
    Decapsulated pkts re-inject failures                    :0
    DS-Lite ICMPv4 Echo replies sent                        :0
    DS-Lite ICMPv4 TTL exceeded messages sent               :0
    ICMPv6 ECHO request messages received destined to AFTR  :0
    ICMPv6 ECHO reply messages sent from AFTR               :0
    ICMPv6 ECHO requests to AFTR process failures           :0
    V6 untunnelled packets destined to AFTR dropped         :1
    Softwire policy add errors                              :0
    Softwire policy delete errors                           :0
    Softwire policy memory alloc failures                   :0
    Softwire Untunnelled packets ignored                    :0
Softwire Misc errors
    DS-Lite ICMPv4 TTL exceed message process errors        :0
```

SEE ALSO

show services nat source mappings address-pooling-paired | 1949

show services softwire statistics | 2056

Configuring DS-Lite Per Subnet Session Limitation to Prevent Denial of Service Attacks

You can configure the DS-Lite per subnet limitation on MX Series routers equipped with MS-DPCs. Starting in Junos OS Release 18.2R1, MS-MPCs and MS-MICs also support the subnet limitation feature. Starting in Junos OS Release 20.2R1, the Next Gen Services MX-SPC3 security services card supports the subnet limitation feature.

Starting in Junos OS Release 19.2R1, MX Virtual Chassis and MX Broadband Network Gateway (BNG) routers also support the subnet limitation feature.

To configure DS-Lite per subnet session limitation:

1. Configure the size of the subnet prefix to which limiting is applied. Specify a prefix length of 56, 64, 96, or 128.

   ```
   [edit}
   user@host# set services service-set service-set-name softwire-options dslite-ipv6-prefix-length
     dslite-ipv6-prefix-length
   ```

   NOTE: Ensure that all mappings are cleared before changing the prefix length.

2. If you are using a next-hop service set on an AMS interface for DS-Lite, set the AMS inside interface's IPv6 source prefix length to the same value you use for the subnet prefix in Step 1.

   ```
   [edit interfaces interface-name unit interface-unit-number load-balancing-options hash-keys]
   user@host# set ipv6-source-prefix-length ipv6-source-prefix-length
   ```

3. Configure the maximum number of subscriber sessions allowed per prefix. You can configure from 0 through 16,384 sessions.

   ```
   [edit}
   user@host# set services softwire softwire-concentrator dslite dslite-concentrator-name session-limit-per-prefix
     12
   ```

   For Next Gen Services DS-Lite, MAP-E and V6rd softwires, configure the maximum number of subscriber sessions allowed per prefix:

```
[edit}
user@host# set services softwires softwire-types ds-lite | map-e | v6rd session-limit-per-prefix limit
```

NOTE: You cannot use **flow-limit** and **session-limit-per-prefix** in the same **dslite** configuration.

SEE ALSO

- DS-Lite Per Subnet Limitation Overview | **410**
- clear services nat mappings | **1646**
- softwire-options | **1474**
- ds-lite | **1184**

CHAPTER 24

Transitioning to IPv6 Using 6rd Softwires

IN THIS CHAPTER

Configuring a 6rd Softwire Concentrator

The 6rd feature is supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. The 6rd feature is not supported on MX Series routers with MS-MPCs or MS-MICs.

To configure a 6rd softwire concentrator:

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

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

2. Specify the address of the softwire tunnel.

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

3. Specify the MTU for the softwire tunnel.

```
[edit services softwire softwire-concentrator v6rd v6rd-softwire-concentator]
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.

NOTE: Configuration changes to 6rd softwire concentrators do not become effective in the Packet Forwarding Engine. This is a known limitation. If you attempt to add the new configuration of softwire concentrators by overriding the existing configuration of 1024 softwire concentrators, which is the maximum limit of softwire concentrators that the system supports, the new configuration is not updated. To work around this limitation, you must delete the existing configuration and commit the settings, and then add the new configuration of softwire concentrators and commit the settings.

NOTE: For 6rd softwire concentrators, packet drops are observed and error messages logged on the virtual terminal session (VTY) console, if one inline services (**si-**) interface is replaced with another **si-** interface without stopping the traffic during the replacement of the interface. In a scenario in which an **si-** interface is associated with a service set that has a large number of softwire concentrators, replacing that interface without halting the traffic causes traffic disruption. You must stop the traffic and restart it during such a replacement of **si-** interfaces with 6rd softwire concentrators. The following error messages are displayed on the VTY console of the FPC:

packet discarded because no ifl or not SI ifl

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | **375**
- Configuring Softwire Rules | **381**
- Configuring Stateful Firewall Rules for 6rd Softwire | **416**
- Configuring Service Sets for Softwire | **383**
- Example: Basic 6rd Configuration | **417**

Example: Configuring DS-Lite and 6rd in the Same Service Set | 400

Configuring Stateful Firewall Rules for 6rd Softwire

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

The 6rd feature is supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. The 6rd feature is not supported on MX Series routers with MS-MPCs or MS-MICs.

To include a stateful firewall rule for 6rd softwire 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 softwire process.

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

RELATED DOCUMENTATION

Example: Basic 6rd Configuration

IN THIS SECTION

Requirements

NOTE: The 6rd feature is supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. The 6rd feature is not supported on MX Series routers with MS-MPCs or MS-MICs.

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 5G Universal Routing Platforms 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 softwire softwire-concentrator v6rd v6rd-dom1 softwire-address 30.30.30.1
set services softwire softwire-concentrator v6rd v6rd-dom1 ipv4-prefix 10.10.10.0/24
set services softwire softwire-concentrator v6rd v6rd-dom1 v6rd-prefix 3040::0/16
set services softwire softwire-concentrator v6rd v6rd-dom1 mtu-v4 9192
set services softwire rule v6rd-dom1 match-direction input
set services softwire rule v6rd-dom1 term t1 then v6rd v6rd-dom1
set services service-set v6rd-dom1-service-set softwire-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@host# 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;
        }
    }
}
```

Softwire Concentrator, Softwire Rule, and Stateful Firewall Rule Configuration

Step-by-Step Procedure

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

1. Define the 6rd softwire concentrator.

```
user@host# top
user@host# edit services softwire softwire-concentrator v6rd v6rd-dom1
```

2. Configure the softwire concentrator properties. Here, softwire address 30.30.30.1 is the softwire 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 softwire softwire-concentrator v6rd v6rd-dom1]
user@host# set softwire-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 softwire rule.

```
[edit services softwire softwire-concentrator v6rd v6rd-dom1]
user@host# up 2
[edit services softwire]
user@host# edit rule v6rd-dom1
[edit services softwire rule v6rd-dom1]
user@host# set match-direction input
[edit services softwire 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 softwire softwire-concentrator v6rd v6rd-dom1]
user@host# up 3
[edit servicesl]
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 softwire]
```

```
user@host# show
```

```
softwire-concentrator {
    v6rd v6rd-dom1 {
        softwire-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 softwire and stateful firewall rules for the service set.

   ```
   [edit services service-set v6rd-dom1-service-set]
   user@host# set softwire-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
```

```
softwire-rules v6rd-dom1-r1
    interface-service {
        service-interface sp-0/2/0;
    }
```

RELATED DOCUMENTATION

- Tunneling Services for IPv4-to-IPv6 Transition Overview | 375
- Configuring a 6rd Softwire Concentrator | 414
- Configuring Softwire Rules | 381
- Configuring Stateful Firewall Rules for 6rd Softwire | 416
- Configuring Service Sets for Softwire | 383
- Example: Basic DS-Lite Configuration | 391
- Example: Configuring DS-Lite and 6rd in the Same Service Set | 400

High Availability and Load Balancing for 6rd Softwires

IN THIS SECTION

NOTE: The 6rd feature is supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. The 6rd feature is not supported on MX Series routers with MS-MPCs or MS-MICs.

Load Balancing a 6rd Domain Across Multiple Services PICs

The 6rd domain is an IPv6 network, which can potentially be very large. A single PIC, or network processing unit (NPU) on a Multiservices DPC, might not be able to handle all the traffic for the 6rd domain. To alleviate load problems, you can load-balance the 6rd domain traffic across multiple PICs. To do so, assign the same softwire rule to different services sets that use different interfaces. Configure explicit routes and equal-cost multipath (ECMP) to load-balance the 6rd traffic.

Example: Load Balancing a 6rd Domain Across Multiple Services PICs

IN THIS SECTION

Hardware and Software Requirements

This example requires the following hardware:

- An MX Series 5G Universal Routing Platform with a services DPC with two available NPUs or an M Series Multiservice Edge router with two services PICs available for 6rd softwire concentrator processing
- A domain name server (DNS)

This example uses the following software:

- Junos OS Release 11.4 or higher

Overview

Because of anticipated volume, a provider needs to balance 6rd softwire traffic between two services PICs.

Configuration

IN THIS SECTION

Chassis Configuration

Step-by-Step Procedure

To configure the chassis:

1. Define the ingress interface and its properties.

```
user@host# edit interfaces ge-1/2/0
user@host# set unit 0 family inet address 10.10.10.1/16
```

2. Define the egress interface and its properties. In this example, the IPv6 clients try to reach the IPv6 server at 3abc::2/16.

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

3. Define the services PICs for selection as softwire concentrators by the load-balancing process. This configuration uses two PICs/NPUs: sp-3/0/0 and sp-3/1/0. A next-hop style service set is configured (shown in the next section).

```
user@host# edit interfaces sp-3/0/0
[edit interfaces ge-3/0/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
user@host# set unit 1 family inet service-domain inside
user@host# set unit 1 family inet service-domain outside
user@host# set unit 2 family inet service-domain inside
user@host# set unit 2 family inet service-domain outside
```

```
user@host# up 1
[edit]
user@host# edit interfaces sp-3/1/0
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host local services any
user@host# set unit 0 family inet
user@host# set unit 0 family inet6
user@host# set unit 1 family inet service-domain inside
user@host# set unit 1 family inet service-domain outside
user@host# set unit 2 family inet service-domain inside
user@host# set unit 2 family inet service-domain outside
```

Softwire Concentrator and Softwire Rule Configuration

Step-by-Step Procedure

The softwire configuration is straightforward. In this example, the 6rd domain prefix is 3040::0/16, the 6rd softwire concentrator IPv4 address is 30.30.30.1, and the customer IPv4 network is 10.10.0.0/16. In the customer premises equipment (CPE) network, all customer edge (CE) devices have addresses that belong to the 10.10.0.0/16 network. To configure the softwire:

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

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

2. Configure IPv6 multicast.

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

3. Go to the softtwire concentrator v6rd hierarchy level and name the softwire concentrator **shenick01-rd1**.

```
[edit services softwire]
user@host# edit softwire-concentrator v6rd shenick01-rd1
```

4. Configure the softwire concentrator properties.

```
[edit services softwire softwire-concentrator v6rdshenick01-rd1 ]
user@host# set softwire-address 30.30.30.1
user@host# set ipv4-prefix 10.10.0.0/16
user@host# set v6rd-prefix 3040::/16
```

```
user@host# set mtu-v4 9192
```

5. Configure a softwire rule for incoming 6rd traffic.

```
[edit services softwire softwire-concentrator v6rd shenick01-rd1 ]
user@host# up 1
[edit services softwire ]
user@host# edit rule shenick01-r1
[edit services softwire rule shenick01-r1]
user@host# set match-direction input
user@host# set term t1 then v6rd shenick01-rd1
```

Stateful Firewall Configuration

Step-by-Step Procedure

To configure the stateful firewall rule:

1. Go to the stateful firewall hierarchy level and define a rule.

```
user@host# edit services stateful-firewall rule r1
```

2. Set the match direction.

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

3. Configure a term that accepts all traffic.

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

Service Set Configuration

Step-by-Step Procedure

This configuration provides two service sets, each pointing to a different network processing unit (NPU). Both service sets use the same stateful firewall and softwire rules. Because they use the same softwire rule, they refer to same 6rd softwire concentrator. This results in the software concentrator being hosted on both the NPUs.

To configure the service set:

1. Define a service set for the first NPU.

```
user@host# edit services service-set v6rd-sset1
```

2. Configure the softwire and stateful firewall rules for the first NPU.

```
[edit services service-set v6rd-sset1]
user@host# set softwire-rules shenick01-r1
user@host# set stateful-firewall-rules r1
```

3. Configure the inside and outside interfaces for the next-hop service.

```
[edit services service-set v6rd-sset1]
user@host# set next-hop-service inside-service-interface sp-3/0/0.1
user@host# set next-hop-service outside-service-interface sp-3/0/0.2
```

4. Define a service set for the second NPU.

```
user@host# edit services service-set v6rd-sset2
```

5. Configure the softwire and stateful firewall rules for the second NPU.

```
[edit services service-set v6rd-sset2]
user@host# set softwire-rules shenick01-r1
user@host# set stateful-firewall-rules r1
```

6. Configure the inside and outside interfaces for the next-hop service.

```
[edit services service-set v6rd-sset1]
user@host# set next-hop-service inside-service-interface sp-3/1/0.1
user@host# set next-hop-service outside-service-interface sp-3/1/0.2
```

Load-Balancing Configuration

Step-by-Step Procedure

To configure load balancing:

Configure explicit routes and ECMP to load-balance the 6rd traffic. Configure explicit routes for both the 6rd concentrator IPv4 address and the 6rd domain prefix, so that they point to both NPUs.

1. To configure static routes for the 6rd domain using the routing-table inet6.0, go to the **[edit forwarding-options rib inet6.0 static]** hierarchy level and set the routes for the 6rd domain and the 6rd concentrator IPv4 address.

```
user@host edit forwarding-options rib inet6.0 static
[edit forwarding-options rib inet6.0 static]
user@host# set route 3040::0/16 next-hop [ sp-3/0/0.2 sp-3/1/0.2 ]
user@host# set route 30.30.30.1/32 next-hop [ sp-3/0/0.1 sp-3/1/0.1 ]
```

   The service PIC daemon (spd) also adds default routes to these addresses pointing to the NPUs. However, the routes added by the spd use different metrics, which are computed based on the FPC, PIC, slot numbers, and subunit of the services PIC if used in the service set configuration. The static routes configured in this sample configuration will have metrics of 5 and therefore a higher preference than the spd-added routes.

   The explicitly configured routes are as follows:

   root@host# `run show route 30.30.30.1`

```
inet.0: 37 destinations, 40 routes (36 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

30.30.30.1/32      *[Static/5] 00:00:10
                    > via sp-3/0/0.1
                      via sp-3/1/0.1
                    [Static/786433] 00:23:03
                    > via sp-3/0/0.1
                    [Static/851969] 00:00:09
                    > via sp-3/1/0.1
```

   root@host# `run show route 3040::/16`

```
inet6.0: 20 destinations, 33 routes (20 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

3040::/16          *[Static/5] 00:00:15
                      via sp-3/0/0.2
```

```
                    > via sp-3/1/0.2
                    [Static/786434] 00:23:08
                    > via sp-3/0/0.2
                    [Static/851970] 00:00:14
                    > via sp-3/1/0.2
```

BEST PRACTICE: The spd-installed routes have higher metric values (hence a low preference) and the metrics are different. If the metrics are different and ECMP is not enabled, even though multiple routes exist for the same destination, only one of the routes is picked up all the time (based on the metric). For ECMP you must configure equal-cost routes, and hence a manual configuration of routes is needed as shown above.

2. Configure equal-cost multipath (ECMP) load balancing by configuring the hash key at the **[edit forwarding-optionshash-key]** hierarchy level.

```
user@host#  forwarding-options hash-key
[edit forwarding-options hash-key]
user@host#  set family inet layer-3 destination-address
user@host#  set family inet layer-3 source-address
user@host#  set family inet6 layer-3 destination-address
user@host#  set family inet6 layer-3 source-address
```

3. Verify your configuration by displaying **forwarding-options**.

user@host# show forwarding-options

```
hash-key {
    family inet {  <== IPv4 traffic from CEs uses this
        layer-3 {
            destination-address;
            source-address;
        }
    }
    family inet6 {  <== IPv6 traffic from Internet uses this
        layer-3 {
            destination-address;
            source-address;
        }
    }
}
```

TIP: Both IPv4 and IPv6 hash keys must be configured. The IPv4 hash key is used to distribute the traffic coming from CPE devices to the 6rd branch relay. The IPv6 hash key is used to distribute the traffic coming from the IPv6 Internet to the 6rd domain. Because the hash in the forward and reverse direction is for different families, different flows from the same session can reside on different NPUs. However, 6rd processing is stateless (as far as mapping IPv6 packets to softwires is concerned), so this should not be a problem.

Configuring High Availability for 6rd Using 6rd Anycast

You configure 6rd Anycast by defining two service sets that use the same softwire rule in both service sets, just as you do when you configure load balancing for 6rd. However, you do not configure ECMP, and as a result, the services PIC daemon (spd) installs two routes *each* for the softwire concentrator address and 6rd domain pointing to each service interface. The forwarding plane can select any route based on the priority, which is computed when the spd installs the routes. The priority is computed based on the FPC, PIC, slot numbers, and subunit number used on the sp- interface. *Only one PIC is used* based on the route priority, and that PIC gets all of the 6rd traffic. If the PIC goes down. the route pointing to it is also deleted and the forwarding plane automatically selects the alternate available PIC.

6rd Anycast is completely stateless. The spd installs the route and doesn't run any state machine for the PIC. Because the routes are pre-installed and service sets are already on the PIC, there is no service delay if a failover occurs.

RELATED DOCUMENTATION

Tunneling Services for IPv4-to-IPv6 Transition Overview | 375

Configuring Inline 6rd

IN THIS SECTION

Junos OS supports inline 6rd on all Modular Port Concentrator (MPC) line cards on MX Series routers. This saves customers the cost of using MS-DPCs for the required tunneling, encapsulation, and decapsulation processes. Anycast is supported for 6to4 (next-hop service interfaces only). Hairpinning is also supported for traffic between 6rd domains.

Junos OS supports inline 6rd on the following MPCs:

- MPC5 and MPC6—Support starting in Junos OS Release 15.1R3.
- MPC7, MPC8, and MPC9—Support starting in Junos OS Release 17.2R1.
- MPC10E-15C-MRATE and MPC10E-10C-MRATE—Support starting in Junos OS Release 20.3R1.
- MX2K-MPC11E—Support starting in Junos OS Release 20.3R1.

To implement the inline functionality, you configure service interfaces on the MPC as inline services interfaces (si-) rather than as multiServices (ms-) interfaces.

Configuring the Bandwidth for Inline Services

You must provide bandwidth configuration for inline services on the modular port concentrator (MPC) used for inline 6rd processing.

To configure bandwidth:

- Specify the MPC and logical interface, and the desired bandwidth, 1g or 10g.

  ```
  user@host# set chassis fpc mpc-number pic logical-interface-number inline-services bandwidth bandwidth
  ```

  For example:

  ```
  user@host# set chassis fpc 0 pic 0 inline-services bandwidth 10g
  ```

Configuring the Interfaces

Configure the si- interfaces for 6rd control and data. 6rd services must be configured on port 0.

To configure the si- interfaces:

1. Configure the 6rd services on port 0 and include units for IPv4 and IPv6.

   ```
   user@host# set interfaces si-mpc-number/logical-interface-number/0 unit 0 family inet
   user@host# set interfaces si-mpc-number/logical-interface-number/0 unit 0 family inet6
   ```

   For example:

```
user@host# set interfaces si-0/0/0 unit 0 family inet
user@host# set interfaces si-0/0/0 unit 0 family inet6
```

2. Configure the media interfaces for the inside service domain.

```
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number family inet
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number family inet6
user@host# set interfaces si-0/0/0 unit unit-number service-domain inside
```

For example:

```
user@host# set interfaces si-0/0/0 unit 1 family inet
user@host# set interfaces si-0/0/0 unit 1 family inet6
user@host# set interfaces si-0/0/0 unit 1 service-domain inside
```

3. Configure the media interfaces for the outside service domain.

```
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number family inet
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number family inet6
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number service-domain outside
```

For example:

```
user@host# set interfaces si-0/0/0 unit 2 family inet
user@host# set interfaces si-0/0/0 unit 2 family inet family inet6
user@host# set interfaces si-mpc-number/logical-interface-number/0 unit unit-number service-domain outside
```

4. Configure the IPv4-facing interface for use with an interface-style or next-hop service set.

   - To configure for use with an interface-style service set, configure input and output service and specify the service set.

```
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet service
    input service-set service-set-name
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet service
    output service-set service-set-name
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet
    address ip-address
```

   For example:

```
user@host# set interfaces ge-0/2/7 unit 0 family inet service input service-set vrf-intf-service-set
user@host# set interfaces ge-0/2/7 unit 0 family inet service output service-set vrf-intf-service-set
user@host# set interfaces ge-0/2/7 unit 0 family inet address 10.10.10.1/16
```

- To configure for use with a next-hop style service set, omit the **service input** and **service output** references.

```
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet
    address ip-address
```

For example:

```
user@host# set interfaces ge-0/2/7 unit 0 family inet
user@host# set interfaces ge-0/2/7 unit 0 family inet address 10.10.10.1/16
```

5. Configure the IPv6 facing interface.

```
user@host# set interfaces ge-mpc-number/logical-interface-number/port unit unit-number family inet6 address
    ipv6-address
```

For example:

```
user@host# set interfaces ge-0/2/8 unit 0 family inet6 address 3abc::1/16
```

Configuring the Softwire Concentrator and Rule

Define the softwire concentrator and rule used for encapsulation and decapsulation of IPv6 over IPv4 packets for CE.

To define the softwire concentrator:

1. Specify a 6rd softwire concentrator and its address.

```
user@host# set services softwire softwire-concentrator v6rd concentrator-name softwire-address ip-address
```

For example:

```
user@host# set services softwire softwire-concentrator v6rd swire01-rd1 softwire-address 30.30.30.1
```

2. Configure the IPv4 address prefix for the customer edge network and the IPv6 address prefix for the 6rd domain.

```
user@host# set services softwire softwire-concentrator v6rd concentrator-name ipv4-prefix ipv4-prefix
  v6rd-prefix v6rd-prefix
```

   For example:

```
user@host# set services softwire softwire-concentrator v6rd swire01-rd1 ipv4-prefix 10.10.0.0/16 v6rd-prefix
  3040::0/16
```

3. Configure the size, in bytes, of the maximum transmission unit **mtu-ipv4** for IPv6 packets encapsulated in IPv4. Compute this as the maximum expected IPv4 packet size plus 20.

```
user@host# set services softwire softwire-concentrator v6rd concentrator-name set mtu-ipv4 number-of-bytes
```

   For example:

```
user@host# set services softwire softwire-concentrator v6rd swire01-rd1 set mtu-ipv4 9192
```

To configure the softwire rule:

- Specify the softwire rule, specifying the direction of traffic to be tunneled and the 6rd softwire concentrator to be used.

```
user@host# set services softwire rule softwire-rule-name match-direction match-direction term
  rule-term-number then v6rd concentrator-name
```

   For example:

```
user@host# set services softwire rule swire01-r1 match-direction input term t1 then v6rd swire01-rd1
```

Configuring the Service Set

To configure an interface style or next-hop service set for 6rd processing:

- Specify an interface style service set.

```
user@host# set services service-set service-set-name softwire-rules softwire-rule-name service-interface
  interface-name
```

For example:

```
user@host# set services service-set vrf-intf-service-set softwire-rules swire01-r1 service-interface si-0/0/0.0
```

or

- Configure a next-hop service set.

```
user@host# set services service-set service-set-name softwire-rules softwire-rule-name
user@host# set services service-set service-set-name next-hop-service inside-service-interface inside-interface
    outside-service-interface outside-interface
```

```
user@host# set services service-set vrf-nh-service-set softwire-rules swire01-r1
user@host# set services service-set vrf-nh-service-set next-hop-service inside-service-interface si-0/0/0.1
    outside-service-interface si-0/0/0.2
```

Configuring the Routing Instance

To configure the routing instance:

1. Specify the routing instance and each interface it serves.

```
user@host# set routing-instance routing-instance-name instance-type vrf interface interface-name
```

For example:

```
user@host# set routing-instance v6rd-vrf instance-type vrf interface si-0/0/0.1
user@host# set routing-instance v6rd-vrf instance-type vrf interface interface ge-0/2/7.0
```

2. Specify the route distinguisher and vrf-target.

```
user@host# set routing-instance v6rd-vrf route-distinguisher 1.1.1.1:1
user@host# set routing-instance v6rd-vrf vrf-target target:100:100
```

RELATED DOCUMENTATION

Configuring a 6rd Softwire Concentrator | 414

Configuring Softwire Rules

Configuring Inline 6rd | 431

Inline 6rd and 6to4 Configuration Guidelines

Keep the following points in mind when you are configuring and using inline 6rd and 6to4.

- You can configure a maximum of 1024 softwire concentrators on a single line card.
- Reassembly of 6rd IPv4 packet from CE is not added as part of this release.
- 6rd multicast is not supported.
- Any ICMPv4 errors generated in the IPv4 access network (between CPE and border relays) are dropped on the border relay. They are not converted into IPv6 errors and forwarded to IPv6 side.
- 6rd/6to4 Anycast and load balancing can be configured only using next-hop style service-interface configuration, not interface style.
- The si- interface input features are not exercised for packets flowing to the 6rd tunnel.
- Bandwidth for traffic from the 6rd tunnel is limited by the available PFE bandwidth; bandwidth for traffic to the 6rd tunnel is limited by the internal VRF loopback bandwidth. SI-IFD loopback bandwidth configuration under the **[edit chassis]** hierarchy has no impact on the 6rd loopback bandwidth.
- If the packet length is more than Tunnel MTU for downlink packets after encapsulating with an IPv4 header, the packet is dropped as v4 MTU errors. For these packet drops an **ICMPv6 packet too big error** message is sent back to the sender. Typically 6rd Tunnel MTU is configured with a high value so if the packet size is larger than the configured value, fragmentation occurs at the egress interface (towards the IPv4 access network).

Examples: 6rd and 6to4 Configurations

IN THIS SECTION

NOTE: The 6rd and 6to4 features are supported on Multiservices 100, 400, and 500 PICs on M Series routers, and on MX Series routers equipped with Multiservices DPCs. MX Series routers with MS-MPCs or MS-MICs support inline 6rd and inline 6to4 features.

Example: 6rd with Interface-Style Service Set Configuration

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 10g;
            }
        }
    }
}
services {
    service-set vrf-intf-service-set {
        softwire-rules swire01-r1;
        interface-service {
            service-interface si-0/0/0.0;
        }
    }
    softwire {
        softwire-concentrator {
            v6rd swire01-rd1 {
                softwire-address 30.30.30.1;
                ipv4-prefix 10.10.0.0/16;
                v6rd-prefix 3040::0/16;
                mtu-v4 9192;
            }
        }
        rule swire01-r1 {
            match-direction input;
            term t1 {
                then {
                    v6rd swire01-rd1;
                }
            }
        }
    }
}
```

```
interfaces {
    si-0/0/0 {
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
    ge-0/2/7 {
        unit 0 {
            family inet {
                address 10.10.10.1/16;
            }
        }
    }
    ge-0/2/8 {
        unit 0 {
            family inet6 {
                address 3abc::1/16;
            }
        }
    }
}
routing-instances {
    v6rd-vrf {
        instance-type vrf;
        interface si-0/0/0.1;
        interface ge-0/2/7.0;
        route-distinguisher 1.1.1.1:1;
        vrf-target target:100:100;
    }
}
```

Example: 6rd with Next-Hop-Style Service Set Configuration

```
chassis {
    fpc 0 {
        pic 0 {
```

```
            inline-services {
                bandwidth 10g;
            }
        }
    }
}
services {
    service-set vrf-nh-service-set {
        softwire-rules swire01-r1;
        next-hop-service {
            inside-service-interface si-0/0/0.1;
            outside-service-interface si-0/0/0.2;
        }
    }
    softwire {
        softwire-concentrator {
            v6rd swire01-rd1 {
                softwire-address 30.30.30.1;
                ipv4-prefix 10.10.0.0/16;
                v6rd-prefix 3040::0/16;
                mtu-v4 9192;
            }
        }
        rule swire01-r1 {
            match-direction input;
            term t1 {
                then {
                    v6rd swire01-rd1;
                }
            }
        }
    }
}
interfaces {
    si-0/0/0 {
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
```

```
        }
    }
    ge-0/2/7 {
        unit 0 {
            family inet {
                address 10.10.10.1/16;
            }
        }
    }
    ge-0/2/8 {
        unit 0 {
            family inet6 {
                address 3abc::1/16;
            }
        }
    }
}
routing-instances {
    v6rd-vrf {
        instance-type vrf;
        interface si-0/0/0.1;
        interface ge-0/2/7.0;
        route-distinguisher 1.1.1.1:1;
        vrf-target target:100:100;
    }
}
```

Example: 6rd Anycast Configuration

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 10g;
            }
        }
        pic 2 {
            inline-services {
                bandwidth 1g;
            }
        }
    }
}
```

```
services {
    service-set anycast-nh-set1 {
        softwire-rules swire01-r1;
        next-hop-service {
            inside-service-interface si-0/0/0.1;
            outside-service-interface si-0/0/0.2;
        }
    }
    service-set anycast-nh-set2 {
        softwire-rules swire01-r1;
        next-hop-service {
            inside-service-interface si-0/2/0.1;
            outside-service-interface si-0/2/0.2;
        }
    }
    softwire {
        softwire-concentrator {
            v6rd swire01-rd1 {
                softwire-address 30.30.30.1;
                ipv4-prefix 10.10.0.0/16;
                v6rd-prefix 3040::0/16;
                mtu-v4 9192;
            }
        }
        rule swire01-r1 {
            match-direction input;
            term t1 {
                then {
                    v6rd swire01-rd1;
                }
            }
        }
    }
}
interfaces {
    si-0/0/0 {
        unit 0 {
            family inet;
            family inet6;
        }
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
```

```
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
    si-0/2/0 {
        unit 0 {
            family inet;
            family inet6;
        }
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
    ge-0/2/7 {
        unit 0 {
            family inet {
                address 10.10.10.1/16;
            }
        }
    }
    ge-0/2/8 {
        unit 0 {
            family inet6 {
                address 3abc::1/16;
            }
        }
    }
}
```

Example: Hairpinning Between 6rd Domains Configuration

This example uses an interface service-set and a next-hop service set as hairpinning domains.

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 10g;
            }
        }
    }
}
services {
    service-set hairpin-intf-service-set {
        softwire-rules swire01-r1;
        interface-service {
            service-interface si-0/0/0.0;
        }
    }
    service-set hairpin-nh-service-set {
        softwire-rules swire01-r2;
        next-hop-service {
            inside-service-interface si-0/0/0.1;
            outside-service-interface si-0/0/0.2;
        }
    }
    softwire {
        softwire-concentrator {
            v6rd swire01-rd1 {
                softwire-address 30.30.30.1;
                ipv4-prefix 10.10.0.0/16;
                v6rd-prefix 3040::0/16;
                mtu-v4 9192;
            }
            v6rd swire01-rd2 {
                softwire-address 60.60.60.1;
                ipv4-prefix 40.40.40.0/24;
                v6rd-prefix 3050::0/16;
                mtu-v4 9192;
            }
        }
        rule swire01-r1 {
            match-direction input;
            term t1 {
                then {
                    v6rd swire01-rd1;
                }
```

```
            }
        }
        rule swire01-r2 {
            match-direction input;
            term t1 {
                then {
                    v6rd swire01-rd2;
                }
            }
        }
    }
}
interfaces {
    si-0/0/0 {
        unit 0 {
            family inet;
            family inet6;
        }
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
    ge-0/2/7 {
        unit 0 {
            family inet {
                service {
                    input {
                        service-set hairpin-intf-service-set;
                    }
                    output {
                        service-set hairpin-intf-service-set;
                    }
                }
                address 10.10.10.1/16;
            }
        }
    }
```

```
    ge-0/2/8 {
        unit 0 {
            family inet {
                address 40.40.40.1/24;
            }
        }
    }
}
```

Example: 6to4 Configuration

```
chassis {
    fpc 0 {
        pic 0 {
            inline-services {
                bandwidth 10g;
            }
        }
    }
}
services {
    service-set 6to4-intf-service-set {
        softwire-rules shenick01-r1;
        interface-service {
            service-interface si-0/0/0.0;
        }
    }
    interfaces {
        si-0/0/0 {
            unit 0 {
                family inet;
                family inet6;
            }
            unit 1 {
                family inet;
                family inet6;
                service-domain inside;
            }
            unit 2 {
                family inet;
                family inet6;
                service-domain outside;
            }
```

```
    }
    ge-0/2/7 {
      unit 0 {
        family inet {
          service {
            input {
              service-set 6to4-intf-service-set;
            }
            output {
              service-set 6to4-intf-service-set;
            }
          }
          address 10.10.10.1/16;
        }
      }
    }
    ge-0/2/8 {
      unit 0 {
        family inet6 {
          address 3abc::1/16;
        }
      }
    }
  }
```

RELATED DOCUMENTATION

- Configuring a 6to4 Provider-Managed Tunnel

CHAPTER 25

Transitioning to IPv6 Using Mapping of Address and Port with Encapsulation (MAP-E)

IN THIS CHAPTER

Configuring Mapping of Address and Port with Encapsulation (MAP-E)

IN THIS SECTION

Understanding Mapping of Address and Port with Encapsulation (MAP-E)

IN THIS SECTION

This topic provides an overview of Mapping of Address and Port with Encapsulation (MAP-E) feature and its benefit to service providers when used as an inline service on MX Series routers with MPC and MIC

interfaces. Starting in Junos OS release 20.2R1, MAP-E softwires are supported under Next Gen Services on either an MPC or MIC by specifying the inline services **si-1/1/0** naming convention. Starting in Junos OS release 20.3R1, MPC10E and MX2K-MPC11E support MAP-E.

Benefits of Mapping of Address and Port with Encapsulation (MAP-E)

Reduces administrative overhead and creates a scalable network infrastructure that easily supports connectivity to a large number of IPv4 subscribers over the ISP's IPv6 access network.

Mapping of Address and Port with Encapsulation (MAP-E) Terminology

Border Relay (BR)—MAP-E-enabled provider edge device in a MAP domain. A BR device has at least an IPv6-enabled interface and an IPv4 interface connected to the native IPv4 network.

MAP-E Customer Edge (CE)—MAP-E-enabled customer edge device in a MAP deployment.

MAP domain—One or more MAP-E CE devices and BR devices connected to the same virtual link.

Port Set ID (PSID)—Separate part of the transport layer port space that is denoted as port set ID.

Embedded Address (EA) Bits—EA-bits in the IPv6 address identify an IPv4 prefix or address or a shared IPv4 address and a port-set identifier.

Softwire—Tunnel between two IPv6 end-points to carry IPv4 packets or two IPv4 end-points to carry IPv6 packets.

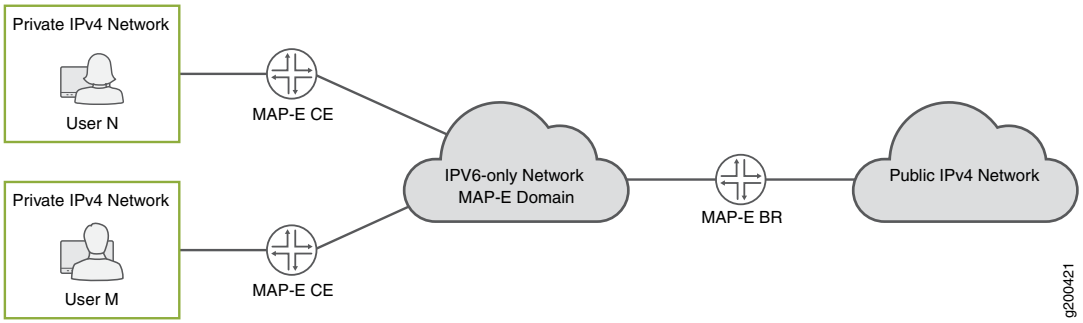
Softwire Initiator (SI)—Softwire at the customer end that encapsulates native packets and tunnels them to a softwire concentrator at the service provider.

Softwire Concentrator (SC)—Softwire that decapsulates the packets received from a softwire initiator and sends them to their destination.

Mapping of Address and Port with Encapsulation (MAP-E) Functionality

Figure 27 on page 449 illustrates a simple MAP-E deployment scenario.

Figure 27: Sample MAP-E Deployment



In the MAP-E network topology, there are two MAP-E customer edge (CE) devices, each connected to a private IPv4 host. The MAP-E CE devices are dual stack and are capable of Network Address Port Translation (NAPT). The MAP-E CE devices connect to a MAP-E Border Relay (BR) device through an IPv6-only MAP-E

network domain. The MAP-E BR device is dual stack and is connected to both a public IPv4 network and an IPv6 MAP-E network.

The MAP-E functionality is as follows:

1. The MAP-E CE devices are capable of NAPT. On receiving an IPv4 packet from the host, the MAP-E CE device performs NAT translation on the incoming IPv4 packets.

2. The NAT translated IPv4 packets are then encapsulated into IPv6 packets by the MAP-E CE device, and sent to the MAP-E BR device.

3. The IPv6 packet gets transported through the IPv6-only service provider network and reaches the MAP-E BR device.

4. On receiving the IPv6 packets, the incoming IPv6 packets are decapsulated by the MAP-E CE device and routed to the IPv4 public network.

In the reverse path, the incoming IPv4 packet is encapsulated into an IPv6 packet by the MAP-E BR device, and routed to the MAP-E CE devices.

Mapping of Address and Port with Encapsulation (MAP-E) Supported and Unsupported Features

Junos OS supports the following MAP-E features and functionality:

- MAP-E implementation supports line card throughput of 100 Gigabits.
- support for Inline MAP-E Border Relay (BR) solution that adheres to draft version 03 of RFC 7597

  Fully compliant with draft version 03 of RFC 7597, *Mapping of Address and Port with Encapsulation (MAP)*, when the **version-3** option is disabled at the **services softwires softwire-types map-e *map-e-concentrator-name***
- Support chassis-wide scale of 250 shared MAP-E rules.
- Support the feature on all MPCs using service interfaces with 100 Gigabits.
- Ability to ping MAP-E BR IPv6 address.
- Support only next-hop style of configuration for MAP-E.
- Support reassembly of fragmented IPv4 traffic arriving from IPv4 network before encapsulating it into an IPv6 packet.
- Support fragmentation of inner IPv4 packet if the packet size after encapsulation exceeds the MAP-E maximum transmission unit (MTU).
- Packets having Internet Control Message Protocol (ICMP) payload with the following message types are accepted for MAP-E encapsulation and decapsulation:

  - Echo or Echo Reply Message of type 0 and 8
  - Timestamp or Timestamp Reply Message of type 13 and 14
  - Information Request or Information Reply Message of type 15 and 16
  - Source quench, destination_unreachable, time_exceeded, Icmp_redirect, Icmp_address_mask_reply and parameter_problem errors
- Border Relay (BR) anycast is supported.

The following features and functionality are not supported with the MAP-E feature:

- Anti-spoof check is not supported for fragmented IPv4 packets coming from a customer edge (CE) device.
- Section 8.2 of the Internet draft draft-ietf-softwire-map-03 (expires on July 28, 2013), *Mapping of Address and Port with Encapsulation (MAP)* is not supported. Instead of responding with an ICMPv6 Destination Unreachable, Source address failed ingress/egress policy (Type 1, Code 5) message, spoof packets are silently dropped and the counter is incremented.
- IPv6 reassembly is not supported.
- ICMP v6-to-v4 translation at the BR is not supported.
- Inline MAP-E with virtual routing and forwarding (VRF) is not supported.
- Inline MAP-E with inline Network Address Translation (NAT) or dual stack (DS)-Lite is not supported.
- Interface-style MAP-E configuration is not supported.

Configuring Mapping of Address and Port with Encapsulation (MAP-E)

This example shows you how to configure the MAP-E Border Relay (BR) solution using a next hop-based style of configuration.

To configure MAP-E:

1. Create service interface on the device with 100g bandwidth support.

```
[edit chassis]
user@host# set fpc 0 pic 0 inline-services bandwidth 100g
```

2. Configure the dual stack service interface unit 0.

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

3. Configure service interface inside the dual stack domain.

```
[edit interfaces]
user@host# set si-0/0/0 unit 1 family inet
user@host# set si-0/0/0 unit 1 family inet family inet6
user@host# set si-0/0/0 unit 1 service-domain inside
```

4. Configure service interface outside the dual stack domain.

```
[edit interfaces]
user@host# set si-0/0/0 unit 2 family inet
user@host# set si-0/0/0 unit 2 family inet family inet6
user@host# set si-0/0/0 unit 2 service-domain outside
```

5. Configure the IPv4-facing interface on BR.

```
[edit interfaces]
user@host# set ge-0/2/7 unit 0 family inet address 10.10.10.1/16
```

6. Configure the CPE-facing interface on BR.

```
[edit interfaces]
user@host# set ge-0/2/8 unit 0 family inet6 address 3abc::1/16
```

7. Configure the MAP-E softwire concentrator and associated parameters.

```
[edit services softwire softwire-concentrator]
user@host# set map-e swire01-rd1 version03
user@host# set map-e swire01-rd1 softwire-address 2001:db8:ffff::1
user@host# set map-e swire01-rd1 ipv4-prefix 10.10.0.0/16 mape-prefix 3040::0/16
user@host# set map-e swire01-rd1 ea-bits-len 16
user@host# set map-e swire01-rd1 psid-offset 6
user@host# set map-e swire01-rd1 psid-length 8
user@host# set map-e swire01-rd1
user@host# set mtu-ipv6 9192
user@host# set map-e swire01-rd1 v4-reassembly
```

NOTE:

When configuring the MAP-E softwire concentrator, take the following into consideration:

- Possible values for **ea-bits-len** is 0 through 48.
- Possible values for **v4-prefix-len** is 0 through 32.
- If **v4-prefix-len** is 0 then **ea-bits-len** must be non-zero, and vice versa.
- It is possible that **ea-bits-len** is equal to 0, but **psid-len** is non-zero.
- If the sum of **v4-prefix-len** and **ea-bits-len** is less than 32, then the **psid-len** must be equal to the difference between 32 and the sum total of **v4-prefix-len** and **ea-bits-len**.
- The MAP-E IPv4 and IPv6 prefix must be unique per softwire concentrator.
- MAP-E PSID offset has a default value of 4, and MAP-E tunnel maximum transmission unit (MTU) has a default value of 9192.

8. Configure a softwire rule to specify the direction of traffic to be tunneled and the MAP-E softwire concentrator to be used.

```
[edit services softwire]
user@host# set rule swire01-r1 match-direction input term t1 then map-e swire01-rd1
```

9. Configure the service set for MAP-E.

```
[edit services service-set]
user@host# set mape-nh-service-set softwire-rules swire01-r1
user@host# set mape-nh-service-set next-hop-service inside-service-interface si-0/0/0.1
   outside-service-interface si-0/0/0.2
```

For example:

```
chassis {
   fpc 4 {
      pic 0 {
         inline-services {
            bandwidth 100g;
         }
      }
   }
   fpc 5 {
```

```
        pic 0 {
            inline-services {
                bandwidth 100g;
            }
        }
    }
}
services {
    service-set sset1 {
        softwire-rules sw-rule1;
        next-hop-service {
            inside-service-interface si-4/0/0.1;
            outside-service-interface si-4/0/0.2;
        }
    }
    service-set sset2 {
        softwire-rules sw-rule1;
        next-hop-service {
            inside-service-interface si-5/0/0.1;
            outside-service-interface si-5/0/0.2;
        }
    }
    softwire {
        softwire-concentrator {
            map-e mape-domain-1 {
                softwire-address 2001:db8:ffff::1;
                ipv4-prefix 192.0.2.0/24;
                mape-prefix 2001:db8:1234:ab00::/56;
                ea-bits-len 16;
                psid-offset 4;
                psid-length 8;
                mtu-v6 9192;
                version-03;
            }
        }
        rule sw-rule1 {
            match-direction input;
            term t1 {
                then {
                    map-e mape-domain-1;
                }
            }
        }
    }
```

```
}
interfaces {
    xe-0/1/1 {
        unit 0 {
            family inet6 {
                address 2001:db8::1/32 {
                    ndp 2001:db8:6434:0:00c0:0002:6400:3400 mac 00:11:22:33:44:55;
                }
            }
        }
    }
    xe-0/1/2 {
        unit 0 {
            family inet {
                address 100.1.1.1/24 {
                    arp 100.1.1.2 mac 00:11:22:33:44:55;
                }
            }
        }
    }
    si-4/0/0 {
        unit 1 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
    si-5/0/0 {
        unit 1 {
            family inet6;
            service-domain inside;
        }
        unit 2 {
            family inet;
            family inet6;
            service-domain outside;
        }
    }
}
```

Release History Table

Release	Description
20.3R1	Starting in Junos OS release 20.3R1, MPC10E and MX2K-MPC11E support MAP-E.
20.2R1	Starting in Junos OS release 20.2R1, MAP-E softwires are supported under Next Gen Services on either an MPC or MIC by specifying the inline services **si-1/1/0** naming convention.

RELATED DOCUMENTATION

map-e | **1293**

Equal Cost Multiple Path (ECMP) support for Mapping of Address and Port with Encapsulation (MAP-E)

IN THIS SECTION

Equal Cost Multiple Path (ECMP) support for Mapping of Address and Port with Encapsulation (MAP-E)

This topic provides an overview of Equal Cost Multiple Path (ECMP) support for Mapping of Address and Port with Encapsulation (MAP-E) feature and its benefit to service providers when used as an inline service on MX Series routers with MPC and MIC interfaces.

In a MAP-E network topology, in the reverse path, the border relay router receives IPv4 traffic and encapsulates it in a IPv6 packet. Longer routes are used for faster matching. However, they do not facilitate EMCP load balancing on the PIC, as the routes point to a single PIC. Starting in 19.3R1, you can disable auto-routes by configuring the **disable-auto-route** statement at the **[edit services softwire softwire-concentrator map-e <*domain-name*>]** hierarchy, and direct the static routes to an ECMP load balancer. Hence, the packets can be distributed among different inline service interfaces.

Benefits

Enable load-balancing by distributing packets among different inline service interfaces.

Disabling auto-routes to support ECMP with Mapping of Address and Port with Encapsulation (MAP-E)

This example shows you how to disable auto-routes on a MAP-E Border Relay (BR) solution to support ECMP.

1. Create service interface on the device with 100g bandwidth support.

```
[edit chassis]
user@host# set fpc 0 pic 0 inline-services bandwidth 100g
```

2. Configure the dual stack service interface unit 0.

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

3. Configure service interface inside the dual stack domain.

```
[edit interfaces]
user@host# set si-0/0/0 unit 1 family inet
user@host# set si-0/0/0 unit 1 family inet family inet6
user@host# set si-0/0/0 unit 1 service-domain inside
```

4. Configure service interface outside the dual stack domain.

```
[edit interfaces]
user@host# set si-0/0/0 unit 2 family inet
user@host# set si-0/0/0 unit 2 family inet family inet6
user@host# set si-0/0/0 unit 2 service-domain outside
```

5. Configure the IPv4-facing interface on BR.

```
[edit interfaces]
user@host# set ge-0/2/7 unit 0 family inet address 10.10.10.1/16
```

6. Configure the CPE-facing interface on BR.

```
[edit interfaces]
user@host# set ge-0/2/8 unit 0 family inet6 address 3abc::1/16
```

7. Configure MAP-E domain 1 and associated parameters.

```
[edit services softwire softwire-concentrator]
user@host# set map-e mape-domain-1 version03
user@host# set map-e mape-domain-1 softwire-address 2001:db8:ffff::1
user@host# set map-e mape-domain-1 ipv4-prefix 192.0.2.0/24 mape-prefix 2001:db8::/32
user@host# set map-e mape-domain-1 ea-bits-len 16
user@host# set map-e mape-domain-1 psid-offset 4
user@host# set map-e mape-domain-1 psid-length 8
user@host# set map-e mape-domain-1 mtu-ipv6 9192
user@host# set map-e mape-domain-1 disable-auto-route
```

8. Configure MAP-E domain 2 and associated parameters.

```
[edit services softwire softwire-concentrator]
user@host# set map-e mape-domain-2 version03
user@host# set map-e mape-domain-2 softwire-address 2001:db8:ffff::1
user@host# set map-e mape-domain-2 ipv4-prefix 192.0.3.0/24 mape-prefix 2002:db8::/32
user@host# set map-e mape-domain-2 ea-bits-len 16
user@host# set map-e mape-domain-2 psid-offset 4
user@host# set map-e mape-domain-2 psid-length 8
user@host# set map-e mape-domain-2 mtu-ipv6 9192
user@host# set map-e mape-domain-2 disable-auto-route
```

9. Configure a softwire rule for MAP-E domain-1 to specify the direction of traffic to be tunneled.

```
[edit services softwire]
user@host# set rule sw-rule1 match-direction input term t1 then map-e mape-domain-1
```

10. Configure a softwire rule for MAP-E domain-2 to specify the direction of traffic to be tunneled.

```
[edit services softwire]
user@host# set rule sw-rule2 match-direction input term t1 then map-e mape-domain-2
```

11. Configure a single rule-set to combine both the rules.

```
[edit services softwire]
user@host# set rule-set ecmp-rules rule sw-rule1
user@host# set rule-set ecmp-rules rule sw-rule2
```

12. Configure the service set for MAP-E.

```
[edit services service-set]
user@host# set sset1 softwire-rule-sets ecmp-rules
user@host# set sset1 next-hop-service inside-service-interface si-0/0/0.1
user@host# set sset1 next-hop-service outside-service-interface si-0/0/0.2
user@host# set sset2 softwire-rule-sets ecmp-rules
user@host# set sset2 next-hop-service inside-service-interface si-0/1/0.1
user@host# set sset2 next-hop-service outside-service-interface si-0/1/0.2
```

13. Configure static routes for MAP-E BR IPv6 address.

```
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:ffff::1/128 next-hop si-0/0/0.1
user@host# set rib inet6.0 static route 2001:db8:ffff::1/128 next-hop si-0/1/0.1
user@host# set rib inet.0 static route 192.0.2.0/24 next-hop si-0/0/0.2
user@host# set rib inet.0 static route 192.0.2.0/24 next-hop si-0/1/0.2
user@host# set rib inet.0 static route 192.0.3.0/24 next-hop si-0/0/0.2
user@host# set rib inet.0 static route 192.0.3.0/24 next-hop si-0/1/0.2
```

14. Enable load balancing.

```
[edit ]
user@host# set policy-options policy-statement LB then load-balance per-packet
user@host# set routing-options forwarding-table export LB
```

15. Verify the status of the routes.

```
[edit ]
user@host# run show route 2001:db8:ffff::1
inet6.0: 10 destinations, 10 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:db8:ffff::1/128
                   *[Static/5] 00:00:12
```

```
                    >  via si-1/0/0.1
                       via si-1/1/0.1
```

The service sets of the PICs have *ecmp-rules* configured and they carry the MAP-E rules of domain-1 and domain-2. From the output, you can understand that when the **disable-auto-route** is enabled and *ecmp -rules* configured, instead of the longer auto routes, static routes are created.

RELATED DOCUMENTATION

map-e | **1293**

CHAPTER 26

Monitoring and Troubleshooting Softwires

IN THIS CHAPTER

Ping and Traceroute for DS-Lite

With Junos OS Release 11.4, you can use the **ping** and **traceroute** commands to determine the status of the DS-Lite softwire tunnels:

- IPv6 ping—The softwire address endpoint on the DS-Lite softwire terminator (AFTR) is usually configured only at the **[edit services softwire]** hierarchy level; it need not be hosted on any interface. Previous releases of the Junos OS software did not provide replies to pings to the IPv6 softwire address when the AFTR was not configured on a specific interface or loopback. An IPv6 ping enables the softwire initiator (B4) to verify the softwire address of the AFTR before creating a tunnel.
- IPv4 ping—A special IPv4 address, 192.0.0.1, is reserved for the AFTR. Previous releases of the Junos OS did not respond to any pings sent to this address. A B4 and other IPv4 nodes can now ping to this address to determine whether the DS-Lite tunnel is working.
- Traceroute—The AFTR now generates and forwards traceroute packets over the DS-Lite tunnel.

NOTE: No additional CLI configuration is necessary to use the new functionality.

Monitoring Softwire Statistics

Purpose

You can review softwire global statistics by using the **show services softwire** or **show services softwire statistics** command.

Action

`user@host#` **show services softwire**

```
Interface: sp-0/0/0, Service set: sset
Softwire Direction Flow count
2001:0:0:1::1 -> 1001::1 I 3
```

`user@host#` **show services softwire statistics**

```
DS-Lite Statistics:
Service PIC Name: :sp-0/0/0
Statistics
----------
Softwires Created :2
Softwires Deleted :1
Softwires Flows Created :2
Softwires Flows Deleted :1
Slow Path Packets Processed :2
Fast Path Packets Processed :274240
Fast Path Packets Encapsulated :583337
Rule Match Failed :0
Rule Match Succeeded :2
IPv6 Packets Fragmented :0
Transient Errors
----------------
Flow Creation Failed - Retry :0
Slow Path Failed - Retry :0
Errors
------
Softwire Creation Failed :0
Flow Creation Failed :0
Slow Path Failed :0
Packet not IPv4-in-IPv6 :0
IPv6 Fragmentation Error :0
Slow Path Failed - IPv6 Next Header Offset :0
Decapsulated Packet not IPv4 :0
Fast Path Failed - IPv6 Next Header Offset :0
No Softwire ID :0
No Flow Extension :0
Flow Limit Exceeded :0
6rd Statistics:
Service PIC Name :sp-0/0/0
```

```
Statistics
----------
Softwires Created :0
Softwires Deleted :0
Softwires Flows Created :0
Softwires Flows Deleted :0
Slow Path Packets Processed :0
Fast Path Packets Processed :0
Fast Path Packets Encapsulated :0
Rule Match Failed :0
Rule Match Succeeded :0
Transient Errors
----------------
Flow Creation Failed - Retry :0
Slow Path Failed - Retry :0
Errors
------
Softwire Creation Failed :0
Flow Creation Failed :0
Slow Path Failed :0
Packet not IPv6-in-IPv4 :0
Slow Path Failed - IPv6 Next Header Offset :0
Decapsulated Packet not IPv6 :0
Encapsulation Failed - No packet memory :0
No Softwire ID :0
No Flow Extension :0
ICMPv4 Dropped Packets :0
```

Monitoring CGN, Stateful Firewall, and Softwire Flows

Purpose

Use the following commands to check the creation of the softwires, pre-NAT flows, and post-NAT flows. Output can be filtered using more specific fields such as AFTR or B4 address or both for DS-Lite, and softwire-concentrator or softwire-initiator or both for 6rd.

- show services stateful-firewall flows
- show services softwire flows

Action

`user@host#` **show services stateful-firewall flows**

```
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow                                                State    Dir       Frm count
TCP      200.200.200.2:80    ->     44.44.44.1:1025  Forward  O          219942
    NAT dest        44.44.44.1:1025    ->       20.20.1.4:1025
    Softwire           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
    Softwire           2001::2         ->         1001::1
TCP      200.200.200.2:80    ->     44.44.44.1:1024  Forward  O          219140
    NAT dest        44.44.44.1:1024    ->       20.20.1.2:1025
    Softwire           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  O          218906
    NAT dest        44.44.44.1:1026    ->       20.20.1.3:1025
    Softwire           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
    Softwire           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
    Softwire           2001::2         ->         1001::1
```

RELATED DOCUMENTATION

Tunneling Services for IPv4-to-IPv6 Transition Overview | 375

4

PART

Enabling Traffic to Pass Securely Using ALGs

CHAPTER 27

ALG Overview

IN THIS CHAPTER

ALG Descriptions

IN THIS SECTION

This topic describes the Application Layer Gateways (ALGs) supported by Junos OS. ALG support includes managing pinholes and parent-child relationships for the supported ALGs.

Supported ALGs

Table 16 on page 467 lists ALGs supported by Junos OS. For information about which ALGs are supported on MS-DPCs, MS-MPCs, MS-MICs, see “ALGs Available for Junos OS Address Aware NAT” on page 208.

Table 16: ALGs Supported by Junos OS

ALGs Supported	v4 - v4	v6 - v4	v6 - v6	DS-Lite (Support for ALGs with DS-lite on MS-MPC and MS-MIC starts in Junos OS Release 18.1R1)
Basic TCP ALG	Yes	Yes	Yes	Yes
Basic UPD ALG	Yes	Yes	Yes	Yes
BOOTP	Yes	No	No	No
DCE RPC Services	Yes	No	No	No
DNS	Yes	Yes	No	Yes
FTP	Yes	No	No	Yes
Gatekeeper RAS	Yes (Starting in Junos OS Release 17.1R1)	Yes (Starting in Junos OS Release 17.2R1)	No	No
H323	Yes	Yes (Starting in Junos OS Release 17.2R1)	No	No
ICMP	Yes	Yes	Yes	Yes
IKE ALG (Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1)	Yes	Yes	No	No
IIOP	Yes	No	No	No
IP	Yes	No	No	No
NETBIOS	Yes	No	No	No
NETSHOW	Yes	No	No	No
PPTP	Yes	No	No	Yes

Table 16: ALGs Supported by Junos OS *(continued)*

ALGs Supported	v4 - v4	v6 - v4	v6 - v6	DS-Lite (Support for ALGs with DS-lite on MS-MPC and MS-MIC starts in Junos OS Release 18.1R1)
REALAUDIO	Yes	No	No	No
Sun RPC and RPC Port Map Services	Yes	No	No	No
RTSP	Yes	No	No	Yes
SIP	Yes	No	No	SIP supported for DS-Lite on MS-MPC and MS-MIC starting in Junos OS Release 18.2R1.
SNMP	Yes	No	No	No
SQLNET	Yes	No	No	No
TFTP	Yes	No	No	Yes
Traceroute	Yes	Yes	No	Yes
Unix Remote Shell Service	Yes	No	No	No
WINFrame	Yes	No	No	No

ALG Support Details

IN THIS SECTION

This section includes details about the ALGs. It includes the following:

Basic TCP ALG

This ALG performs basic sanity checking on TCP packets. If it finds errors, it generates the following anomaly events and system log messages:

- TCP source or destination port zero
- TCP header length check failed
- TCP sequence number zero and no flags are set

- TCP sequence number zero and FIN/PSH/RST flags are set
- TCP FIN/RST or SYN(URG|FIN|RST) flags are set

The TCP ALG performs the following steps:

1. When the router receives a SYN packet, the ALG creates TCP forward and reverse flows and groups them in a *conversation*. It tracks the TCP three-way handshake.
2. The SYN-defense mechanism tracks the TCP connection establishment state. It expects the TCP session to be established within a small time interval (currently 4 seconds). If the TCP three-way handshake is not established in that period, the session is terminated.
3. A keepalive mechanism detects TCP sessions with nonresponsive endpoints.
4. ICMP errors are allowed only when a flow matches the selector information specified in the ICMP data.

Basic UDP ALG

This ALG performs basic sanity checking on UDP headers. If it finds errors, it generates the following anomaly events and system log messages:

- UDP source or destination port 0
- UDP header length check failed

The UDP ALG performs the following steps:

1. When it receives the first packet, the ALG creates bidirectional flows to accept forward and reverse UDP session traffic.
2. If the session is idle for more than the maximum allowed idle time (the default is 30 seconds), the flows are deleted.
3. ICMP errors are allowed only when a flow matches the selector information specified in the ICMP data.

BOOTP

The Bootstrap Protocol (BOOTP) client retrieves its networking information from a server across the network. It sends out a general broadcast message to request the information, which is returned by the BOOTP server. For the protocol specification, see **ftp://ftp.isi.edu/in-notes/rfc951.txt**.

Stateful firewall support requires that you configure the BOOTP ALG on UDP server port 67 and client port 68. If the client sends a broadcast message, you should configure the broadcast address in the **from** statement of the service rule. Network Address Translation (NAT) is not performed on the BOOTP traffic, even if the NAT rule matches the traffic. If the BOOTP relay feature is activated on the router, the remote BOOTP server is assumed to assign addresses for clients masked by NAT translation.

DCE RPC Services

Distributed Computing Environment (DCE) Remote Procedure Call (RPC) services are mainly used by Microsoft applications. The ALG uses well-known TCP port 135 for port mapping services, and uses the

universal unique identifier (UUID) instead of the program number to identify protocols. The main application-based DCE RPC is the Microsoft Exchange Protocol.

Support for stateful firewall and NAT services requires that you configure the DCE RPC portmap ALG on TCP port 135. The DCE RPC ALG uses the TCP protocol with application-specific UUIDs.

DNS

The Domain Name System (DNS), which typically runs on port 53, handles the data associated with locating and translating domain names into IP addresses. The MX Series DNS ALG monitors the DNS query and reply packets, and supports UDP and TCP DNS traffic independently. The DNS ALG does not support payload translations for NAT, but an operator can use it to efficiently remove the NAT or stateful firewall DNS sessions from memory after the DNS server sends its response. The DNS ALG closes the session only when a reply is received or an idle timeout is reached.

There might be issues with TCP DNS traffic when the TCP-DNS-ALG is used if the DNS traffic is not just the standard request and reply type. For example, the TCP-DNS-ALG might break DNS server-to-server communication that uses TCP, such as DNS Replication or Zone transfers. This type of traffic might get dropped by the NAT or stateful firewall plugins because the TCP-DNS-ALG closes the session after the TCP handshake is complete and after each server has sent one packet to the other. In these instances do not use the TCP-DNS-ALG.

> **NOTE:**
>
> The TCP-DNS-ALG is not supported on the MS-DPC service cards.

FTP

FTP is the File Transfer Protocol, specified in RFC 959. In addition to the main control connection, data connections are also made for any data transfer between the client and the server; and the host, port, and direction are negotiated through the control channel.

For non-passive-mode FTP, Junos OS stateful firewall service scans the client-to-server application data for the PORT command, which provides the IP address and port number to which the server connects. For passive-mode FTP, Junos OS stateful firewall service scans the client-to-server application data for the PASV command and then scans the server-to-client responses for the 227 response, which contains the IP address and port number to which the client connects.

There is an additional complication: FTP represents these addresses and port numbers in ASCII. As a result, when addresses and ports are rewritten, the TCP sequence number might be changed, and thereafter the NAT service needs to maintain this delta in SEQ and ACK numbers by performing sequence NAT on all subsequent packets.

Support for stateful firewall and NAT services requires that you configure the FTP ALG on TCP port 21 to enable the FTP control protocol. The ALG performs the following tasks:

- Automatically allocates data ports and firewall permissions for dynamic data connection
- Creates flows for the dynamically negotiated data connection
- Monitors the control connection in both active and passive modes
- Rewrites the control packets with the appropriate NAT address and port information

On MS-MPCs, MS-MICs, for passive FTP to work properly without FTP application layer gateway (ALG) enabled (by not specifying the **application junos-ftp** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from]** and the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy levels), you must enable the address pooling paired (APP) functionality enabled (by including the **address-pooling** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level). Such a configuration causes the data and control FTP sessions to receive the same NAT address.

Gatekeeper RAS

Starting in Junos OS Release 17.1R1, the gatekeeper registration, administration, and status (RAS) ALG allows full support of gatekeeper mode for H.323 calls. An endpoint registers to a gatekeeper and asks for its management. Before making a call, an endpoint asks its gatekeeper for permission to place the call. In both registration and admission phases, the RAS channel is used. Use the gatekeeper RAS ALG and the H323 ALG in IPv4 and IPv6 stateful-firewall rules or NAPT-44 rules. Starting in Junos OS Release 17.2R1, NAT-64 rules are also supported. The Junos default application set **junos-h323-suite** includes the H323 ALG and the gatekeeper RAS ALG.

H323

H323 is a suite of ITU protocols for audio and video conferencing and collaboration applications. H323 consists of H.225 call signaling protocols and H.245 control protocol for media communication. During H.225 negotiation, the endpoints create a call by exchanging call signaling messages on the control channel and negotiate a new control channel for H.245. A new control connection is created for H.245 messages. Messages are exchanged on the H.245 control channel to open media channels.

Stateful firewall monitors the H.225 control channel to open the H.245 control channel. After the H.245 channel is created, stateful firewall also monitors this channel for media channel information and allows the media traffic through the firewall.

H323 ALG supports static destination, static and dynamic source NAT by rewriting the appropriate addresses and ports in the H.225 and H.245 messages.

To support gatekeeper mode for H.323 calls, use the H323 ALG and the gatekeeper RAS ALG in IPv4 and IPv6 stateful-firewall rules or NAPT-44 rules. Starting in Junos OS Release 17.2R1, NAT-64 rules are also supported. The Junos default application set **junos-h323-suite** includes the H323 ALG and the gatekeeper RAS ALG.

ICMP

The Internet Control Message Protocol (ICMP) is defined in RFC 792. The Junos OS stateful firewall service allows ICMP messages to be filtered by specific type or specific type code value. ICMP error packets that lack a specifically configured type and code are matched against any existing flow in the opposite direction to check for the legitimacy of the error packet. ICMP error packets that pass the filter matching are subject to NAT translation.

The ICMP ALG always tracks ping traffic statefully using the ICMP sequence number. Each echo reply is forwarded only if there is an echo request with the corresponding sequence number. For any ping flow, only 20 echo requests can be forwarded without receiving an echo reply. When you configure dynamic NAT, the PING packet identifier is translated to allow additional hosts in the NAT pool to use the same identifier.

Support for stateful firewall and NAT services requires that you configure the ICMP ALG if the protocol is needed. You can configure the ICMP type and code for additional filtering.

IIOP

The Oracle Application Server Name Server Internet Inter-ORB Protocol (IIOP). This ALG is used in Common Object Request Broker Architecture (CORBA) based on distributed computing. Even though CORBA and IIOP are Object Management Group (OMG) standards, no fixed port is assigned for IIOP. Each vendor implementing CORBA chooses a port. Java Virtual machine uses port 1975 by default, while ORBIX uses port 3075 as a default.

Stateful firewall and NAT require ALG IIOP be configured for TCP port 1975 for Java VM IIOP, and 3075 for CORBA applications ORBIX, a CORBA framework from Iona Technologies.

IKE ALG

Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers. Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG enables the passing of IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant. This ALG supports only ESP tunnel mode.

Use this ALG in NAT rules and specify the UDP protocol and port 500.

This ALG performs the following:

- Tracks IKEv1 connection-initiation requests to determine whether NAT processing is required.
- Performs NAT translation on outgoing and incoming IKEv1 requests and creates IKE sessions.
- Identifies IPsec packets related to the established IKE session and establishes security association between peers.
- Performs NAT translation on IPsec packets.

IP

The IP ALG is used to create unidirectional flows only. In case of TCP traffic, it does not check the 3-way handshake process. This ALG is useful in case of stateful firewall only service sets, where it allows traffic to flow uni-directionally only. When configuring in conjunction with **match-direction input-output** it allows the return traffic to flow through the stateful firewall as well. Typical scenarios are static NAT, destination NAT or scenarios where traffic is expected to traverse the stateful firewall in the presence of asymmetric routing. The Junos IP ALG is not intended for use with NAPT, which causes matching traffic to be discarded through the creation of a drop flow.

NetBIOS

A NetBIOS ALG translates NetBIOS IP addresses and port numbers when NAT is used.

NetBIOS supports the TCP and UDP transport protocols. Support for stateful firewall and NAT services requires that you configure the NetBIOS ALG on UDP port 138 and TCP port 139.

NetShow

The Microsoft protocol ms-streaming is used by NetShow, the Microsoft media server. This protocol supports several transport protocols: TCP, UDP, and HTTP. The client starts a TCP connection on port 1755 and sends the PORT command to the server. The server then starts UDP on that port to the client. Support for stateful firewall and NAT services requires that you configure the NetShow ALG on UDP port 1755.

ONC RPC Services

Open Networks Computing (ONC) RPC services function similarly to DCE RCP services. However, the ONC RPC ALG uses TCP/UDP port 111 for port mapping services, and uses the program number to identify protocols rather than the UUID.

Support for stateful firewall and NAT services requires that you configure the ONC RPC portmap ALG on TCP port 111. The ONC RPC ALG uses the TCP protocol with application-specific program numbers.

PPTP

The Point-to-Point Tunneling Protocol (PPTP) ALG is a TCP-based ALG. PPTP allows the Point-to-Point Protocol (PPP) to be tunneled through an IP network. PPTP defines a client-server architecture, a PPTP Network Server, and a PPTP Access Concentrator. The PPTP ALG requires a control connection and a data tunnel. The control connection uses TCP to establish and disconnect PPP sessions, and runs on port 1723. The data tunnel carries PPP traffic in generic routing encapsulated (GRE) packets that are carried over IP.

RealAudio

Real Networks PNA protocol RealVideo is not a separate service. It is part of the RealPlayer and most likely uses another channel for video. The RealPlayer versions G2, 7, and 8 use PNA and RTSP. For this version to work, the ALG must allow both PNA(7070) and RTSP(554). For the media, the server selects from a range of UDP ports(6970 through 7170), or TCP port 7071, or HTTP. The client can be configured to use a particular port. The RealPlayer versions 4.0 and 5.0 use control channel 7070 media UDP ports 6970 through 7170, or TCP port 7071, or HTTP. RealAudio player version 3.0 uses control channel 7070 media, UDP ports 6770-7170, or TCP port 7071.

Real products use the ports and ranges of ports shown in Table 17 on page 475.

Table 17: RealAudio Product Port Usage

Real Product	Port Usage
4.0 and 5.0 Servers/Players	Control channel (bidirectional) on TCP port 7070. Data channel from server to player on TCP port 7070 or UDP port 6970-7170.
4.0 and 5.0 Servers/Encoders	Control channel (bidirectional) on TCP port 7070. Data channel from encoder or server on TCP port 7070.
G2 Servers/Players	Control channel (bidirectional) on TCP port 80, 554, 7070, or 8080. Data channel from server to player on TCP port 80, 554, 7070, 8080 or UDP port 6970-32,000.
G2 Server/3.1, and 5.x Encoders	Control channel (bidirectional) on TCP port 7070. Data channel from encoder to server on TCP port 7070.
G2 Server/G2 Producer	Control channel (bidirectional) on TCP port 4040. Data channel from encoder to server on TCP port 4040 and UDP port 6970-32,000.
2 Server/G2 Producer (TCP ONLY)	Control channel (bidirectional) on TCP port 4040 Data channel from encoder to server on TCP port 4040. Note: TCP-ONLY option available in version 6.1 or above.

NOTE: RealAudio was the original protocol by RealPlayers. Newer versions of RealPlayer use RTSP. Stateful firewall and NAT require ALG RealAudio to be programmed on TCP port 7070.

Sun RPC and RPC Portmap Services

The Remote Procedure Call (RPC) ALG uses well-known ports TCP 111 and UDP 111 for port mapping, which dynamically assigns and opens ports for RPC services. The RPC Portmap ALG keeps track of port requests and dynamically opens the firewall for these requested ports. The RPC ALG can further restrict the RPC protocol by specifying allowed program numbers.

The ALG includes the RPC services listed in Table 18 on page 475.

Table 18: Supported RPC Services

Name	Description	Comments
rpc-mountd	Network File Server (NFS) mount daemon; for details, see the UNIX man page for **rpc.mountd(8)**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).

Table 18: Supported RPC Services *(continued)*

Name	Description	Comments
rpc-nfsprog	Used as part of NFS. For details, see RFC 1094. See also RFC1813 for NFS v3.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
rpc-nisplus	Network Information Service Plus (NIS+), designed to replace NIS; it is a default naming service for Sun Solaris and is not related to the old NIS. No protocol information is available.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050).
rpc-nlockmgr	Network lock manager.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-nlockmgr** service can be allowed or blocked based on RPC program 100021.
rpc-pcnfsd	Kernel statistics server. For details, see the UNIX man pages for **rstatd** and **rpc.rstatd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-rstat** service can be allowed or blocked based on RPC program 150001.
rpc-rwall	Used to write a message to users; for details, see the UNIX man page for **rpc.rwalld**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-rwall** service can be allowed or blocked based on RPC program 150008.
rpc-ypbind	NIS binding process. For details, see the UNIX man page for **ypbind**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypbind** service can be allowed or blocked based on RPC program 100007.
rpc-yppasswd	NIS password server. For details, see the UNIX man page for **yppasswd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-yppasswd** service can be allowed or blocked based on RPC program 100009.
rpc-ypserv	NIS server. For details, see the UNIX man page for **ypserv**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypserv** service can be allowed or blocked based on RPC program 100004.

Table 18: Supported RPC Services *(continued)*

Name	Description	Comments
rpc-ypupdated	Network updating tool.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypupdated** service can be allowed or blocked based on RPC program 100028.
rpc-ypxfrd	NIS map transfer server. For details, see the UNIX man page for **rpc.ypxfrd**.	The base support is RPC v2 and the port mapper service on port 111 (see RFC 1050). Once the RPC program table is built, **rpc-ypxfrd** service can be allowed or blocked based on RPC program 100069.

Support for stateful firewall and NAT services that use port mapping requires that you configure the RPC portmap ALG on TCP/UDP destination port 111 and the RPC ALG for both TCP and UDP. You can specify one or more **rpc-program-number** values to further restrict allowed RPC protocols.

RTSP

The Real-Time Streaming Protocol (RTSP) controls the delivery of data with real-time properties such as audio and video. The streams controlled by RTSP can use RTP, but it is not required. Media can be transmitted on the same RTSP control stream. This is an HTTP-like text-based protocol, but client and server maintain session information. A session is established using the SETUP message and terminated using the TEARDOWN message. The transport (the media protocol, address, and port numbers) is negotiated in the setup and the setup-response.

Support for stateful firewall and NAT services requires that you configure the RTSP ALG for TCP port 554.

The ALG monitors the control connection, opens flows dynamically for media (RTP/RTSP) streams, and performs NAT address and port rewrites.

SIP

The Session Initiation Protocol (SIP) is an application layer protocol that can establish, maintain, and terminate media sessions. It is a widely used voice over IP (VoIP) signaling protocol. The SIP ALG monitors SIP traffic and dynamically creates and manages pinholes on the signaling and media paths. The ALG only allows packets with the correct permissions. The SIP ALG also performs the following functions:

- Manages parent-child session relationships.
- Enforces security policies.
- Manages pinholes for VoIP traffic.

The SIP ALG supports the following features:

- Stateful firewall
- Static source NAT

- Dynamic address only source NAT
- Network Address Port Translation (NAPT)

> **NOTE:** SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. SIP sessions on the MS-DPC have no time limit.

SNMP

SNMP is a communication protocol for managing TCP/IP networks, including both individual network devices and aggregated devices. The protocol is defined by RFC 1157. SNMP runs on top of UDP.

The Junos OS stateful firewall service implements the SNMP ALG to inspect the SNMP type. SNMP does not enforce stateful flow. Each SNMP type needs to be specifically enabled. Full SNMP support of stateful firewall services requires that you configure the SNMP ALG on UDP port 161. This enables the SNMP ***get*** and **get-next** commands, as well as their response traffic in the reverse direction: UDP port 161 enables the SNMP **get-response** command. If SNMP traps are permitted, you can configure them on UDP port 162, enabling the SNMP **trap** command.

SQLNet

The SQLNet protocol is used by Oracle SQL servers to execute SQL commands from clients, including load balancing and application-specific services.

Support of stateful firewall and NAT services requires that you configure the SQLNet ALG for TCP port 1521.

The ALG monitors the control packets, opens flows dynamically for data traffic, and performs NAT address and port rewrites.

TFTP

The Trivial File Transfer Protocol (TFTP) is specified in RFC 1350. The initial TFTP requests are sent to UDP destination port 69. Additional flows can be created to **get** or **put** individual files. Support of stateful firewall and NAT services requires that you configure the TFTP ALG for UDP destination port 69.

Traceroute

Traceroute is a tool for displaying the route that packets take to a network host. It uses the IP time-to-live (TTL) field to trigger ICMP time-exceeded messages from routers or gateways. It sends UDP datagrams to destination ports that are believed to be not in use; destination ports are numbered using the formula: + *n*hops – 1. The default base port is 33434. To support traceroute through the firewall, two types of traffic must be passed through:

1. UDP probe packets (UDP destination port > 33000, IP TTL < 30)
2. ICMP response packets (ICMP type time-exceeded)

When NAT is applied, the IP address and port within the ICMP error packet also must be changed.

Support of stateful firewall and NAT services requires you to configure the Traceroute ALG for UDP destination port 33434 to 33450. In addition, you can configure the TTL threshold to prevent UDP flood attacks with large TTL values.

UNIX Remote-Shell Services

Three protocols form the basis for UNIX remote-shell services:

- Exec—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 512. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.
- Login—Better known as **rlogin**; uses well-known TCP port 513. For details, see RFC 1282. No special firewall processing is required.
- Shell—Remote command execution; enables a user on the client system to execute a command on the remote system. The first command from client (**rcmd**) to server (**rshd**) uses well-known TCP port 514. A second TCP connection can be opened at the request of **rcmd**. The client port number for the second connection is sent to the server as an ASCII string.

Support of stateful firewall services requires that you configure the Exec ALG on TCP port 512, the Login ALG on TCP port 513, and the Shell ALG on TCP port 514. NAT remote-shell services require that any dynamic source port assigned be within the port range 512 to 1023. If you configure a NAT pool, this port range is reserved exclusively for remote shell applications.

WinFrame

WinFrame application server software provides access to virtually any Windows application, across any type of network connection to any type of client.

This protocol is mainly used by Citrix Windows applications.

Stateful firewall and NAT require the ALG Winframe to be configured on TCP destination port 1494 and UDP port 1604.

Juniper Networks Defaults

The Junos OS provides a default, hidden configuration group called **junos-defaults** that is automatically applied to the configuration of your router. The **junos-defaults** group contains preconfigured statements that contain predefined values for common applications. Some of the statements must be referenced to take effect, such as applications like FTP or Telnet. Other statements are applied automatically, such as terminal settings. All of the preconfigured statements begin with the reserved name **junos-**.

NOTE: You can override the Junos OS default configuration values, but you cannot delete or edit them. If you delete a configuration, the defaults return when a new configuration is added.

You cannot use the **apply-groups** statement with the Junos OS defaults group.

To view the full set of available preset statements from the Junos OS default group, issue the **show groups junos-defaults** configuration mode command. The following example displays the list of Junos OS default groups that use application protocols (ALGs):

```
user@host# show groups junos-defaults
applications {
    #
    # File Transfer Protocol
    #
    application junos-ftp {
        application-protocol ftp;
        protocol tcp;
        destination-port 21;
    }
    #
    # Trivial File Transfer Protocol
    #
    application junos-tftp {
        application-protocol tftp;
        protocol udp;
        destination-port 69;
    }
    #
    # RPC portmapper on TCP
    #
    application junos-rpc-portmap-tcp {
        application-protocol rpc-portmap;
        protocol tcp;
        destination-port 111;
    }
    #
    # RPC portmapper on UDP
    #
    application junos-rpc-portmap-udp {
        application-protocol rpc-portmap;
        protocol udp;
        destination-port 111;
```

```
}
#
# SNMP get
#
application junos-snmp-get {
    application-protocol snmp;
    protocol udp;
    destination-port 161;
    snmp-command get;
}
#
# SNMP get next
#
application junos-snmp-get-next {
    application-protocol snmp;
    protocol udp;
    destination-port 161;
    snmp-command get-next;
}
#
# SNMP response
#
application junos-snmp-response {
    application-protocol snmp;
    protocol udp;
    source-port 161;
    snmp-command get-response;
}
#
# SNMP trap
#
application junos-snmp-trap {
    application-protocol snmp;
    protocol udp;
    destination-port 162;
    snmp-command trap;
}
#
# remote exec
#
application junos-rexec {
    application-protocol exec;
    protocol tcp;
    destination-port 512;
```

```
}
#
# remote login
#
application junos-rlogin {
    application-protocol shell;
    protocol tcp;
    destination-port 513;
}
#
# remote shell
#
application junos-rsh {
    application-protocol shell;
    protocol tcp;
    destination-port 514;
}
#
# Real Time Streaming Protocol
#
application junos-rtsp {
    application-protocol rtsp;
    protocol tcp;
    destination-port 554;
}
#
# Citrix windows application server protocol
# windows applications remotely on windows/non-windows clients
#
# citrix needs udp 1604 to be open
#
application junos-citrix-winframe {
    application-protocol winframe;
    protocol tcp;
    destination-port 1494;
}
application junos-citrix-winframe-udp {
    protocol udp;
    destination-port 1604;
}
#
# Oracle SQL servers use this protocol to execute sql commands
# from clients, load balance, use application-specific servers, etc
#
```

```
application junos-sqlnet {
    application-protocol sqlnet;
    protocol tcp;
    destination-port 1521;
}
#
# H.323 Protocol for audio/video conferencing
#
application junos-h323 {
    application-protocol h323;
    protocol tcp;
    destination-port 1720;
}
application junos-h323-ras {
    application-protocol ras;
    protocol udp;
    destination-port 1719;
}
#
# Internet Inter-ORB Protocol - used for CORBA applications
# The ORB protocol in Java virtual machines uses port 1975 as default
#
application junos-iiop-java {
    application-protocol iiop;
    protocol tcp;
    destination-port 1975;
}
#
# Internet Inter-ORB Protocol - used for CORBA applications
# ORBIX is a CORBA framework from Iona Technologies that uses port
# 3075 as default
#
application junos-iiop-orbix {
    application-protocol iiop;
    protocol tcp;
    destination-port 3075;
}
#
# Real players use this protocol for real time streaming
# This was the original protocol for real players.
# RTSP is more widely used by real players
# but they still support realaudio.
#
application junos-realaudio {
```

```
    application-protocol realaudio;
    protocol tcp;
    destination-port 7070;
}
#
# traceroute application.
#
application junos-traceroute {
    application-protocol traceroute;
    protocol udp;
    destination-port 33435-33450;
    ttl-threshold 30;
}
#
# The full range of known RPC programs using UDP
# The program numbers can be more specific to certain applications.
#
application junos-rpc-services-udp {
    application-protocol rpc;
    protocol udp;
    rpc-program-number 100000-400000;
}
#
# The full range of known RPC programs using TCP
# The program numbers can be more specific to certain applications.
#
application junos-rpc-services-tcp {
    application-protocol rpc;
    protocol tcp;
    rpc-program-number 100000-400000;
}
#
# All ICMP traffic
# This can be made to be more restrictive by specifying ICMP type
# and code.
#
application junos-icmp-all {
    application-protocol icmp;
}
#
# Protocol used by Windows media server and windows media player
#
application junos-netshow {
    application-protocol netshow;
```

```
    protocol tcp;
    destination-port 1755;
}
#
# NetBIOS - networking protocol used on
# Windows networks name service port, both UDP and TCP
#
application junos-netbios-name-udp {
    application-protocol netbios;
    protocol udp;
    destination-port 137;
}
application junos-netbios-name-tcp {
    protocol tcp;
    destination-port 137;
}
#
# NetBIOS - networking protocol used on
# Windows networks datagram service port
#
application junos-netbios-datagram {
    application-protocol netbios;
    protocol udp;
    destination-port 138;
}
#
# NetBIOS - networking protocol used on
# Windows networks session service port
#
application junos-netbios-session {
    protocol tcp;
    destination-port 139;
}
#
# DCE-RPC portmapper on TCP
#
application junos-dce-rpc-portmap {
    application-protocol dce-rpc-portmap;
    protocol tcp;
    destination-port 135;
}
#
# DCE-RPC application on TCP sample UUID
# This application requires user to specify the UUID value
```

```
#
    # application junos-dcerpc {
        # application-protocol dce-rpc;
        # protocol tcp;
        #
        # # UUID also needs to be defined as shown below
        # UUID 11223344 22334455 33445566 44556677;
        #
        # }
        #
        # ms-exchange needs these 3 UUIDs
        #
        application junos-dcerpc-endpoint-mapper-service {
            application-protocol dce-rpc;
            protocol tcp;
            uuid e1af8308-5d1f-11c9-91a4-08002b14a0fa;
        }
        application junos-dcerpc-msexchange-directory-rfr {
            application-protocol dce-rpc;
            protocol tcp;
            uuid 1544f5e0-613c-11d1-93df-00c04fd7bd09;
        }
        application junos-dcerpc-msexchange-information-store {
            application-protocol dce-rpc;
            protocol tcp;
            uuid a4f1db00-ca47-1067-b31f-00dd010662da;
        }
        application junos-ssh {
            protocol tcp;
            destination-port 22;
        }
        application junos-telnet {
            protocol tcp;
            destination-port 23;
        }
        application junos-smtp {
            protocol tcp;
            destination-port 25;
        }
        application junos-dns-udp {
            protocol udp;
            destination-port 53;
        }
        application junos-dns-tcp {
```

```
    protocol tcp;
    destination-port 53;
}
application junos-tacacs {
    protocol tcp;
    destination-port 49;
}
# TACACS Database Service
application junos-tacacs-ds {
    protocol tcp;
    destination-port 65;
}
application junos-dhcp-client {
    protocol udp;
    destination-port 68;
}
application junos-dhcp-server {
    protocol udp;
    destination-port 67;
}
application junos-bootpc {
    protocol udp;
    destination-port 68;
}
application junos-bootps {
    protocol udp;
    destination-port 67;
}
application junos-finger {
    protocol tcp;
    destination-port 79;
}
application junos-http {
    protocol tcp;
    destination-port 80;
}
application junos-https {
    protocol tcp;
    destination-port 443;
}
application junos-pop3 {
    protocol tcp;
    destination-port 110;
}
```

```
application junos-ident {
    protocol tcp;
    destination-port 113;
}
application junos-nntp {
    protocol tcp;
    destination-port 119;
}
application junos-ntp {
    protocol udp;
    destination-port 123;
}
application junos-imap {
    protocol tcp;
    destination-port 143;
}
application junos-imaps {
    protocol tcp;
    destination-port 993;
}
application junos-bgp {
    protocol tcp;
    destination-port 179;
}
application junos-ldap {
    protocol tcp;
    destination-port 389;
}
application junos-snpp {
    protocol tcp;
    destination-port 444;
}
application junos-biff {
    protocol udp;
    destination-port 512;
}
# UNIX who
application junos-who {
    protocol udp;
    destination-port 513;
}
application junos-syslog {
    protocol udp;
    destination-port 514;
```

```
}
# line printer daemon, printer, spooler
application junos-printer {
    protocol tcp;
    destination-port 515;
}
# UNIX talk
application junos-talk-tcp {
    protocol tcp;
    destination-port 517;
}
application junos-talk-udp {
    protocol udp;
    destination-port 517;
}
application junos-ntalk {
    protocol udp;
    destination-port 518;
}
application junos-rip {
    protocol udp;
    destination-port 520;
}
# INA sanctioned RADIUS port numbers
application junos-radius {
    protocol udp;
    destination-port 1812;
}
application junos-radacct {
    protocol udp;
    destination-port 1813;
}
application junos-nfsd-tcp {
    protocol tcp;
    destination-port 2049;
}
application junos-nfsd-udp {
    protocol udp;
    destination-port 2049;
}
application junos-cvspserver {
    protocol tcp;
    destination-port 2401;
}
```

```
#
# Label Distribution Protocol
#
application junos-ldp-tcp {
    protocol tcp;
    destination-port 646;
}
application junos-ldp-udp {
    protocol udp;
    destination-port 646;
}
#
# JUNOScript and JUNOScope management
#
application junos-xnm-ssl {
    protocol tcp;
    destination-port 3220;
}
application junos-xnm-clear-text {
    protocol tcp;
    destination-port 3221;
}
#
# IPsec tunnel
#
application junos-ipsec-esp {
    protocol esp;
}
#
#IKE application for IPSec VPN
#
application junos-ike {
    application-protocol ike-esp-nat;
    protocol udp;
    destination-port 500;
}
#
# 'junos-algs-outbound' defines a set of all applications
# requiring an ALG. Useful for defining rule to the the public
# internet allowing private network users to use all JUNOS OS
# supported ALGs initiated from the private network.
#
# NOTE: the contents of this set might grow in future JUNOS OS versions.
#
```

```
application-set junos-algs-outbound {
    application junos-ftp;
    application junos-tftp;
    application junos-rpc-portmap-tcp;
    application junos-rpc-portmap-udp;
    application junos-snmp-get;
    application junos-snmp-get-next;
    application junos-snmp-response;
    application junos-snmp-trap;
    application junos-rexec;
    application junos-rlogin;
    application junos-rsh;
    application junos-rtsp;
    application junos-citrix-winframe;
    application junos-citrix-winframe-udp;
    application junos-sqlnet;
    application junos-h323;
    application junos-iiop-java;
    application junos-iiop-orbix;
    application junos-realaudio;
    application junos-traceroute;
    application junos-rpc-services-udp;
    application junos-rpc-services-tcp;
    application junos-icmp-all;
    application junos-netshow;
    application junos-netbios-name-udp;
    application junos-netbios-datagram;
    application junos-dcerpc-endpoint-mapper-service;
    application junos-dcerpc-msexchange-directory-rfr;
    application junos-dcerpc-msexchange-information-store;
}
#
# 'junos-management-inbound' represents the group of applications
# that might need access the router from public network for
# for management purposes.
#
# Set is intended for a UI to display management choices.
#
# NOTE: It is not recommended the user to use the entire set
# directly in a firewall rule and open up firewall to all
# of these applications. Also, the user should always
# specify the source and destination prefixes when using
# each application.
#
```

```
    # NOTE: the contents of this set may grow in future JUNOS versions.
    #
    application-set junos-management-inbound {
        application junos-snmp-get;
        application junos-snmp-get-next;
        application junos-snmp-response;
        application junos-snmp-trap;
        application junos-ssh;
        application junos-telnet;
        application junos-http;
        application junos-https;
        application junos-xnm-ssl;
        application junos-xnm-clear-text;
    }
    #
    # 'junos-routing-inbound' represents routing protocols that might
    # need to access the router from public network.
    #
    # Set is intended for a UI to display routing involvement choices.
    #
    # NOTE: It is not recommended the user to use the entire set
    # directly in a firewall rule and open up firewall to all
    # of these applications. Also, the user should always
    # specify the source and destination prefixes when using
    # each application.
    #
    # NOTE: the contents of this set might grow in future JUNOS OS versions.
    #
    application-set junos-routing-inbound {
        application junos-bgp;
        application junos-rip;
        application junos-ldp-tcp;
        application junos-ldp-udp;
    }
    application-set junos-h323-suite {
        application junos-h323-ras,
        application junos-h323;
    }
}
```

To reference statements available from the **junos-defaults** group, include the selected **junos-*default-name*** statement at the applicable hierarchy level. To configure application protocols, see “Configuring Application Properties” on page 502; for details about a specific protocol, see “ALG Descriptions” on page 466.

Examples: Referencing the Preset Statement from the Junos OS Default Group

The following example is a preset statement from the Junos OS default groups that is available for FTP in a stateful firewall:

```
[edit]
groups {
    junos-defaults {
        applications {
            application junos-ftp { # Use FTP default configuration
            application-protocol ftp;
            protocol tcp;
            destination-port 21;
        }
    }
}
```

To reference a preset Junos OS default statement from the Junos OS default groups, include the **junos-*default-name*** statement at the applicable hierarchy level. For example, to reference the Junos OS default statement for FTP in a stateful firewall, include the **junos-ftp** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* from applications]** hierarchy level.

```
[edit]
services {
    stateful-firewall {
        rule my-rule {
            term my-term {
                from {
                    applications junos-ftp; #Reference predefined statement, junos-ftp,
                }
            }
        }
    }
}
```

The following example shows configuration of the default Junos IP ALG:

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

```
            from {
                applications junos-ip;
            }
            then {
                accept;
                syslog;
            }
        }
    }
  }
}
```

If you configure the IP ALG in the stateful firewall rule, it is matched by any IP traffic, but when any other more specific application matches the same traffic, the IP ALG is not matched. For example, in the following configuration, both the ICMP ALG and the IP ALG are configured, but traffic is matched for ICMP packets, because it is the more specific match.

```
[edit]
services {
   stateful-firewall {
      rule r1 {
         match-direction input;
         term t1 {
            from {
               applications [ junos-ip junos-icmp-all ];
            }
            then {
               accept;
               syslog;
            }
         }
      }
   }
}
```

Release History Table

Release	Description
18.2R1	SIP supported for DS-Lite on MS-MPC and MS-MIC starting in Junos OS Release 18.2R1.
18.1R1	Support for ALGs with DS-lite on MS-MPC and MS-MIC starts in Junos OS Release 18.1R1
17.2R1	(Starting in Junos OS Release 17.2R1)
17.2R1	(Starting in Junos OS Release 17.2R1)
17.2R1	Starting in Junos OS Release 17.2R1, NAT-64 rules are also supported.
17.2R1	Starting in Junos OS Release 17.2R1, NAT-64 rules are also supported.
17.1R1	(Starting in Junos OS Release 17.1R1)
17.1R1	Starting in Junos OS Release 17.1R1, the gatekeeper registration, administration, and status (RAS) ALG allows full support of gatekeeper mode for H.323 calls.
14.2R7	IKE ALG (Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1)
14.2R7	Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG enables the passing of IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant.

RELATED DOCUMENTATION

Configuring Application Sets | **501**

Configuring Application Properties | **502**

ALGs Available for Junos OS Address Aware NAT

The following Application Level Gateways (ALGs) listed in Table 13 on page 209 are supported for NAT processing on the listed platforms.

To view the implementation details (port, protocol, and so on) for these Junos OS default applications, locate the Junos OS Default ALG Name in the table and then look up the listed name in the **groups**. For example, for details about TFTP, look up **junos-tftp** as shown.

TIP: The Junos OS provides the **junos-alg**, which enables other ALGs to function by handling ALG registrations, causing slow path packets to flow through registered ALGs, and transferring ALG events to the ALG plug-ins. The **junos-alg** ALG is automatically available on the MS-MPC and MS-MIC platforms and does not require further configuration.

NOTE: The remote shell (RSH) and remote login (rlogin) application layer gateways (ALGs) are not supported with network address port translation (NAPT) on MX Series routers with MS-MICs and MS-MPCs.

`user@host#` **show groups junos-defaults applications application junos-tftp**

```
application-protocol tftp;
protocol udp;
destination-port 69;
```

Table 13 on page 209 summarizes the ALGs available for Junos OS Address Aware NAT for services interfaces cards.

Table 19: ALGs Available for NAT by Type of Interface Card

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
Basic TCP ALG	yes	yes	**NOTE:** Specific Junos OS ALGs are not supported. However, a feature called TCP tracker, available by default, performs segment ordering and retransmit and connection tracking, validations for TCP connections.
Basic UDP ALG	yes	yes	**NOTE:** TCP tracker performs limited integrity and validation checks for UDP.

Table 19: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
BOOTP	yes	no	• **junos-bootpc** • **junos-bootps**
DCE RPC Services	yes	yes	• **junos-dce-rpc-portmap** • **junos-dce-rpc-endpoint-mapper-service** • **junos-dce-rpc-exchange-dcbcymp** • **junos-dce-rpc-exchange-dcbcymf** • **junos-dce-rpc-exchange-information-store**
DNS	yes	yes	• **junos-dns-udp**
DNS	no	no	• **junos-dns-tcp**
FTP	yes	yes	• **junos-ftp**
Gatekeeper RAS (Starting in Junos OS Release 17.1R1)	no	yes	• **junos-h323-ras**
H323	no	yes	• **junos-h323**
ICMP	yes	yes **NOTE:** In Junos OS Release 14.1 and earlier, ICMP messages are handled by default, but PING ALG support is not provided. Starting In Junos OS 14.2, ICMP messages are handled by default and PING ALG support is provided.	• **junos-icmp-all** • **junos-icmp-ping**
IIOP	yes	no	• **junos-iiop-java** • **junos-iiop-orbix**

Table 19: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
IKE ALG	no	yes **NOTE:** Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG ALG is supported on MS-MPCs and MS-MICs.	• **junos-ike**
IP	yes	The TCP tracker, available by default on these platforms, performs limited integrity and validation checks.	• **junos-ip**
NETBIOS	yes	no	• **junos-netbios-datagram** • **junos-netbios-name-tcp** • **junos-netbios-name-udp** • **junos-netbios-session**
NETSHOW	yes	no	• **junos-netshow**
PPTP	yes	yes	• **junos-pptp**
REALAUDIO	yes	no	• **junos-realaudio**
Sun RPC and RPC Port Map Services	yes	yes	• **junos-rpc-portmap-tcp** • **junos-rpc-portmap-udp**
RTSP	yes	yes	• **junos-rtsp**

Table 19: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
SIP	yes	Yes	• **junos-sip** The SIP **callid** is *not* translated in **register** messages. **NOTE:** SIP sessions are limited to 12 hours (720 minutes) for NAT processing on the MS-MIC and MS-MPC interface cards. SIP sessions on the MS-DPC have no time limits.
SNMP	yes	No	• **junos-snmp-get** • **junos-snmp-get-next** • **junos-snmp-response** • **junos-snmp-trap**
SQLNET	yes	yes	• **junos-sqlnet**
TFTP	yes	yes	• **junos-tftp**
Traceroute	yes	yes	• **junos-traceroute**
Unix Remote Shell Service	yes	yes **NOTE:** Remote Shell (RSH) ALG is not supported for network address port translation (NAPT).	• **junos-rsh**
WINFrame	yes	No	• **junos-citrix-winframe** • **junos-citrix-winframe-udp**
TALK-UDP	No	Yes	• **junos-talk-udp**

Table 19: ALGs Available for NAT by Type of Interface Card *(continued)*

ALG	MS-DPC	MS-MPC, MS-MIC	Junos OS Default ALG Name
MS RPC	No	Yes	• **junos-rpc-portmap-tcp** • **junos-rpc-portmap-udp** • **junos-rpc-services-tcp** • **junos-rpc-services-udp**

Release History Table

Release	Description
17.1R1	Gatekeeper RAS (Starting in Junos OS Release 17.1R1)
14.2R7	Starting in Junos OS Release 14.2R7, 15.1R5, 16.1R2, and 17.1R1, the IKE ALG ALG is supported on MS-MPCs and MS-MICs.
14.2	Starting In Junos OS 14.2, ICMP messages are handled by default and PING ALG support is provided.

RELATED DOCUMENTATION

ALG Descriptions | 466

CHAPTER 28

ALGs Configuration Overview

IN THIS CHAPTER

Configuring Application Sets

You can group the applications you have defined into a named object by including the **application-set** statement at the **[edit applications]** hierarchy level with an **application** statement for each application:

```
[edit applications]
   application-set application-set-name {
   application application;
}
```

For an example of a typical application set, see "Examples: Configuring Application Protocols" on page 524.

RELATED DOCUMENTATION

ALG Descriptions | 466

Configuring Application Properties | 502

Examples: Configuring Application Protocols | 524

Verifying the Output of ALG Sessions | 525

Configuring Application Properties

IN THIS SECTION

To configure application properties, include the **application** statement at the **[edit applications]** hierarchy level:

```
[edit applications]
application application-name {
    application-protocol protocol-name;
    child-inactivity-timeout seconds;
    destination-port port-number;
    gate-timeout seconds;
    icmp-code value;
    icmp-type value;
    inactivity-timeout value;
    protocol type;
    rpc-program-number number;
    snmp-command command;
    source-port port-number;
    ttl-threshold value;
    uuid hex-value;
}
```

You can group application objects by configuring the **application-set** statement; for more information, see "Configuring Application Sets" on page 501.

This section includes the following tasks for configuring applications:

Configuring an Application Protocol

The **application-protocol** statement allows you to specify which of the supported application protocols (ALGs) to configure and include in an application set for service processing. To configure application protocols, include the **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
application-protocol protocol-name;
```

Table 20 on page 503 shows the list of supported protocols. For more information about specific protocols, see "ALG Descriptions" on page 466.

Table 20: Application Protocols Supported by Services Interfaces

Protocol Name	CLI Value	Comments
Bootstrap protocol (BOOTP)	**bootp**	Supports BOOTP and dynamic host configuration protocol (DHCP).
Distributed Computing Environment (DCE) remote procedure call (RPC)	**dce-rpc**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **uuid** value. You cannot specify **destination-port** or **source-port** values.
DCE RPC portmap	**dce-rpc-portmap**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **destination-port** value.
Domain Name System (DNS)	**dns**	Requires the **protocol** statement to have the value **udp**. This application protocol closes the DNS flow as soon as the DNS response is received.
Exec	**exec**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
FTP	**ftp**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
H.323	**h323**	–
IKE ALG	**ike-esp-nat**	Requires the **protocol** statement to have the value **udp** and requires the **destination-port** value to be 500.

Table 20: Application Protocols Supported by Services Interfaces *(continued)*

Protocol Name	CLI Value	Comments
Internet Control Message Protocol (ICMP)	**icmp**	Requires the **protocol** statement to have the value **icmp** or to be unspecified.
Internet Inter-ORB Protocol	**iiop**	–
IP	**ip**	–
Login	**login**	–
NetBIOS	**netbios**	Requires the **protocol** statement to have the value **udp** or to be unspecified. Requires a **destination-port** value.
NetShow	**netshow**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
Point-to-Point Tunneling Protocol	**pptp**	–
RealAudio	**realaudio**	–
Real-Time Streaming Protocol (RTSP)	**rtsp**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
RPC User Datagram Protocol (UDP) or TCP	**rpc**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **rpc-program-number** value. You cannot specify **destination-port** or **source-port** values.
RPC port mapping	**rpc-portmap**	Requires the **protocol** statement to have the value **udp** or **tcp**. Requires a **destination-port** value.
Shell	**shell**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** value.
Session Initiation Protocol	**sip**	–
SNMP	**snmp**	Requires the **protocol** statement to have the value **udp** or to be unspecified. Requires a **destination-port** value.
SQLNet	**sqlnet**	Requires the **protocol** statement to have the value **tcp** or to be unspecified. Requires a **destination-port** or **source-port** value.
Talk Program	**talk**	

Table 20: Application Protocols Supported by Services Interfaces *(continued)*

Protocol Name	CLI Value	Comments
Trace route	**traceroute**	Requires the **protocol** statement to have the value **udp** or to be unspecified. Requires a **destination-port** value.
Trivial FTP (TFTP)	**tftp**	Requires the **protocol** statement to have the value **udp** or to be unspecified. Requires a **destination-port** value.
WinFrame	**winframe**	–

NOTE: You can configure application-level gateways (ALGs) for ICMP and trace route under stateful firewall, NAT, or CoS rules when twice NAT is configured in the same service set. These ALGs cannot be applied to flows created by the Packet Gateway Controller Protocol (PGCP). Twice NAT does not support any other ALGs. NAT applies only the IP address and TCP or UDP headers, but not the payload.

For more information about configuring twice NAT, see "Junos Address Aware Network Addressing Overview" on page 78.

RELATED DOCUMENTATION

ALGs Available for Junos OS Address Aware NAT | 208

Configuring the Network Protocol

The **protocol** statement allows you to specify which of the supported network protocols to match in an application definition. To configure network protocols, include the **protocol** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
protocol type;
```

You specify the protocol type as a numeric value; for the more commonly used protocols, text names are also supported in the command-line interface (CLI). Table 21 on page 506 shows the list of the supported protocols.

Table 21: Network Protocols Supported by Services Interfaces

Network Protocol Type	CLI Value	Comments
IP Security (IPsec) authentication header (AH)	**ah**	–
External Gateway Protocol (EGP)	**egp**	–
IPsec Encapsulating Security Payload (ESP)	**esp**	–
Generic routing encapsulation (GR)	**gre**	–
ICMP	**icmp**	Requires an **application-protocol** value of **icmp**.
ICMPv6	**icmp6**	Requires an **application-protocol** value of **icmp**.
Internet Group Management Protocol (IGMP)	**igmp**	–
IP in IP	**ipip**	–
OSPF	**ospf**	–
Protocol Independent Multicast (PIM)	**pim**	–
Resource Reservation Protocol (RSVP)	**rsvp**	–
TCP	**tcp**	Requires a **destination-port** or **source-port** value unless you specify **application-protocol rcp** or **dce-rcp**.
UDP	**udp**	Requires a **destination-port** or **source-port** value unless you specify **application-protocol rcp** or **dce-rcp**.

For a complete list of possible numeric values, see RFC 1700, *Assigned Numbers (for the Internet Protocol Suite)*.

NOTE: IP version 6 (IPv6) is not supported as a network protocol in application definitions.

By default, the twice NAT feature can affect 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 twice NAT configurations. For more information about configuring twice NAT, see "Junos Address Aware Network Addressing Overview" on page 78.

Configuring the ICMP Code and Type

The ICMP code and type provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ICMP settings, include the **icmp-code** and **icmp-type** statements at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
icmp-code value;
icmp-type value;
```

You can include only one ICMP code and type value. The **application-protocol** statement must have the value **icmp**. Table 22 on page 508 shows the list of supported ICMP values.

Table 22: ICMP Codes and Types Supported by Services Interfaces

CLI Statement	Description
icmp-code	This value or keyword provides more specific information than **icmp-type**. Because the value's meaning depends upon the associated **icmp-type** value, you must specify **icmp-type** along with **icmp-code**. For more information, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed). The keywords are grouped by the ICMP type with which they are associated: parameter-problem: **ip-header-bad** (0), **required-option-missing** (1) redirect: **redirect-for-host** (1), **redirect-for-network** (0), **redirect-for-tos-and-host** (3), **redirect-for-tos-and-net** (2) time-exceeded: **ttl-eq-zero-during-reassembly** (1), **ttl-eq-zero-during-transit** (0) unreachable: **communication-prohibited-by-filtering** (13), **destination-host-prohibited** (10), **destination-host-unknown** (7), **destination-network-prohibited** (9), **destination-network-unknown** (6), **fragmentation-needed** (4), **host-precedence-violation** (14), **host-unreachable** (1), **host-unreachable-for-TOS** (12), **network-unreachable** (0), **network-unreachable-for-TOS** (11), **port-unreachable** (3), **precedence-cutoff-in-effect** (15), **protocol-unreachable** (2), **source-host-isolated** (8), **source-route-failed** (5)
icmp-type	Normally, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port. For more information, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*. In place of the numeric value, you can specify one of the following text synonyms (the field values are also listed): **echo-reply** (0), **echo-request** (8), **info-reply** (16), **info-request** (15), **mask-request** (17), **mask-reply** (18), **parameter-problem** (12), **redirect** (5), **router-advertisement** (9), **router-solicit** (10), **source-quench** (4), **time-exceeded** (11), **timestamp** (13), **timestamp-reply** (14), or **unreachable** (3).

NOTE: If you configure an interface with an input firewall filter that includes a reject action and with a service set that includes stateful firewall rules, the router executes the input firewall filter before the stateful firewall rules are run on the packet. As a result, when the Packet Forwarding Engine sends an ICMP error message out through the interface, the stateful firewall rules might drop the packet because it was not seen in the input direction.

Possible workarounds are to include a forwarding-table filter to perform the reject action, because this type of filter is executed after the stateful firewall in the input direction, or to include an output service filter to prevent the locally generated ICMP packets from going to the stateful firewall service.

Configuring Source and Destination Ports

The TCP or UDP source and destination port provide additional specification, in conjunction with the network protocol, for packet matching in an application definition. To configure ports, include the **destination-port** and **source-port** statements at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
destination-port value;
source-port value;
```

You must define one source or destination port. Normally, you specify this match in conjunction with the **protocol** match statement to determine which protocol is being used on the port; for constraints, see Table 20 on page 503.

You can specify either a numeric value or one of the text synonyms listed in Table 23 on page 509.

Table 23: Port Names Supported by Services Interfaces

Port Name	Corresponding Port Number
afs	**1483**
bgp	**179**
biff	**512**
bootpc	**68**
bootps	**67**

Table 23: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
cmd	**514**
cvspserver	**2401**
dhcp	**67**
domain	**53**
eklogin	**2105**
ekshell	**2106**
exec	**512**
finger	**79**
ftp	**21**
ftp-data	**20**
http	**80**
https	**443**
ident	**113**
imap	**143**
kerberos-sec	**88**
klogin	**543**
kpasswd	**761**
krb-prop	**754**
krbupdate	**760**
kshell	**544**
ldap	**389**

Table 23: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
login	**513**
mobileip-agent	**434**
mobilip-mn	**435**
msdp	**639**
netbios-dgm	**138**
netbios-ns	**137**
netbios-ssn	**139**
nfsd	**2049**
nntp	**119**
ntalk	**518**
ntp	**123**
pop3	**110**
pptp	**1723**
printer	**515**
radacct	**1813**
radius	**1812**
rip	**520**
rkinit	**2108**
smtp	**25**
snmp	**161**
snmptrap	**162**

Table 23: Port Names Supported by Services Interfaces *(continued)*

Port Name	Corresponding Port Number
snpp	**444**
socks	**1080**
ssh	**22**
sunrpc	**111**
syslog	**514**
tacacs-ds	**65**
talk	**517**
telnet	**23**
tftp	**69**
timed	**525**
who	**513**
xdmcp	**177**
zephyr-clt	**2103**
zephyr-hm	**2104**

For more information about matching criteria, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

Configuring the Inactivity Timeout Period

You can specify a timeout period for application inactivity. If the software has not detected any activity during the duration, the flow becomes invalid when the timer expires. To configure a timeout period, include the **inactivity-timeout** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
```

```
inactivity-timeout seconds;
```

The default value is 14,400 seconds. The value you configure for an application overrides any global value configured at the **[edit interfaces *interface-name* service-options]** hierarchy level; for more information, see *Configuring Default Timeout Settings for Services Interfaces*.

Configuring an IKE ALG Application

Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers. The IKE ALG enables the passing of IKEv1 and IPsec packets through NAPT-44 and NAT64 filters between IPsec peers that are not NAT-T compliant. This ALG supports only ESP tunnel mode. You can use the predefined IKE ALG application **junos-ike**, which has predefined values for the destination port (500), inactivity timeout (14,400 seconds), gate timeout (120 seconds), and ESP session idle timeout (800 seconds). If you want to use the IKE ALG with values different from the predefined **junos-ike** application, you need to configure a new IKE ALG application.

To configure an IKE ALG application:

1. Specify a name for the application.

```
[edit applications]
user@host# set application junos-ike
```

2. Specify the IKE ALG.

```
[edit applications application junos-ike]
user@host# set application-protocol ike-esp-nat
```

3. Specify the UDP protocol.

```
[edit applications application junos-ike]
user@host# set protocol udp
```

4. Specify 500 for the destination port.

```
[edit applications application junos-ike]
user@host# set destination-port 500
```

5. Specify the number of seconds that the IKE session is inactive before it is deleted. The default is 14,400 seconds.

```
[edit applications application junos-ike]
user@host# set inactivity-timeout seconds
```

6. Specify the number of seconds that can pass after IKE establishes the security association between the IPsec client and server and before the ESP traffic starts in both directions. If the ESP traffic has not started before this timeout value, the ESP gates are deleted and the ESP traffic is blocked. The default is 120 seconds.

```
[edit applications application junos-ike]
user@host# set gate-timeout seconds
```

7. Specify the ESP session (IPsec data traffic) idle timeout in seconds. If no IPsec data traffic is passed on the ESP session in this time, the session is deleted. The default is 800 seconds.

```
[edit applications application junos-ike]
user@host# set child-inactivity-timeout seconds
```

Configuring SIP

The Session Initiation Protocol (SIP) is a generalized protocol for communication between endpoints involved in Internet services such as telephony, fax, video conferencing, instant messaging, and file exchange.

The Junos OS provides ALG services in accordance with the standard described in RFC 3261, *SIP: Session Initiation Protocol*. SIP flows under the Junos OS are as described in RFC 3665, *Session Initiation Protocol (SIP) Basic Call Flow Examples*.

> **NOTE:** Before implementing the Junos OS SIP ALG, you should be familiar with certain limitations, discussed in "Junos OS SIP ALG Limitations" on page 522
>
> The use of NAT in conjunction with the SIP ALG results in changes in SIP header fields due to address translation. For an explanation of these translations, refer to "SIP ALG Interaction with Network Address Translation" on page 516.

To implement SIP on adaptive services interfaces, you configure the **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level with the value **sip**. For more information

about this statement, see "Configuring an Application Protocol" on page 503. In addition, there are two other statements you can configure to modify how SIP is implemented:

- You can enable the router to accept any incoming SIP calls for the endpoint devices that are behind the NAT firewall. When a device behind the firewall registers with the proxy that is outside the firewall, the AS or Multiservices PIC maintains the registration state. When the **learn-sip-register** statement is enabled, the router can use this information to accept inbound calls. If this statement is not configured, no inbound calls are accepted; only the devices behind the firewall can call devices outside the firewall.

  To configure SIP registration, include the **learn-sip-register** statement at the **[edit applications application *application-name*]** hierarchy level:

  ```
  [edit applications application application-name]
  learn-sip-register;
  ```

  NOTE: The **learn-sip-register** statement is not applicable to the Next Gen Services MX-SPC3.

  You can also manually inspect the SIP register by issuing the **show services stateful-firewall sip-register** command; for more information, see the *Junos OS System Basics and Services Command Reference*. The **show services stateful-firewall sip-register** command is not supported for Next Gen Services.

- You can specify a timeout period for the duration of SIP calls that are placed on hold. When a call is put on hold, there is no activity and flows might time out after the configured **inactivity-timeout** period expires, resulting in call state teardown. To avoid this, when a call is put on hold, the flow timer is reset to the **sip-call-hold-timeout** cycle to preserve the call state and flows for longer than the **inactivity-timeout** period.

  NOTE: The **sip-call-hold-timeout** statement is not applicable to the Next Gen Services MX-SPC3.

  To configure a timeout period, include the **sip-call-hold-timeout** statement at the **[edit applications application *application-name*]** hierarchy level:

  ```
  [edit applications application application-name]
  sip-call-hold-timeout seconds;
  ```

  The default value is 7200 seconds and the range is from 0 through 36,000 seconds (10 hours).

SIP ALG Interaction with Network Address Translation

IN THIS SECTION

The Network Address Translation (NAT) protocol enables multiple hosts in a private subnet to share a single public IP address to access the Internet. For outgoing traffic, NAT replaces the private IP address of the host in the private subnet with the public IP address. For incoming traffic, the public IP address is converted back into the private address, and the message is routed to the appropriate host in the private subnet.

Using NAT with the Session Initiation Protocol (SIP) service is more complicated because SIP messages contain IP addresses in the SIP headers as well as in the SIP body. When using NAT with the SIP service, the SIP headers contain information about the caller and the receiver, and the device translates this information to hide it from the outside network. The SIP body contains the Session Description Protocol (SDP) information, which includes IP addresses and port numbers for transmission of the media. The device translates SDP information for allocating resources to send and receive the media.

How IP addresses and port numbers in SIP messages are replaced depends on the direction of the message. For an outgoing message, the private IP address and port number of the client are replaced with the public IP address and port number of the Juniper Networks firewall. For an incoming message, the public address of the firewall is replaced with the private address of the client.

When an INVITE message is sent out across the firewall, the SIP Application Layer Gateway (ALG) collects information from the message header into a call table, which it uses to forward subsequent messages to the correct endpoint. When a new message arrives, for example an ACK or 200 OK, the ALG compares the “From:, To:, and Call-ID:” fields against the call table to identify the call context of the message. If a new INVITE message arrives that matches the existing call, the ALG processes it as a REINVITE.

When a message containing SDP information arrives, the ALG allocates ports and creates a NAT mapping between them and the ports in the SDP. Because the SDP requires sequential ports for the Real-Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) channels, the ALG provides consecutive even-odd ports. If it is unable to find a pair of ports, it discards the SIP message.

This topic contains the following sections:

Outgoing Calls

When a SIP call is initiated with a SIP request message from the internal to the external network, NAT replaces the IP addresses and port numbers in the SDP and binds the IP addresses and port numbers to the Juniper Networks firewall. Via, Contact, Route, and Record-Route SIP header fields, if present, are also bound to the firewall IP address. The ALG stores these mappings for use in retransmissions and for SIP response messages.

The SIP ALG then opens pinholes in the firewall to allow media through the device on the dynamically assigned ports negotiated based on information in the SDP and the Via, Contact, and Record-Route header fields. The pinholes also allow incoming packets to reach the Contact, Via, and Record-Route IP addresses and ports. When processing return traffic, the ALG inserts the original Contact, Via, Route, and Record-Route SIP fields back into packets.

Incoming Calls

Incoming calls are initiated from the public network to public static NAT addresses or to interface IP addresses on the device. Static NATs are statically configured IP addresses that point to internal hosts; interface IP addresses are dynamically recorded by the ALG as it monitors REGISTER messages sent by internal hosts to the SIP registrar. When the device receives an incoming SIP packet, it sets up a session and forwards the payload of the packet to the SIP ALG.

The ALG examines the SIP request message (initially an INVITE) and, based on information in the SDP, opens gates for outgoing media. When a 200 OK response message arrives, the SIP ALG performs NAT on the IP addresses and ports and opens pinholes in the outbound direction. (The opened gates have a short time-to-live, and they time out if a 200 OK response message is not received quickly.)

When a 200 OK response arrives, the SIP proxy examines the SDP information and reads the IP addresses and port numbers for each media session. The SIP ALG on the device performs NAT on the addresses and port numbers, opens pinholes for outbound traffic, and refreshes the timeout for gates in the inbound direction.

When the ACK arrives for the 200 OK, it also passes through the SIP ALG. If the message contains SDP information, the SIP ALG ensures that the IP addresses and port numbers are not changed from the previous INVITE—if they are, the ALG deletes old pinholes and creates new pinholes to allow media to pass through. The ALG also monitors the Via, Contact, and Record-Route SIP fields and opens new pinholes if it determines that these fields have changed.

Forwarded Calls

A forwarded call is when, for example, user A outside the network calls user B inside the network, and user B forwards the call to user C outside the network. The SIP ALG processes the INVITE from user A as

a normal incoming call. But when the ALG examines the forwarded call from B to C outside the network and notices that B and C are reached using the same interface, it does not open pinholes in the firewall, because media will flow directly between user A and user C.

Call Termination

The BYE message terminates a call. When the device receives a BYE message, it translates the header fields just as it does for any other message. But because a BYE message must be acknowledged by the receiver with a 200 OK, the ALG delays call teardown for five seconds to allow time for transmission of the 200 OK.

Call Re-INVITE Messages

Re-INVITE messages add new media sessions to a call and remove existing media sessions. When new media sessions are added to a call, new pinholes are opened in the firewall and new address bindings are created. The process is identical to the original call setup. When one or more media sessions are removed from a call, pinholes are closed and bindings released just as with a BYE message.

Call Session Timers

The SIP ALG uses the Session-Expires value to time out a session if a Re-INVITE or UPDATE message is not received. The ALG gets the Session-Expires value, if present, from the 200 OK response to the INVITE and uses this value for signaling timeout. If the ALG receives another INVITE before the session times out, it resets all timeout values to this new INVITE or to default values, and the process is repeated.

As a precautionary measure, the SIP ALG uses hard timeout values to set the maximum amount of time a call can exist. This ensures that the device is protected should one of the following events occur:

- End systems crash during a call and a BYE message is not received.
- Malicious users never send a BYE in an attempt to attack a SIP ALG.
- Poor implementations of SIP proxy fail to process Record-Route and never send a BYE message.
- Network failures prevent a BYE message from being received.

Call Cancellation

Either party can cancel a call by sending a CANCEL message. Upon receiving a CANCEL message, the SIP ALG closes pinholes through the firewall—if any have been opened—and releases address bindings. Before releasing the resources, the ALG delays the control channel age-out for approximately five seconds to allow time for the final 200 OK to pass through. The call is terminated when the five second timeout expires, regardless of whether a 487 or non-200 response arrives.

Forking

Forking enables a SIP proxy to send a single INVITE message to multiple destinations simultaneously. When the multiple 200 OK response messages arrive for the single call, the SIP ALG parses but updates call information with the first 200 OK messages it receives.

SIP Messages

The SIP message format consists of a SIP header section and the SIP body. In request messages, the first line of the header section is the request line, which includes the method type, request-URI, and protocol version. In response messages, the first line is the status line, which contains a status code. SIP headers contain IP addresses and port numbers used for signaling. The SIP body, separated from the header section by a blank line, is reserved for session description information, which is optional. Junos OS currently supports the SDP only. The SIP body contains IP addresses and port numbers used to transport the media.

SIP Headers

In the following sample SIP request message, NAT replaces the IP addresses in the header fields to hide them from the outside network.

```
INVITE bob@10.150.20.5 SIP/2.0
Via: SIP/2.0/UDP 10.150.20.3:5434
From: alice@10.150.20.3
To: bob@10.150.20.5
Call-ID: a12abcde@10.150.20.3
Contact: alice@10.150.20.3:5434
Route: <sip:netscreen@10.150.20.3:5060>
Record-Route: <sip:netscreen@10.150.20.3:5060>
```

How IP address translation is performed depends on the type and direction of the message. A message can be any of the following:

- Inbound request
- Outbound response
- Outbound request
- Inbound response

Table 24 on page 520 shows how NAT is performed in each of these cases. Note that for several of the header fields the ALG determine more than just whether the messages comes from inside or outside the network. It must also determine what client initiated the call, and whether the message is a request or response.

Table 24: Requesting Messages with NAT Table

Inbound Request (from public to private)	To:	Replace domain with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	Replace ALG address with local address
	Contact:	None
	Record-Route:	None
	Route:	None
Outbound Response (from private to public)	To:	Replace ALG address with local address
	From:	None
	Call-ID:	None
	Via:	None
	Request-URI:	N/A
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	None

Table 24: Requesting Messages with NAT Table *(continued)*

Outbound Request (from private to public)	To:	None
	From:	Replace local address with ALG address
	Call-ID:	None
	Via:	Replace local address with ALG address
	Request-URI:	None
	Contact:	Replace local address with ALG address
	Record-Route:	Replace local address with ALG address
	Route:	Replace ALG address with local address
Outbound Response (from public to private)	To:	None
	From:	Replace ALG address with local address
	Call-ID:	None
	Via:	Replace ALG address with local address
	Request-URI:	N/A
	Contact:	None
	Record-Route:	Replace ALG address with local address
	Route:	Replace ALG address with local address

SIP Body

The SDP information in the SIP body includes IP addresses the ALG uses to create channels for the media stream. Translation of the SDP section also allocates resources, that is, port numbers to send and receive the media.

The following excerpt from a sample SDP section shows the fields that are translated for resource allocation.

```
o=user 2344234 55234434 IN IP4 10.150.20.3
c=IN IP4 10.150.20.3
m=audio 43249 RTP/AVP 0
```

SIP messages can contain more than one media stream. The concept is similar to attaching multiple files to an e-mail message. For example, an INVITE message sent from a SIP client to a SIP server might have the following fields:

```
c=IN IP4 10.123.33.4
m=audio 33445 RTP/AVP 0
c=IN IP4 10.123.33.4
m=audio 33447 RTP/AVP 0
c=IN IP4 10.123.33.4
m=audio 33449 RTP/AVP 0
```

Junos OS supports up to 6 SDP channels negotiated for each direction, for a total of 12 channels per call.

Junos OS SIP ALG Limitations

The following limitations apply to configuration of the SIP ALG:

- Only the methods described in RFC 3261 are supported.
- Only SIP version 2 is supported.
- TCP is not supported as a transport mechanism for signaling messages for MS-MPCs but is supported for Next Gen Services.
- *Do not configure the SIP ALG when using STUN.* if clients use STUN/TURN to detect the firewall or NAT devices between the caller and responder or proxy, the client attempts to best-guess the NAT device behavior and act accordingly to place the call.
- On MS-MPCs, do not use the endpoint-independent mapping NAT pool option in conjunction with the SIP ALG. Errors will result. This does not apply to Next Gen Services.
- IPv6 signaling data is not supported for MS-MPCs but is supported for Next Gen Services.
- Authentication is not supported.
- Encrypted messages are not supported.
- SIP fragmentation is not supported for MS-MPCs but is supported for Next Gen Services.
- The maximum UDP packet size containing a SIP message is assumed to be 9 KB. SIP messages larger than this are not supported.
- The maximum number of media channels in a SIP message is assumed to be six.
- Fully qualified domain names (FQDNs) are not supported in critical fields.
- QoS is not supported. SIP supports DSCP rewrites.
- High availability is not supported, except for warm standby.
- A timeout setting of never is not supported on SIP or NAT.
- Multicast (forking proxy) is not supported.

Configuring an SNMP Command for Packet Matching

You can specify an SNMP command setting for packet matching. To configure SNMP, include the **snmp-command** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
snmp-command value;
```

The supported values are **get**, **get-next**, **set**, and **trap**. You can configure only one value for matching. The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **snmp**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 503.

Configuring an RPC Program Number

You can specify an RPC program number for packet matching. To configure an RPC program number, include the **rpc-program-number** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
rpc-program-number number;
```

The range of values used for DCE or RPC is from 100,000 through 400,000. The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **rpc**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 503.

Configuring the TTL Threshold

You can specify a trace route time-to-live (TTL) threshold value, which controls the acceptable level of network penetration for trace routing. To configure a TTL value, include the **ttl-threshold** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
ttl-threshold value;
```

The **application-protocol** statement at the **[edit applications application *application-name*]** hierarchy level must have the value **traceroute**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 503.

Configuring a Universal Unique Identifier

You can specify a Universal Unique Identifier (UUID) for DCE RPC objects. To configure a UUID value, include the **uuid** statement at the **[edit applications application *application-name*]** hierarchy level:

```
[edit applications application application-name]
uuid hex-value;
```

The **uuid** value is in hexadecimal notation. The **application-protocol** statement at the **[edit applications application *application-name*** hierarchy level must have the value **dce-rpc**. For information about specifying the application protocol, see "Configuring an Application Protocol" on page 503. For more information on UUID numbers, see **http://www.opengroup.org/onlinepubs/9629399/apdxa.htm**.

Examples: Configuring Application Protocols

The following example shows an application protocol definition describing a special FTP application running on port 78:

```
[edit applications]
application my-ftp-app {
    application-protocol ftp;
    protocol tcp;
    destination-port 78;
    timeout 100; # inactivity timeout for FTP service
}
```

The following example shows a special ICMP protocol (**application-protocol icmp**) of type 8 (ICMP echo):

```
[edit applications]
application icmp-app {
    application-protocol icmp;
    protocol icmp;
    icmp-type icmp-echo;
}
```

The following example shows a possible application set:

```
[edit applications]
application-set basic {
    http;
```

```
    ftp;
    telnet;
    nfs;
    icmp;
}
```

The software includes a predefined set of well-known application protocols. The set includes applications for which the TCP and UDP destination ports are already recognized by stateless firewall filters.

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring Application Properties | **502**
- Verifying the Output of ALG Sessions | **525**

Verifying the Output of ALG Sessions

IN THIS SECTION

This section contains examples of successful output from ALG sessions and information on system log configuration. You can compare the results of your sessions to check whether the configurations are functioning correctly.

FTP Example

IN THIS SECTION

This example analyzes the output during an active FTP session. It consists of four different flows; two are control flows and two are data flows. The example consists of the following parts:

Sample Output

MS-MPC Card

For MS-MPCs, the following is a complete sample output from the **show services stateful-firewall conversations application-protocol ftp** operational mode command:

```
user@host>show services stateful-firewall conversations application-protocol ftp
```

```
Interface: ms-1/3/0, Service set: CLBJI1-AAF001
Conversation: ALG protocol: ftp
  Number of initiators: 2, Number of responders: 2
Flow        State    Dir       Frm count
TCP           1.1.79.2:14083 ->        2.2.2.2:21    Watch    I             13
    NAT source        1.1.79.2:14083   ->   194.250.1.237:50118
TCP           1.1.79.2:14104 ->        2.2.2.2:20    Forward  I              3
    NAT source        1.1.79.2:14104   ->   194.250.1.237:50119
TCP            2.2.2.2:21    ->  194.250.1.237:50118 Watch    O             12
    NAT dest     194.250.1.237:50118   ->        1.1.79.2:14083
TCP            2.2.2.2:20    ->  194.250.1.237:50119 Forward  O              5
    NAT dest     194.250.1.237:50119   ->        1.1.79.2:14104
```

For each flow, the first line shows flow information, including protocol (TCP), source address, source port, destination address, destination port, flow state, direction, and frame count.

- The state of a flow can be **Watch**, **Forward**, or **Drop**:
  - A **Watch** flow state indicates that the control flow is monitored by the ALG for information in the payload. NAT processing is performed on the header and payload as needed.

  - A **Forward** flow forwards the packets without monitoring the payload. NAT is performed on the header as needed.
  - A **Drop** flow drops any packet that matches the 5 tuple.
- The frame count (**Frm count**) shows the number of packets that were processed on that flow.

The second line shows the NAT information.

- **source** indicates source NAT.
- **dest** indicates destination NAT.
- The first address and port in the NAT line are the original address and port being translated for that flow.
- The second address and port in the NAT line are the translated address and port for that flow.

MX-SPC3 Card

On the MX-SPC3 services card, the following is a complete sample output from the **show services sessions application-protocol ftp** operational mode command:

`user@host>` **show services sessions application-protocol ftp**

```
Session ID: 536870917, Service-set: ss1, Policy name: p1/131085, Timeout: 1, Valid
Logical system: root-logical-system
Resource information : FTP ALG, 1, 1
  In: 12.10.10.10/35281 --> 22.20.20.3/8204;tcp, Conn Tag: 0x0, If: vms-2/0/0.100,
 Pkts: 6, Bytes: 320,
  Out: 22.20.20.3/8204 --> 60.1.1.2/48747;tcp, Conn Tag: 0x0, If: vms-2/0/0.200,
Pkts: 9, Bytes: 8239,

Session ID: 536870919, Service-set: ss1, Policy name: p1/131085, Timeout: 29, Valid
Logical system: root-logical-system
Resource information : FTP ALG, 1, 0
  In: 12.10.10.10/44194 --> 22.20.20.3/21;tcp, Conn Tag: 0x0, If: vms-2/0/0.100,
Pkts: 13, Bytes: 585,
  Out: 22.20.20.3/21 --> 60.1.1.2/48660;tcp, Conn Tag: 0x0, If: vms-2/0/0.200,
Pkts: 11, Bytes: 650,
Total sessions: 2
```

For each session:

- The first line shows flow information, including session ID, service-set name, policy name, session timeout, logical system name, and its state.

- The second line, **Resource information**, indicates the session is created by ALG, including the ALG name (FTP ALG) and ASL group id, which is 1and the ASL resource id, which is 0 for control session and 1 for data session.
- The third line **In** is forward flow and the fourth line **Out** is reverse flow, including the source address, source port, destination address, destination port, protocol (TCP), session conn-tag, incoming for **In**and outgoing for **Out** interface, received frame count and bytes. NAT is performed on the header as needed.

FTP System Log Messages

System log messages are generated during an FTP session. For more information about system logs, see "System Log Messages" on page 535.

MS-MPC Card

The following system log messages are generated during creation of the FTP control flow:

- Rule Accept system log:

```
Oct 27 11:42:54 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]: ASP_SFW_RULE_ACCEPT:
proto 6 (TCP) application: ftp, fe-3/3/3.0:1.1.1.2:4450 -> 2.2.2.2:21, Match SFW
 accept rule-set:, rule: ftp, term: 1
```

- Create Accept Flow system log:

```
Oct 27 11:42:54 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]: ASP_SFW_CREATE_ACCEPT_FLOW: proto 6 (TCP)
application: ftp, fe-3/3/3.0:1.1.1.2:4450 -> 2.2.2.2:21, creating forward or watch flow
```

- System log for data flow creation:

```
Oct 27 11:43:30 (FPC Slot 1, PIC Slot 1) {ss_ftp}[FWNAT]: ASP_SFW_FTP_ACTIVE_ACCEPT: proto 6 (TCP)
application: ftp, so-2/1/2.0:2.2.2.2:20 -> 1.1.1.2:50726, Creating FTP active mode forward flow
```

MX-SPC3 CardCard

The following system log messages are generated during creation of the FTP control flow:

- System log for FTP control session creation:

```
Mar 23 23:58:54  esst480r RT_FLOW: RT_FLOW_SESSION_CREATE_USF: Tag  svc-set-name
 ss1: session created 20.1.1.2/52877->30.1.1.2/21 0x0 junos-ftp
20.1.1.2/52877->30.1.1.2/21 0x0 N/A N/A N/A N/A 6 p1 ss1-ZoneIn ss1-ZoneOut
818413576 N/A(N/A) ge-1/0/2.0 UNKNOWN UNKNOWN UNKNOWN N/A N/A -1 N/A
```

```
Mar 23 23:59:00  esst480r junos-alg: RT_ALG_FTP_ACTIVE_ACCEPT: application:ftp
data, vms-3/0/0.0 30.1.1.2:20  ->  20.1.1.2:33947 (TCP)
```

- System log for FTP data session creation:

```
Mar 23 23:59:00  esst480r RT_FLOW: RT_FLOW_SESSION_CREATE_USF: Tag  svc-set-name
 ss1: session created 30.1.1.2/20->20.1.1.2/33947 0x0 junos-ftp-data
30.1.1.2/20->20.1.1.2/33947 0x0 N/A N/A N/A N/A 6 p1 ss1-ZoneOut ss1-ZoneIn
818413577 N/A(N/A) ge-1/1/6.0 FTP-DATA UNKNOWN UNKNOWN Infrastructure File-Servers
 2 N/A
```

- System log for FTP data session destroy:

```
Mar 23 23:59:02  esst480r RT_FLOW: RT_FLOW_SESSION_CLOSE_USF: Tag  svc-set-name
 ss1: session closed TCP FIN: 30.1.1.2/20->20.1.1.2/33947 0x0 junos-ftp-data
30.1.1.2/20->20.1.1.2/33947 0x0 N/A N/A N/A N/A 6 p1 ss1-ZoneOut ss1-ZoneIn
818413577 2954(4423509) 281(14620) 2 FTP-DATA UNKNOWN N/A(N/A) ge-1/1/6.0 No
Infrastructure File-Servers 2 N/A
```

- System log for FTP control session destroy:

```
Mar 23 23:59:39  esst480r RT_FLOW: RT_FLOW_SESSION_CLOSE_USF: Tag  svc-set-name
 ss1: session closed Closed by junos-tcp-clt-emul: 20.1.1.2/52877->30.1.1.2/21
0x0 junos-ftp 20.1.1.2/52877->30.1.1.2/21 0x0 N/A N/A N/A N/A 6 p1 ss1-ZoneIn
ss1-ZoneOut 818413576 23(1082) 18(1176) 45 UNKNOWN UNKNOWN N/A(N/A) ge-1/0/2.0
No N/A N/A -1 N/A
```

Analysis

Control Flows

MS-MPC Card

The control flows are established after the three-way handshake is complete.

- Control flow from FTP client to FTP server. TCP destination port is 21.

```
TCP           1.1.79.2:14083 ->        2.2.2.2:21    Watch    I              13
    NAT source        1.1.79.2:14083   ->   194.250.1.237:50118
```

- Control flow from FTP server to FTP client. TCP source port is 21.

```
TCP            2.2.2.2:21    ->  194.250.1.237:50118 Watch    0              12
    NAT dest     194.250.1.237:50118   ->        1.1.79.2:14083
```

MX-SPC3 Card

The control flows are established after the three-way handshake is complete.

- Control session from FTP client to FTP server, TCP destination port is 21.

```
Session ID: 536870919, Service-set: ss1, Policy name: p1/131085, Timeout: 29,
Valid
Logical system: root-logical-system
Resource information : FTP ALG, 1, 0
  In: 12.10.10.10/44194 --> 22.20.20.3/21;tcp, Conn Tag: 0x0, If: vms-2/0/0.100,
 Pkts: 13, Bytes: 585,
  Out: 22.20.20.3/21 --> 60.1.1.2/48660;tcp, Conn Tag: 0x0, If: vms-2/0/0.200,
Pkts: 11, Bytes: 650,
```

- Data session from FTP client to FTP server, it's for FTP passive mode.

```
Session ID: 536870917, Service-set: ss1, Policy name: p1/131085, Timeout: 1,
Valid
Logical system: root-logical-system
Resource information : FTP ALG, 1, 1
  In: 12.10.10.10/35281 --> 22.20.20.3/8204;tcp, Conn Tag: 0x0, If: vms-2/0/0.100,
 Pkts: 6, Bytes: 320,
  Out: 22.20.20.3/8204 --> 60.1.1.2/48747;tcp, Conn Tag: 0x0, If: vms-2/0/0.200,
 Pkts: 9, Bytes: 8239,
```

- Data session from FTP server to FTP client, it's for FTP active mode:

```
Session ID: 549978117, Service-set: ss1, Policy name: p1/131085, Timeout: 1,
Valid
Logical system: root-logical-system
Resource information : FTP ALG, 1, 1
  In: 22.20.20.3/20 --> 60.1.1.3/6049;tcp, Conn Tag: 0x0, If: vms-2/0/0.200,
Pkts: 10, Bytes: 8291,
  Out: 12.10.10.10/33203 --> 22.20.20.3/20;tcp, Conn Tag: 0x0, If: vms-2/0/0.100,
 Pkts: 5, Bytes: 268,
```

Data Flows

A data port of 20 is negotiated for data transfer during the course of the FTP control protocol. These two flows are data flows between the FTP client and the FTP server:

```
TCP           1.1.79.2:14104 ->        2.2.2.2:20    Forward  I              3
    NAT source        1.1.79.2:14104   ->   194.250.1.237:50119
TCP            2.2.2.2:20    ->  194.250.1.237:50119 Forward  O              5
    NAT dest     194.250.1.237:50119   ->        1.1.79.2:14104
```

Troubleshooting Questions

1. How do I know if the FTP ALG is active?
   - The ALG protocol field in the conversation should display **ftp**.
   - There should be a valid frame count (**Frm count**) in the control flows.
   - A valid frame count in the data flows indicates that data transfer has taken place.
2. What do I need to check if the FTP connection is established but data transfer does not take place?
   - Most probably, the control connection is up, but the data connection is down.
   - Check the conversations output to determine whether both the control and data flows are present.
3. How do I interpret each flow? What does each flow mean?
   - FTP control flow initiator flow—Flow with destination port 21
   - FTP control flow responder flow—Flow with source port ;21
   - FTP data flow initiator flow—Flow with destination port 20
   - FTP data flow responder flow—Flow with source port 20

RTSP ALG Example

IN THIS SECTION

The following is an example of an RTSP conversation. The application uses the RTSP protocol for control connection. Once the connection is set up, the media is sent using UDP protocol (RTP).

This example consists of the following:

Sample Output for MS-MPCs

Here is the output from the **show services stateful-firewall conversations** operational mode command:

```
user@host# show services stateful-firewall conversations
```

```
Interface: ms-3/2/0, Service set: svc_set
Conversation: ALG protocol: rtsp
  Number of initiators: 5, Number of responders: 5
Flow           State         Dir       Frm count
TCP            1.1.1.3:58795 ->        2.2.2.2:554   Watch    I      7
UDP            1.1.1.3:1028  ->        2.2.2.2:1028  Forward  I      0
UDP            1.1.1.3:1029  ->        2.2.2.2:1029  Forward  I      0
UDP            1.1.1.3:1030  ->        2.2.2.2:1030  Forward  I      0
UDP            1.1.1.3:1031  ->        2.2.2.2:1031  Forward  I      0
TCP            2.2.2.2:554   ->        1.1.1.3:58795 Watch    O      5
UDP            2.2.2.2:1028  ->        1.1.1.3:1028  Forward  O      6
UDP            2.2.2.2:1029  ->        1.1.1.3:1029  Forward  O      0
UDP            2.2.2.2:1030  ->        1.1.1.3:1030  Forward  O      3
UDP            2.2.2.2:1031  ->        1.1.1.3:1031  Forward  O      0
```

Sample Output for MX-SPC3 Services Card

Here is the output from the **show services sessions application-protocol rtsp** operational mode command:

```
user@host# run show services sessions application-protocol rtsp
```

```
Session ID: 1073741828, Service-set: sset1, Policy name: p1/131081, Timeout: 116,
 Valid
Logical system: root-logical-system
Resource information : RTSP ALG, 1, 0
  In: 31.0.0.2/33575 --> 41.0.0.2/554;tcp, Conn Tag: 0x0, If: vms-4/0/0.1, Pkts:
8, Bytes: 948,
  Out: 41.0.0.2/554 --> 131.10.0.1/7777;tcp, Conn Tag: 0x0, If: vms-4/0/0.2, Pkts:
 6, Bytes: 1117,

Session ID: 1073741829, Service-set: sset1, Policy name: p1/131081, Timeout: 120,
 Valid
Logical system: root-logical-system
Resource information : RTSP ALG, 1, 1
```

```
  In: 41.0.0.2/35004 --> 131.10.0.1/7780;udp, Conn Tag: 0x0, If: vms-4/0/0.2, Pkts:
 220, Bytes: 79200,
  Out: 31.0.0.2/30004 --> 41.0.0.2/35004;udp, Conn Tag: 0x0, If: vms-4/0/0.1, Pkts:
 0, Bytes: 0,

Session ID: 1073741830, Service-set: sset1, Policy name: p1/131081, Timeout: 120,
 Valid
Logical system: root-logical-system
Resource information : RTSP ALG, 1, 4
  In: 41.0.0.2/35006 --> 131.10.0.1/7781;udp, Conn Tag: 0x0, If: vms-4/0/0.2, Pkts:
 220, Bytes: 174240,
  Out: 31.0.0.2/30006 --> 41.0.0.2/35006;udp, Conn Tag: 0x0, If: vms-4/0/0.1, Pkts:
 0, Bytes: 0,
Total sessions: 3
```

Analysis

An RTSP conversation should consist of TCP flows corresponding to the RTSP control connection. There should be two flows, one in each direction, from client to server and from server to client:

```
TCP            1.1.1.3:58795 ->        2.2.2.2:554    Watch    I              7
TCP            2.2.2.2:554   ->        1.1.1.3:58795 Watch    O              5
```

- The RTSP control connection for the initiator flow is sent from destination port 554.
- The RTSP control connection for the responder flow is sent from source port 554.

The UDP flows correspond to RTP media sent over the RTSP connection.

Troubleshooting Questions

1. Media does not work when the RTSP ALG is configured. What do I do?
   - Check RTSP conversations to see whether both TCP and UDP flows exist.
   - The ALG protocol should be displayed as **rtsp**.

   > **NOTE:** The state of the flow is displayed as **Watch**, because the ALG processing is taking place and the client is essentially "watching" or processing payload corresponding to the application. For FTP and RTSP ALG flows, the control connections are always **Watch** flows.

2. How do I check for ALG errors?

- You can check for errors by issuing the following command. Each ALG has a separate field for ALG packet errors.

  `user@host#` **show services stateful-firewall statistics extensive**

```
Interface: ms-3/2/0
  Service set: svc_set
    New flows:
      Accepts: 1347, Discards: 0, Rejects: 0
    Existing flows:
      Accepts: 144187, Discards: 0, Rejects: 0
    Drops:
      IP option: 0, TCP SYN defense: 0
      NAT ports exhausted: 0
    Errors:
      IP: 0, TCP: 276
      UDP: 0, ICMP: 0
      Non-IP packets: 0, ALG: 0
    IP errors:
      IP packet length inconsistencies: 0
      Minimum IP header length check failures: 0
      Reassembled packet exceeds maximum IP length: 0
      Illegal source address: 0
      Illegal destination address: 0
      TTL zero errors: 0, Illegal IP protocol number (0 or 255): 0
      Land attack: 0
      Non-IPv4 packets: 0, Bad checksum: 0
      Illegal IP fragment length: 0
      IP fragment overlap: 0
      IP fragment reassembly timeout: 0
      Unknown: 0
    TCP errors:
      TCP header length inconsistencies: 0
      Source or destination port number is zero: 0
      Illegal sequence number and flags combinations: 0
      SYN attack (multiple SYN messages seen for the same flow): 276
      First packet not a SYN message: 0
      TCP port scan (TCP handshake, RST seen from server for SYN): 0
      Bad SYN cookie response: 0
    UDP errors:
      IP data length less than minimum UDP header length (8 bytes): 0
      Source or destination port number is zero: 0
      UDP port scan (ICMP error seen for UDP flow): 0
    ICMP errors:
      IP data length less than minimum ICMP header length (8 bytes): 0
```

```
    ICMP error length inconsistencies: 0
    Duplicate ping sequence number: 0
    Mismatched ping sequence number: 0
  ALG errors:
    BOOTP: 0, DCE-RPC: 0, DCE-RPC portmap: 0
    DNS: 0, Exec: 0, FTP: 0
    ICMP: 0
    Login: 0, NetBIOS: 0, NetShow: 0
    RPC: 0, RPC portmap: 0
    RTSP: 0, Shell: 0
    SNMP: 0, SQLNet: 0, TFTP: 0
    Traceroute: 0
```

System Log Messages

IN THIS SECTION

Enabling system log generation and checking the system log are also helpful for ALG flow analysis. This section contains the following:

System Log Configuration

You can configure the enabling of system log messages at a number of different levels in the Junos OS CLI. As shown in the following sample configurations, the choice of level depends on how specific you want the event logging to be and what options you want to include. For details on the configuration options, see the *Junos OS Administration Library* (system level) or the *Junos OS Services Interfaces Library for Routing Devices* (all other levels).

1. At the topmost global level:

```
user@host# show system syslog
file messages {
    any any;
}
```

2. At the service set level:

```
user@host# show services service-set svc_set
syslog {
    host local {
        services any;
    }
}
stateful-firewall-rules allow_rtsp;
interface-service {
    service-interface ms-3/2/0;
}
```

3. At the service rule level:

```
user@host# show services stateful-firewall rule allow_rtsp
match-direction input-output;
term 0 {
    from {
        applications junos-rtsp;
    }
    then {
        accept;
        syslog;
    }
}
```

System Log Output

System log messages are generated during flow creation, as shown in the following examples:

The following system log message indicates that the ASP matched an accept rule:

```
Oct 25 16:11:37 (FPC Slot 3, PIC Slot 2) {svc_set}[FWNAT]: ASP_SFW_RULE_ACCEPT: proto 6 (TCP) application:
  rtsp, ge-2/0/1.0:1.1.1.2:35595 -> 2.2.2.2:554, Match SFW accept rule-set: , rule: allow_rtsp, term: 0
```

For a complete listing of system log messages, see the System Log Explorer.

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring Application Properties | **502**
- Examples: Configuring Application Protocols | **524**

ICMP, Ping, and Traceroute ALGs for MS-MICs and MS-MPCs

Starting with Junos OS Release 14.2, Junos OS extension-provider packages that are preinstalled and preconfigured on the MS-MIC and MS-MPC offer support for ping, traceroute, and ICMP ALGs in a consistent manner that is identical to the support that the uKernel service provides. Parity and uniformity of support is established for these ALGs between MS-MICs/MS-MPCs and the uKernel service. Until Junos OS Release 14.1, ICMP ALGs, ping ALGs, and traceroute ALGs were not entirely supported on MX Series routers with MS-MICs and MS-MPCs in comparison with the uKernel service that enables Network Address Translation (NAT) with stateful firewall (SFW) on the uKernel PIC. Support was available for handling of ICMP error response packets that match any existing flow in the opposite direction and NAT processing of ICMP packets with NAT processing of ping packets.

On MX Series routers with MS-MICs and MS-MPCs, tracking of ping traffic states wholly using the ICMP sequence numbers (for example, forwarding an echo reply only if the echo request with the corresponding sequence number is identified) is supported. ICMP application layer gateway (ALG) is enhanced to provide detailed logging information. Also, the traceroute ALGs enable UDP probe packets to be processed with the UDP destination port number greater than 33000 and the IP time-to-live (TTL) is less than 30 seconds. Traceroute ALGs enable ICMP response packets for which the ICMP type is time-exceeded to be processed and support a traceroute TTL threshold value, which controls the acceptable level of network penetration for trace routing.

You can configure ICMP and ping messages with the **application junos-icmp-all**, **application junos-icmp-ping**, and **application icmp-code** statements at the **[edit services stateful-firewall rule *rule-name* term *term-name* from]** and the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy levels to define the match condition for the stateful firewall and NAT rules. Until Junos OS Release 14.1, a restriction or a validation on the applications that you could define for ICMP messages was not present. MS-MICs and MS-MPCs function the same way as the uKernel service, which causes the ping traffic to be tracked statefully using the ICMP sequence numbers (an echo reply is forwarded only if echo request with the corresponding sequence number matches). Also, MS-MICs and MS-MPCs impose a limit on the outstanding ping requests and drop the subsequent ping requests when the limit is reached.

Similarly, for traceroute messages, you can configure the **application junos-traceroute** and **application junos-traceroute-ttl-1** statements at the **[edit services stateful-firewall rule *rule-name* term *term-name* from]** and the **[edit services nat rule *rule-name* term *term-name* from]** hierarchy levels to define the match condition for traceroute messages for the stateful firewall and NAT rules.

Traceroute and ICMP messages are supported for both IPv4 and IPv6 packets. For the traceroute functionality to work, you only need to ensure that the user-defined applications are working as expected with the inactivity timeout period and the TTL threshold values are configured to be the same period of time as configured by using the **session-timeout *seconds*** statement at the **[edit services application-identification application *application-name*]** hierarchy level. During the logging of ICMP messages, the ALG information for ping and ICMP utilities is displayed in the output of the relevant show commands, such as **show sessions** and **show conversations**, in the same manner as displayed for uKernel logging.

RELATED DOCUMENTATION

ALG Descriptions | 466

Monitoring Port Control Protocol Operations

You can monitor Port Control Protocol (PCP) operations with the following operational commands:

- For MS-MPCs use the **show services nat mappings pcp** command.

  NOTE: PCP is not supported for Next Gen Services in Junos OS Release 19.3R2

- For MS-MPCs use the **show services nat mappings endpoint-independent** command.

  For Next Gen Services use the **show services nat source mappings endpoint-independent** command.

- **show services pcp statistics protocol**

The following are examples of the output of these commands.

`user@host>` **show services nat mappings pcp**

```
Interface: sp-0/0/0, Service set: in

NAT pool: p
PCP Client       : 10.1.1.2
PCP lifetime     : 995
Mapping          : 10.1.1.2        : 9000  --> 8.8.8.8         : 1025
Session Count    :     1
Mapping State    : Active

DS-LITE output:
===============
PCP Client       : 2222::1
PCP lifetime : 106
Mapping          : 88.1.0.47       :   47  --> 70.70.70.1      :41972
Session Count    :     1
Mapping State    : Active
B4 Address       : 2222::1
```

`user@host>` **show services nat mappings endpoint-independent**

```
Interface: sp-0/0/0, Service set: in

NAT pool: p
Mapping          : 10.1.1.2        :57400  --> 8.8.8.8         : 1024
Session Count    :     0
Mapping State    : Timeout
PCP Client       : 10.1.1.2                 PCP lifetime : 991
Mapping          : 10.1.1.2        : 9000  --> 8.8.8.8         : 1025
Session Count    :     1
Mapping State    : Active

DS-LITE output:
===============
PCP Client       : 2222::1                 PCP lifetime : 190
Mapping          : 88.1.1.3        : 4001  --> 70.70.70.2      :58989
Session Count    :     1
Mapping State    : Active
B4 Address       : 2222::1
```

user@host> **show services pcp statistics protocol**

```
Protocol Statistics:

Operational Statistics

  Map request received               :0
  Peer request received              :0
  Other operational counters         :0

Option Statistics

  Unprocessed requests received      :0
  Third party requets received       :0
  Prefer fail option received        :0
  Filter option received             :0
  Other options counters             :0
  Option optional received           :0

Result Statistics

  PCP success                        :0
  PCP unsupported version            :0
  Not authorized                     :0
```

```
Bad requests                      :0
Unsupported opcode                :0
Unsupported option                :0
Bad option                        :0
Network failure                   :0
Out of resources                  :0
Unsupported protocol              :0
User exceeded quota               :0
Cannot provide external           :0
Address mismatch                  :0
Excessive number of remote peers  :0
Processing error                  :0
Other result counters             :0
```

5

PART

Securing Content Using Junos Network Secure and IDS

CHAPTER 29

Junos Network Secure Overview

IN THIS CHAPTER

Junos Network Secure Overview

Routers use firewalls to track and control the flow of traffic. Adaptive Services and MultiServices PICs employ a type of firewall called a *stateful firewall*. Contrasted with a *stateless* firewall that inspects packets in isolation, a stateful firewall provides an extra layer of security by using state information derived from past communications and other applications to make dynamic control decisions for new communication attempts.

> **NOTE:** On ACX Series routers, the stateful firewall configuration is supported only on the ACX500 indoor routers.

Stateful firewalls group relevant *flows* into *conversations*. A flow is identified by the following five properties:

- Source address
- Source port
- Destination address
- Destination port
- Protocol

A typical Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) conversation consists of two flows: the initiation flow and the responder flow. However, some conversations, such as an FTP conversation, might consist of two control flows and many data flows.

Firewall rules govern whether the conversation is allowed to be established. If a conversation is allowed, all flows within the conversation are permitted, including flows that are created during the life cycle of the conversation.

You configure stateful firewalls using a powerful rule-driven conversation handling path. A *rule* consists of direction, source address, source port, destination address, destination port, IP protocol value, and application protocol or service. In addition to the specific values you configure, you can assign the value **any** to rule objects, addresses, or ports, which allows them to match any input value. Finally, you can optionally negate the rule objects, which negates the result of the type-specific match.

Firewall rules are directional. For each new conversation, the router software checks the initiation flow matching the direction specified by the rule.

Firewall rules are ordered. The software checks the rules in the order in which you include them in the configuration. The first time the firewall discovers a match, the router implements the action specified by that rule. Rules still unchecked are ignored.

> **NOTE:** Starting in Junos OS Release 14.2, MS-MPC and MS-MIC interface cards support IPv6 traffic for Junos Network Secure Stateful Firewall.

For more information, see "Configuring Stateful Firewall Rules" on page 546.

Stateful Firewall Support for Application Protocols

By inspecting the application protocol data, the AS or MultiServices PIC firewall can intelligently enforce security policies and allow only the minimal required packet traffic to flow through the firewall.

The firewall rules are configured in relation to an interface. By default, the stateful firewall allows all sessions initiated from the hosts behind the interface to pass through the router.

> **NOTE:** Stateful firewall ALGs are not supported on ACX500 routers.

Stateful Firewall Anomaly Checking

The stateful firewall recognizes the following events as anomalies and sends them to the IDS software for processing:

- IP anomalies:
  - IP version is not correct.
  - IP header length field is too small.
  - IP header length is set larger than the entire packet.
  - Bad header checksum.

  - IP total length field is shorter than header length.
  - Packet has incorrect IP options.
  - Internet Control Message Protocol (ICMP) packet length error.
  - Time-to-live (TTL) equals 0.
- IP address anomalies:
  - IP packet source is a broadcast or multicast.
  - Land attack (source IP equals destination IP).
- IP fragmentation anomalies:
  - IP fragment overlap.
  - IP fragment missed.
  - IP fragment length error.
  - IP packet length is more than 64 kilobytes (KB).
  - Tiny fragment attack.
- TCP anomalies:
  - TCP port 0.
  - TCP sequence number 0 and flags 0.
  - TCP sequence number 0 and FIN/PSH/RST flags set.
  - TCP flags with wrong combination (TCP FIN/RST or SYN/(URG|FIN|RST).
  - Bad TCP checksum.
- UDP anomalies:
  - UDP source or destination port 0.
  - UDP header length check failed.
  - Bad UDP checksum.
- Anomalies found through stateful TCP or UDP checks:
  - SYN followed by SYN-ACK packets without ACK from initiator.
  - SYN followed by RST packets.
  - SYN without SYN-ACK.
  - Non-SYN first flow packet.

  - ICMP unreachable errors for SYN packets.
  - ICMP unreachable errors for UDP packets.
- Packets dropped according to stateful firewall rules.

> **NOTE:** ACX500 routers do not support IP fragmentation anomalies.

If you employ stateful anomaly detection in conjunction with stateless detection, IDS can provide early warning for a wide range of attacks, including these:

- TCP or UDP network probes and port scanning
- SYN flood attacks
- IP fragmentation-based attacks such as teardrop, bonk, and boink

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, MS-MPC and MS-MIC interface cards support IPv6 traffic for Junos Network Secure Stateful Firewall.

CHAPTER 30

Junos Network Secure Configuration Overview

IN THIS CHAPTER

Configuring Stateful Firewall Rules

IN THIS SECTION

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

```
[edit services stateful-firewall]
rule rule-name {
   match-direction (input | output | input-output);
   term term-name {
      from {
         application-sets set-name;
         applications [ application-names ];
         destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
```

```
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
      }
      then {
        (accept <skip-ids>| discard | reject);
        allow-ip-options [ values ];
        syslog;
      }
    }
  }
```

NOTE: ACX500 routers do not support **applications** and **application-sets** at the [**edit services stateful-firewall rule *rule-name* term *term-name* from**] hierarchy level.

NOTE: On ACX500 routers, to enable syslog, include the **stateful-firewall-logs** CLI statement at the [**edit services service-set service-set-name syslog host local class**] hierarchy level.

Each stateful firewall rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. A term consists of the following:

- **from** statement—Specifies the match conditions and applications that are included and excluded. The **from** statement is optional in stateful firewall rules.
- **then** statement—Specifies the actions and action modifiers to be performed by the router software. The **then** statement is mandatory in stateful firewall rules.

ACX500 Series routers do not support the following while configuring stateful firewall rules:

- **match-direction** (**output | input-output**)
- **post-service-filter** at the interface service input hierarchy level.
- IPv6 source address and destination address.
- **application-sets**, **application**, **allow-ip-options** at the [**edit services stateful-firewall**] hierarchy level.
- Application Layer Gateways (ALGs).
- Chaining of services within Multiservices Modular Interfaces Card (MS-MIC) and with inline-services (-si).

- Class of service.
- The following **show services stateful-firewall** CLI commands are not supported:
  - **show services stateful-firewall conversations**—Show conversations
  - **show services stateful-firewall flow-analysis**—Show flow table entries
  - **show services stateful-firewall redundancy-statistics**—Show redundancy statistics
  - **show services stateful-firewall sip-call**—Show SIP call information
  - **show services stateful-firewall sip-register**—Show SIP register information
  - **show services stateful-firewall subscriber-analysis**—Show subscriber table entries

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

Configuring Match Direction for Stateful Firewall Rules

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

```
[edit services stateful-firewall rule rule-name]
match-direction (input | output | input-output);
```

NOTE: ACX500 Series routers do not support **match-direction (output | input-output)**.

If you configure **match-direction input-output**, sessions initiated from both directions might match this rule.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

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 AS or 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. For more information on inside and outside interfaces, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.

On the PIC, a flow lookup is performed. If no flow is found, rule processing is performed. Rules in this service set are considered in sequence until a match is found. During rule processing, the packet direction

is compared against rule directions. Only rules with direction information that matches the packet direction are considered. Most packets result in the creation of bidirectional flows.

Configuring Match Conditions in Stateful Firewall Rules

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

```
[edit services stateful-firewall rule rule-name term term-name]
from {
    application-sets set-name;
    applications [ application-names ];
    destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
    destination-address-range low minimum-value high maximum-value <except>;
    destination-prefix-list list-name <except>;
    source-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
    source-prefix-list list-name <except>;
}
```

NOTE: ACX500 routers do not support **applications** and **application-sets** at the [**edit services stateful-firewall rule *rule-name* term *term-name* from**] hierarchy level.

The source address and destination address can be either IPv4 or IPv6.

You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*. You can use the wildcard values **any-unicast**, which denotes matching all unicast addresses, **any-ipv4**, which denotes matching all IPv4 addresses, or **any-ipv6**, which denotes matching all IPv6 addresses.

Alternatively, you can specify a list of source or destination prefixes by configuring the **prefix-list** statement at the **[edit policy-options]** hierarchy level and then including either the **destination-prefix-list** or the **source-prefix-list** statement in the stateful firewall rule. For an example, see "Examples: Configuring Stateful Firewall Rules" on page 553.

If you omit the **from** term, the stateful firewall accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.
- IP creates a unidirectional flow.

You can also include application protocol definitions you have configured at the **[edit applications]** hierarchy level; for more information, see "Configuring Application Properties" on page 502.

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

Configuring Actions in Stateful Firewall Rules

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

```
[edit services stateful-firewall rule rule-name term term-name]
then {
    (accept | discard | reject);
    allow-ip-options [ values ];
    syslog;
}
```

You must include one of the following actions:

- **accept**—The packet is accepted and sent on to its destination.
- **accept skip-ids**—The packet is accepted and sent on to its destination, but IDS rule processing configured on an MS-MPC is skipped.
- **discard**—The packet is not accepted and is not processed further.
- **reject**—The packet is not accepted and a rejection message is returned; UDP sends an ICMP unreachable code and TCP sends RST. Rejected packets can be logged or sampled.

> **NOTE:** The ACX500 indoor routers do not support the action **accept skip-ids**.

You can optionally configure the firewall to record information in the system logging facility by including the **syslog** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy

level. This statement overrides any **syslog** setting included in the service set or interface default configuration.

Configuring IP Option Handling

You can optionally configure the firewall to inspect IP header information by including the **allow-ip-options** statement at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy level. When you configure this statement, all packets that match the criteria specified in the **from** statement are subjected to additional matching criteria. A packet is accepted only when all of its IP option types are configured as values in the **allow-ip-options** statement. If you do not configure **allow-ip-options**, only packets without IP header options are accepted.

> **NOTE:** ACX500 indoor routers do not support the configuration of **allow-ip-options** statement.

The additional IP header option inspection applies only to the **accept** and **reject** stateful firewall actions. This configuration has no effect on the **discard** action. When the IP header inspection fails, reject frames are not sent; in this case, the **reject** action has the same effect as **discard**.

If an IP option packet is accepted by the stateful firewall, Network Address Translation (NAT) and intrusion detection service (IDS) are applied in the same way as to packets without IP option headers. The IP option configuration appears only in the stateful firewall rules; NAT applies to packets with or without IP options.

When a packet is dropped because it fails the IP option inspection, this exception event generates both IDS event and system log messages. The event type depends on the first IP option field rejected.

Table 25 on page 551 lists the possible values for the **allow-ip-options** statement. You can include a range or set of numeric values, or one or more of the predefined IP option settings. You can enter either the option name or its numeric equivalent. For more information, refer to http://www.iana.org/assignments/ip-parameters.

Table 25: IP Option Values

IP Option Name	Numeric Value	Comment
any	**0**	Any IP option
ip-security	**130**	–
ip-stream	**136**	–
loose-source-route	**131**	–
route-record	**7**	–

Table 25: IP Option Values *(continued)*

IP Option Name	Numeric Value	Comment
router-alert	**148**	–
strict-source-route	**137**	–
timestamp	**68**	–

Release History Table

Release	Description
17.1	**accept skip-ids**—The packet is accepted and sent on to its destination, but IDS rule processing configured on an MS-MPC is skipped.

RELATED DOCUMENTATION

Junos Network Secure Overview | **542**

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Configuring Stateful Firewall Rule Sets

The **rule-set** statement defines a collection of stateful firewall 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 stateful-firewall]** hierarchy level with a **rule** statement for each rule:

```
[edit services stateful-firewall]
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, the packet is dropped by default.

Examples: Configuring Stateful Firewall Rules

The following example show a stateful firewall configuration containing two rules, one for input matching on a specified application set and the other for output matching on a specified source address:

```
[edit services]
stateful-firewall {
    rule Rule1 {
        match-direction input;
        term 1 {
            from {
                application-sets Applications;
            }
            then {
                accept;
            }
        }
        term accept {
            then {
                accept;
            }
        }
    }
    rule Rule2 {
        match-direction output;
        term Local {
            from {
                source-address {
                    10.1.3.2/32;
                }
            }
            then {
                accept;
            }
        }
    }
}
```

The following example has a single rule with two terms. The first term rejects all traffic in **my-application-group** that originates from the specified source address, and provides a detailed system log record of the rejected packets. The second term accepts Hypertext Transfer Protocol (HTTP) traffic from anyone to the specified destination address.

```
[edit services stateful-firewall]
rule my-firewall-rule {
    match-direction input-output;
    term term1 {
        from {
            source-address 10.1.3.2/32;
            application-sets my-application-group;
        }
        then {
            reject;
            syslog;
        }
    }
    term term2 {
        from {
            destination-address 10.2.3.2/32;
            applications http;
        }
        then {
            accept;
        }
    }
}
```

The following example shows use of source and destination prefix lists. This requires two separate configuration items.

You configure the prefix list at the **[edit policy-options]** hierarchy level:

```
[edit]
policy-options {
    prefix-list p1 {
        1.1.1.1/32;
        2.2.2.0/24;
    }
    prefix-list p2 {
        3.3.3.3/32;
        4.4.4.0/24;
    }
}
```

You reference the configured prefix list in the stateful firewall rule:

```
[edit]
services {
    stateful-firewall {
        rule r1 {
            match-direction input;
            term t1 {
                from {
                    source-prefix-list {
                        p1;
                    }
                    destination-prefix-list {
                        p2;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
}
```

This is equivalent to the following configuration:

```
[edit]
services {
    stateful-firewall {
        rule r1 {
            match-direction input;
            term t1 {
                from {
                    source-address {
                        1.1.1.1/32;
                        2.2.2.0/24;
                    }
                    destination-address {
                        3.3.3.3/32;
                        4.4.4.0/24;
                    }
                }
                then {
                    accept;
                }
            }
```

```
        }
    }
}
```

You can use the **except** qualifier with the prefix lists, as in the following example. In this case, the **except** qualifier applies to all prefixes included in prefix list **p2**.

```
[edit]
services {
    stateful-firewall {
        rule r1 {
            match-direction input;
            term t1 {
                from {
                    source-prefix-list {
                        p1;
                    }
                    destination-prefix-list {
                        p2 except;
                    }
                }
                then {
                    accept;
                }
            }
        }
    }
}
```

For additional examples that combine stateful firewall configuration with other services and with virtual private network (VPN) routing and forwarding (VRF) tables, see the configuration examples.

NOTE: You can define the service-set and assign it either as interface style or next-hop style.

RELATED DOCUMENTATION

Example: BOOTP and Broadcast Addresses | **557**

Example: Dynamic Source NAT as a Next-Hop Service | **193**

Example: Virtual Routing and Forwarding (VRF) and Service Configuration | **578**

Example: BOOTP and Broadcast Addresses

The following example supports Bootstrap Protocol (BOOTP) and broadcast addresses:

```
[edit applications]
application bootp {
    application-protocol bootp;
    protocol udp;
    destination-port 67;
}
[edit services]
stateful-firewall bootp-support {
    rule bootp-allow {
        direction input;
        term bootp-allow {
            from {
                destination-address {
                    any-unicast;
                    255.255.255.255;
                }
                application bootp;
            }
            then {
                accept;
            }
        }
    }
}
```

Example: Configuring Layer 3 Services and the Services SDK on Two PICs

You can configure the Layer 3 service package and the Services SDK on two PICs. For this example, you must configure an FTP or HTTP client and a server. In this configuration, the client side of the router interface is ge-1/2/2.1 and the server side of the router interface is ge-1/1/0.48. This configuration enables Network Address Translation (NAT) with stateful firewall (SFW) on the uKernel PIC and application identification (APPID), application-aware access list (AACL), and intrusion detection and prevention (IDP) on the Services SDK PIC for FTP or HTTP traffic.

NOTE: The Services SDK does not support NAT yet. When NAT is required, you can configure the Layer 3 service package to deploy NAT along with the Services SDK such as APPID, AACL, or IDP.

NOTE: The IDP functionality is deprecated for the MX Series for Junos OS release 17.1R1 and above.

To deploy the Layer 3 service package and the Services SDK on two PICs:

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

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

2. In the hierarchy level, configure the conditions for the stateful firewall rule **r1**.

```
[edit services stateful-firewall]
user@host# set rule rule-name match-direction input-output term term from applications application-name
user@host# set rule rule-name match-direction input-output term term then accept syslog
```

In this example, the stateful firewall term is **ALLOWED-SERVICES**. Enclose the application names—junos-ftp, junos-http, and junos-icmp-ping—in brackets for *application-name*.

```
[edit services stateful-firewall]
user@host# set rule r1 match-direction input-output term ALLOWED-SERVICES from applications [ junos-ftp
    junos-http junos-icmp-ping ]
user@host# set rule r1 match-direction input-output term ALLOWED-SERVICES then accept syslog
```

3. Configure the conditions for the stateful firewall rule **r2**.

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

In this example, the stateful firewall term is **term1**.

```

```

```
[edit services stateful-firewall]
user@host# set rule r2 match-direction input-output term term1 then discard
user@host# set rule r2 match-direction input-output term term1 then syslog
```

4. Go to the following hierarchy level and verify the configuration:

```
[edit services stateful-firewall]
user@host# show
rule r1 {
    match-direction input-output;
    term ALLOWED-SERVICES {
        from {
            applications [ junos-ftp junos-http junos-icmp-ping ];
        }
        then {
            accept;
            syslog;
        }
    }
}
rule r2 {
    match-direction input-output;
    term term1 {
        then {
            discard;
            syslog;
        }
    }
}
```

5. Go to the following hierarchy level:

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

6. In the hierarchy level, configure the NAT pool.

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

In this example, the NAT pool is **OUTBOUND-SERVICES** and the IP address is **10.48.0.2/32**.

```
[edit services natl]
user@host# set pool OUTBOUND-SERVICES address 10.48.0.2/32
user@host# set pool OUTBOUND-SERVICES port automatic
```

7. Configure the NAT rule.

```
[edit services nat]
user@host# set rule rule-name match-direction output term term from applications application-name
user@host# set rule rule-name match-direction output term term then translated source-pool source-pool
    translation-type source dynamic
```

In this example, the NAT rule is **SET-MSR-ADDR**, the NAT term is **TRANSLATE-SOURCE-ADDR**, and the source pool is **OUTBOUND-SERVICES**. Enclose the application names—junos-ftp, junos-http, and junos-icmp-ping—in parentheses for *application-name*.

```
[edit services nat]
user@host# set rule SET-MSR-ADDR match-direction output term TRANSLATE-SOURCE-ADDR from
    applications [ junos-ftp junos-http junos-icmp-ping ]
user@host# set rule SET-MSR-ADDR match-direction output term TRANSLATE-SOURCE-ADDR then
    translated source-pool OUTBOUND-SERVICES translation-type source dynamic
```

8. Go to the following hierarchy level and verify the configuration:

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

```
pool OUTBOUND-SERVICES {
    address 11.48.0.2/32;
    port {
        automatic;
    }
}
rule SET-MSR-ADDR {
    match-direction output;
    term TRANSLATE-SOURCE-ADDR {
        from {
            applications [ junos-ftp junos-http junos-icmp-ping ];
        }
        then {
            translated {
                source-pool OUTBOUND-SERVICES;
                translation-type {
                    source dynamic;
                }
            }
        }
    }
}
```

9. Go to the following hierarchy level:

```
[edit security]
user@host# edit idp
```

> **NOTE:** The [edit security idp] statements are deprecated for the MX Series for Junos OS release 17.1R1 and above.

10. In the hierarchy level, configure the IDP policy.

```
[edit security idp]
user@host# set idp-policy policy-name rulebase-ips rule rule-name match application default attacks
   predefined-attacks attack-name
user@host# set idp-policy policy-name rulebase-ips rule rule-name match application default attacks
   predefined-attack-groups attack-group--name
user@host# set idp-policy policy-name rulebase-ips rule rule-name then action no-action
user@host# set idp-policy policy-name rulebase-ips rule rule-name then notification log-attacks alert
```

In this example, the IDP policy is **test1**, the rule is **r1**, the predefined attack is **FTP:USER:ROOT**, and the predefined attack group is **"Recommended Attacks"**.

```
[edit security idp]
user@host# set idp-policy test1 rulebase-ips rule r1 match application default attacks predefined-attacks
   FTP:USER:ROOT
user@host# set idp-policy test1 rulebase-ips rule r1 match application default attacks
   predefined-attack-groups [ "Recommended Attacks" ]
user@host# set idp-policy test1 rulebase-ips rule r1 then action no-action
user@host# set idp-policy test1 rulebase-ips rule r1 then notification log-attacks alert
```

11. Configure the trace options for IDP services.

```
[edit security idp]
user@host# set traceoptions file filename
user@host# set traceoptions flag all
user@host# set traceoptions level all
```

In this example, the log file name is **idp-demo.log**.

```
[edit security idp]
user@host# set traceoptions file idp-demo.log
user@host# set traceoptions flag all
user@host# set traceoptions level all
```

12. Go to the following hierarchy level and verify the configuration:

```
[edit security idp]
user@host# show
idp-policy test1 {
    rulebase-ips {
        rule r1 {
            match {
                application default;
                attacks {
                    predefined-attacks FTP:USER:ROOT;
                    predefined-attack-groups "Recommended Attacks";
                }
```

```
            }
            then {
                action {
                    no-action;
                }
                notification {
                    log-attacks {
                        alert;
                    }
                }
            }
        }
    }
}
traceoptions {
    file idp-demo.log;
    flag all;
    level all;
}
```

13. Go to the following hierarchy level:

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

14. In the hierarchy level, configure the AACL rules.

```
[edit services aacl]
user@host# set rule rule-name match-direction input-output term term from application-group-any
user@host# set rule rule-name match-direction input-output term term then count application accept
```

In this example, the AACL rule is **app-aware** and the term is **t1**.

```
[edit services aacl]
user@host# set rule app-aware match-direction input-output term t1 from application-group-any
user@host# set rule app-aware match-direction input-output term t1 then count application accept
```

15. Go to the following hierarchy level and verify the configuration:

```
[edit services aacl]
user@host# show
rule app-aware {
            match-direction input-output;
            term t1 {
                from {
                    application-group-any;
                }
                then {
                    count application;
                    accept;
                }
            }
        }
```

16. Go to the following hierarchy level:

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

17. Configure the APPID profile.

```
[edit services service-set App-Aware-Set]
user@host# set application-identification-profile application-identification-profile
```

In this example, the APPID profile is **dummy-profile**.

```
[edit services service-set App-Aware-Set]
user@host# set application-identification-profile dummy-profile
```

18. Configure the IDP profile.

```
[edit services service-set App-Aware-Set]
user@host# set idp-profile idp-profile
```

In this example, the IDP profile is **test1**.

```
[edit services service-set App-Aware-Set]
user@host# set idp-profile test1
```

19. Configure the policy decision statistics profile.

```
[edit services service-set App-Aware-Set]
user@host# set policy-decision-statistics-profile profile-name
```

In this example, the policy decision statistics profile is **lpdf-stats**.

```
[edit services service-set App-Aware-Set]
user@host# set policy-decision-statistics-profile lpdf-stats
```

20. Configure the AACL rules.

```
[edit services service-set App-Aware-Set]
user@host# set aacl-rules rule-name
```

In this example, the AACL rule name is **app-aware**.

```
[edit services service-set App-Aware-Set]
user@host# set aacl-rules app-aware
```

21. Configure two stateful firewall rules.

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

In this example, the first rule is **r1** and the second rule is **r2**.

```
[edit services service-set App-Aware-Set]
user@host# set stateful-firewall-rules r1
user@host# set stateful-firewall-rules r2
```

22. In the hierarchy level, configure the service set to bypass traffic on service PIC failure.

```
[edit services service-set App-Aware-Set]
user@host# set service-set-options bypass-traffic-on-pic-failure
```

23. Configure interface-specific service set options.

```
[edit services service-set App-Aware-Set]
user@host# set interface-service service-interface service-interface
```

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

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

24. Go to the following hierarchy level and verify the configuration:

```
[edit services service-set App-Aware-Set]
user@host# show
application-identification-profile dummy-profile;
idp-profile test1;
policy-decision-statistics-profile {
    lpdf-stats;
}
aacl-rules app-aware;
stateful-firewall-rules r1;
stateful-firewall-rules r2;
service-set-options {
    bypass-traffic-on-pic-failure;
}
interface-service {
```

```
    service-interface ms-0/1/0;
}
```

25. Go to the following hierarchy level:

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

26. In the hierarchy level, configure optional notification parameters for the services interface. Note that it is required only for debugging.

```
[edit services service-set NAT-SFW-SET]
user@host# set syslog host host-name services any
```

In this example, the host to notify is **local**.

```

```

```
[edit services service-set NAT-SFW-SET]
user@host# set services-options syslog host local services any
```

27. Configure two stateful firewall rules.

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

In this example, the first rule is **r1** and the second rule is **r2**.

```
[edit services service-set NAT-SFW-SET]
user@host# set stateful-firewall-rules r1
user@host# set stateful-firewall-rules r2
```

```

```

28. Configure NAT rules.

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

In this example, the NAT rule is **SET-MSR-ADDR**.

```
[edit services service-set NAT-SFW-SET]
user@host# set nat-rules SET-MSR-ADDR
```

29. Configure interface-specific service set options.

```
[edit services service-set NAT-SFW-SET]
user@host# set interface-service service-interface service-interface
```

In this example, the services interface is **sp-3/1/0**.

```
[edit services service-set NAT-SFW-SET]
user@host# set interface-service service-interface sp-3/1/0
```

30. Go to the following hierarchy level and verify the configuration:

```
[edit services service-set NAT-SFW-SET]
user@host# show
syslog {
    host local {
        services any;
    }
}
stateful-firewall-rules r1;
stateful-firewall-rules r2;
interface-service {
    service-interface sp-3/1/0;
}
```

31. Go to the following hierarchy level:

```
user@host# edit interfaces
```

32. In the hierarchy level, configure the interface.

```
[edit interfaces]
user@host# set interface
```

In this example, the interface is **ge-1/2/2.1**.

```
[edit interfaces]
user@host# set ge-1/2/2.1
```

33. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit ge-1/2/2.1
```

34. In the hierarchy level, configure the service set for received packets.

```
[edit interfaces ge-1/2/2 unit 1]
user@host#  set family inet service input service-set service-set-name
```

In this example, the input service set is **App-Aware-Set**.

```
[edit interfaces ge-1/2/2 unit 1]
user@host# set family inet service input service-set App-Aware-Set
```

35. Configure the service set for transmitted packets.

```
[edit interfaces ge-1/2/2 unit 1]
user@host#  set family inet service output service-set service-set-name
```

In this example, the output service set is **App-Aware-Set**.

```
[edit interfaces ge-1/2/2 unit 1]
user@host# set family inet service output service-set App-Aware-Set
```

36. Go to the following hierarchy level:

```
[edit interfaces ge-1/2/2 unit 1]
user@host# edit family inet
```

37. In the hierarchy level, configure the interface address.

```
[edit interfaces ge-1/2/2 unit 1 family inet]
user@host# set address source
```

In this example, the interface address is **10.10.9.10/30**.

```
[edit interfaces]
user@host# set address 10.10.9.10/30
```

38. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ge-1/2/2 unit 1]
user@host# show
family inet {
    service {
        input {
            service-set App-Aware-Set;
        }
        output {
            service-set App-Aware-Set;
        }
    }
    address 10.10.9.10/30;
}
```

39. Go to the following hierarchy level:

```
user@host# edit interfaces
```

40. In the hierarchy level, configure the interface.

```
[edit interfaces]
user@host# set interface
```

In this example, the interface is **ge-1/1/0.48**.

```
[edit interfaces]
user@host# set ge-1/1/0.48
```

41. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit ge-1/1/0.48
```

42. In the hierarchy level, configure the service set for received packets.

```
[edit interfaces ge-1/1/0 unit 48]
user@host# set family inet service input service-set service-set-name
```

In this example, the service set is **NAT-SFW-SET**.

```
[edit interfaces ge-1/1/0 unit 48]
user@host# set family inet service input service-set NAT-SFW-SET
```

43. Configure the service set for transmitted packets.

```
[edit interfaces ge-1/1/0 unit 48]
user@host# set family inet service output service-set service-set-name
```

In this example, the service set is **NAT-SFW-SET**.

```
[edit interfaces ge-1/1/0 unit 48]
user@host# set family inet service output service-set NAT-SFW-SET
```

44. Go to the following hierarchy level:

```
[edit interfaces ge-1/1/0 unit 48]
user@host# edit family inet
```

45. Configure the interface address.

```
[edit interfaces ge-1/1/0 unit 48 family inet]
```

```
user@host# set address source
```

In this example, the interface address is **10.48.0.1/31**.

```
[edit interfaces ge-1/1/0 unit 48 family inet]
user@host# set address 10.48.0.1/31
```

46. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ge-1/1/0 unit 48]
user@host# show
family inet {
    service {
        input {
            service-set NAT-SFW-SET;
            }
        output {
            service-set NAT-SFW-SET;
        }
    }
    address 10.48.0.1/31;
}
```

47. Go to the following hierarchy level:

```
user@host# edit interfaces
```

48. In the hierarchy level, configure the interface.

```
[edit interfaces]
set interface
```

In this example, the interface is **ms-0/1/0.0**.

```
[edit interfaces]
user@host# set ms-0/1/0.0
```

49. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit ms-0/1/0.0
```

50. In the hierarchy level, configure the protocol family.

```
[edit interfaces ms-0/1/0 unit 0]
user@host# set family inet
```

51. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces ms-0/1/0]
user@host# show
unit 0 {
    family inet;
}
```

52. Go to the following hierarchy level:

```
user@host# edit interfaces
```

53. In the hierarchy level, configure the interface.

```
[edit interfaces]
set interface
```

In this example, the interface is **sp-3/1/0.0**.

```
[edit interfaces]
user@host# set sp-3/1/0.0
```

54. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit sp-3/1/0
```

55. In the hierarchy level, configure optional notification parameters for the services interface. Note that it is required only for debugging.

```
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host host-name services any
```

In this example, the host to notify is **local**.

```

```

```
[edit interfaces sp-3/1/0]
user@host# set services-options syslog host local services any
```

56. Go to the following hierarchy level:

```
[edit interfaces]
user@host# edit sp-3/1/0.0
```

57. In the hierarchy level, configure the protocol family.

```
[edit interfaces sp-3/1/0 unit 0]
user@host# set family inet
```

58. Go to the following hierarchy level and verify the configuration:

```
[edit interfaces sp-3/1/0]
user@host# show
services-options {
    syslog {
        host local {
            services any;
        }
    }
}
unit 0 {
    family inet;
}
```

59. Go to the following hierarchy level:

```
[edit chassis]
```

60. In the hierarchy level, configure the redundancy settings.

```
[edit chassis]
user@host# set no-service-pic-restart-on-failover
user@host# set redundancy graceful-switchover
```

61. Configure the FPC and PIC.

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

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

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

62. 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
```

63. 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
```

64. Configure the size of the object cache in megabytes. Only values in increments of 128 MB are allowed and the maximum value of object cache can be 1280 MB. On MS-100, the value is 512 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 1280 MB.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider object-cache-size 1280
```

65. Configure the size of the policy database in megabytes.

```
[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
```

66. Configure the packages.

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

In this example, the first package is **jservices-appid**, the second package is **jservices-aacl**, the third package is **jservices-llpdf**, the fourth package is **jservices-idp**, and the fifth package is **jservices-sfw**. jservices-sfw is available only in Junos OS Release 10.1 and later.

```
[edit chassis fpc 1 pic 0]
user@host# set adaptive-services service-package extension-provider package jservices-appid
user@host# set adaptive-services service-package extension-provider package jservices-aacl
user@host# set adaptive-services service-package extension-provider package jservices-llpdf
user@host# set adaptive-services service-package extension-provider package jservices-idp
user@host# set adaptive-services service-package extension-provider package jservices-sfw
```

67. Configure the IP network services.

```
[edit chassis]
user@host# set network-services ip
```

68. Go to the following hierarchy level and verify the configuration:

```
[edit chassis]
user@host# show chassis
no-service-pic-restart-on-failover;
filter-memory-enhanced;
redundancy {
    graceful-switchover;
}
fpc 0 {
    pic 1 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 7;
                    object-cache-size 1280;
                    policy-db-size 64;
                    package jservices-appid;
                    package jservices-aacl;
                    package jservices-llpdf;
                    package jservices-idp;
                    package jservices-sfw;
                }
```

```
            }
        }
    }
}
network-services ip;
```

Release History Table

Release	Description
17.1R1	The IDP functionality is deprecated for the MX Series for Junos OS release 17.1R1 and above.
17.1R1	The [edit security idp] statements are deprecated for the MX Series for Junos OS release 17.1R1 and above.

Example: Virtual Routing and Forwarding (VRF) and Service Configuration

The following example combines virtual routing and forwarding (VRF) and services configuration:

```
[edit policy-options]
policy-statement test-policy {
   term t1 {
      then reject;
   }
}
[edit routing-instances]
test {
   interface ge-0/2/0.0;
   interface sp-1/3/0.20;
   instance-type vrf;
   route-distinguisher 10.58.255.1:37;
   vrf-import test-policy;
   vrf-export test-policy;
   routing-options {
      static {
         route 0.0.0.0/0 next-table inet.0;
      }
   }
}
```

```
[edit interfaces]
ge-0/2/0 {
    unit 0 {
        family inet {
            service {
                input service-set nat-me;
                output service-set nat-me;
            }
        }
    }
}
sp-1/3/0 {
    unit 0 {
        family inet;
    }
    unit 20 {
        family inet;
        service-domain inside;
    }
    unit 21 {
        family inet;
        service-domain outside;
    }
    [edit services]
    stateful-firewall {
        rule allow-any-input {
            match-direction input;
            term t1 {
                then accept;
            }
        }
    }
    nat {
        pool hide-pool {
            address 10.58.16.100;
            port automatic;
        }
        rule hide-all-input {
            match-direction input;
            term t1 {
                then {
                    translated {
                        source-pool hide-pool;
                        translation-type source napt-44;
```

```
                }
            }
        }
    }
}
service-set nat-me {
    stateful-firewall-rules allow-any-input;
    nat-rules hide-all-input;
    interface-service {
        service-interface sp-1/3/0.20;
    }
}
```

CHAPTER 31

IDS Configuration on MS-DPC Overview

IN THIS CHAPTER

Understanding SYN Cookie Protection on an MS-DPC

SYN cookie is a stateless SYN proxy mechanism you can use in conjunction with other defenses against a SYN flood attack. SYN cookie is supported on the MS-DPC multiservices card.

As with traditional SYN proxying, SYN cookie is activated when the SYN flood attack threshold is exceeded. However, because SYN cookie is stateless, it does not set up a session or policy and route lookups upon receipt of a SYN segment, and it maintains no connection request queues. This dramatically reduces CPU and memory usage and is the primary advantage of using SYN cookie over the traditional SYN proxying mechanism.

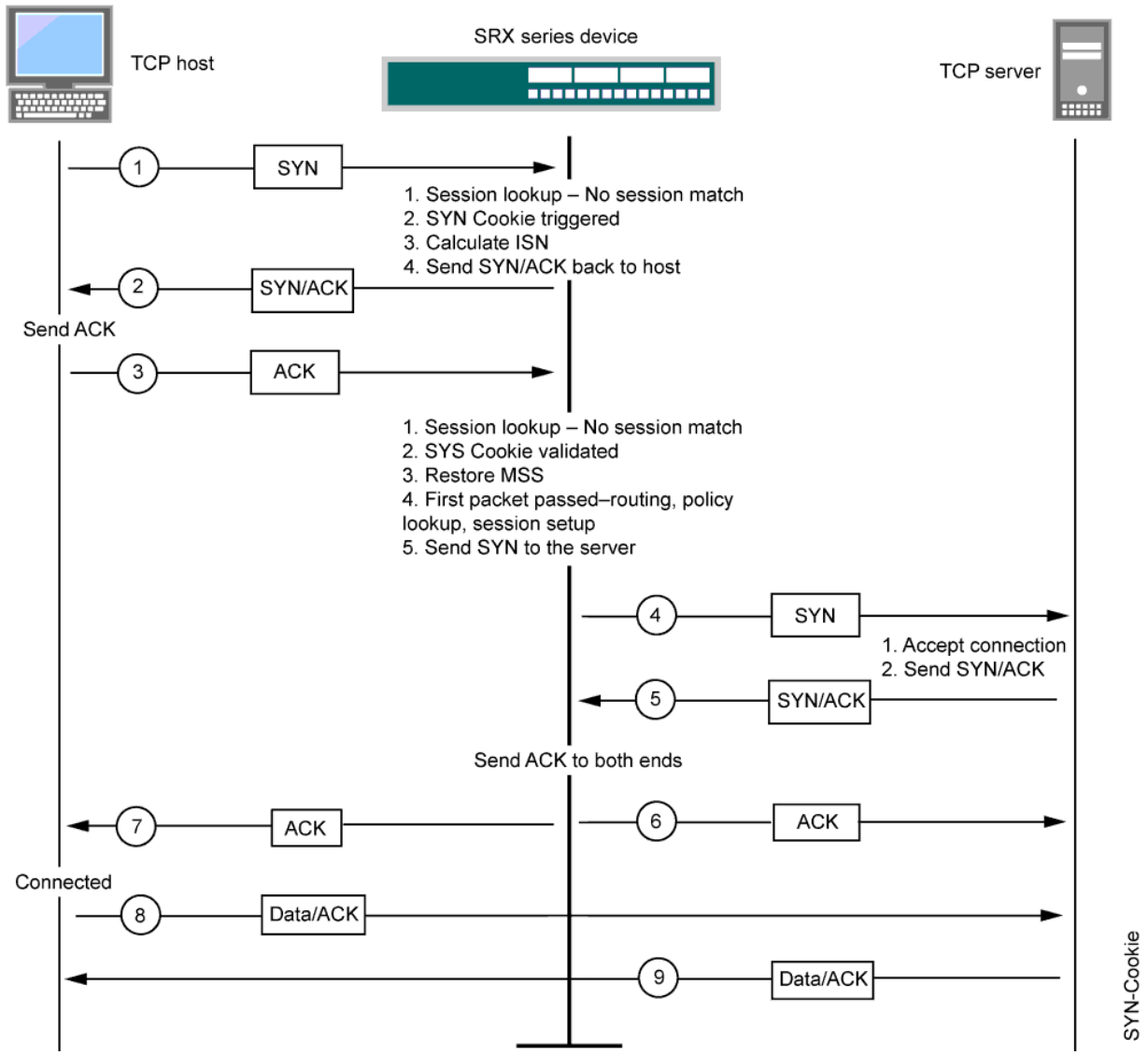
When SYN cookie is enabled on Junos OS and becomes the TCP-negotiating proxy for the destination server, it replies to each incoming SYN segment with a SYN/ACK containing an encrypted cookie as its initial sequence number (ISN). The cookie is an MD5 hash of the original source address and port number, destination address and port number, and ISN from the original SYN packet. After sending the cookie, Junos OS drops the original SYN packet and deletes the calculated cookie from memory. If there is no response to the packet containing the cookie, the attack is noted as an active SYN attack and is effectively stopped.

If the initiating host responds with a TCP packet containing the cookie +1 in the TCP ACK field, Junos OS extracts the cookie, subtracts 1 from the value, and recomputes the cookie to validate that it is a legitimate ACK. If it is legitimate, Junos OS starts the TCP proxy process by setting up a session and sending a SYN to the server containing the source information from the original SYN. When Junos OS receives a SYN/ACK from the server, it sends ACKs to the server and to the initiation host. At this point the connection is established and the host and server are able to communicate directly.

NOTE: The use of SYN cookie or SYN proxy enables the router device to protect the TCP servers behind it from SYN flood attacks in IPv6 flows.

Figure 28 on page 582 shows how a connection is established between an initiating host and a server when SYN cookie is active on Junos OS.

Figure 28: Establishing a Connection with SYN Cookie Active



RELATED DOCUMENTATION

Configuring IDS Rule Sets on an MS-DPC | 592

Configuring IDS Rules on an MS-DPC

IN THIS SECTION

IDS rules configured with an MS-DPC identify traffic for which you want the router software to count events. Because IDS is based on stateful firewall properties, you must configure at least one stateful firewall rule and include it in the service set with the IDS rules; for more information, see "Configuring Stateful Firewall Rules" on page 546.

> **NOTE:** To configure network attack protection with an MS-MPC, see "Configuring Protection Against Network Attacks on an MS-MPC" on page 601.

To configure an IDS rule, include the **rule *rule-name*** statement at the **[edit services ids]** hierarchy level:

```
[edit services ids]
rule rule-name {
   match-direction (input | output | 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 {
```

```
        aggregation (IDS) {
            destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
            source-prefix prefix-value | source-prefix-ipv6 prefix-value;
        }
        (force-entry | ignore-entry);
        logging {
            syslog;
            threshold rate;
        }
        session-limit {
            by-destination (IDS MS-DPC) {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
            by-pair (IDS MS-DPC) {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
            by-source (IDS MS-DPC) {
                hold-time seconds;
                maximum number;
                packets number;
                rate number;
            }
        }
        syn-cookie {
            mss value;
            threshold rate;
        }
    }
  }
}
```

Each IDS rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. 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 describe IDS rule content in more detail:

Configuring Match Direction for IDS Rules

Each rule must include a **match-direction** statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the **match-direction (input | input-output | output)** statement at the **[edit services ids rule *rule-name*]** hierarchy level:

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

If you configure **match-direction input-output**, bidirectional rule creation is .

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

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 AS or 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. For more information on inside and outside interfaces, see “Configuring Service Sets to be Applied to Services Interfaces” on page 9.

On the AS or 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 match the packet direction are considered.

Configuring Match Conditions in IDS Rules

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

```
[edit services ids 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>;
}
```

If you omit the **from** statement, the software accepts all events and places them in the IDS cache for processing.

The source address and destination address can be either IPv4 or IPv6. You can use the destination address, a range of destination addresses, a 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 *Routing Policies, Firewall Filters, and Traffic Policers User 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 IDS rule. For an example, see "Examples: Configuring Stateful Firewall Rules" on page 553.

You can also include application protocol definitions that you have configured at the **[edit applications]** hierarchy level; for more information, see "Configuring Application Properties" on page 502.

- To apply one or more specific application protocol definitions, include the **applications** statement at the **[edit services ids 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 ids 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.

If a match occurs on an application, the application protocol is displayed separately in the **show services ids** command output. For more information, see the CLI Explorer.

Configuring Actions in IDS Rules

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

```
[edit services ids rule rule-name term term-name]
then {
    aggregation (IDS) {
        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    (force-entry | ignore-entry);
    logging {
        syslog;
```

```
        threshold rate;
    }
    session-limit {
        by-destination (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-pair (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-source (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
    }
    syn-cookie {
        mss value;
        threshold rate;
    }
}
```

You can configure the following possible actions:

- **aggregation**—The router aggregates traffic labeled with the specified source or destination prefixes before passing the events to IDS processing. This is helpful if you want to examine all the traffic connected with a particular source or destination host. To collect traffic with some other marker, such as a particular application or port, configure that value in the match conditions.

  To configure aggregation prefixes, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level and specify values for **source-prefix**, **destination-prefix source-prefix-ipv6**, or **destination-prefix-ipv6**:

  ```
  [edit services ids rule rule-name term term-name then]
      aggregation (IDS) {
      destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
      source-prefix prefix-value | source-prefix-ipv6 prefix-value;
  }
  ```

The value of **source-prefix** and **destination-prefix** must be an integer between 1 and 32. The value of **source-prefix-ipv6** and **destination-prefix-ipv6** must be an integer between 1 and 128.

- **(force-entry | ignore-entry)**—**force-entry** provides a permanent spot in IDS caches for subsequent events after one event is registered. By default, the IDS software does not record information about "good" packets that do not exhibit suspicious behavior. You can use the **force-entry** statement to record all traffic from a suspect host, even traffic that would not otherwise be counted.

  ignore-entry ensures that all IDS events are ignored. You can use this statement to disregard all traffic from a host you trust, including any temporary anomalies that IDS would otherwise count as events.

  To configure an entry behavior different from the default, include the **force-entry** or **ignore-entry** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ids rule rule-name term term-name then]
(force-entry | ignore-entry);
```

- **logging**—The event is logged in the system log file.

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

```
[edit services ids rule rule-name term term-name then]
logging {
    syslog;
    threshold rate;
}
```

  You can optionally include a threshold rate to trigger the generation of system log messages. The threshold rate is specified in events per second. IDS logs are generated once every 60 seconds for each anomaly that is reported. The logs are generated as long as the events continue.

- **session-limit**—The router limits open sessions when the specified threshold is reached.

  To configure a threshold, include the **session-limit** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ids rule rule-name term term-name then]
session-limit {
    by-destination (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
    by-pair (IDS MS-DPC) {
```

```
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
    by-source (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
}
```

You configure the thresholds for flow limitation based on traffic direction:

- To limit the number of outgoing sessions from one internal host or subnet, configure the **by-source** statement.
- To limit the number of sessions between a pair of IP addresses, subnets, or applications, configure the **by-pair** statement.
- To limit the number of incoming sessions to one external public IP address or subnet, configure the **by-destination** statement.

For each direction, you can configure the following threshold values:

- **hold-time *seconds***—When the **rate** or **packets** measurement reaches the threshold value, stop all new flows for the specified number of seconds. Once **hold-time** is in effect, the traffic is blocked for the specified time even if the rate subsides below the specified limit. By default, **hold-time** has a value of 0; the range is 0 through 60 seconds.
- **maximum *number***—Maximum number of open sessions per IP address or subnet per application. The range is 1 through 32,767.
- **packets *number***—Maximum number of packets per second (pps) per IP address or subnet per application. The range is 4 through 2,147,483,647.
- **rate *number***—Maximum number of sessions per second per IP address or subnet per application. The range is 4 through 32,767.

  If you include more than one source address in the match conditions configured at the **[edit services ids rule *rule-name* term *term-name* from]** hierarchy level, limits are applied for each source address independently. For example, the following configuration allows 20 connections from each source address (**10.1.1.1** and **10.1.1.2**), not 20 connections total. The same logic applies to the **applications** and **destination-address** match conditions.

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

```
    from {
    source-address 10.1.1.1;
    source-address 10.1.1.2;
    }
    then {
    session-limit by-source {
       maximum 20;
    }
}
```

NOTE: IDS limits are applied to packets that are accepted by stateful firewall rules. They are not applied to packets discarded or rejected by stateful firewall rules. For example, if the stateful firewall accepts 75 percent of the incoming traffic and the remaining 25 percent is rejected or discarded, the IDS limit applies only to 75 percent of the traffic.

- **syn-cookie**—The router activates SYN-cookie defensive mechanisms.

  To configure SYN-cookie values, include the **syn-cookie** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ids rule rule-name term term-name then]
syn-cookie {
   mss value;
   threshold rate;
}
```

  If you enable SYN-cookie defenses, you must include both a threshold rate to trigger SYN-cookie activity and a Transmission Control Protocol (TCP) maximum segment size (MSS) value for TCP delayed binding. The threshold rate is specified in SYN attacks per second. By default, the TCP MSS value is 1500; the range is from 128 through 8192.

Handling of SYN Flood Attacks and SYN Cookie Protection

The main purpose of a SYN flood attack is to consume all new network connections at a site and thereby prevent authorized and legitimate users from being able to connect to network resources. The SYN (synchronize sequence number) packet is the first request to connect sent to a system. The SYN packet contains an ID to which the receiver is required to respond. If the packet contains an illegal ID, the receiving system does receive a connection acknowledgment when it responds to the intended connection initiator. Eventually, this half-open connection times out and the incoming channel on the receiver becomes available again to normally handle another request. A SYN flood attack sends so many such requests that all incoming connections are continuously tied up waiting for acknowledgments that are never received. This condition causes the server to be unavailable to legal users (except in cases where

a user session is established when it is exactly at the moment when one of the tied-up connections times out). A SYN flood attack is a connectionless attack. It does not require a real source IP addresses and, because it uses legitimate destination IP or port addresses, is practically impossible to distinguish from legitimate packets. Therefore, it is very difficult to prevent this type of attack by using only filters or stateful firewall rules. Basically, there are only three methods to protect from this type of attack:

- Intercept (delayed binding)—The firewall intercepts incoming TCP synchronization requests and establishes a connection with the client on the server's behalf, and with the server on the client's behalf. If both connections are successful, the firewall transparently merges the two connections. The firewall usually has aggressive timeouts to prevent its own resources from being consumed by a SYN attack. This the most intensive solution in terms of processing and memory requirements.
- Watch (SYN defense)—The firewall passively watches half-open connections and actively closes connections on the server after a configurable length of time.
- SYN cookie—SYN cookies are particular choices for the initial TCP sequence number chosen by the TCP server. A host requesting a connection must answer with the cookie to connect to an open TCP socket while a SYN-flood has been detected as in progress by the IDS.

Juniper Networks routers support the combination of stateful firewall and IDS mechanisms to support the SYN cookie and watch (SYN defense) methods. The key to the SYN flood attack is the filling of the SYN queue of the victim or the attacked network element. The SYN cookie defense method enables the victim to continue accepting connection requests when the SYN queue is full or, in the case of the firewall or IDS applications, when a certain threshold has been reached. After the threshold is reached, a cryptographic cookie (a 32-bit number) is created from information in the SYN segment and the SYN segment is dropped. The cookie is used as the initial sequence number in the SYN-ACK sent to the client. The cookie (plus one) is returned to the firewall or IDS application as the acknowledgment number in the ACK from a legitimate client. The returned cookie can be validated and the most important parts of the SYN segment can be reconstructed from the cookie, thereby allowing a connection to be established. Because the spoofed clients of the SYN flood never send ACKs, no resources are allocated for them in any state when SYN cookies are in use. It is preferred that you use SYN flood countermeasures only for hosts under attack. The anomaly table can be used for reliable attack recognition or they can be enabled within the stateful firewall. Such a type of configuration also helps prevent the depletion of system resources (especially the flow table) in case of attacks.

When combining multiple services, the general path is an important factor for consideration in the forward and reverse directions. This is especially true when NAT is deployed to determine whether the pre-NAT or post-NAT address must be used to match a rule. In the forward path from a LAN interface to a WAN interface, IDS and stateful firewall are performed first, then NAT, and finally IPSec. This sequence of processing of services denotes that the stateful firewall must match on a pre-NAT address, whereas the IPSec tunnel matches on the post-NAT address. In the return path, the IPSec packet is processed first, then NAT, and finally the stateful firewall. This order of processing still allows IPSec to match a public address and the stateful firewall to match on a private address. You must separately configure the firewall, NAT, and IDS services. The processing of packets becomes much more complicated when IPSec over GRE is implemented in the router with other services turned on. This behavior occurs

because Junos OS treats GRE packets in a unique fashion after GRE encapsulation. After a packet is encapsulated in a GRE packet, it is marked with an input interface as the next-hop outgoing interface. This method of marking causes GRE packets to be blocked if any input filters or input services are that do not allow for this service.

Junos OS services support a limited set of IDS rules to help detect attacks such as port scanning and anomalies in traffic patterns. It also supports some attack prevention by limiting the number of flows, sessions, and rates. In addition, it protects against SYN attacks by implementing a SYN cookie mechanism. Because the intrusion detection and prevention (IDP) service does not support higher-layer application signatures, an effective approach against attacks is that protection against a SYN attack can be configured. The IDP solution is largely a monitoring tool and not an essential prevention tool. To prevent a SYN attack, the router will operate as a type of SYN "proxy" and utilizes cookie values. When this feature is turned on, the router responds to the initial SYN packet with a SYN-ACK packet that contains a unique cookie value in the sequence number field. If the initiator responds with the same cookie in the sequence field, the TCP flow is accepted; if the responder does not respond or if it responds with the wrong cookie, the flow is dropped. To trigger this defense, you must configure a SYN cookie threshold. To enable the SYN cookie defense, an IDS rule action must contain a threshold that indicates when the feature should be enabled and an MSS value to avoid having the router manage segmented fragments when acting as a SYN proxy:

```
[edit]
user@host# set services ids rule simple-ids term 1 then syn-cookie
```

RELATED DOCUMENTATION

Configuring IDS Rule Sets on an MS-DPC | 592

Examples: Configuring IDS Rules on an MS-DPC | 593

Configuring Protection Against Network Attacks on an MS-MPC | 601

Configuring IDS Rule Sets on an MS-DPC

You can use **rule-set** statement to define a collection of IDS rules that determine what actions the router software performs on packets in the data stream. This is supported on the MS-DPC multiservices card. (To configure network attack protection with an MS-MPC, see "Configuring Protection Against Network Attacks on an MS-MPC" on page 601.)

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 ids]** hierarchy level with a **rule** statement for each rule:

```
[edit services ids]
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, the packet is dropped by default.

RELATED DOCUMENTATION

Configuring IDS Rules on an MS-DPC | 583

Examples: Configuring IDS Rules on an MS-DPC | 593

Examples: Configuring IDS Rules on an MS-DPC

The following configuration adds a permanent entry to the IDS anomaly table when it encounters a flow with the destination address 10.410.6.2. This example is supported on the MS-DPC multiservices card. (To configure network attack protection with an MS-MPC, see "Configuring Protection Against Network Attacks on an MS-MPC" on page 601.)

```
[edit services ids]
rule simple_ids {
    term 1 {
        from {
            destination-address 10.410.6.2/32;
        }
        then {
            force-entry;
            logging {
                threshold 1;
                syslog;
            }
        }
    }
    term default {
        then {
            aggregation {
```

```
            source-prefix 24;
        }
    }
  }
  match-direction input;
}
```

The IDS configuration works in conjunction with the stateful firewall mechanism and relies heavily on the anomalies reported by the stateful firewall. The following configuration example shows this relationship:

```
[edit services ids]
rule simple_ids {
  term 1 {
    from {
      source-address 10.30.20.2/32;
      destination-address {
        10.30.10.2/32;
        10.30.1.2/32 except;
      }
      applications appl-ftp;
    }
    then {
      force-entry;
      logging {
        threshold 5;
        syslog;
      }
      syn-cookie {
        threshold 10;
      }
    }
  }
  match-direction input;
}
```

```
[edit services stateful-firewall]
rule my-firewall-rule {
  match-direction input-output;
  term term1 {
    from {
      source-address 10.30.20.2/32;
      applications appl-ftp ;
      destination-address {
```

```
            10.30.10.2/32;
            10.30.1.2/32 except;
          }
        }
        then {
          accept;
          syslog;
        }
      }
    }
```

The stateful firewall or NAT service is used to generate the input data for the IDS application. When you enable and configure an IDS service, you must also enable stateful firewall with at least one rule (accept or discard all traffic). When the system is under an attack, the stateful firewall sends the correct and complete list of attack events to the IDS system. In your network environment, you can ensure that the system is wholly protected against a whole range of attacks so that the IDS system reports all such attacks. You must exercise caution when you configure the system to be protected from all attacks and unauthenticated access scenarios so that the traffic bandwidth that the system handles is not burdened. It is also important to verify the correlation between the firewall syslog messages corresponding to the attacks and IDS tables. The IDS tables must have the same or slightly less number of anomalies or errors compared to the firewall-based syslog messages. You can use the appropriate show commands are used to display the IDS tables.

A default stateful firewall rule can be as simple as only allowing connection initiation from the inside interface to the outside interface and discarding all other packets. However, in a real-word network environment, rules are generally more complex, such as configuring only a certain tributary unit ports are to be opened, using application layer gateways (ALGs) for complicated protocols, and using NAT for both outgoing connections and inside hosts such as HTTP servers. Therefore, it is necessary to also configure the system as needed to interwork with simple and complicated rules. For example, if a SYN attack is directed towards an inside address that is simply discarded, no anomalies need to be reported to the IDS system. But if the SYN attack is directed towards the real HTTP server, anomalies must be reported. The IDS system can mitigate SYN attacks by using the TCP SYN cookie defense capability. You can enable the SYN cookie protection methodology by setting a threshold for SYNs per second for a given host and also a maximum segment size (MSS). Because the IDS system uses the stateful firewall, a firewall rule must be defined in the service-set. If you do not configure the **from** statement in a stateful firewall (rule term match condition) at the **[edit services service-set service-set-name stateful-firewall-rules *rule-name* term *term-name*]** hierarchy level, it signifies that all events are placed into the IDS cache.

The following example shows configuration of flow limits:

```
[edit services ids]
rule ids-all {
   match-direction input;
```

```
    term t1 {
      from {
        application-sets alg-set;
      }
      then {
        aggregation {
          destination-prefix 30; /* IDS action aggregation */
        }
        logging {
          threshold 10;
        }
        session-limit {
          by-destination {
            hold-time 0;
            maximum 10;
            packets 200;
            rate 100;
          }
          by-pair {
            hold-time 0;
            maximum 10;
            packets 200;
            rate 100;
          }
          by-source {
            hold-time 5;
            maximum 10;
            packets 200;
            rate 100;
          }
        }
      }
    }
}
```

RELATED DOCUMENTATION

Configuring IDS Rules on an MS-DPC | **583**

Configuring IDS Rule Sets on an MS-DPC | **592**

CHAPTER 32

IDS Configuration on MS-MPC for Network Attack Protection

IN THIS CHAPTER

Understanding IDS on an MS-MPC

IN THIS SECTION

Intrusion Detection Services

Intrusion detection services (IDS) rules on an MS-MPC give you a way to identify and drop traffic that is part of a network attack.

IDS rules provide a more granular level of filtering than firewall filters and policers, which can stop illegal TCP flags and other bad flag combinations, and can enforce general rate limiting (see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*). You can use firewall filters and policers along with IDS to reduce the traffic that needs to be processed by an IDS rule.

In an IDS rule, you can specify:

- Limits on the sessions that originate from individual sources or that terminate at individual destinations. This protects against network probing and flooding attacks.
- Types of suspicious packets to drop.

To protect against header anomaly attacks, a header integrity check is automatically performed if you configure an IDS rule, stateful firewall rule, or a NAT rule and apply it to the service set. You can also explicitly configure a header integrity check for the service set if you do not assign the service set an IDS rule, stateful firewall rule, or a NAT rule.

Benefits

- Provides protection against several types of network attacks.

Session Limits

You can use IDS rules to set session limits for traffic from an individual source or to an individual destination. This protects against network probing and flooding attacks. Traffic that exceeds the session limits is dropped. You can specify session limits either for traffic with a particular IP protocol, such as ICMP, or for traffic in general.

You decide whether the limits apply to individual addresses or to an aggregation of traffic from individual subnets of a particular prefix length. For example, if you aggregate limits for IPv4 subnets with a prefix length of 24, traffic from 192.0.2.2 and 192.0.2.3 is counted against the limits for the 192.0.2.0/24 subnet.

Some common network probing and flooding attacks that session limits protect against include:

ICMP Address Sweep—The attacker sends ICMP request probes (pings) to multiple targets. If a target machine replies, the attacker receives the IP address of the target.

ICMP Flood—The attacker floods a target machine by sending a large number of ICMP packets from one or more source IP addresses. The target machine uses up its resources as it attempts to process those ICMP packets, and can no longer process valid traffic.

TCP Port Scan—The attacker sends TCP SYN packets from one source to multiple destination ports of the target machine. If the target replies with a SYN-ACK from one or more destination ports, the attacker learns which ports are open on the target.

TCP SYN Flood—The attacker floods a target machine by sending a large number of TCP SYN packets from one or more source IP addresses. The attacker might use real source IP addresses, which results in a completed TCP connection, or might use fake source IP addresses, resulting in the TCP connection not being completed. The target creates states for all the completed and uncompleted TCP connections. The target uses up its resources as it attempts to manage the connection states, and can no longer process valid traffic.

UDP Flood—The attacker floods a target machine by sending a large number of UDP packets from one or more source IP addresses. The target machine uses up its resources as it attempts to process those UDP packets, and can no longer process valid traffic.

Session limits for traffic from a source or to a destination include:

- maximum number of concurrent sessions
- maximum number of packets per second
- maximum number of connections per second

IDS also installs a dynamic filter on the PFEs of line cards for suspicious activity when the following conditions occur:

- Either the packets per second or the number of connections per second for an individual source or destination address (not for a subnet) exceeds four times the session limit in the IDS rule. This session limit is the general source or destination limit for the IDS rule, not the limit specified for a particular protocol.
- The services card CPU utilization percentage exceeds a configured value (default value is 90 percent).

The dynamic filter drops the suspicious traffic at the PFE, and the traffic is not sent to the MS-MPC to be processed by the IDS rule. When the packet or connection rate no longer exceeds four times the limit in the IDS rule, the dynamic filter is removed.

Suspicious Packet Patterns

You can use IDS rules to identify and drop traffic with a suspicious packet pattern. This protects against attackers that craft unusual packets to launch denial-of-service attacks.

Suspicious packet patterns and attacks that you can specify in an IDS rule are:

ICMP fragmentation attack—The attacker sends the target ICMP packets that are IP fragments. These are considered suspicious packets because ICMP packets are usually short. When the target receives these packets, the results can range from processing packets incorrectly to crashing the entire system.

ICMP large packet attack—The attacker sends the target ICMP frames with an IP length greater than 1024 bytes. These are considered suspicious packets because most ICMP messages are small.

ICMP Ping of death attack—The attacker sends the target ICMP ping packets whose IP datagram length (ip_len) exceeds the maximum legal length (65,535 bytes) for IP packets, and the packet is fragmented. When the target attempts to reassemble the IP packets, a buffer overflow might occur, resulting in a system crashing, freezing, and restarting.

IP Bad option attack—The attacker sends the target packets with incorrectly formatted IPv4 options or IPv6 extension headers. This can cause unpredictable issues, depending on the IP stack implementation of routers and the target.

IPv4 options—Attackers can maliciously use IPv4 options for denial-of-service attacks.

IPv6 extension headers—Attackers can maliciously use extension headers for denial-of-service attacks or to bypass filters.

IP teardrop attack—The attacker sends the target fragmented IP packets that overlap. The target machine uses up its resources as it attempts to reassemble the packets, and can no longer process valid traffic.

IP unknown protocol attack—The attacker sends the target packets with protocol numbers greater than 137 for IPv4 and 139 for IPv6. An unknown protocol might be malicious.

Land attack—The attacker sends the target spoofed SYN packets that contain the target's IP address as both the destination and the source IP address. The target uses up its resources as it repeatedly replies to itself. In another variation of the land attack, the SYN packets also contain the same source and destination ports.

SYN fragment attack—The attacker sends the target SYN packet fragments. The target caches SYN fragments, waiting for the remaining fragments to arrive so it can reassemble them and complete the connection. A flood of SYN fragments eventually fills the host's memory buffer, preventing valid traffic connections.

TCP FIN No ACK attack—The attacker sends the target TCP packets that have the FIN bit set but have the ACK bit unset. This can allow the attacker to identify the operating system of the target or to identify open ports on the target.

TCP no flag attack—The attacker sends the target TCP packets containing no flags. This can cause unpredictable behavior on the target, depending on its TCP stack implementation.

TCP SYN FIN attack—The attacker sends the target TCP packets that have both the SYN and the FIN bits set. This can cause unpredictable behavior on the target, depending on its TCP stack implementation.

TCP WinNuke attack—The attacker sends a TCP segment with the urgent (URG) flag set and destined for port 139 of a target running Windows. This might cause the target machine to crash.

Header Anomaly Attacks

To protect against header anomaly attacks, a header integrity check is automatically performed if you configure an IDS rule, a stateful firewall rule, or a NAT rule and apply it to the service set. You can also explicitly configure a header integrity check for the service set if you do not assign the service set an IDS rule, stateful firewall rule, or a NAT rule.

The header integrity check provides protection against the following header anomaly attacks:

ICMP Ping of death attack—The attacker sends the target ICMP ping packets whose IP datagram length (ip_len) exceeds the maximum legal length (65,535 bytes) for IP packets, and the packet is fragmented. When the target attempts to reassemble the IP packets, a buffer overflow might occur, resulting in a system crashing, freezing, and restarting.

IP unknown protocol attack—The attacker sends the target packets with protocol numbers greater than 137 for IPv4 and 139 for IPv6. An unknown protocol might be malicious.

TCP no flag attack—The attacker sends the target TCP packets containing no flags. This can cause unpredictable behavior on the target, depending on its TCP stack implementation.

TCP SYN FIN attack—The attacker sends the target TCP packets that have both the SYN and the FIN bits set. This can cause unpredictable behavior on the target, depending on its TCP stack implementation.

TCP FIN No ACK attack—The attacker sends the target TCP packets that have the FIN bit set but have the ACK bit unset. This can allow the attacker to identify the operating system of the target or to identify open ports on the target.

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | 601

Configuring Protection Against Network Attacks on an MS-MPC

IN THIS SECTION

This topic includes the following tasks, which describe how to protect against network attacks when using an MS-MPC:

Configuring Protection Against Network Probing, Network Flooding, and Suspicious Pattern Attacks

IN THIS SECTION

You configure protection against network probing attacks, network flooding attacks, and suspicious pattern attacks by configuring an intrusion detection service (IDS) rule, and then applying that rule to a service set that is on an MS-MPC. Only the first term of an IDS rule is used, and only the first IDS input rule and the first IDS output rule for a service set are used.

Configuring protection against network probing, network flooding, and suspicious pattern attacks includes:

Configuring IDS Rule Name and Direction

For each IDS rule, you must configure a name and the direction of traffic to which it is applied.

To configure the IDS rule name and direction:

1. Specify a name for the IDS rule.

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

2. Specify whether the IDS rule is applied to input traffic, output traffic, or both.

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

Configuring Session Limits for Subnets

If you want to apply session limits to an aggregation of all attacks to or from individual destination or source subnets rather than for individual addresses, configure aggregation.

To configure subnet aggregation:

- If you want to apply session limits to an aggregation of all attacks from within an individual IPv4 subnet, specify the subnet prefix length. The range is from 1 through 32.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set aggregation source-prefix prefix-value
  ```

  For example, the following statement configures an IPv4 prefix length of 24, and attacks from 10.1.1.2 and 10.1.1.3 are counted as attacks from the 10.1.1/24 subnet.

  ```
  [edit services ids rule rule1 term term1 then]
  user@host# set aggregation source-prefix 24
  ```

  However, if a single host on a subnet generates a large number of network probing or flooding attacks, the flows for the entire subnet might be stopped.

- If you want to apply session limits to an aggregation of all attacks from within an individual IPv6 subnet, specify the subnet prefix length. The range is from 1 through 128.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set aggregation source-prefix-ipv6 prefix-value
  ```

  For example, the following statement configures an IPv6 prefix length of 64, and attacks from 2001:db8:1234:72a2::2 and 2001:db8:1234:72a2::3 are counted as attacks from the 2001:db8:1234:72a2::/64 subnet.

  ```
  [edit services ids rule rule1 term term1 then]
  user@host# set aggregation source-prefix-ipv6 64
  ```

  However, if a single host on a subnet generates a large number of network probing or flooding attacks, the flows for the entire subnet might be stopped.

- If you want to apply session limits to an aggregation of all attacks to an individual IPv4 subnet, specify the subnet prefix length. The range is from 1 through 32.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set aggregation destination-prefix prefix-value
  ```

For example, the following statement configures an IPv4 prefix length of 24, and attacks to 10.1.1.2 and 10.1.1.3 are counted as attacks to the 10.1.1/24 subnet.

```
[edit services ids rule rule1 term term1 then]
user@host# set aggregation destination-prefix 24
```

- If you want to apply session limits to an aggregation of all attacks to an individual IPv6 subnet, specify the subnet prefix length. The range is from 1 through 128.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set aggregation destination-prefix-ipv6 prefix-value
  ```

  For example, the following statement configures an IPv6 prefix length of 64, and attacks to 2001:db8:1234:72a2::2 and 2001:db8:1234:72a2::3 are counted as attacks to the 2001:db8:1234:72a2::/64 subnet.

  ```
  [edit services ids rule rule1 term term1 then]
  user@host# set aggregation destination-prefix-ipv6 64
  ```

Configuring Session Limits Independent of the Protocol

If you want to configure session limits for traffic to an individual destination or from an individual source independent of the protocol, then perform one or more of the following tasks:

- To configure session limits for source IP addresses or subnets independent of a protocol:
  - Configure the maximum number of concurrent sessions allowed from an individual source IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-source maximum number
    ```

  - Configure the maximum number of packets per second allowed from an individual source IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-source packets number
    ```

  - Configure the maximum number of connections per second allowed from an individual source IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-source rate number
    ```

- To configure session limits for destination IP addresses or subnets independent of a protocol:
  - Configure the maximum number of concurrent sessions allowed for an individual destination IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-destination maximum number
    ```

  - Configure the maximum number of packets per second allowed for an individual destination IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-destination packets number
    ```

  - Configure the maximum number of connections per second allowed for an individual destination IP address or subnet.

    ```
    [edit services ids rule rule-name term term-name then]
    user@host# set session-limit by-destination rate number
    ```

Configuring ICMP Address Sweep Protection

To configure protection against ICMP address sweeps, configure any combination of the maximum allowed ICMP concurrent sessions, packets per second, and connections per second for a source:

- Configure the maximum number of concurrent ICMP sessions allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol icmp maximum number
  ```

- Configure the maximum number of ICMP packets per second allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol icmp packets number
  ```

- Configure the maximum number of ICMP connections per second allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol icmp rate number
  ```

Configuring TCP Port Scanner Protection

To configure protection against TCP port scanner attacks, configure any combination of the maximum allowed TCP concurrent sessions and connections per second for a source or destination:

- Configure the maximum number of concurrent TCP sessions allowed from an individual source IP address or subnet.

```
[edit services ids rule rule-name term term-name then]
user@host# set session-limit by-source by-protocol tcp maximum number
```

- Configure the maximum number of TCP connections per second allowed for an individual source IP address or subnet.

```
[edit services ids rule rule-name term term-name then]
user@host# set session-limit by-source by-protocol tcp rate number
```

- Configure the maximum number of TCP sessions allowed for an individual destination IP address or subnet.

```
[edit services ids rule rule-name term term-name then]
user@host# set session-limit by-destination by-protocol tcp maximum number
```

- Configure the maximum number of TCP connections per second allowed for an individual destination IP address or subnet.

```
[edit services ids rule rule-name term term-name then]
user@host# set session-limit by-destination by-protocol tcp rate number
```

Configuring ICMP Flooding Protection

To configure protection against ICMP flooding attacks, configure any combination of the maximum allowed ICMP concurrent sessions, packets per second, and number of connections per second for a destination:

- Configure the maximum number of concurrent ICMP sessions allowed for an individual destination IP address or subnet.

```
[edit services ids rule rule-name term term-name then]
user@host# set session-limit by-destination by-protocol icmp maximum number
```

- Configure the maximum number of ICMP packets per second allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol icmp packets number
  ```

- Configure the maximum number of ICMP connections per second allowed for an individual destination IP address or subnet for ICMP.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol icmp rate number
  ```

Configuring UDP Flooding Protection

To configure protection against UDP flooding attacks, configure any combination of the maximum allowed UDP concurrent sessions, packets per second, and connections per second for a destination:

- Configure the maximum number of concurrent UDP sessions allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol udp maximum number
  ```

- Configure the maximum number of UDP packets per second allowed for an individual destination IPaddress or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol udp packets number
  ```

- Configure the maximum number of UDP connections per second allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol udp rate number
  ```

Configuring TCP SYN Flooding Protection

To configure protection against TCP SYN flooding attacks, configure any combination of the maximum allowed TCP concurrent sessions, packets per second, and connections per second for a source or destination. You can also configure the closing of unestablished TCP connections after a timeout:

- Configure the maximum number of concurrent TCP sessions allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol tcp maximum number
  ```

- Configure the maximum number of TCP packets per second allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol tcp packets number
  ```

- Configure the maximum number of TCP connections per second allowed from an individual source IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-source by-protocol tcp rate number
  ```

- Configure the maximum number of concurrent TCP sessions allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol tcp maximum number
  ```

- Configure the maximum number of TCP connections per second allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set session-limit by-destination by-protocol tcp rate number
  ```

- Configure the maximum number of TCP packets per second allowed for an individual destination IP address or subnet.

  ```
  [edit services ids rule rule-name term term-name then]
  ```

```
user@host# set session-limit by-destination by-protocol tcp packets number
```

- Configure the closing of unestablished TCP connections and the delivery of a TCP RST to the end host to clear the TCP states on it when the **open-timeout** value at the **[edit interfaces *interface-name* service-options]** hierarchy level expires.

```
[edit services ids rule rule-name term term-name then]
user@host# set tcp-syn-defense
```

Configuring ICMP Fragmentation Protection

To protect against ICMP fragmentation attacks:

- Configure the identification and dropping of ICMP packets that are IP fragments.

```
[edit services ids rule rule-name term term-name then]
user@host# set icmp-fragment-check
```

Configuring ICMP Large Packet Protection

To protect against ICMP large packet attacks:

- Configure the identification and dropping of ICMP packets that are larger than 1024 bytes.

```
[edit services ids rule rule-name term term-name then]
user@host# set icmp-large-packet-check
```

Configuring IP Bad Options Protection

To protect against bad IPv4 options or IPv6 extension header attacks:

1. Configure the type of IPv4 options that the packet can include. If the packet includes an option that is not configured, then the packet is blocked. If the packet includes a configured option whose length is an illegal value, then the packet is dropped. Specifying **any** allows all options.

   ```
   [edit services ids rule rule-name term term-name then]
   user@host# set allow-ip-options [ip-options]
   ```

   The IPv4 options supported are **any**, **loose-source-route**, **route-record**, **security**, **stream-id**, **strict-source-route**, and **timestamp**.

   If you do not include the **allow-ip-options** statement in the IDS rule, packets with any type of IPv4 option are blocked.

2. Configure the type of IPv6 extension headers that the packet can include. If the packet includes an extension header that is not configured, then the packet is blocked. If the packet includes configured extension headers that are incorrect, then the packet is dropped. Specifying **any** allows all extension headers.

   ```
   [edit services ids rule rule-name term term-name then]
   user@host# set allow-ipv6-extension-header extension-header
   ```

   The IPv6 extension headers supported are **any**, **ah**, **dstopts**, **esp**, **fragment**, **hop-by-hop**, **mobility**, and **routing**.

   If you do not include the **allow-ipv6-extension-header** statement in the IDS rule, packets with any type of extension header are dropped.

Configuring Land Attack Protection

To protect against land attacks:

- Configure the identification and dropping of SYN packets that have the same source and destination IP address or the same source and destination IP address and port.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set land-attack-check (ip-only | ip-port)
  ```

  To specify that the packets have the same source and destination IP address, use the **ip-only** option; to specify that the packets have the same source and destination IP address and port, use the **ip-port** option.

Configuring TCP SYN Fragment Protection

To protect against TCP SYN fragment attacks:

- Configure the identification and dropping of TCP SYN packets that are IP fragments:

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set tcp-syn-fragment-check
  ```

Configuring WinNuke Protection

To protect against WinNuke attacks:

- Configure the identification and dropping of TCP segments that are destined for port 139 and have the urgent (URG) flag set.

  ```
  [edit services ids rule rule-name term term-name then]
  user@host# set tcp-winnuke-check
  ```

Configuring the Service Set

To apply the IDS rule actions to a service set:

1. Assign the IDS rule to a service set that is on an MS-MPC.

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

   If the service set is associated with an AMS interface, then the session limits you configure are applicable to each member interface.

2. Limit the packets that the IDS rule processes by configuring a stateful firewall rule (see "Configuring Stateful Firewall Rules" on page 546). The stateful firewall rule can identify either the traffic that should undergo IDS processing or the traffic that should skip IDS processing:
   - To allow IDS processing on the traffic that matches the stateful firewall rule, include **accept** at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy level.
   - To skip IDS processing on the traffic that matches the stateful firewall rule, include **accept skip-ids** at the **[edit services stateful-firewall rule *rule-name* term *term-name* then]** hierarchy level.
3. Assign the stateful firewall rule to the service set.

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

Configuring Protection Against Header Anomaly Attacks

Protect against header anomaly attacks by using either of the following methods to enable a header integrity check, which drops any packets with header anomalies:

- Configure a stateful firewall rule, a NAT rule, or an IDS rule and apply it to the service set that is on an MS-MPC. A header integrity check is automatically enabled.

- Configure a header integrity check for the service set that is on an MS-MPC.

```
[edit services]
user@host# set service-set service-set-name service-set-options header-integrity-check enable-all
```

RELATED DOCUMENTATION

Understanding IDS on an MS-MPC | **597**

Configuring Logging of Network Attack Protection Packet Drops on an MS-MPC | **613**

Configuring Logging of Network Attack Protection Packet Drops on an MS-MPC

To configure the logging of packet drops resulting from header integrity, suspicious packet pattern, and session limit checks performed by an MS-MPC:

1. Configure the logging of packet drops resulting from header integrity failures and suspicious packet patterns.

   ```
   [edit services set service-set service-set-name syslog host hostname class]
   user@host# set packet-logs
   ```

2. Configure the logging of packet drops resulting from session limit violations.

   ```
   [edit services set service-set service-set-name syslog host hostname class]
   user@host# set ids-log
   ```

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | 601

CHAPTER 33

Monitoring Junos Network Secure

IN THIS CHAPTER

Monitoring Stateful Firewall Conversations

Purpose

Use the **show services stateful-firewall conversations** command to show conversations, or collections of related flows.

Action

`user@host#` **show services stateful-firewall conversations**

```
Interface: sp-0/0/0, Service set: sset
Conversation: ALG protocol: tcp
Number of initiators: 1, Number of responders: 1
Flow State Dir Frm
count
TCP 10.0.0.1:1025 -> 128.0.0.1:80 Forward I 372755
NAT source 10.0.0.1:1025 -> 129.0.0.1:1024
Softwire 2001:0:0:1::1 -> 1001::1
TCP 128.0.0.1:80 -> 129.0.0.1:1024 Forward O 794083
NAT dest 129.0.0.1:1024 -> 10.0.0.1:1025
Softwire 2001:0:0:1::1 -> 1001::1
```

Monitoring CGN, Stateful Firewall, and Softwire Flows

Purpose

Use the following commands to check the creation of the softwires, pre-NAT flows, and post-NAT flows. Output can be filtered using more specific fields such as AFTR or B4 address or both for DS-Lite, and softwire-concentrator or softwire-initiator or both for 6rd.

- **show services stateful-firewall flows**
- **show services softwire flows**

Action

`user@host#` **show services stateful-firewall flows**

```
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow                                                State    Dir       Frm count
TCP      200.200.200.2:80    ->     44.44.44.1:1025  Forward  O          219942
    NAT dest        44.44.44.1:1025    ->       20.20.1.4:1025
    Softwire           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
    Softwire           2001::2         ->         1001::1
TCP      200.200.200.2:80    ->     44.44.44.1:1024  Forward  O          219140
    NAT dest        44.44.44.1:1024    ->       20.20.1.2:1025
    Softwire           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  O          218906
    NAT dest        44.44.44.1:1026    ->       20.20.1.3:1025
    Softwire           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
    Softwire           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
    Softwire           2001::2         ->         1001::1
```

RELATED DOCUMENTATION

Tunneling Services for IPv4-to-IPv6 Transition Overview | 375

Monitoring Global Stateful Firewall Statistics

Purpose

Use the **show services stateful-firewall statistics** command to observe statistics for service sets containing softwire rules.

Action

`user@host#` **show services stateful-firewall statistics**

```
Interface Service set Accept Discard Reject Errors
sp-0/0/0 dslite-svc-set2 118991296 0 0 0
sp-0/1/0 dslite-svc-set1 237615050 0 0 0
```

PART 6

Creating Secure Tunnels Using Junos VPN Site Secure

CHAPTER 34

Junos VPN Site Secure Overview

IN THIS CHAPTER

Understanding Junos VPN Site Secure

IN THIS SECTION

Junos VPN Site Secure is a suite of IPsec features supported on multiservices line cards (MS-DPC, MS-MPC, and MS-MIC), and was referred to as IPsec services in Junos releases earlier than 13.2. In Junos OS Release 13.2 and later, the term IPsec features is used exclusively to refer to the IPsec implementation on Adaptive Services and Encryption Services PICs. This topic provides you an overview of Junos VPN Site Secure, and has the following sections:

IPsec

The IPsec architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, the Junos OS also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

IPsec also defines a security association and key management framework that can be used with any network-layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. IPsec provides secure tunnels between two peers.

Security Associations

To use IPsec security services, you create SAs between hosts. An SA is a simplex connection that enables two hosts to communicate with each other securely by means of IPsec. There are two types of SAs:

- Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the security parameter index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic SAs require additional configuration. With dynamic SAs, you configure IKE first and then the SA. IKE creates dynamic security associations; it negotiates SAs for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPsec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPsec SAs.

IKE

IKE is a key management protocol that creates dynamic SAs; it negotiates SAs for IPsec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE performs the following tasks:

- Negotiates and manages IKE and IPsec parameters.
- Authenticates secure key exchange.
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys.
- Provides identity protection (in main mode).

Two versions of the IKE protocol (IKEv1 and IKEv2) are supported now. IKE negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In IKE, inbound and outbound IPsec SAs are established and the IKE SA secures the exchanges. Starting with Junos OS Release 11.4, both IKEv1

and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.

Starting in Junos OS Release 18.2R1, you can configure an MX Series router with MS-MPCs or MS-MICs to act only as an IKE responder. In this responder-only mode, the MX Series router does not initiate IKE negotiations, it only responds to IKE negotiations initiated by the peer gateway. This might be required when inter-operating with other vendor's equipment, such as Cisco devices. Because the MX Series does not support the protocol and port values in the traffic selector, it cannot initiate an IPsec tunnel to another vendor's peer gateway that expects these values. By configuring the response-only mode on the MX Series, the MX can accept the traffic selector in the IKE negotiation initiated from the peer gateway.

Starting in Junos OS Release 18.2R1, you can configure the MX Series router with MS-MPCs or MS-MICs to send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain. This avoids IKE fragmentation.

Starting with Junos OS Release 19.1R1, distinguished name support is added to the IKE identification (IKE ID) that is used for validation of VPN peer devices during IKE negotiation. The IKE ID received by an MX Series router from a remote peer can be an IPv4 or an IPv6 address, a hostname, a fully qualified domain name (FQDN), or a distinguished name (DN). The IKE ID sent by the remote peer needs to match what is expected by the MX Series router. Otherwise, IKE ID validation fails and the VPN is not established.

Non-Support for NAT-T

Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers, and you must disable NAT-T on the MX Series router to avoid running unsupported NAT-T (see "Disabling NAT-T on MX Series Routers for Handling NAT with IPsec-Protected Packets" on page 709). NAT-T is a method for getting around IP address translation issues encountered when data protected by IPsec passes through a NAT device for address translation.

Comparison of IPsec on ES PICs and Junos VPN Site Secure on Multiservices LIne Cards

Table 26 on page 620 compares the top-level configuration of IPsec features on the ES PIC interfaces, and IPsec on the Adaptive Services PICs and Junos VPN Site Secure on Multiservices Line Cards .

Table 26: Statement Equivalents for ES and AS Interfaces

ES PIC Configuration	AS and MultiServices Line Cards Configuration
[edit security ipsec] proposal {...}	[edit services ipsec-vpn ipsec] proposal {...}
[edit security ipsec] policy {...}	[edit services ipsec-vpn ipsec] policy {...}

Table 26: Statement Equivalents for ES and AS Interfaces *(continued)*

ES PIC Configuration	AS and MultiServices Line Cards Configuration
[edit security ipsec] security-association sa-dynamic {...}	[edit services ipsec-vpn rule *rule-name*] term *term-name* match-conditions {...} then dynamic {...}]
[edit security ipsec] security-association sa-manual {...}	[edit services ipsec-vpn rule *rule-name*] term *term-name* match-conditions {...} then manual {...}]
[edit security ike] proposal {...}	[edit services ipsec-vpn ike] proposal {...}
[edit security ike] policy {...}	[edit services ipsec-vpn ike] policy {...}
Not available	[edit services ipsec-vpn] rule-set {...}
Not available	[edit services ipsec-vpn] service-set {...}
[edit interfaces es-*fpc*/*pic*/*port*] tunnel source *address*	[edit services ipsec-vpn service-set *set-name* ipsec-vpn local-gateway *address*]
[edit interfaces es-*fpc*/*pic*/*port*] tunnel destination *address*	[edit services ipsec-vpn rule *rule-name*] remote-gateway *address*

NOTE: Although many of the same statements and properties are valid on both platforms (MultiServices and ES), the configurations are not interchangeable. You must commit a complete configuration for the PIC type that is installed in your router.

Release History Table

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, you can configure an MX Series router with MS-MPCs or MS-MICs to act only as an IKE responder.
18.2R1	Starting in Junos OS Release 18.2R1, you can configure the MX Series router with MS-MPCs or MS-MICs to send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain.

RELATED DOCUMENTATION

Authentication Algorithms | 622
Encryption Algorithms | 623
IPsec Protocols | 625
Service Sets | 697
Configuring Security Associations | 639

Authentication Algorithms

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The Junos OS uses the following authentication algorithms:

- Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

  To verify that the message has not been tampered with, the Junos OS compares the calculated message digest against a message digest that is decrypted with a shared key. The Junos OS uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with authentication header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

- Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. The Junos OS uses the SHA-1 HMAC variant that provides an additional level of hashing. SHA-1 can be used with AH, ESP, and IKE.

- SHA-256, SHA-384, and SHA-512 (sometimes grouped under the name SHA-2) are variants of SHA-1 and use longer message digests. The Junos OS supports the SHA-256 version of SHA-2, which can process all versions of Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption.

RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | 618
Encryption Algorithms | 623

Encryption Algorithms

Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users. Like authentication algorithms, a shared key is used with encryption algorithms to verify the authenticity of the IPsec devices. The Junos OS uses the following encryption algorithms:

- Data Encryption Standard cipher-block chaining (DES-CBC) is a symmetric secret-key block algorithm. DES uses a key size of 64 bits, where 8 bits are used for error detection and the remaining 56 bits provide encryption. DES performs a series of simple logical operations on the shared key, including permutations and substitutions. CBC takes the first block of 64 bits of output from DES, combines this block with the second block, feeds this back into the DES algorithm, and repeats this process for all subsequent blocks.
- Triple DES-CBC (3DES-CBC) is an encryption algorithm that is similar to DES-CBC, but provides a much stronger encryption result because it uses three keys for 168-bit (3 x 56-bit) encryption. 3DES works by using the first key to encrypt the blocks, the second key to decrypt the blocks, and the third key to re-encrypt the blocks.
- Advanced Encryption Standard (AES) is a next-generation encryption method based on the Rijndael algorithm developed by Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. It uses a 128-bit block and three different key sizes (128, 192, and 256 bits). Depending on the key size, the algorithm performs a series of computations (10, 12, or 14 rounds) that include byte substitution, column mixing, row shifting, and key addition. The use of AES in conjunction with IPsec is defined in RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.
- Starting In Junos OS Release 17.3R1, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) is supported for MS-MPCs and MS-MICs. However, in Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode. AES-GCM is an authenticated encryption algorithm designed to provide both authentication and privacy. AES-GCM uses universal hashing over a binary Galois field to provide authenticated encryption and allows authenticated encryption at data rates of tens of Gbps.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.
17.3R1	Starting In Junos OS Release 17.3R1, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) is supported for MS-MPCs and MS-MICs.

RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | 618

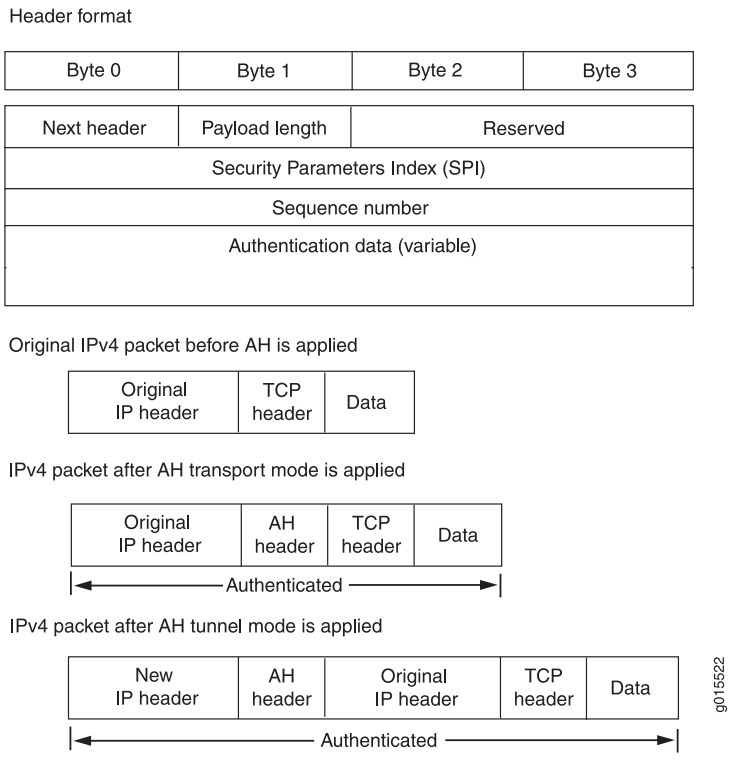
IPsec Protocols

IPsec protocols determine the type of authentication and encryption applied to packets that are secured by the router. The Junos OS supports the following IPsec protocols:

- AH—Defined in RFC 2402, AH provides connectionless integrity and data origin authentication for IPv4 and IPv6 packets. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper-level protocol data. However, some IP header fields might change in transit. Because the value of these fields might not be predictable by the sender, they cannot be protected by AH. In an IP header, AH can be identified with a value of **51** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by AH is shown in Figure 29 on page 625.

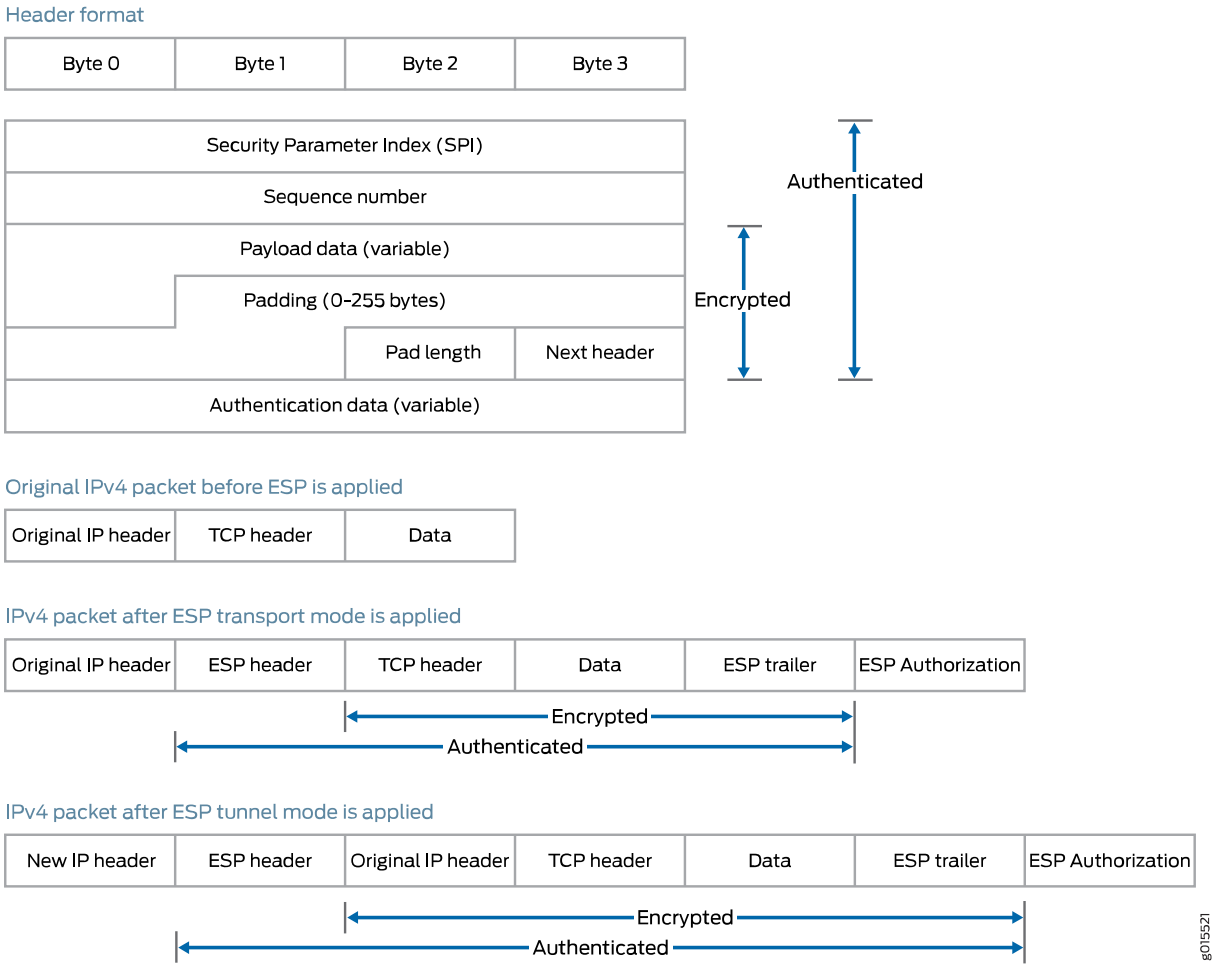
  NOTE: AH is not supported on the T Series, M120, and M320 routers.

Figure 29: AH Protocol



- ESP—Defined in RFC 2406, ESP can provide encryption and limited traffic flow confidentiality, or connectionless integrity, data origin authentication, and an anti-replay service. In an IP header, ESP can be identified a value of **50** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by ESP is shown in Figure 30 on page 626.

Figure 30: ESP Protocol



- Bundle—When you compare AH with ESP, there are some benefits and shortcomings in both protocols. ESP provides a decent level of authentication and encryption, but does so only for part of the IP packet. Conversely, although AH does not provide encryption, it does provide authentication for the entire IP packet. Because of this, the Junos OS offers a third form of IPsec protocol called a protocol bundle. The bundle option offers a hybrid combination of AH authentication with ESP encryption.

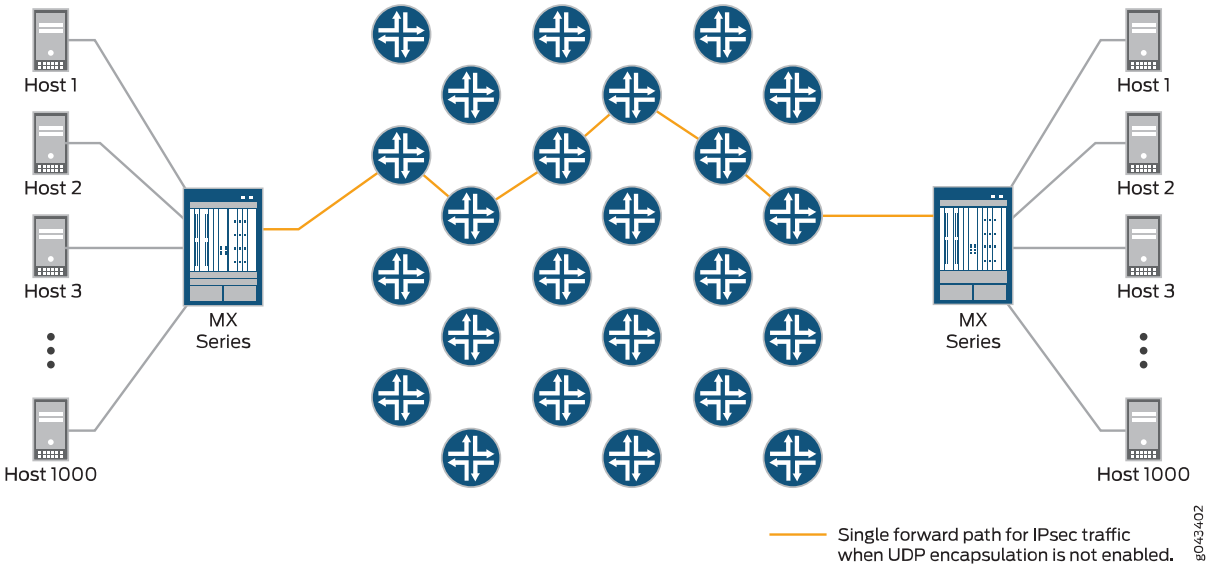
RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | 618
Configuring IPsec Proposals | 680
Configuring Security Associations | 639
protocol (IPsec) | 1387

IPsec Multipath Forwarding with UDP Encapsulation

IPsec provides secure tunnels between two peers, and IPsec encapsulated packets have IP headers that contain tunnel endpoint IPs that do not change. This results in the selection of a single forwarding path between the peers, as shown in Figure 31 on page 627. When IPsec traffic is flowing between data centers with thousands of hosts, this single path selection limits the throughput.

Figure 31: IPsec with One Forwarding Path



You can overcome this problem by enabling UDP encapsulation of the IPsec packets, which appends a UDP header after the ESP header, as shown in Figure 32 on page 628. This provides Layer 3 and 4 information to the intermediate routers, and the IPsec packets are forwarded over multiple paths, as shown in Figure 33 on page 628. You enable UDP encapsulation for the service set.

Figure 32: Appended UDP Header

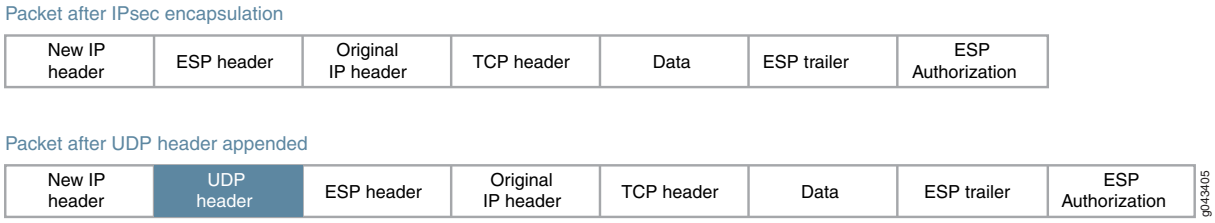
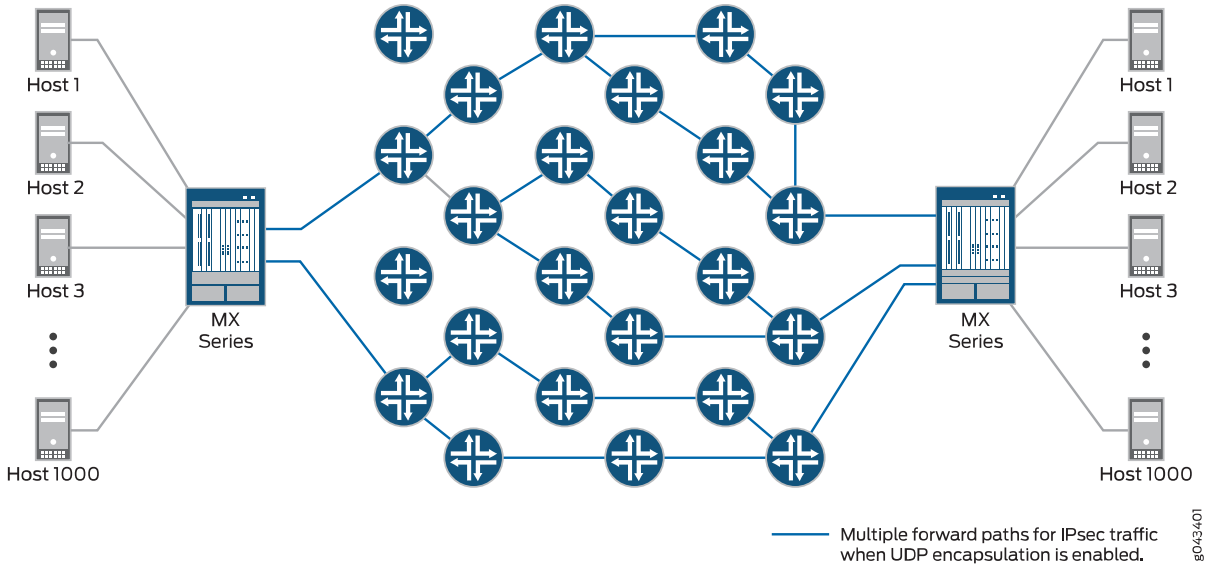


Figure 33: IPsec with Multiple Forwarding Paths



You can configure the UDP destination port or use the default value of 4565. You cannot configure 4500 as the destination port because it is a well-known port for NAT traversals.

Junos OS generates the source UDP port through a hash function that operates on the following data:

- Source IP address
- Destination IP address
- Transport protocol
- Transport source port
- Transport destination port
- A random number

Only the last two bytes of the resulting hash are used, so the internal IP header details are hidden.

When NAT-T is detected, only NAT-T UDP encapsulation occurs, not the UDP encapsulation for IPsec packets.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

Supported IPsec and IKE Standards

On routers equipped with one or more MS-MPCs, MS-MICs, or DPCs, the Canada and U.S. version of Junos OS substantially supports the following RFCs, which define standards for IP Security (IPsec) and Internet Key Exchange (IKE).

- RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*
- RFC 2401, *Security Architecture for the Internet Protocol* (obsoleted by RFC 4301)
- RFC 2402, *IP Authentication Header* (obsoleted by RFC 4302)
- RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*
- RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH* (obsoleted by RFC 4305)
- RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*
- RFC 2406, *IP Encapsulating Security Payload (ESP)* (obsoleted by RFC 4303 and RFC 4305)
- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP* (obsoleted by RFC 4306)
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)* (obsoleted by RFC 4306)
- RFC 2409, *The Internet Key Exchange (IKE)* (obsoleted by RFC 4306)
- RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*
- RFC 2451, *The ESP CBC-Mode Cipher Algorithms*
- RFC 2460, *Internet Protocol, Version 6 (IPv6)*
- RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*
- RFC 3193, *Securing L2TP using IPsec*
- RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
- RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*
- RFC 3948, *UDP Encapsulation of IPsec ESP Packets*
- RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*

- RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*
- RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*
- RFC 4301, *Security Architecture for the Internet Protocol*
- RFC 4302, *IP Authentication Header*
- RFC 4303, *IP Encapsulating Security Payload (ESP)*
- RFC 4305, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*
- RFC 4308, *Cryptographic Suites for IPsec*

  Only Suite VPN-A is supported in Junos OS.
- RFC 4754, *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*
- RFC 4835, *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*
- RFC 5996, *Internet Key Exchange Protocol Version 2 (IKEv2)*

Junos OS partially supports the following RFCs for IPsec and IKE:

- RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*
- RFC 5114, *Additional Diffie-Hellman Groups for Use with IETF Standards*
- RFC 5903, *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*

The following RFCs and Internet draft do not define standards, but provide information about IPsec, IKE, and related technologies. The IETF classifies them as “Informational.”

- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
- RFC 2412, *The OAKLEY Key Determination Protocol*
- RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*
- Internet draft draft-eastlake-sha2-02.txt, *US Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006)

RELATED DOCUMENTATION

Services Interfaces Overview for Routing Devices

MX Series 5G Universal Routing Platform Interface Module Reference

Accessing Standards Documents on the Internet

IPSec Terms and Acronyms

A

Adaptive Services PIC — A next-generation Physical Interface Card (PIC) that provides IPsec services and other services, such as Network Address Translation (NAT) and stateful firewall, on M Series and T Series platforms.

Advanced Encryption Standard (AES) — A next-generation encryption method that is based on the Rijndael algorithm and uses a 128-bit block, three different key sizes (128, 192, and 256 bits), and multiple rounds of processing to encrypt data.

authentication header (AH) — A component of the IPsec protocol used to verify that the contents of a packet have not changed (data integrity), and to validate the identity of the sender (data source authentication). For more information about AH, see RFC 2402.

C

certificate authority (CA) — A trusted third-party organization that generates, enrolls, validates, and revokes digital certificates. The CA guarantees the identity of a user and issues public and private keys for message encryption and decryption.

certificate revocation list (CRL) — A list of digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the entities that have issued them. A CRL prevents usage of digital certificates and signatures that have been compromised.

cipher block chaining (CBC) — A cryptographic method that encrypts blocks of ciphertext by using the encryption result of one block to encrypt the next block. Upon decryption, the validity of each block of ciphertext depends on the validity of all the preceding ciphertext blocks. For more information on how to use CBC with DES and ESP to provide confidentiality, see RFC 2405.

D

Data Encryption Standard (DES) — An encryption algorithm that encrypts and decrypts packet data by processing the data with a single shared key. DES operates in increments of 64-bit blocks and provides 56-bit encryption.

digital certificate — Electronic file that uses private and public key technology to verify the identity of a certificate creator and distribute keys to peers.

E

Encapsulating Security Payload (ESP) — A component of the IPsec protocol used to encrypt data in an IPv4 or IPv6 packet, provide data integrity, and ensure data source authentication. For more information about ESP, see RFC 2406.

ES PIC — A PIC that provides first-generation encryption services and software support for IPsec on M Series and T Series platforms.

H

Hashed Message Authentication Code (HMAC) — A mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, such as MD5 or SHA-1, in combination with a secret shared key. For more information on HMAC, see RFC 2104.

I

Internet Key Exchange (IKE) — Establishes shared security parameters for any hosts or routers using IPsec. IKE establishes the SAs for IPsec. For more information about IKE, see RFC 2407.

M

Message Digest 5 (MD5) — An authentication algorithm that takes a data message of arbitrary length and produces a 128-bit message digest. For more information, see RFC 1321.

P

Perfect Forward Secrecy (PFS) — Provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

public key infrastructure (PKI) — A trust hierarchy that enables users of a public network to securely and privately exchange data through the use of public and private cryptographic key pairs that are obtained and shared with peers through a trusted authority.

R

registration authority (RA) — A trusted third-party organization that acts on behalf of a CA to guarantee the identity of a user.

Routing Engine — A PCI-based architectural portion of a Junos OS-based router that handles the routing protocol process, the interface process, some of the chassis components, system management, and user access.

S

Secure Hash Algorithm 1 (SHA-1) — An authentication algorithm that takes a data message of less than 264 bits in length and produces a 160-bit message digest. For more information on SHA-1, see RFC 3174.

Secure Hash Algorithm 2 (SHA-2) — A successor to the SHA-1 authentication algorithm that includes a group of SHA-1 variants (SHA-224, SHA-256, SHA-384, and SHA-512). SHA-2 algorithms use larger hash sizes and are designed to work with enhanced encryption algorithms such as AES.

security association (SA) — Specifications that must be agreed upon between two network devices before IKE or IPsec are allowed to function. SAs primarily specify protocol, authentication, and encryption options.

Security Association Database (SADB) — A database where all SAs are stored, monitored, and processed by IPsec.

Security Parameter Index (SPI) An identifier that is used to uniquely identify an SA at a network host or router.

Security Policy Database (SPD) A database that works with the SADB to ensure maximum packet security. For inbound packets, IPsec checks the SPD to verify if the incoming packet matches the security configured for a particular policy. For outbound packets, IPsec checks the SPD to see if the packet needs to be secured.

Simple Certificate Enrollment Protocol (SCEP) A protocol that supports CA and registration authority (RA) public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation list (CRL) queries.

T

Triple Data Encryption Standard (3DES) An enhanced DES algorithm that provides 168-bit encryption by processing data three times with three different keys.

CHAPTER 35

Junos VPN Site Secure Configuration Overview

IN THIS CHAPTER

IPsec for ACX Series Overview

IN THIS SECTION

The Juniper Networks Junos operating system (Junos OS) supports IPsec. This topic includes the following sections, which provide background information about configuring IPsec on ACX Series Universal Metro Routers.

NOTE: IPsec is supported only on the ACX1100 AC-powered router and ACX500 routers. Service chaining (GRE, NAT, and IPSec) on ACX1100-AC and ACX500 routers is not supported.

NOTE: ACX5048 and ACX5096 routers do not support IPsec configurations.

For a list of the IPsec and IKE standards supported by Junos OS, see the *Junos OS Hierarchy and RFC Reference*.

IPsec

The IPsec architecture provides a security suite for the IP version 4 (IPv4) network layer. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, Junos OS also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations.

IPsec also defines a security association and key management framework that can be used with any transport layer protocol. The security association specifies what protection policy to apply to traffic between two IP-layer entities. IPsec provides secure tunnels between two peers.

Security Associations

To use IPsec security services, you create security associations between hosts. A security association is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. There are two types of security associations:

- Manual security associations require no negotiation; all values, including the keys, are static and specified in the configuration. Manual security associations statically define the security parameter index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic security associations require additional configuration. With dynamic security associations, you configure IKE first and then the security association. IKE creates dynamic security associations; it negotiates security associations for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPsec security association. The IKE security association is negotiated first and then used to protect the negotiations that determine the dynamic IPsec security associations.

IKE

IKE is a key management protocol that creates dynamic security associations; it negotiates security associations for IPsec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE performs the following tasks:

- Negotiates and manages IKE and IPsec parameters.
- Authenticates secure key exchange.
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys.
- Provides identity protection (in main mode).

RELATED DOCUMENTATION

Enabling Inline Services Interface on ACX Series | 116

Minimum Security Association Configurations

IN THIS SECTION

The following sections show the minimum configurations necessary to set up security associations (SAs) for IPsec services:

Minimum Manual SA Configuration

To define a manual SA configuration, you must include at least the following statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
direction (inbound | outbound | bidirectional) {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    encryption {
        algorithm algorithm;
        key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
}
```

Minimum Dynamic SA Configuration

To define a dynamic SA configuration, you must include at least the following statements at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
ike {
    proposal proposal-name {
        authentication-algorithm (md5 | sha1 | sha-256);
```

```
        authentication-method pre-shared-keys;
        dh-group (group1 | group2 | group5 |group14 | group15 | group16 | group19 | group20 | group24);
        encryption-algorithm algorithm;
    }
    policy policy-name {
        proposals [ ike-proposal-names ];
        pre-shared-key (ascii-text key | hexadecimal key);
        version (1 | 2);
        mode (aggressive | main);
    }
}
ipsec {
    policy policy-name {
        proposals [ ipsec-proposal-names ];
    }
    proposal proposal-name {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
        encryption-algorithm algorithm;
        protocol (ah | esp | bundle);
    }
}
```

NOTE:

- Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. The **version** statement at the **[edit services ipsec-vpn ike policy *name*]** hierarchy level allows you to configure the specific IKE version to be supported.
- The **mode** statement at the **[edit services ipsec-vpn ike policy *name*]** hierarchy level is required only if the **version** option is set to **1**.

You must also include the **ipsec-policy** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then dynamic]** hierarchy level.

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | 618
- Configuring Security Associations | 639
- Configuring IKE Proposals | 665
- Configuring IKE Policies | 671
- Configuring IPsec Proposals | 680

Configuring Security Associations

To use IPsec services, you create a security association (SA) between hosts. An SA is a simplex connection that enables two hosts to communicate with each other securely using IPsec.

> **NOTE:** Both OSPFv2 and OSPFv3 support IPsec authentication. However, dynamic or tunnel mode IPsec SAs are not supported for OSPFv3. If you add SAs into OSPFv3 by including the **ipsec-sa** statement at the **[edit protocols ospf3 area *area-number* interface *interface-name*]** hierarchy level, your configuration commit fails. For more information about OSPF authentication and other OSPF properties, see the *Junos OS Routing Protocols Library*.

You can configure two types of SAs:

- Manual—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place.
- Dynamic—Specifies proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more **proposal** statements that prioritizes a list of protocols and algorithms to be negotiated with the peer.

This section includes the following topics:

Configuring Manual Security Associations

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. Manual SAs are best suited for small, static networks where the distribution, maintenance, and tracking of keys are not difficult.

To configure a manual IPsec security association, include the following statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
direction (inbound | outbound | bidirectional) {
    authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);;
        key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
}
```

To configure manual SA statements, do the following:

Configuring the Direction for IPsec Processing

The **direction** statement specifies inbound or outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the **inbound** and **outbound** options. If you want the same attributes in both directions, use the **bidirectional** option.

To configure the direction of IPsec processing, include the **direction** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
    direction (inbound | outbound | bidirectional) {
    ...
}
```

The following two examples illustrate this:

- Example: Using Different Configuration for the Inbound and Outbound Directions

  Define different algorithms, keys, and security parameter index values for each direction:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
direction bidirectional {
    protocol ah;
    spi 20001;
    authentication {
        algorithm hmac-md5-96;
        key ascii-text 123456789012abcd;
    }
}
direction outbound {
    protocol esp;
    spi 24576;
    encryption {
        algorithm 3des-cbc;
        key ascii-text 12345678901234567890abcd;
    }
}
```

- Example: Using the Same Configuration for the Inbound and Outbound Directions

  Define one set of algorithms, keys, and security parameter index values that is valid in both directions:

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
direction bidirectional {
    protocol ah;
    spi 20001;
    authentication {
        algorithm hmac-md5-96;
        key ascii-text 123456789012abcd;
    }
}
```

Configuring the Protocol for a Manual IPsec SA

IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). The AH protocol is used for strong authentication. A third option, **bundle**, uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the IPsec protocol, include the **protocol** statement and specify the **ah**, **esp**, or **bundle** option at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
```

```
protocol (ah | bundle | esp);
```

Configuring the Security Parameter Index

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.

> **NOTE:** Each manual SA must have a unique SPI and protocol combination. Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

To configure the SPI, include the **spi** statement and specify a value (from 256 through 16,639) at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
spi spi-value;
```

Configuring the Auxiliary Security Parameter Index

Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

> **NOTE:** Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the **auxiliary-spi** statement and specify a value (from 256 through 16,639) at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
auxiliary-spi auxiliary-spi-value;
```

Configuring Authentication for a Manual IPsec SA

To configure an authentication algorithm, include the **authentication** statement and specify an authentication algorithm and a key at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
  authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96 | hmac-sha-256-128)
  key (ascii-text key | hexadecimal key);
```

```
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and a 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.
- **hmac-sha-256-128**—Hash algorithm that authenticates packet data. It produces a 256-bit authenticator value 256-bit digest, truncated to 128 bits.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

Configuring Encryption for a Manual IPsec SA

To configure IPsec encryption, include the **encryption** statement and specify an algorithm and key at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then manual direction *direction*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
    encryption {
    algorithm algorithm;
    key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

NOTE: For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option. For reference information on AES encryption, see RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

If you configure an authentication proposal but do not include the **encryption** statement, the result is NULL encryption. Certain applications expect this result. If you configure no specific authentication or encryption values, the Junos OS uses the default values of **sha1** for the authentication and **3des-cbc** for the encryption.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.

NOTE: You cannot configure encryption when you use the AH protocol.

Configuring Dynamic Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To enable a dynamic SA, follow these steps:

1. Configure Internet Key Exchange (IKE) proposals and IKE policies associated with these proposals.
2. Configure IPsec proposals and an IPsec policy associated with these proposals.
3. Associate an SA with an IPsec policy by configuring the **dynamic** statement.

To configure a dynamic SA, include the **dynamic** statement and specify an IPsec policy name at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. The **ike-policy** statement is optional unless you use the preshared key authentication method.

```
[edit services ipsec-vpn rule rule-name term term-name then]
dynamic {
    ike-policy policy-name;
    ipsec-policy policy-name;
}
```

NOTE: If you want to establish a dynamic SA, the attributes in at least one configured IPsec and IKE proposal must match those of its peer.

Clearing Security Associations

You can set up the router software to clear IKE or IPsec SAs automatically when the corresponding services PIC restarts or is taken offline. To configure this property, include the **clear-ike-sas-on-pic-restart** or **clear-ipsec-sas-on-pic-restart** statement at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
clear-ike-sas-on-pic-restart;
clear-ipsec-sas-on-pic-restart;
```

After you add this statement to the configuration, all the IKE or IPsec SAs corresponding to the tunnels in the PIC will be cleared when the PIC restarts or goes offline.

Starting in Junos OS Release 17.2R1, you can enable the cleanup of IKE triggers and IKE and IPsec SAs when an IPsec tunnel's local gateway IP address goes down or the MS-MIC or MS-MPC being used in the tunnel's service set goes down. This reduces dropped traffic and unnecessary IKE triggers. To enable this feature, include the **gw-interface** statement at the **[edit services service set *service-set-name* ipsec-vpn-options local-gateway *address*]** hierarchy level. If the local gateway IP address for an IPsec tunnel's service set goes down or the MS-MIC or MS-MPC that is being used in the service set goes down, the service set no longer sends IKE triggers.

In addition, when the local gateway IP address goes down, the IKE and IPsec SAs are cleared for next-hop service sets, and go to the Not Installed state for interface-style service sets. The SAs that have the Not Installed state are deleted when the local gateway IP address comes back up. If the local gateway IP address that goes down for a next-hop service set is for the responder peer, then you need to clear the IKE and IPsec SAs on the initiator peer so that the IPsec tunnel comes back up once the local gateway IP address comes back up. You can either manually clear the IKE and IPsec SAs on the initiator peer or enable dead peer detection on the initiator peer.

Release History Table

Release	Description
17.2R1	Starting in Junos OS Release 17.2R1, you can enable the cleanup of IKE triggers and IKE and IPsec SAs when an IPsec tunnel's local gateway IP address goes down or the MS-MIC or MS-MPC being used in the tunnel's service set goes down.

RELATED DOCUMENTATION

- Configuring IPsec Policies | 685
- Configuring IPsec Proposals | 680
- Configuring IKE Policies | 671
- Configuring IKE Proposals | 665

Example: Configuring Manual SAs

IN THIS SECTION

This example shows how to create an IPsec tunnel by using manual security associations (SAs), and contains the following sections:

Requirements

This example uses the following hardware and software components:

- Four M Series, MX Series, or T Series routers with multiservices interfaces installed in them.
- Junos OS Release 9.4 and later.

No special configuration beyond device initialization is required before you can configure this feature.

Overview and Topology

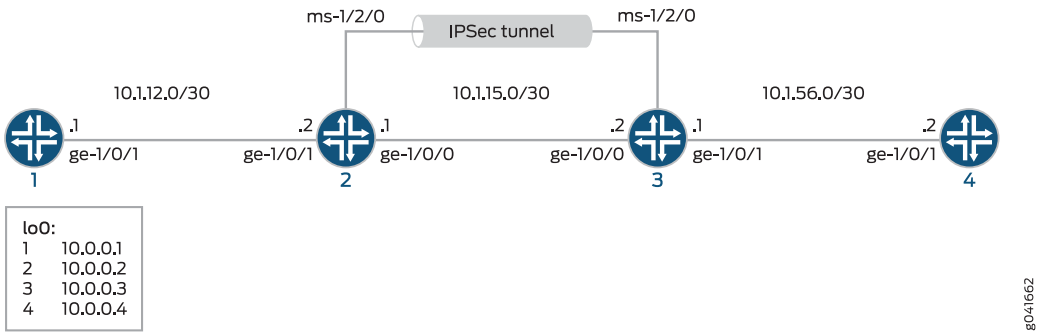
A security association (SA) is a simplex connection that enables two hosts to securely communicate with each other by means of IPsec. There are two types of SAs: manual SA and dynamic SA. This example explains a manual SA configuration.

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs use statically defined security parameter index (SPI) values, algorithms, and keys, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.

Manual SAs are best suited for small, static networks where the distribution, maintenance, and tracking of keys are not difficult.

Figure 34 on page 647 shows an IPsec topology that contains a group of four routers: Routers 1, 2, 3, and 4.

Figure 34: Manual SA Topology



Routers 2 and 3 establish an IPsec tunnel by using a multiservices PIC and manual SA settings. Routers 1 and 4 provide basic connectivity and are used to verify that the IPsec tunnel is operational.

Configuration

IN THIS SECTION

This example uses four routers, and involves the following configurations:

- Routers 1 and 4 are configured for basic OSPF connectivity with Routers 2 and 3 respectively.
- Routers 2 and 3 are configured for OSPF connectivity with Routers 1 and 4 respectively. Routers 2 and 3 are also configured to create an IPsec tunnel by using manual SAs between these two routers. To direct traffic to the IPsec tunnel through the multiservices interface, next-hop style service sets are configured on Routers 2 and 3, and the multiservices interfaces that are configured as the IPsec inside interface are added to the OSPF configuration on the respective routers.

> **NOTE:** The interface types shown in this example are for indicative purpose only. For example, you can use **so-** interfaces instead of **ge-** and **sp-** instead of **ms-**.

This section contains:

Configuring Router 1

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, of Router 1.

```
set interfaces ge-1/0/1 description "to R2 ge-1/0/1"
set interfaces ge-1/0/1 unit 0 family inet address 10.1.12.1/30
set interfaces lo0 unit 0 family inet address 10.0.0.1/32
set protocols ospf area 0.0.0.0 interface ge-1/0/1.0
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options router-id 10.0.0.1
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router 1 for OSPF connectivity with Router 2:

1. Configure an Ethernet interface and loopback interface.

```
[edit interfaces]
user@router1# set ge-1/0/1 description "to R2 ge-1/0/1"
user@router1# set ge-1/0/1 unit 0 family inet address 10.1.12.1/30
user@router1# set lo0 unit 0 family inet address 10.0.0.1/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit protocols]
user@router1# set ospf area 0.0.0.0 interface ge-1/0/1.0
user@router1# set ospf area 0.0.0.0 interface lo0.0
```

3. Configure the router ID.

```
[edit routing-options]
user@router1# set router-id 10.0.0.1
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router1# show interfaces
interfaces {
    ...
    ge-1/0/1 {
        description "to R2 ge-1/0/1";
        unit 0 {
            family inet {
                address 10.1.12.1/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
    ...
}
```

```
user@router1# show protocols ospf
ospf {
    area 0.0.0.0 {
        interface ge-1/0/1.0;
        interface lo0.0;
    }
```

```
}
```

```
user@router1# show routing-options
routing-options {
   router-id 10.0.0.1;
}
```

Configuring Router 2

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, of Router 2.

Configuring Interfaces and OSPF Connectivity (with Router 1 and Router 3) on Router 2

```
set interfaces ge-1/0/0 unit 0 description "to R3 ge-1/0/0"
set interfaces ge-1/0/0 unit 0 family inet address 10.1.15.1/30
set interfaces ge-1/0/1 unit 0 description "to R1 ge-1/0/0"
set interfaces ge-1/0/1 unit 0 family inet address 10.1.12.2/30
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.2/32
set protocols ospf area 0.0.0.0 interface ge-1/0/1.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then remote-gateway
   10.1.15.2
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional protocol esp
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional spi 261
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication algorithm hmac-sha1-96
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication key ascii-text demokeyipsecmanualsa
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional encryption algorithm des-cbc
```

```
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
    bidirectional encryption key ascii-text manualsa
set services ipsec-vpn rule demo-rule-r1-manual-sa match-direction input
set services service-set demo-ss-manual-sa next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-ss-manual-sa next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-ss-manual-sa ipsec-vpn-options local-gateway 10.1.15.1
set services service-set demo-ss-manual-sa ipsec-vpn-rules demo-rule-r1-manual-sa
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF connectivity and IPsec tunnel parameters on Router 2:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), a loopback interface, and a multiservices interface (ms-1/2/0).

```
[edit interfaces]
user@router2# set ge-1/0/0 unit 0 description "to R3 ge-1/0/0"
user@router2# set ge-1/0/0 unit 0 family inet address 10.1.15.1/30
user@router2# set ge-1/0/1 unit 0 description "to R1 ge-1/0/0"
user@router2# set ge-1/0/1 unit 0 family inet address 10.1.12.2/30
user@router2# set ms-1/2/0 unit 0 family inet
user@router2# set ms-1/2/0 unit 1 family inet
user@router2# set ms-1/2/0 unit 1 service-domain inside
user@router2# set ms-1/2/0 unit 2 family inet
user@router2# set ms-1/2/0 unit 2 service-domain outside
user@router2# set lo0 unit 0 family inet address 10.0.0.2/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit protocols]
user@router2# set ospf area 0.0.0.0 interface ge-1/0/1.0
user@router2# set ospf area 0.0.0.0 interface lo0.0
user@router2# set ospf area 0.0.0.0 interface ms-1/2/0.1
```

3. Configure the router ID.

```
[edit routing-options]
```

```
user@router2# set router-ID 10.0.0.2
```

4. Configure an IPsec rule. In this step, you configure an IPsec rule and specify manual SA parameters, such as the remote-gateway address, authentication and encryption properties, and so on.

```
[edit services ipsec-vpn]
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then remote-gateway 10.1.15.2
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional protocol esp
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional spi 261
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication algorithm hmac-sha1-96
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication key ascii-text demokeyipsecmanualsa
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional encryption algorithm des-cbc
user@router2# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional encryption key ascii-text manualsa
user@router2# set rule demo-rule-r1-manual-sa match-direction input
```

5. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router2# set service-set demo-ss-manual-sa next-hop-service inside-service-interface ms-1/2/0.1
user@router2# set service-set demo-ss-manual-sa next-hop-service outside-service-interface ms-1/2/0.2
user@router2# set service-set demo-ss-manual-sa ipsec-vpn-options local-gateway 10.1.15.1
user@router2# set service-set demo-ss-manual-sa ipsec-vpn-rules demo-rule-r1-manual-sa
```

6. Commit the configuration.

```
[edit]
user@router2# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router1# show interfaces
interfaces {
    ...
    ge-1/0/0 {
        unit 0 {
            description "to R3 ge-1/0/0";
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    ge-1/0/1 {
        unit 0 {
            description "to R1 ge-1/0/1";
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    ms-1/2/0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.2/32;
            }
        }
    }
    ...
}
```

```
user@router2# show protocols ospf
protocols {
```

```
    ospf {
        area 0.0.0.0 {
            interfaces ge-1/0/1.0;
            interface lo0;
            interface ms-1/2/0;
        }
    }
}
```

```
user@router2# show routing-options
routing-options {
    router-id 10.0.0.2;
}
```

```
user@router2# show services
services {
    ipsec-vpn {
        rule demo-rule-r1-manual-sa {
            term demo-term-manual-sa {
                then {
                    remote-gateway 10.1.15.2;
                    manual {
                        direction bidirectional {
                            protocol esp;
                            spi 261;
                            authentication {
                                algorithm hmac-sha1-96;
                                key ascii-text "$ABC1223"; ## SECRET-DATA
                            }
                            encryption {
                                algorithm des-cbc;
                                key ascii-text "$ABC123"; ## SECRET-DATA
                            }
                        }
                    }
                }
            }
            match-direction input;
        }
    }
    service-set demo-ss-manual-sa {
        next-hop-service {
            inside-service-interface ms-1/2/0.1;
```

```
            outside-service-interface ms-1/2/0.2;
        }
        ipsec-vpn-options {
            local-gateway 10.1.15.1;
        }
        ipsec-vpn-rules demo-rule-r1-manual-sa;
    }
}
```

Configuring Router 3

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, of Router 3.

```
set interfaces ge-1/0/1 unit 0 description "to R4 ge-1/0/1"
set interfaces ge-1/0/0 unit 0 family inet address 10.1.56.1/30
set interfaces ge-1/0/0 unit 0 description "to R2 ge-1/0/0"
set interfaces ge-1/0/0 unit 0 family inet address 10.1.15.2/30
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.3/32
set protocols ospf area 0.0.0.0 interface ge-1/0/1.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set routing-options router-id 10.0.0.3
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then remote-gateway 10.1.15.1
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    protocol esp
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    spi 261
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    authentication algorithm hmac-sha1-96
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    authentication key ascii-text demokeyipsecmanualsa
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    encryption algorithm des-cbc
set services ipsec-vpn rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction bidirectional
    encryption key ascii-text manualsa
set services ipsec-vpn rule demo-rule-r1-manual-sa match-direction input
```

```
set services service-set demo-ss-manual-sa next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-ss-manual-sa next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-ss-manual-sa ipsec-vpn-options local-gateway 10.1.15.2
set services service-set demo-ss-manual-sa ipsec-vpn-rules demo-rule-r1-manual-sa
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF connectivity and IPsec tunnel parameters on Router 3:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), a loopback interface, and a multiservices interface (ms-1/2/0).

   ```
   [edit interfaces]
   user@router3# set ge-1/0/0 unit 0 description "to R4 ge-1/0/0"
   user@router3# set ge-1/0/0 unit 0 family inet address 10.1.56.1/30
   user@router3# set ge-1/0/1 unit 0 description "to R2 ge-1/0/1"
   user@router3# set ge-1/0/1 unit 0 family inet address 10.1.15.2/30
   user@router3# set ms-1/2/0 unit 0 family inet
   user@router3# set ms-1/2/0 unit 1 family inet
   user@router3# set ms-1/2/0 unit 1 service-domain inside
   user@router3# set ms-1/2/0 unit 2 family inet
   user@router3# set ms-1/2/0 unit 2 service-domain outside
   user@router3# set lo0 unit 0 family inet address 10.0.0.3/32
   ```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

   ```
   [edit protocols]
   user@router3# set ospf area 0.0.0.0 interface ge-1/0/1.0
   user@router3# set ospf area 0.0.0.0 interface lo0.0
   user@router3# set ospf area 0.0.0.0 interface ms-1/2/0.1
   ```

3. Configure a router ID.

   ```
   [edit routing-options]
   user@router3# set router-id 10.0.0.3
   ```

4. Configure an IPsec rule. In this step, you configure an IPsec rule and specify manual SA parameters, such as the remote-gateway address, authentication and encryption properties, and so on.

```
[edit services ipsec-vpn]
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then remote-gateway 10.1.15.1
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional protocol esp
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional spi 261
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication algorithm hmac-sha1-96
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional authentication key ascii-text demokeyipsecmanualsa
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional encryption algorithm des-cbc
user@router3# set rule demo-rule-r1-manual-sa term demo-term-manual-sa then manual direction
   bidirectional encryption key ascii-text manualsa
user@router3# set rule demo-rule-r1-manual-sa match-direction input
```

5. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router3# set service-set demo-ss-manual-sa next-hop-service inside-service-interface ms-1/2/0.1
user@router3# set service-set demo-ss-manual-sa next-hop-service outside-service-interface ms-1/2/0.2
user@router3# set service-set demo-ss-manual-sa ipsec-vpn-options local-gateway 10.1.15.2
user@router3# set service-set demo-ss-manual-sa ipsec-vpn-rules demo-rule-r1-manual-sa
```

6. Commit the configuration.

```
[edit]
user@router3# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router3# show interfaces
interfaces {
   ge-1/0/1 {
      unit 0 {
         description "to R4 ge-1/0/1";
```

```
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    ge-1/0/0 {
        unit 0 {
            description "to R2 ge-1/0/0";
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    ms-1/2/0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.3/32;
            }
        }
    }
}
```

```
user@router3# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-1/0/1.0;
            interface lo0.0;
            interface ms-1/2/0.1;
        }
    }
```

```
}
```

```
user@router3# show routing-options
routing-options {
    router-id 10.0.0.3;
}
```

```
user@router3# show services
services {
    ipsec-vpn {
        rule demo-rule-r1-manual-sa {
            term demo-term-manual-sa {
                then {
                    remote-gateway 10.1.15.1;
                    manual {
                        direction bidirectional {
                            protocol esp;
                            spi 261;
                            authentication {
                                algorithm hmac-sha1-96;
                                key ascii-text "$ABC123"; ## SECRET-DATA
                            }
                            encryption {
                                algorithm des-cbc;
                                key ascii-text "$ABC123"; ## SECRET-DATA
                            }
                        }
                    }
                }
            }
            match-direction input;
        }
    }
    service-set demo-ss-manual-sa {
        next-hop-service {
            inside-service-interface ms-1/2/0.1;
            outside-service-interface ms-1/2/0.2;
        }
        ipsec-vpn-options {
            local-gateway 10.1.15.2;
        }
        ipsec-vpn-rules demo-rule-r1-manual-sa;
    }
```

```
}
```

Configuring Router 4

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, of Router 4.

```
set interfaces ge-1/0/1 description "to R3 ge-1/0/1"
set interfaces ge-1/0/1 unit 0 family inet address 10.1.56.2/30
set interfaces lo0 unit 0 family inet address 10.0.0.4/32
set protocols ospf area 0.0.0.0 interface ge-1/0/1.0
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options router-id 10.0.0.4
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To set up OSPF connectivity with Router 3

1. Configure the interfaces. In this step, you configure an Ethernet interface (ge-1/0/1) and a loopback interface.

   ```
   user@router4# set interfaces ge-1/0/1 description "to R3 ge-1/0/1"
   user@router4# set interfaces ge-1/0/1 unit 0 family inet address 10.1.56.2/30
   user@router4# set interfaces lo0 unit 0 family inet address 10.0.0.4/32
   ```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

   ```
   user@router4# set protocols ospf area 0.0.0.0 interface ge-1/0/1.0
   user@router4# set protocols ospf area 0.0.0.0 interface lo0.0
   ```

3. Configure the router ID.

   ```
   [edit routing-options]
   user@router4# set router-id 10.0.0.4
   ```

4. Commit the configuration.

```
[edit]
user@router4# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router4# show interfaces
interfaces {
    ge-1/0/1 {
        description "to R3 ge-1/0/1";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0{
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}
```

```
user@router4# show routing-options
routing-options {
    router-id 10.0.0.4;
}
```

```
user@router4# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface lo0.0;
            interface ge-1/0/1.0;
        }
    }
}
```

Verification

IN THIS SECTION

To confirm that the manual SA configuration is working properly, perform the following tasks:

Verifying Traffic Flow Through the IPsec Tunnel

Purpose

Verify that the IPsec tunnel carries traffic between Router 1 and Router 4.

Action

Issue a **ping** command from Router 1 to **lo0** on Router 4.

```
user@router1> ping 10.0.0.4
```

```
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=254 time=1.375 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=254 time=18.375 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=254 time=1.120 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.120/6.957/18.375/8.075 ms
```

Meaning

The output shows that Router 1 is able to reach Router 4 over the IPsec tunnel.

Verifying the Security Associations on Router 2

Purpose

Verify that the security associations are active on Router 2 and that the traffic is flowing over the IPsec tunnel.

Action

- To verify that the security associations are active, Issue **show services ipsec-vpn ipsec security-associations detail** on Router 2.

  user@router2> **show services ipsec-vpn ipsec security-associations detail**

```
Service set: demo-ss-manual-sa
Rule: demo-rule-r1-manual-sa, Term: demo-term-manual-sa,
Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

- To verify that traffic is traveling over the bidirectional IPsec tunnel, issue **show services ipsec-vpn ipsec statistics** on Router 2.

  user@router2> **show services ipsec-vpn ipsec statistics**

```
PIC: ms-1/2/0, Service set: demo-ss-manual-sa
sESP Statistics:
Encrypted bytes: 1616
Decrypted bytes: 1560
Encrypted packets: 20
Decrypted packets: 19
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Meaning

The **show services ipsec-vpn ipsec security-associations detail** command output shows the SA properties that you configured.

The **show services ipsec-vpn ipsec statistics** command output shows the traffic flow over the IPsec tunnel.

Verifying the Security Associations on Router 3

Purpose

Verify the security associations and flow of traffic over the IPsec tunnel.

Action

- To verify that the security associations are active, Issue **show services ipsec-vpn ipsec security-associations detail** on Router 3.

```
user@router3> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: demo-ss-manual-sa
Rule: demo-rule-r1-manual-sa, Term: demo-term-manual-sa,
Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

- To verify that traffic is traveling over the bidirectional IPsec tunnel, issue **show services ipsec-vpn ipsec statistics** on Router 3.

```
user@router3> show services ipsec-vpn ipsec statistics
```

```
PIC: ms-1/2/0, Service set: demo-ss-manual-sa
ESP Statistics:
Encrypted bytes: 1560
Decrypted bytes: 1616
Encrypted packets: 19
Decrypted packets: 20
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
```

```
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Meaning

The **show services ipsec-vpn ipsec security-associations detail** command output shows the SA properties that you configured.

The **show services ipsec-vpn ipsec statistics** command output shows the traffic flow over the IPsec tunnel.

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | 618
- Configuring Security Associations | 639
- Example: Configuring IKE Dynamic SAs | 768

Configuring IKE Proposals

Dynamic security associations (SAs) require IKE configuration. With dynamic SAs, you configure IKE first, and then the SA. IKE creates the dynamic SAs and negotiates them for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway.

You can configure one or more IKE proposals. Each proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer.

To configure an IKE proposal, include the **proposal** statement and specify a name at the **[edit services ipsec-vpn ike]** hierarchy level:

```
[edit services ipsec-vpn ike]
proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
    dh-group (group1 | group2 | group5 |group14 | group 15 | group16 | group19 | group20 | group24);
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
}
```

> **NOTE:** In Junos FIPS mode, ECDSA is not supported for the authentication method in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.

This section includes the following topics:

Configuring the Authentication Algorithm for an IKE Proposal

To configure the authentication algorithm for an IKE proposal, include the **authentication-algorithm** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
authentication-algorithm (md5 | sha1 | sha-256);
```

The authentication algorithm can be one of the following:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.
- **sha-256**—Produces a 256-bit digest.

> **NOTE:** For reference information on Secure Hash Algorithms (SHAs), see Internet draft **draft-eastlake-sha2-02.txt**, *Secure Hash Algorithms (SHA and HMAC-SHA)* (expires July 2006).

Configuring the Authentication Method for an IKE Proposal

To configure the authentication method for an IKE proposal, include the **authentication-method** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
authentication-method (ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
```

NOTE: In IKEv1, the authentication method for SAs is negotiated with the remote peer based on the type of authentication method configured in the IKE proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the authentication method that is locally configured for them.

For SAs in IKEv2, the authentication method is the default value as IKEv1 if an authentication method is not configured in the IKE proposal. If you are configuring an authentication method for IKEv2, you must have the same authentication method configured for all proposals referenced in the policy.

The authentication method can be one of the following:

NOTE: In Junos FIPS mode, ECDSA is not supported for the authentication method in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.

- **ecdsa-signatures-256**—Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Elliptic Curve Digital Signature Algorithm (ECDSA) for 256-bit moduli.
- **ecdsa-signatures-384**—Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Elliptic Curve Digital Signature Algorithm (ECDSA) for 384-bit moduli.
- **pre-shared-keys**—A key derived from an out-of-band mechanism; the key authenticates the exchanges.
- **rsa-signatures**—Public key algorithm (supports encryption and digital signatures).

Configuring the Diffie-Hellman Group for an IKE Proposal

Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.

To configure the Diffie-Hellman group for an IKE proposal, include the **dh-group** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
dh-group (group1 | group2 | group5 |group14 | group15 | group16 | group19 | group20 | group24);
```

The group can be one of the following:

- **group1**—Specifies that IKE uses the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specifies that IKE uses the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group5**—Specifies that IKE uses the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group14**—Specifies that IKE uses the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group19**—Specifies that IKE uses the 256-bit random Elliptic Curve Diffie-Hellman Group when performing the new Diffie-Hellman exchange.
- **group20**—-Specifies that IKE uses the 384-bit random Elliptic Curve Diffie-Hellman Group when performing the new Diffie-Hellman exchange.

Starting in Junos OS release 17.4R1, group15, group16, and group 24 can also be used:

- **group15**—Specifies that IKE use the 3072-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group16**—Specifies that IKE use the 4096-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group24**—Specifies that IKE use the 2048-bit Diffie-Hellman prime modulus group with 256-bit Prime Order Subgroup when performing the new Diffie-Hellman exchange.

Using a Diffie-Hellman group based on a greater number of bits results a more secure IKE tunnel than using a group based on fewer bits. However, this additional security might require additional processing time.

Configuring the Encryption Algorithm for an IKE Proposal

To configure the encryption algorithm for an IKE proposal, include the **encryption-algorithm** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
encryption-algorithm algorithm;
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Cipher block chaining encryption algorithm with a key size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Cipher block chaining encryption algorithm with a key size of 8 bytes; its key size is 56 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

> **NOTE:** For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option.
>
> For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.
>
> If you configure an authentication proposal but do not include the **encryption** statement, the result is NULL encryption. Certain applications expect this result. If you configure no specific authentication or encryption values, the Junos OS uses the default values of **sha1** for the authentication and **3des-cbc** for the encryption.

Configuring the Lifetime for an IKE SA

The **lifetime-seconds** statement sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or the IPsec connection is terminated.

To configure the lifetime for an IKE SA, include the **lifetime-seconds** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ike proposal proposal-name]
lifetime-seconds seconds;
```

By default, the IKE SA lifetime is 3600 seconds. The range is from 180 through 86,400 seconds.

NOTE: In IKEv1, the lifetime for SAs is negotiated with the remote peer based on the type of lifetime configured in the IKE proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the lifetime that is locally configured for them.

For SAs in IKEv2, the lifetime is either the default value as IKEv1 (if another lifetime is not configured in the IKE proposal) or all IKEv2 proposals in the IKE policy must be configured with the same lifetime value.

NOTE: For IKE proposals, there is only one SA lifetime value, specified by the Junos OS. IPsec proposals use a different mechanism.

Example: Configuring an IKE Proposal

Configure an IKE proposal:

```
[edit services ipsec-vpn ike]
proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.
17.4R1	Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.
17.4R1	Starting in Junos OS release 17.4R1, group15, group16, and group 24 can also be used
17.3R1	Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Elliptic Curve Digital Signature Algorithm (ECDSA) for 256-bit moduli.
17.3R1	Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Elliptic Curve Digital Signature Algorithm (ECDSA) for 384-bit moduli.

RELATED DOCUMENTATION

Configuring IPsec Proposals | 680
Configuring IKE Policies | 671
Configuring IPsec Policies | 685
Configuring Security Associations | 639

Configuring IKE Policies

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address and the proposals needed for that connection. Depending on which authentication method is used, it defines the preshared key for the given peer or the local certificate. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. You can configure the specific IKE phase to be supported for the negotiation. However, if only IKEv1 is supported, the Junos OS rejects IKEv2 negotiations. Similarly, if only IKEv2 is supported, the Junos OS rejects all IKEv1 negotiations.

The key management process (kmd) daemon determines which version of IKE is used in a negotiation. If kmd is the IKE initiator, it uses IKEv1 by default and retains the configured version for negotiations. If kmd is the IKE responder, it accepts connections from both IKEv1 and IKEv2.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal matches a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the **policy** statement and specify a policy name at the **[edit services ipsec-vpn ike]** hierarchy level:

```
[edit services ipsec-vpn ike]
policy policy-name {
    description description;
    local-certificate identifier;
```

```
    local-id (ipv4_addr ipv4-address | ipv6-addr ipv6-address | key-id identifier);
    version (1 | 2);
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
    remote-id {
        any-remote-id;
        ipv4_addr [ values ];
        ipv6_addr [ values ];
        key_id [ values ];
    }
    respond-bad-spi max-responses;
}
```

This section includes the following topics:

Configuring the IKE Phase

Starting with Junos OS Release 11.4, both IKEv1 and IKEv2 are supported by default on all M Series, MX Series, and T Series routers. You can configure the specific IKE phase to be supported for the negotiation. However, if only IKEv1 is supported, the Junos OS rejects IKEv2 negotiations. Similarly, if only IKEv2 is supported, the Junos OS rejects all IKEv1 negotiations.

To configure the IKE phase used, include the **version** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
version (1 | 2);
```

SEE ALSO

- Related documentation link #1
- Related documentation link #2

Configuring the Mode for an IKE Policy

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.

NOTE: The mode configuration is required only if the **version** option is set to **1**.

To configure the mode for an IKE policy, include the **mode** statement and specify **aggressive** or **main** at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
mode (aggressive | main);
```

SEE ALSO

- Related documentation link #1
- Related documentation link #2

Configuring the Proposals in an IKE Policy

The IKE policy includes a list of one or more proposals associated with an IKE policy.

To configure the proposals in an IKE policy, include the **proposals** statement and specify one or more proposal names at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
proposals [ proposal-names ];
```

Configuring the Preshared Key for an IKE Policy

When you include the **authentication-method pre-shared-keys** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level, IKE policy preshared keys authenticate peers. You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

To configure the preshared key in an IKE policy, include the **pre-shared-key** statement and a key at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
pre-shared-key (ascii-text key | hexadecimal key);
```

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.

Configuring the Local Certificate for an IKE Policy

IN THIS SECTION

When you include the **authentication-method rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name*]** hierarchy level, public key infrastructure (PKI) digital certificates authenticate peers. You must identify a local certificate that is sent to the peer during the IKE authentication phase.

To configure the local certificate for an IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
local-certificate identifier;
```

The **local-certificate** statement specifies the identifier used to obtain the end entity's certificate from the certification authority. Configuring it in an IKE policy allows you the flexibility of using a separate certificate

with each remote peer if that is needed. You must also specify the identity of the certification authority by configuring the **ca-profile** statement at the **[edit security pki]** hierarchy level.

You can use the configured profiles to establish a set of trusted certification authorities for use with a particular service set. This enables you to configure separate service sets for individual clients to whom you are providing IP services; the distinct service sets provide logical separation of one set of IKE sessions from another, using different local gateway addresses, or *virtualization*. To configure the set of trusted certification authorities, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
trusted-ca ca-profile;
```

See the following to configure a certificate revocation list:

Configuring a Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been cancelled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

> **NOTE:** By default, certificate revocation list verification is enabled. You can disable CRL verification by including the **disable** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check]** hierarchy level.
>
> By default, if the router either cannot access the Lightweight Directory Access Protocol (LDAP) URL or retrieve a valid certificate revocation list, certificate verification fails and the IPsec tunnel is not established. To override this behavior and permit the authentication of the IPsec peer when the CRL is not downloaded, include the **disable on-download-failure** statement at the **[edit security pki ca-profile *ca-profile-name* revocation-check crl]** hierarchy level.

To use the CA certificate revocation list, you include statements at the **[edit security pki ca-profile *ca-profile-name* revocation-check]** hierarchy level. For details, see the *Junos OS System Basics Configuration Guide*.

Configuring the Description for an IKE Policy

To specify an optional text description for an IKE policy, include the **description** statement at the **[edit services ipsec-vpn ike policy *policy-name*** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
```

```
description description;
```

Configuring Local and Remote IDs for IKE Phase 1 Negotiation

You can optionally specify local identifiers for use in IKE phase 1 negotiation. If the **local-id** statement is omitted, the local gateway address is used.

Starting with Junos OS Release 19.1R1, you can configure one of the local id type as distinguished name and you can configure one of the remote id type as distinguished name. The distinguished name field can be a container with container string values or wildcard with wildcard string values.

A distinguished name is a name used with digital certificates to uniquely identify a user. For example a distinguished name can be:

- CN=user
- DC=example
- DC=com

For the container string, the order of the fields and their values must exactly match the distinguished name in the peer's digital certificate. Example: **container ["C=US, ST=CA, L=Sunnyvale, O=Juniper, CN=local_neg, CN=test@juniper.net, OU=QA" "cn=admin, ou=eng, o=example, dc=net"];**

For the wildcard string, the configured field and value must match the distinguished name in the peer's digital certificate but the order of the fields in the DN does not matter. Example: **wildcard ["L=Sunnyvale, O=Juniper" "C=US, ST=CA"];**

To specify one or more local IDs, include the **local-id** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
local-id (distinguished-name container container-string-values |wildcard wildcard-string-values fqdn fqdn-name
    ipv4_addr ipv4-address | ipv6-addr ipv6-address | key-id identifier);
```

You can also specify remote gateway identifiers for which the IKE policy is used. The remote gateway address in which this policy is defined is added by default.

To specify one or more remote IDs, include the **remote-id** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
    remote-id {
    distinguished-name container container-string-values |wildcard wildcard-string-values
    fqdn fqdn-name
```

```
    any-remote-id;
    ipv4_addr [ values ];
    ipv6_addr [ values ];
    key_id [ values ];
}
```

The **any-remote-id** option allows any remote address to connect. This option is supported only in dynamic endpoints configurations and cannot be configured along with specific values.

Enabling Invalid SPI Recovery

When peers in a security association (SA) become unsynchronized, packets with invalid security parameter index (SPI) values can be sent out, and the receiving peer drops these packets. For example, this could occur when one of the peers reboots. Starting in Junos OS Release 14.2, you can enable the device to recover when packets with invalid SPIs are received by resynchronizing the SAs.

To enable recovery from invalid SPI values, include the **respond-bad-spi** statement at the **[edit services ipsec-vpn ike policy]** ***policy-name*** hierarchy level:

```
[edit services ipsec-vpn ike policy policy-name]
respond-bad-spi max-responses;
```

Example: Configuring an IKE Policy

Define two IKE policies: **policy 10.1.1.2** and **policy 10.1.1.1**. Each policy is associated with **proposal-1** and **proposal-2**. The following configuration uses only IKEv1 for negotiation.

```
[edit services ipsec-vpn]
ike {
    proposal proposal-1 {
        authentication-method pre-shared-keys;
        dh-group group1;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 1000;
    }
    proposal proposal-2 {
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm md5;
        encryption-algorithm des-cbc;
        lifetime-seconds 10000;
```

```
    }
    proposal proposal-3 {
        authentication-method rsa-signatures;
        dh-group group2;
        authentication-algorithm md5;
        encryption-algorithm des-cbc;
        lifetime-seconds 10000;
    }
    policy 10.1.1.2 {
        mode main;
        proposals [ proposal-1 proposal-2 ];
        pre-shared-key ascii-text example-pre-shared-key;
    }
    policy 10.1.1.1 {
        local-certificate certificate-file-name;
        local-key-pair private-public-key-file;
        mode aggressive;
        proposals [ proposal-2 proposal-3 ]
        pre-shared-key hexadecimal 0102030abbcd;
    }
}
```

NOTE: Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see **clear services ipsec-vpn ike security-associations**.

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, you can enable the device to recover when packets with invalid SPIs are received by resynchronizing the SAs.

RELATED DOCUMENTATION

Configuring Dynamic Endpoints for IPsec Tunnels | 750

Configuring IKE Proposals | 665
Configuring IPsec Policies | 685
Configuring IPsec Proposals | 680
Configuring Security Associations | 639

Configuring IKE Activation Time

You can choose the time at which IKE is activated.

To choose the time at which IKE is activated:

- Configure the **establish-tunnels** value.

  ```
  [edit services ipsec-vpn]
  user@host set establish-tunnels (immediately | on-traffic | responder-only)
  ```

  The following describes each option:

  - **immediately**—Activate IKE immediately after VPN information is configured and configuration changes are committed.
  - **on-traffic**—Activate IKE only when data flows. IKE needs to be negotiated with the peer gateway.
  - **responder-only**—Starting in Junos OS Release 18.2R1, only respond to IKE negotiations initiated by the peer gateway. Do not initiate IKE negotiations. This option is required when another vendor's peer gateway expects the protocol and port values in the traffic selector from the initiating gateway, which the MX Series does not provide.

Release History Table

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, only respond to IKE negotiations initiated by the peer gateway.

RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | 618

Configuring IPsec Proposals

An IPsec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPsec peer.

To configure an IPsec proposal, include the **proposal** statement and specify an IPsec proposal name at the **[edit services ipsec-vpn ipsec]** hierarchy level:

```
[edit services ipsec-vpn ipsec]
proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
}
```

This section discusses the following topics:

Configuring the Authentication Algorithm for an IPsec Proposal

To configure the authentication algorithm for an IPsec proposal, include the **authentication-algorithm** statement at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit digest. Only 96 bits are used for authentication.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit digest. Only 96 bits are used for authentication.
- **hmac-sha-256-128**—Hash algorithm that authenticates packet data. Produces a 256-bit authenticator value.

NOTE: Keep the following points in mind when you configure the authentication algorithm in an IPsec proposal:

- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, an error occurs and the tunnel is not established in this scenario. For example, if one end of the tunnel contains router 1 configured with the authentication algorithm as hmac-sha- 256-128 and the other end of the tunnel contains router 2 configured with the authentication algorithm as hmac-md5-96, the VPN tunnel is not established.
- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, and when one end of the tunnel contains two IPsec proposals to check whether a less secure algorithm is selected or not, an error occurs and the tunnel is not established. For example, if you configure two authentication algorithms for an IPsec proposal as hmac-sha-256-128 and hmac-md5-96 on one end of the tunnel, router 1, and if you configure the algorithm for an IPsec proposal as hmac-md5-96 on the other end of the tunnel, router 2, the tunnel is not established and the number of proposals mismatch.
- When you configure two IPsec proposals at both ends of a tunnel, such as the **authentication-algorithm hmac-sha-256-128** and **authentication- algorithm hmac-md5-96** statements at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level on one of the tunnel, router 1 (with the algorithms in two successive statements to specify the order), and the **authentication-algorithm hmac-md5-96** and **authentication- algorithm hmac-sha-256-128** statements at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level on one of the tunnel, router 2 (with the algorithms in two successive statements to specify the order, which is the reverse order of router 1), the tunnel is established in this combination as expected because the number of proposals is the same on both ends and they contain the same set of algorithms. However, the authentication algorithm selected is hmac-md5-96 and not the stronger algorithm of hmac-sha-256-128. This method of selection of the algorithm occurs because the first matching proposal is selected. Also, for a default proposal, regardless of whether the router supports the Advanced Encryption Standard (AES) encryption algorithm, the 3des-cbc algorithm is chosen and not the aes-cfb algorithm, which is because of the first algorithm in the default proposal being selected. In the sample scenario described here, on router 2, if you reverse the order of the algorithm configuration in the proposal so that it is the same order as the one specified on router 1, hmac-sha-256-128 is selected as the authentication method.
- You must be aware of the order of proposals in an IPsec policy at the time of configuration if you want the matching of proposals to happen in a certain order of preference, such as the strongest algorithm to be considered first when a match is made when both policies from the two peers have a proposal.

Configuring the Description for an IPsec Proposal

To specify an optional text description for an IPsec proposal, include the **description** statement at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
description description;
```

Configuring the Encryption Algorithm for an IPsec Proposal

To configure encryption algorithm for an IPsec proposal, include the **encryption-algorithm** statement at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
encryption-algorithm algorithm;
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

> **NOTE:** In Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.

- **aes-128-gcm**—Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 128-bit encryption algorithm with a 16 octet integrity check value (ICV).
- **aes-192-gcm**—Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 192-bit encryption algorithm with a 16 octet integrity check value ICV.
- **aes-256-gcm**—Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 256-bit encryption algorithm with a 16 octet integrity check value ICV.
- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.

NOTE: For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409, *The Internet Key Exchange (IKE)*. The AES encryption algorithms use a software implementation that has much lower throughput, so DES remains the recommended option.

For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

If you do not configure specific authentication or encryption settings, Junos OS uses the default values of **sha1** for the authentication and **3des-cbc** for the encryption. For NULL encryption to be effective, you must always specify the Encapsulating Security Payload (ESP) protocol for the NULL encryption algorithm by including the **protocol esp** statement at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level, regardless of other system configurations.

Configuring the Lifetime for an IPsec SA

When a dynamic IPsec SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires.

NOTE: In IKEv1, the lifetime for SAs is negotiated with the remote peer based on the type of lifetime configured in the IPsec proposal. In IKEv2, such a negotiation is not performed with the remote peer. Instead, each IKE peer uses the lifetime that is locally configured for them.

For SAs in IKEv2, the lifetime is either the default value as IKEv1 (if another lifetime is not configured in the IPsec proposal) or all IKEv2 proposals in the IPsec policy must be configured with the same lifetime value.

To configure the hard lifetime value, include the **lifetime-seconds** statement and specify the number of seconds at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
lifetime-seconds seconds;
```

The default lifetime is 28,800 seconds. The range is from 180 through 86,400 seconds.

The soft lifetime values are as follows:

- Initiator: Soft lifetime = Hard lifetime – 135 seconds.

- Responder: Soft lifetime = Hard lifetime – 90 seconds.

Configuring the Protocol for a Dynamic SA

The **protocol** statement sets the protocol for a dynamic SA. IPsec uses two protocols to protect IP traffic: ESP and AH. The ESP protocol can support authentication, encryption, or both. The AH protocol is used for strong authentication. AH also authenticates the IP packet. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the protocol for a dynamic SA, include the **protocol** statement and specify the **ah**, **esp**, or **bundle** option at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec proposal proposal-name]
protocol (ah | esp | bundle);
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.
17.3R1	Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 128-bit encryption algorithm with a 16 octet integrity check value (ICV).
17.3R1	Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 192-bit encryption algorithm with a 16 octet integrity check value ICV.
17.3R1	Starting In Junos OS Release 17.3R1 for MS-MPCs and MS-MICs, Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 256-bit encryption algorithm with a 16 octet integrity check value ICV.

RELATED DOCUMENTATION

- Configuring IPsec Policies | 685
- Configuring IKE Proposals | 665
- Configuring IKE Policies | 671
- Configuring Security Associations | 639

Configuring IPsec Policies

An IPsec policy defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPsec negotiation, IPsec looks for a proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPsec proposals at each peer to ensure that at least one proposal matches a remote peer's proposal.

First, you configure one or more IPsec proposals; then you associate these proposals with an IPsec policy. You can prioritize a list of proposals used by IPsec in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IPsec policy, include the **policy** statement, and specify the policy name and one or more proposals to associate with the policy, at the **[edit services ipsec-vpn ipsec]** hierarchy level:

```
[edit services ipsec-vpn ipsec]
policy policy-name {
   description description;
   perfect-forward-secrecy {
      keys (group1 | group2 | group5 | group14 |group15 |group16 | group24);
   }
   proposals [ proposal-names ];
}
```

This section includes the following topics related to configuring an IPsec policy:

Configuring the Description for an IPsec Policy

To specify an optional text description for an IPsec policy, include the **description** statement at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]
description description;
```

Configuring Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the **perfect-forward-secrecy** statement and specify a Diffie-Hellman group at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]
perfect-forward-secrecy {
    keys (group1 | group2 | group5 | group14 | group15 |group16 | group24);
}
```

The key can be one of the following:

- **group1**—Specifies that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specifies that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group5**—Specifies that IKE use the 1536-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group14**—Specifies that IKE use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Starting in Junos OS release 17.4R1, group15, group16, and group 24 can also be used for the key:

- **group15**—Specifies that IKE use the 3072-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group16**—Specifies that IKE use the 4096-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group24**—Specifies that IKE use the 2048-bit Diffie-Hellman prime modulus group with 256-bit Prime Order Subgroup when performing the new Diffie-Hellman exchange.

The higher numbered groups provide more security than the lowered numbered groups, but require more processing time.

Configuring the Proposals in an IPsec Policy

The IPsec policy includes a list of one or more proposals associated with an IPsec policy.

To configure the proposals in an IPsec policy, include the **proposals** statement and specify one or more proposal names at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level:

```
[edit services ipsec-vpn ipsec policy policy-name]
proposals [ proposal-names ];
```

IPsec Policy for Dynamic Endpoints

An IPsec policy for dynamic endpoints defines a combination of security parameters (IPsec proposals) used during IPsec negotiation between dynamic peer security gateways, in which the remote ends of tunnels do not have a statically assigned IP address. During the IPsec negotiation, the IPsec policy looks for an IPsec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match. A match is made when the policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

If no policy is set, any policy proposed by the dynamic peer is accepted.

Example: Configuring an IPsec Policy

Define an IPsec policy, **dynamic policy-1**, that is associated with two proposals (**dynamic-1** and **dynamic-2**):

```
[edit services ipsec-vpn ipsec]
proposal dynamic-1 {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 6000;
}
proposal dynamic-2 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 6000;
}
policy dynamic-policy-1 {
    perfect-forward-secrecy {
        keys group1;
    }
```

```
    proposals [ dynamic-1 dynamic-2 ];
}
```

> **NOTE:** Updates to the current IPsec proposal and policy configuration are not applied to the current IPsec SA; updates are applied to new IPsec SAs.
>
> If you want the new updates to take immediate effect, you must clear the existing IPsec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPsec security association, see the *Junos OS System Basics and Services Command Reference*.

Release History Table

Release	Description
17.4R1	Starting in Junos OS release 17.4R1, group15, group16, and group 24 can also be used for the key

RELATED DOCUMENTATION

- Configuring IPsec Proposals | 680
- Configuring IKE Proposals | 665
- Configuring IKE Policies | 671
- Configuring Security Associations | 639

Configuring IPsec Rules

To configure an IPsec rule, include the **rule** statement and specify a rule name at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
```

```
            destination-address address;
            ipsec-inside-interface interface-name;
            source-address address;
        }
        then {
            anti-replay-window-size bits;
            backup-remote-gateway address;
            clear-dont-fragment-bit;
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            initiate-dead-peer-detection;
            dead-peer-detection {
                interval seconds;
                threshold number;
            }
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm algorithm;
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            no-anti-replay;
            remote-gateway address;
            syslog;
            tunnel-mtu bytes;
        }
    }
}
```

Each IPsec 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 IPsec rules:

Configuring Match Direction for IPsec Rules

Each rule must include a **match-direction** statement that specifies whether the match is applied on the input or output side of the interface. To configure where the match is applied, include the **match-direction (input | output)** statement at the **[edit services ipsec-vpn rule *rule-name*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name]
match-direction (input | output);
```

NOTE: ACX Series routers do not support **match-direction** as **output**.

The match direction is used with respect to the traffic flow through the AS or Multiservices PIC. When a packet is sent to the PIC, direction information is carried along with it.

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 AS or 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 AS or 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 IPsec Rules

To configure the match conditions in an IPsec rule, include the **from** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name]
from {
```

```
    destination-address address;
    ipsec-inside-interface interface-name;
    source-address address;
}
```

You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Junos OS Routing Protocols Library*.

IPsec services support both IPv4 and IPv6 address formats. If you do not specifically configure either the source address or destination address, the default value **0.0.0.0/0** (IPv4 ANY) is used. To use IPv6 ANY (**0::0/128**) as either the source or destination address, you must configure it explicitly.

NOTE: IPsec services on ACX series support IPv4 address formats. If you do not specifically configure either the source address or destination address, the default value **0.0.0.0/0** (IPv4 ANY) is used.

For next-hop-style service sets only, the **ipsec-inside-interface** statement allows you to assign a logical interface to the tunnels established as a result of this match condition. The **inside-service-interface** statement that you can configure at the **[edit services service-set *name* next-hop-service]** hierarchy level allows you to specify **.1** and **.2** as inside and outside interfaces. However, you can configure multiple adaptive services logical interfaces with the **service-domain inside** statement and use one of them to configure the **ipsec-inside-interface** statement.

The Junos OS evaluates the criteria you configure in the **from** statement. If multiple link-type tunnels are configured within the same next-hop-style service set, the **ipsec-inside-interface** value enables the rule lookup module to distinguish a particular tunnel from other tunnels in case the source and destination addresses for all of them are **0.0.0.0/0** (ANY-ANY).

NOTE: When you configure the **ipsec-inside-interface** statement, interface-style service sets are not supported.

A special situation is provided by a term containing an “any-any” match condition (usually because the **from** statement is omitted). If there is an any-any match in a tunnel, a flow is not needed, because all flows within this tunnel use the same security association (SA) and packet selectors do not play a significant role. As a result, these tunnels will use packet-based IPsec. This strategy saves some flow resources on the PIC, which can be used for other tunnels that need a flow-based service.

The following configuration example shows an any-any tunnel configuration with no **from** statement in **term-1**. Missing selectors in the **from** clause result in a packet-based IPsec service.

```
services {
    ipsec-vpn {
        rule rule-1 {
            term term-1 {
                then {
                    remote-gateway 10.1.0.1;
                    dynamic {
                        ike-policy ike_policy;
                        ipsec-policy ipsec_policy;
                    }
                }
            }
            match-direction input;
        }
        .....
    }
```

Flowless IPsec service is provided to link-type tunnels with an any-any matching, as well as to dynamic tunnels with any-any matching in both dedicated and shared mode.

For link-type tunnels, a mixture of flowless and flow-based IPsec is supported within a service set. If a service set includes some terms with any-any matching and some terms with selectors in the **from** clause, packet-based service is provided for the any-any tunnels and flow-based service is provided for the other tunnels with selectors.

For non link-type tunnels, if a service set contains both any-any terms and selector-based terms, flow-based service is provided to all the tunnels.

Configuring Actions in IPsec Rules

To configure actions in an IPsec rule, include the **then** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name*]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name]
then {
    anti-replay-window-size bits;
    backup-remote-gateway address;
    clear-dont-fragment-bit;
    dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
    }
    initiate-dead-peer-detection;
    dead-peer-detection {
```

```
        interval seconds;
        threshold number;
    }
    manual {
        direction (inbound | outbound | bidirectional) {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key (ascii-text key | hexadecimal key);
            }
            auxiliary-spi spi-value;
            encryption {
                algorithm algorithm;
                key (ascii-text key | hexadecimal key);
            }
            protocol (ah | bundle | esp);
            spi spi-value;
        }
    }
    no-anti-replay;
    remote-gateway address;
    syslog;
    tunnel-mtu bytes;
}
```

The principal IPsec actions are to configure a dynamic or manual SA:

- You configure a dynamic SA by including the **dynamic** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level and referencing policies you have configured at the **[edit services ipsec-vpn ipsec]** and **[edit services ipsec-vpn ike]** hierarchy levels.
- You configure a manual SA by including the **manual** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

You can configure the following additional properties:

Enabling IPsec Packet Fragmentation

To enable fragmentation of IP version 4 (IPv4) packets in IPsec tunnels, include the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
clear-dont-fragment-bit;
```

Setting the **clear-dont-fragment-bit** statement clears the Don't Fragment (DF) bit in the packet header, regardless of the packet size. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting.

Configuring Destination Addresses for Dead Peer Detection

To specify the remote address to which the IPsec traffic is directed, include the **remote-gateway** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
remote-gateway address;
```

To specify a backup remote address, include the **backup-remote-gateway** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
backup-remote-gateway address;
```

These two statements support both IPv4 and IPv6 address formats.

Configuring the **backup-remote-gateway** statement enables the dead peer detection (DPD) protocol, which monitors the tunnel state and remote peer availability. When the primary tunnel defined by the **remote-gateway** statement is active, the backup tunnel is in standby mode. If the DPD protocol determines that the primary remote gateway address is no longer reachable, a new tunnel is established to the backup address.

If there is no incoming traffic from a peer during a defined interval of 10 seconds, the router detects a tunnel as inactive. A global timer polls all tunnels every 10 seconds and the Adaptive Services (AS) or Multiservices Physical Interface Card (PIC) sends a message listing any inactive tunnels. If a tunnel becomes inactive, the router takes the following steps to fail over to the backup address:

1. The adaptive services message triggers the DPD protocol to send a hello message to the peer.
2. If no acknowledgment is received, two retries are sent at 2-second intervals, and then the tunnel is declared dead.
3. Failover takes place if the tunnel is declared dead or there is an IPsec Phase 1 negotiation timeout. The primary tunnel is put in standby mode and the backup becomes active.
4. If the negotiation to the backup tunnel times out, the router switches back to the primary tunnel. If both peers are down, it tries the failover six times. It then stops failing over and reverts to the original configuration, with the primary tunnel active and the backup in standby mode.

You can also enable triggering of DPD hello messages without configuring a backup remote gateway by including the **initiate-dead-peer-detection** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
initiate-dead-peer-detection;
dead-peer-detection {
    interval seconds;
    threshold number;
}
```

In addition, for IKEv1 SAs you can set **interval** and **threshold** options under the **dead-peer-detection** statement when using the **initiate-dead-peer-detection** statement. Starting in Junos OS Release 17.2R1, the **interval** and **threshold** options are also applicable to IKEv2 SAs. In Junos OS Release 17.1 and earlier, the **interval** and **threshold** options are not applicable to IKEv2 SAs, which use the default values. The interval is the amount of time that the peer waits for traffic from its destination peer before sending a DPD request packet, and the threshold is the maximum number of unsuccessful DPD requests to be sent before the peer is considered unavailable.

The monitoring behavior is the same as described for the **backup-remote-gateway** statement. This configuration enables the router to initiate DPD hellos when a backup IPsec gateway does not exist, and clean up the IKE and IPsec SAs in case the IKE peer is not reachable.

If the DPD protocol determines that the primary remote gateway address is no longer reachable, a new tunnel is established to the backup address. However, when you configure **initiate-dead-peer-detection** without a backup remote gateway address and the DPD protocol determines that the primary remote gateway address is no longer reachable, the tunnel is declared dead and IKE and IPsec SAs are cleaned up.

For more information on the DPD protocol, see RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*.

Configuring or Disabling IPsec Anti-Replay

To configure the size of the IPsec antireplay window, include the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
anti-replay-window-size bits;
```

anti-replay-window-size can take values in the range from 64 through 4096 bits. The default value is 64 bits for AS PICs and 128 bits for Multiservices PICs and DPCs. AS PICs can support a maximum replay window size of 1024 bits, whereas Multiservices PICs and DPCs can support a maximum replay window size of 4096 bits. When the software is committing an IPsec configuration , the key management process (kmd) is unable to differentiate between the service interface types. As a result, if the maximum antireplay

window size exceeds 1024 for AS PICs, the commit succeeds and no error message is produced. However, the software internally sets the antireplay window size for AS PICs to 1024 bits even if the configured value of the **anti-replay-window-size** is larger.

To disable the IPsec antireplay feature, include the **no-anti-replay** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
no-anti-replay;
```

By default, antireplay service is enabled. Occasionally this can cause interoperability issues with other vendors' equipment.

Enabling System Log Messages

To record an alert in the system logging facility, include the **syslog** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
syslog;
```

Specifying the MTU for IPsec Tunnels

To configure a specific maximum transmission unit (MTU) value for IPsec tunnels, include the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services ipsec-vpn rule rule-name term term-name then]
tunnel-mtu bytes;
```

NOTE: The **tunnel-mtu** setting is the only place you need to configure an MTU value for IPsec tunnels. Inclusion of an **mtu** setting at the **[edit interfaces sp-*fpc/pic/port* unit *logical-unit-number* family inet]** hierarchy level is not supported.

Release History Table

Release	Description
17.2R1	Starting in Junos OS Release 17.2R1, the **interval** and **threshold** options are also applicable to IKEv2 SAs.

RELATED DOCUMENTATION

Configuring IPsec Rule Sets | 697
Configuring Security Associations | 639

Configuring IPsec Rule Sets

The **rule-set** statement defines a collection of IPsec 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 ipsec-vpn]** hierarchy level with a **rule** statement for each rule:

```
[edit services ipsec-vpn]
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 match the packet, the packet is dropped by default.

RELATED DOCUMENTATION

Configuring IPsec Rules | 688
Configuring Security Associations | 639

Service Sets

The Adaptive Services PIC supports two types of service sets when you configure IPSec tunnels. Because they are used for different purposes, it is important to know the differences between these service set types.

- Next-hop service set—Supports multicast and multicast-style dynamic routing protocols (such as OSPF) over IPSec. Next-hop service sets allow you to use *inside* and *outside* logical interfaces on the Adaptive Services PIC to connect with multiple routing instances. They also allow the use of Network Address Translation (NAT) and stateful firewall capabilities. However, next-hop service sets do not monitor

Routing Engine traffic by default and require configuration of multiple service sets to support traffic from multiple interfaces.

- Interface service set—Applied to a physical interface and similar to a stateless firewall filter. They are easy to configure, can support traffic from multiple interfaces, and can monitor Routing Engine traffic by default. However, they cannot support dynamic routing protocols or multicast traffic over the IPSec tunnel.

In general, we recommend that you use next-hop service sets because they support routing protocols and multicast over the IPSec tunnel, they are easier to understand, and the routing table makes forwarding decisions without administrative intervention.

RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | **618**

Configuring Junos VPN Site Secure or IPSec VPN

Configuring IPsec Service Sets

IN THIS SECTION

IPsec service sets require additional specifications that you configure at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
anti-replay-window-size bits;
```

```
clear-dont-fragment-bit;
copy-dont-fragment-bit
set-dont-fragment-bit
ike-access-profile profile-name;
local-gateway address <gw-interface interface-name.logical-unit-number>;
no-anti-replay;
no-certificate-chain-in-ike;
passive-mode-tunneling;
trusted-ca [ ca-profile-names ];
tunnel-mtu bytes;
```

Configuration of these statements is described in the following sections:

Configuring the Local Gateway Address for IPsec Service Sets

If you configure an IPsec service set, you must also configure a local IPv4 or IPv6 address by including the **local-gateway** statement:

- If the Internet Key Exchange (IKE) gateway IP address is in inet.0 (the default situation), you configure the following statement:

  ```
  local-gateway address;
  ```

- If the IKE gateway IP address is in a VPN routing and forwarding (VRF) instance, you configure the following statement:

  ```
  local-gateway address routing-instance instance-name;
  ```

You can configure all the link-type tunnels that share the same local gateway address in a single next-hop-style service set. You must specify a value for the **inside-service-interface** statement at the **[edit services service-set *service-set-name*]** hierarchy level that matches the **ipsec-inside-interface** value, which you configure at the **[edit services ipsec-vpn rule *rule-name* term *term-name* from]** hierarchy level. For more information about IPsec configuration, see "Configuring IPsec Rules" on page 688.

> **NOTE:** Starting in Junos OS Release 16.1, to configure link-type tunnels, (i.e., next-hop style), for HA purposes, you can configure AMS logical interfaces as the IPsec internal interfaces by using the **ipsec-inside-interface *interface-name*** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* from]** hierarchy level.

Starting in Junos OS Release 17.1, AMS supports IPSec tunnel distribution.

IKE Addresses in VRF Instances

You can configure Internet Key Exchange (IKE) gateway IP addresses that are present in a VPN routing and forwarding (VRF) instance as long as the peer is reachable through the VRF instance.

For next-hop service sets, the key management process (kmd) places the IKE packets in the routing instance that contains the **outside-service-interface** value you specify, as in this example:

```
routing-instances vrf-nxthop {
    instance-type vrf;
    interface sp-1/1/0.2;
    ...
}
services service-set service-set-1 {
    next-hop-service {
        inside-service-interface sp-1/1/0.1;
        outside-service-interface sp-1/1/0.2;
    }
    ...
}
```

For interface service sets, the **service-interface** statement determines the VRF, as in this example:

```
routing-instances vrf-intf {
    instance-type vrf;
    interface sp-1/1/0.3;
    interface ge-1/2/0.1; # interface on which service set is applied
    ...
}
services service-set service-set-2 {
    interface-service {
        service-interface sp-1/1/0.3;
    }
    ...
}
```

Clearing SAs When Local Gateway Address or MS-MPC or MS-MIC Goes Down

Starting in Junos OS Release 17.2R1, tou can use the **gw-interface** statement to enable the cleanup of IKE triggers and IKE and IPsec SAs when an IPsec tunnel's local gateway IP address goes down, or the MS-MIC or MS-MPC being used in the tunnel's service set goes down.

```
local-gateway address <gw-interface interface-name.logical-unit-number>;
```

The *interface-name* and *logical-unit-number* must match the interface and logical unit on which the local gateway IP address is configured.

If the local gateway IP address for an IPsec tunnel's service set goes down or the MS-MIC or MS-MPC that is being used in the service set goes down, the service set no longer sends IKE triggers. In addition, when the local gateway IP address goes down, the IKE and IPsec SAs are cleared for next-hop service sets, and go to the Not Installed state for interface-style service sets. The SAs that have the Not Installed state are deleted when the local gateway IP address comes back up.

If the local gateway IP address that goes down for a next-hop service set is for the responder peer, then you need to clear the IKE and IPsec SAs on the initiator peer so that the IPsec tunnel comes back up once the local gateway IP address comes back up. You can either manually clear the IKE and IPsec SAs on the initiator peer (see **clear services ipsec-vpn ike security-associations** and **clear services ipsec-vpn ipsec security-associations**) or enable dead peer detection on the initiator peer (see "Configuring Stateful Firewall Rules" on page 546).

Configuring IKE Access Profiles for IPsec Service Sets

For dynamic endpoint tunneling only, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level. To do this, include the **ike-access-profile** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level:

```
[edit services service-set service-set-name ipsec-vpn-options]
ike-access-profile profile-name;
```

The **ike-access-profile** statement must reference the same name as the **profile** statement you configured for IKE access at the **[edit access]** hierarchy level. You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.

> **NOTE:** If you configure an IKE access profile in a service set, no other service set can share the same **local-gateway** address.
>
> Also, you must configure a separate service set for each VRF. All interfaces referenced by the **ipsec-inside-interface** statement within a service set must belong to the same VRF.

Configuring Certification Authorities for IPsec Service Sets

You can specify one or more trusted certification authorities by including the **trusted-ca** statement:

```
trusted-ca [ ca-profile-names ];
```

When you configure public key infrastructure (PKI) digital certificates in the IPsec configuration, each service set can have its own set of trusted certification authorities. The names you specify for the **trusted-ca** statement must match profiles configured at the **[edit security pki]** hierarchy level; for more information, see the *Junos OS Administration Library*. For more information about IPsec digital certificate configuration, see "Configuring IPsec Rules" on page 688.

Starting in Junos OS Release 18.2R1, you can configure the MX Series router with MS-MPCs or MS-MICs to send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain. This avoids IKE fragmentation. To configure this feature, include the **no-certificate-chain-in-ike** statement:

```
[edit services service-set service-set-name ipsec-vpn-options]
no-certificate-chain-in-ike;
```

Configuring or Disabling Antireplay Service

You can include the **anti-replay-window-size** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to specify the size of the antireplay window.

```
anti-replay-window-size bits;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the **no-anti-replay** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

> **NOTE:** The **anti-replay-window-size** and **no-anti-replay** settings at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level override the settings specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

You can also include the **no-anti-replay** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to disable IPsec antireplay service. It occasionally causes interoperability issues for security associations.

```
no-anti-replay;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **no-anti-reply** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

> **NOTE:** Setting the **anti-replay-window-size** and **no-anti-replay** statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level overrides the settings specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

Clearing the Do Not Fragment Bit

You can include the **clear-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to clear the do not fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation.

```
clear-dont-fragment-bit;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

Starting in Junos OS Release 14.1, in packets that are transmitted through dynamic endpoint IPSec tunnels, you can enable the value set in the DF bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet. If the packet size exceeds the tunnel maximum transmission unit (MTU) value, the packet is fragmented before encapsulation. For IPsec tunnels, the default MTU value is 1500 regardless of the interface MTU setting. To copy the DF bit value to only the outer header and not modify the inner header, use the **copy-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level. You can also configure the DF bit to be set only in the outer IPv4 header of the IPsec packet and not be defined in the inner IPv4 header. To configure the DF bit in only

the outer header of the IPsec packet and to leave the inner header unmodified, include the **set-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **copy-dont-fragment-bit** and **set-dont-fragment-bit** statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level to clear the DF bit in the IPv4 packets that enter the static tunnel. These functionalities are supported on MX Series routers with MS-MICs and MS-MPCs.

Configuring Passive-Mode Tunneling

You can include the **passive-mode-tunneling** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to enable the service set to tunnel malformed packets.

```
[edit services service-set service-set-name ipsec-vpn-options]
passive-mode-tunneling;
```

This functionality bypasses the active IP checks, such as version, TTL, protocol, options, address and other land attack checks, and tunnels the packets as is. If this statement is not configured, packets failing the IP checks are dropped in the PIC. In passive mode, the inner packet is not touched; an ICMP error is not generated if the packet size exceeds the tunnel MTU value.

The IPsec tunnel is not treated as a next hop and TTL is not decremented. Because an ICMP error is not generated if the packet size exceeds the tunnel MTU value, the packet is tunnelled even if it crosses the tunnel MTU threshold.

> **NOTE:** This functionality is similar to that provided by the **no-ipsec-tunnel-in-traceroute** statement, described in "Tracing Junos VPN Site Secure Operations" on page 710. Starting in Junos OS Release 14.2, passive mode tunneling is supported on MS-MICs and MS-MPCs.

NOTE: Starting in Junos OS Release 14.2, the **header-integrity-check** option that is supported on MS-MICs and MS-MPCs to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information and flag such anomalies and errors has a functionality that is opposite to the functionality caused by passive mode tunneling. If you configure both the **header-integrity-check** statement and the **passive-mode tunneling** statement on MS-MICs and MS-MPCs, and attempt to commit such a configuration, an error is displayed during commit.

The passive mode tunneling functionality (by including the **passive-mode-tunnelin** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level) is a superset of the capability to disable IPsec tunnel endpoint in the traceroute output (by including **no-ipsec-tunnel-in-traceroute** statement at the **[edit services ipsec-vpn]** hierarchy level). Passive mode tunneling also bypasses the active IP checks and tunnel MTU check in addition to not treating an IPsec tunnel as a next-hop as configured by the **no-ipsec-tunnel-in-traceroute** statement.

Configuring the Tunnel MTU Value

You can include the **tunnel-mtu** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to set the maximum transmission unit (MTU) value for IPsec tunnels.

```
tunnel-mtu bytes;
```

This statement is useful for dynamic endpoint tunnels for which you cannot configure the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

NOTE: The **tunnel-mtu** setting at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level overrides the value specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

Configuring IPsec Multipath Forwarding with UDP Encapsulation

Starting in Junos OS Release 16.1, you can enable multipath forwarding of IPsec traffic by configuring UDP encapsulation in the service set, which adds a UDP header to the IPsec encapsulation of packets. This results in the forwarding of IPsec traffic over multiple paths, increasing the throughput of IPsec traffic. If you do not enable UDP encapsulation, all the IPsec traffic follows a single forwarding path.

When NAT-T is detected, only NAT-T UDP encapsulation occurs, not the UDP encapsulation for IPsec packets.

To enable UDP encapsulation:

1. Enable UDP encapsulation.

   ```
   [edit services service-set service-set-name ipsec-vpn-options]
   user@host set udp-encapsulation
   ```

2. (Optional) Specify the UDP destination port number.

   ```
   [edit services service-set service-set-name ipsec-vpn-options udp-encapsulation]
   user@host set udp-dest-port destination-port
   ```

   Use a destination port number from 1025 through 65536, but do not use 4500. If you do not specify a port number, the default destination port is 4565.

Release History Table

Release	Description
18.2R1	Starting in Junos OS Release 18.2R1, you can configure the MX Series router with MS-MPCs or MS-MICs to send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain.
17.2R1	Starting in Junos OS Release 17.2R1, tou can use the **gw-interface** statement to enable the cleanup of IKE triggers and IKE and IPsec SAs when an IPsec tunnel's local gateway IP address goes down, or the MS-MIC or MS-MPC being used in the tunnel's service set goes down.
17.1	Starting in Junos OS Release 17.1, AMS supports IPSec tunnel distribution
16.1	Starting in Junos OS Release 16.1, to configure link-type tunnels, (i.e., next-hop style), for HA purposes, you can configure AMS logical interfaces as the IPsec internal interfaces by using the **ipsec-inside-interface *interface-name*** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* from]** hierarchy level.
16.1	Starting in Junos OS Release 16.1, you can enable multipath forwarding of IPsec traffic by configuring UDP encapsulation in the service set, which adds a UDP header to the IPsec encapsulation of packets.
14.2	Starting in Junos OS Release 14.2, passive mode tunneling is supported on MS-MICs and MS-MPCs.
14.2	Starting in Junos OS Release 14.2, the **header-integrity-check** option that is supported on MS-MICs and MS-MPCs to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information and flag such anomalies and errors has a functionality that is opposite to the functionality caused by passive mode tunneling.
14.1	Starting in Junos OS Release 14.1, in packets that are transmitted through dynamic endpoint IPSec tunnels, you can enable the value set in the DF bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet.

RELATED DOCUMENTATION

- Understanding Service Sets | 6
- Configuring Service Sets to be Applied to Services Interfaces | 9
- Configuring Service Set Limitations | 23
- Configuring System Logging for Service Sets | 36

Tracing IPsec Operations

Trace operations track IPsec events and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/kmd**.

To trace IPsec operations, include the **traceoptions** statement at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
traceoptions {
    file <filename> <files number> <match regular-expression> <size bytes> <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
}
```

You can specify the following IPsec tracing flags:

- **all**—Trace everything.
- **certificates**—Trace certificates events.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

The **level** statement sets the key management process (kmd) tracing level. The following values are supported:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**–Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

Disabling NAT-T on MX Series Routers for Handling NAT with IPsec-Protected Packets

Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers. By default, Junos OS detects whether either one of the IPsec tunnels is behind a NAT device and automatically switches to using NAT-T for the protected traffic. To avoid running unsupported NAT-T in Junos OS releases before 17.4R1, you must disable NAT-T by including the **disable-natt** statement at the **[edit services ipsec-vpn]** hierarchy level. When you disable NAT-T, the NAT-T functionality is globally switched off. When you disable NAT-T and a NAT device is present between the two IPsec gateways, ISAKMP messages are negotiated using UDP port 500 and data packets are encapsulated with Encapsulating Security Payload (ESP).

Network Address Translation-Traversal (NAT-T) is a method for getting around IP address translation issues encountered when data protected by IPsec passes through a NAT device for address translation. Any changes to the IP addressing, which is the function of NAT, causes IKE to discard packets. After detecting one or more NAT devices along the data path during Phase 1 exchanges, NAT-T adds a layer of User Datagram Protocol (UDP) encapsulation to IPsec packets so they are not discarded after address translation. NAT-T encapsulates both IKE and ESP traffic within UDP with port 4500 used as both the source and destination port. Because NAT devices age out stale UDP translations, keepalive messages are required between the peers.

The location of a NAT device can be such that:

- Only the IKEv1 or IKEv2 initiator is behind a NAT device. Multiple initiators can be behind separate NAT devices. Initiators can also connect to the responder through multiple NAT devices.
- Only the IKEv1 or IKEv2 responder is behind a NAT device.
- Both the IKEv1 or IKEv2 initiator and the responder are behind a NAT device.

Dynamic endpoint VPN covers the situation where the initiator's IKE external address is not fixed and is therefore not known by the responder. This can occur when the initiator's address is dynamically assigned by an ISP or when the initiator's connection crosses a dynamic NAT device that allocates addresses from a dynamic address pool.

Configuration examples for NAT-T are provided for the topology in which only the responder is behind a NAT device and the topology in which both the initiator and responder are behind a NAT device. Site-to-site IKE gateway configuration for NAT-T is supported on both the initiator and responder. A remote IKE ID is used to validate a peer’s local IKE ID during Phase 1 of IKE tunnel negotiation. Both the initiator and responder require a local identify and remote identity string.

RELATED DOCUMENTATION

disable-natt | 1174

Tracing Junos VPN Site Secure Operations

> **NOTE:** Junos VPN Site Secure is a suite of IPsec features supported on multiservices line cards (MS-DPC, MS-MPC, and MS-MIC), and was previously referred to as IPsec services.

Trace operations track IPsec events and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/kmd**.

To trace IPsec operations, include the **traceoptions** statement at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
traceoptions {
    file <filename> <files number> <match regular-expression> <size bytes> <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
}
```

You can specify the following IPsec tracing flags:

- **all**—Trace everything.
- **certificates**—Trace certificates events.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

The **level** statement sets the key management process (kmd) tracing level. The following values are supported:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**–Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

This section includes the following topics:

Disabling IPsec Tunnel Endpoint in Traceroute

If you include the **no-ipsec-tunnel-in-traceroute** statement at the **[edit services ipsec-vpn]** hierarchy level, the IPsec tunnel is not treated as a next hop and the time to live (TTL) is not decremented. Also, if the TTL reaches zero, an ICMP time exceeded message is not generated.

```
[edit services ipsec-vpn]
no-ipsec-tunnel-in-traceroute;
```

NOTE: This functionality is also provided by the **passive-mode-tunneling** statement. You can use the **no-ipsec-tunnel-in-traceroute** statement in specific scenarios in which the IPsec tunnel should not be treated as a next hop and passive mode is not desired.

Tracing IPsec PKI Operations

Trace operations track IPsec PKI events and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/pkid**.

To trace IPsec PKI operations, include the **traceoptions** statement at the **[edit security pki]** hierarchy level:

```
[edit security pki]
traceoptions {
```

```
    file filename <files number> <match regular-expression> <size maximum-file-size> <world-readable |
      no-world-readable>;
    flag flag (all | certificate-verification | enrollment | online-crl-check);
}
```

You can specify the following PKI tracing flags:

- **all**—Trace everything.
- **certificates**—Trace certificates events.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

Configuring IKE Proposals | 665

Multitask Example: Configuring IPsec Services

The following example-based instructions show how to configure IPsec services. The configuration involves defining an IKE policy, an IPsec policy, IPsec rules, trace options, and service sets.

This topic includes the following tasks:

1. Configuring the IKE Proposal | 713
2. Configuring the IKE Policy (and Referencing the IKE Proposal) | 714
3. Configuring the IPsec Proposal | 715
4. Configuring the IPsec Policy (and Referencing the IPsec Proposal) | 716

5. Configuring the IPsec Rule (and Referencing the IKE and IPsec Policies) | **717**
6. Configuring IPsec Trace Options | **719**
7. Configuring the Access Profile (and Referencing the IKE and IPsec Policies) | **720**
8. Configuring the Service Set (and Referencing the IKE Profile and the IPsec Rule) | **721**

Configuring the IKE Proposal

The IKE proposal configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. For more information about IKE proposals, see "Configuring IKE Proposals" on page 665.

To define the IKE proposal:

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

```
user@host# edit services ipsec-vpn
```

2. Configure the authentication method, which is **pre-shared keys** in this example:

```
[edit services ipsec-vpn]
user@host# set ike proposal test-IKE-proposal authentication-method pre-shared-keys
```

3. Configure the Diffie-Hellman Group and specify a name—for example, **group1**:

```
[edit services ipsec-vpn]
user@host# set ike proposal test-IKE-proposal dh-group group1
```

4. Configure the authentication algorithm, which is **sha1** in this example:

```
[edit services ipsec-vpn]
user@host# set ike proposal test-IKE-proposal authentication-algorithm sha1
```

5. Configure the encryption algorithm, which is **aes-256-cbc** in this example:

```
[edit services ipsec-vpn]
user@host# set ike proposal test-IKE-proposal encryption-algorithm aes-256-cbc
```

The following sample output shows the configuration of the IKE proposal:

```
[edit services ipsec-vpn]
user@host# show ike
proposal test-IKE-proposal {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
```

SEE ALSO

Configuring IKE Proposals | 665

Configuring the IKE Policy (and Referencing the IKE Proposal)

The IKE policy configuration defines the proposal, mode, addresses, and other security parameters used during IKE negotiation. For more information about IKE policies, see "Configuring IKE Policies" on page 671.

To define the IKE policy and reference the IKE proposal:

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

   ```
   user@host# edit services ipsec-vpn
   ```

2. Configure the IKE first phase mode—for example, **main**:

   ```
   [edit services ipsec-vpn]
   user@host# set ike policy test-IKE-policy mode main
   ```

3. Configure the proposal, which is **test-IKE-proposal** in this example:

   ```
   [edit services ipsec-vpn]
   user@host# set ike policy test-IKE-policy proposals test-IKE-proposal
   ```

4. Configure the local identification with an IPv4 address—for example, **192.168.255.2**:

   ```
   [edit services ipsec-vpn]
   user@host# set ike policy test-IKE-policy local-id ipv4_addr 192.168.255.2
   ```

5. Configure the preshared key in ASCII text format, which is **TEST** in this example:

```
[edit services ipsec-vpn]
user@host# set ike policy test-IKE-policy pre-shared-key ascii-text TEST
```

The following sample output shows the configuration of the IKE policy:

```
[edit services ipsec-vpn]
user@host# show ike
policy test-IKE-policy {
    mode main;
    proposals test-IKE-proposal;
    local-id ipv4_addr 192.168.255.2;
    pre-shared-key ascii-text TEST;
}
```

SEE ALSO

Configuring IKE Policies | 671

Configuring the IPsec Proposal

The IPsec proposal configuration defines the protocols and algorithms (security services) that are required to negotiate with the remote IPsec peer. For more information about IPsec proposals, see “Configuring IPsec Proposals” on page 680.

To define the IPsec proposal:

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

```
user@host# edit services ipsec-vpn
```

2. Configure the IPsec protocol for the proposal—for example, **esp**:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal protocol esp
```

3. Configure the authentication algorithm for the proposal, which is **hmac-sha1-96** in this example:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal authentication-algorithm hmac-sha1-96
```

4. Configure the encryption algorithm for the proposal, which is **aes-256-cbc** in this example:

```
[edit services ipsec-vpn]
user@host# set ipsec proposal test-IPsec-proposal encryption-algorithm aes-256-cbc
```

The following sample output shows the configuration of the IPsec proposal:

```
[edit services ipsec-vpn]
user@host# show ike
proposal test-IPsec-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
```

SEE ALSO

Configuring IPsec Proposals | 680

Configuring the IPsec Policy (and Referencing the IPsec Proposal)

The IPsec policy configuration defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines PFS and the proposals needed for the connection. For more information about IPsec policies, see “Configuring IPsec Policies” on page 685.

To define the IPsec policy and reference the IPsec proposal:

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

```
user@host# edit services ipsec-vpn
```

2. Configure the keys for perfect forward secrecy in the IPsec policy—for example, **group1**:

```
[edit services ipsec-vpn]
user@host# set ipsec policy test-IPsec-policy perfect-forward-secrecy keys group1
```

3. Configure a set of IPsec proposals in the IPsec policy—for example, **test-IPsec-proposal**:

```
[edit services ipsec-vpn]
user@host# set ipsec policy test-IPsec-policy proposals test-IPsec-proposal
```

The following sample output shows the configuration of the IPsec policy:

```
[edit services ipsec-vpn]
user@host# show ipsec policy test-IPsec-policy
perfect-forward-secrecy {
    keys group1;
}
proposals test-IPsec-proposal;
```

SEE ALSO

Configuring IPsec Policies | 685

Configuring the IPsec Rule (and Referencing the IKE and IPsec Policies)

The IPsec rule configuration defines the direction that specifies whether the match is applied on the input or output side of the interface. The configuration also consists of a set of terms that specify the match conditions and applications that are included and excluded and also specify the actions and action modifiers to be performed by the router software. For more information about IPsec rules, see "Configuring IPsec Rules" on page 688.

To define the IPsec rule and reference the IKE and IPsec policies:

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

```
user@host# edit services ipsec-vpn
```

2. Configure the IP destination address for the IPsec term in the IPsec rule—for example, **192.168.255.2/32**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 from destination-address 192.168.255.2/32
```

3. Configure the remote gateway address for the IPsec term in the IPsec rule—for example, **0.0.0.0**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then remote-gateway 0.0.0.0
```

4. Configure a dynamic security association for IKE policy for the IPsec term in the IPsec rule, which is **test-IKE-policy** in this example:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then dynamic ike-policy test-IKE-policy
```

5. Configure a dynamic security association for IKE proposal for the IPsec term in the IPsec rule, which is **test-IPsec-proposal** in this example:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule term 10 then dynamic ipsec-policy test-IPsec-policy
```

6. Configure a direction for which the rule match is being applied in the IPsec rule—for example, **input**:

```
[edit services ipsec-vpn]
user@host# set rule test-IPsec-rule match-direction input
```

The following sample output shows the configuration of the IPsec rule:

```
[edit services ipsec-vpn]
user@host# show rule test-IPsec-rule
term 10 {
    from {
        destination-address {
            192.168.255.2/32;
        }
    }
    then {
        remote-gateway 0.0.0.0;
        dynamic {
            ike-policy test-IKE-policy;
            ipsec-policy test-IPsec-policy;
        }
    }
}
match-direction input;
```

SEE ALSO

Configuring IPsec Rules | 688

Configuring IPsec Trace Options

The IPsec trace options configuration tracks IPsec events and records them in a log file in the **/var/log** directory. By default, this file is named **/var/log/kmd**. For more information about IPsec rules, see "Tracing Junos VPN Site Secure Operations" on page 710.

To define the IPsec trace options:

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

```
user@host# edit services ipsec-vpn
```

2. Configure the trace file, which is **ipsec.log** in this example:

```
[edit services ipsec-vpn]
user@host# set traceoptions file ipsec.log
```

3. Configure all the tracing parameters with the option **all** in this example:

```
[edit services ipsec-vpn]
user@host# set traceoptions flag all
```

The following sample output shows the configuration of the IPsec trace options:

```
[edit services ipsec-vpn]
user@host# show traceoptions
file ipsec.log;
flag all;
```

SEE ALSO

Tracing Junos VPN Site Secure Operations | 710

Configuring the Access Profile (and Referencing the IKE and IPsec Policies)

The access profile configuration defines the access profile and references the IKE and IPsec policies. For more information about access profile, see *Configuring an IKE Access Profile*.

To define the access profile and reference the IKE and IPsec policies:

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

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

2. Configure the list of local and remote proxy identity pairs with the **allowed-proxy-pair** option. In this example, **10.0.0.0/24** is the IP address for local proxy identity and **10.0.1.0/24** is the IP address for remote proxy identity:

   ```
   [edit access]
   user@host# set profile IKE-profile-TEST client * ike allowed-proxy-pair local 10.0.0.0/24 remote 10.0.1.0/24
   ```

3. Configure the IKE policy—for example, **test-IKE-policy**:

   ```
   [edit access]
   user@host# set profile IKE-profile-TEST client * ike ike-policy test-IKE-policy
   ```

4. Configure the IPsec policy—for example, **test-IPsec-policy**:

   ```
   [edit access]
   user@host# set profile IKE-profile-TEST client * ike ipsec-policy test-IPsec-policy
   ```

5. Configure the identity of logical service interface pool, which is **TEST-intf** in this example:

   ```
   [edit access]
   user@host# set profile IKE-profile-TEST client * ike interface-id TEST-intf
   ```

The following sample output shows the configuration of the access profile:

```
[edit access]
user@host# show
profile IKE-profile-TEST {
    client * {
```

```
        ike {
            allowed-proxy-pair local 10.0.0.0/24 remote 10.0.1.0/24;
            ike-policy test-IKE-policy;
            ipsec-policy test-IPsec-policy; # new statement
            interface-id TEST-intf;
        }
    }
}
```

SEE ALSO

Configuring an IKE Access Profile

Configuring the Service Set (and Referencing the IKE Profile and the IPsec Rule)

The service set configuration defines IPsec service sets that require additional specifications and references the IKE profile and the IPsec rule. For more information about IPsec service sets, see "Configuring IPsec Service Sets" on page 698.

To define the service set configuration with the next-hop service sets and IPsec VPN options:

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

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

2. Configure a service set with parameters for next hop service interfaces for the inside network—for example, **sp-1/2/0.1**:

   ```
   [edit services]
   user@host# set service-set TEST next-hop-service inside-service-interface sp-1/2/0.1
   ```

3. Configure a service set with parameters for next hop service interfaces for the outside network—for example, **sp-1/2/0.2**:

   ```
   [edit services]
   user@host# set service-set TEST next-hop-service outside-service-interface sp-1/2/0.2
   ```

4. Configure the IPsec VPN options with the address and routing instance for the local gateway—for example, **192.168.255.2**:

```
[edit services]
user@host# set service-set TEST ipsec-vpn-options local-gateway 192.168.255.2
```

5. Configure the IPsec VPN options with the IKE access profile for dynamic peers, which is **IKE-profile-TEST** in this example:

```
[edit services]
user@host# set service-set TEST ipsec-vpn-options ike-access-profile IKE-profile-TEST
```

6. Configure a service set with IPsec VPN rules, which is **test-IPsec-rule** in this example:

```
[edit services]
user@host# set service-set TEST ipsec-vpn-rules test-IPsec-rule
```

The following sample output shows the configuration of the service set configuration referencing the IKE profile and the IPsec rule:

```
[edit services]user@host# show service-set TEST
next-hop-service {
    inside-service-interface sp-1/2/0.1;
    outside-service-interface sp-1/2/0.2;
}
ipsec-vpn-options {
    local-gateway 192.168.255.2;
    ike-access-profile IKE-profile-TEST;
}
ipsec-vpn-rules test-IPsec-rule;
```

SEE ALSO

Configuring IPsec Service Sets | 698

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

Configuring IKE Policies | 671

Example: Configuring Junos VPN Site Secure on MS-MIC and MS-MPC

IN THIS SECTION

NOTE: You can follow the same procedure and use the same configuration given in this example, to configure Junos VPN Site Secure (previously known as IPsec features) on MS-MPCs.

This example contains the following sections:

Requirements

This example uses the following hardware and software components:

- Two MX Series routers with MS-MICs
- Junos OS Release 13.2 or later

Overview

Junos OS Release 13.2, extends support for Junos VPN Site Secure (formerly known as IPsec features) to the newly-introduced Multiservices MIC and MPC (MS-MIC and MS-MPC) on MX Series routers. The Junos OS extension-provider packages come preinstalled and preconfigured on the MS-MIC and MS-MPC.

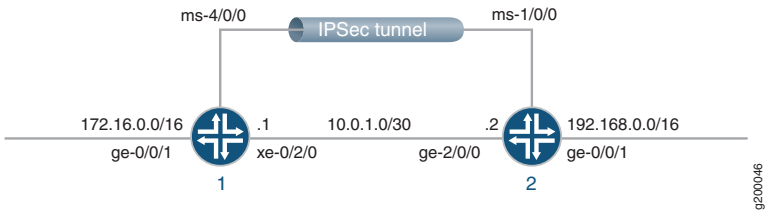
The following Junos VPN Site Secure features are supported on the MS-MIC and MS-MPC in Release 13.2:

- Dynamic End Points (DEP)
- Encapsulating Security Payload (ESP) protocol
- Dead Peer Detection (DPD) trigger messages
- Sequence Number Rollover notifications
- Static IPsec tunnels with next-hop-style and interface-style service sets

However, in Junos OS Release 13.2, the Junos VPN Site Secure support on the MS-MIC and MS-MPC is limited to IPv4 traffic. Passive module tunneling is not supported on MS-MICs and MS-MPCs.

Figure 35 on page 724 shows the IPsec VPN tunnel topology.

Figure 35: IPsec VPN Tunnel Topology



This example shows configuration of two routers, Router 1 and Router 2, that have an IPsec VPN tunnel configured between them.

While configuring the routers, note the following points:

- The IP address you configure for **source-address** under the **[edit services ipsec-vpn rule *name* term *term* from]** hierarchy level on Router 1 must be the same as the IP address you configure for **destination-address** under the same hierarchy on Router 2, and vice versa.
- The IP address of the **remote-gateway** you configure under the **[edit services ipsec-vpn rule *name* term *term* then]** hierarchy level should match the IP address of the **local-gateway** you configure under the **[edit services service-set *name* ipsec-vpn-options]** hierarchy level of Router 2, and vice versa.

Configuration

IN THIS SECTION

This section contains:

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.

Configuring Interfaces on Router 1

```
set interfaces ms-4/0/0 unit 0 family inet
set interfaces ms-4/0/0 unit 1 family inet
set interfaces ms-4/0/0 unit 1 family inet6
set interfaces ms-4/0/0 unit 1 service-domain inside
set interfaces ms-4/0/0 unit 2 family inet
set interfaces ms-4/0/0 unit 2 family inet6
set interfaces ms-4/0/0 unit 2 service-domain outside
set interfaces xe-0/2/0 unit 0 family inet address 10.0.1.1/30
```

Configuring IPsec VPN Service on Router 1

```
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from source-address 172.16.0.0/16
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from destination-address 192.168.0.0/16
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then remote-gateway 10.0.1.2
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ike-policy
  ike_policy_ms_4_0_0
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ipsec-policy
  ipsec_policy_ms_4_0_0
set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_4_0_01 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 proposals ipsec_proposal_ms_4_0_0
set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 dh-group group2
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 version 2
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 proposals ike_proposal_ms_4_0_0
set services ipsec-vpn ike policy ike_policy_ms_4_0_0 pre-shared-key ascii-text secret-data
```

Configuring a Service Set on Router 1

```
set services service-set ipsec_ss_ms_4_0_01 next-hop-service inside-service-interface ms-4/0/0.1
set services service-set ipsec_ss_ms_4_0_01 next-hop-service outside-service-interface ms-4/0/0.2
set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-options local-gateway 10.0.1.1
set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-rules vpn_rule_ms_4_0_01
```

Configuring Routing Options on Router 1

```
set routing-options static route 192.168.0.0/16 next-hop ms-4/0/0.1
```

Configuring Interfaces on Router 2

```
set interfaces ms-1/0/0 unit 0 family inet
set interfaces ms-1/0/0 unit 1 family inet
set interfaces ms-1/0/0 unit 1 family inet6
set interfaces ms-1/0/0 unit 1 service-domain inside
set interfaces ms-1/0/0 unit 2 family inet
set interfaces ms-1/0/0 unit 2 family inet6
set interfaces ms-1/0/0 unit 2 service-domain outside
set interfaces ge-2/0/0 unit 0 family inet address 10.0.1.2/30
```

Configuring IPsec VPN Service on Router 2

```
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from source-address 192.168.0.0/16
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from destination-address 172.16.0.0/16
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then remote-gateway 10.0.1.1
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ike-policy
   ike_policy_ms_5_2_0
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ipsec-policy
   ipsec_policy_ms_5_2_0
set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then anti-replay-window-size 4096
set services ipsec-vpn rule vpn_rule_ms_5_2_01 match-direction input
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 protocol esp
```

```
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 proposals ipsec_proposal_ms_5_2_0
set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 dh-group group2
set services ipsec-vpn ike policy ike_policy_ms_5_2_0 version 2
set services ipsec-vpn ike policy ike_policy_ms_5_2_0 proposals ike_proposal_ms_5_2_0
set services ipsec-vpn ike policy ike_policy_ms_5_2_0 pre-shared-key ascii-text secret-data
set services ipsec-vpn establish-tunnels immediately
```

Configuring a Service Set on Router 2

```
set services service-set ipsec_ss_ms_5_2_01 next-hop-service inside-service-interface ms-1/0/0.1
set services service-set ipsec_ss_ms_5_2_01 next-hop-service outside-service-interface ms-1/0/0.2
set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-options local-gateway 10.0.1.2
set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-rules vpn_rule_ms_5_2_01
```

Configuring Routing Options on Router 2

```
set routing-options static route 172.16.0.0/16 next-hop ms-1/0/0.1
```

Configuring Router 1

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

NOTE: Starting with Release 13.2, the Junos OS extension-provider packages come preinstalled on multiservices MICs and MPCs (MS-MICs and MS-MPCs). The **adaptive-services** configuration at the **[edit chassis fpc *number* pic *number*]** hierarchy level is preconfigured on these cards.

1. Configure the interface properties such as family, service-domain, and unit.

```
user@router1# set interfaces ms-4/0/0 unit 0 family inet
user@router1# set interfaces ms-4/0/0 unit 1 family inet
user@router1# set interfaces ms-4/0/0 unit 1 family inet6
user@router1# set interfaces ms-4/0/0 unit 1 service-domain inside
user@router1# set interfaces ms-4/0/0 unit 2 family inet
user@router1# set interfaces ms-4/0/0 unit 2 family inet6
user@router1# set interfaces ms-4/0/0 unit 2 service-domain outside
user@router1# set interfaces xe-0/2/0 unit 0 family inet address 10.0.1.1/30
```

2. Configure IPsec properties such as address, remote-gateway, policies, match-direction, protocol, replay window size, algorithm details, secrecy keys, proposal, authentication method, groups, and version.

```
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from source-address
  172.16.0.0/16
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 from destination-address
  192.168.0.0/16
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then remote-gateway 10.0.1.2
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ike-policy
  ike_policy_ms_4_0_0
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then dynamic ipsec-policy
  ipsec_policy_ms_4_0_0
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 term term11 then anti-replay-window-size
  4096
user@router1# set services ipsec-vpn rule vpn_rule_ms_4_0_01 match-direction input
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 protocol esp
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 authentication-algorithm
  hmac-sha1-96
user@router1# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_4_0_0 encryption-algorithm 3des-cbc
user@router1# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 perfect-forward-secrecy keys
  group2
user@router1# set services ipsec-vpn ipsec policy ipsec_policy_ms_4_0_0 proposals ipsec_proposal_ms_4_0_0
user@router1# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 authentication-method
  pre-shared-keys
user@router1# set services ipsec-vpn ike proposal ike_proposal_ms_4_0_0 dh-group group2
user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 version 2
user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 proposals ike_proposal_ms_4_0_0
user@router1# set services ipsec-vpn ike policy ike_policy_ms_4_0_0 pre-shared-key ascii-text secret-key
```

3. Configure a service set, the ipsec-vpn options, and rules.

```
user@router1# set services service-set ipsec_ss_ms_4_0_01 next-hop-service inside-service-interface
  ms-4/0/0.1
```

```
user@router1# set services service-set ipsec_ss_ms_4_0_01 next-hop-service outside-service-interface
  ms-4/0/0.2
user@router1# set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-options local-gateway 10.0.1.1
user@router1# set services service-set ipsec_ss_ms_4_0_01 ipsec-vpn-rules vpn_rule_ms_4_0_01
```

4. Configure routing options static route and next hop.

```
user@router1# set routing-options static route 192.168.0.0/16 next-hop ms-4/0/0.1
```

Results

From the configuration mode of Router 1, confirm your configuration by entering the **show interfaces**, **show services ipsec-vpn**, and **show services service-set** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces
ms-4/0/0{
   unit 0 {
      family inet;
   }
   unit 1 {
      family inet;
      family inet6;
      service-domain inside;
   }
   unit 2 {
      family inet;
      family inet6;
      service-domain outside;
   }
}
xe-0/2/0 {
   unit 0 {
      family inet {
         address 10.0.1.1/30;
      }
   }
}
```

```
user@router1# show services ipsec-vpn
rule vpn_rule_ms_4_0_01 {
   term term11 {
```

```
        from {
            source-address {
                172.16.0.0/16;
            }
            destination-address {
                192.168.0.0/16;
            }
        }
        then {
            remote-gateway 10.0.1.2;
            dynamic {
                ike-policy ike_policy_ms_4_0_0;
                ipsec-policy ipsec_policy_ms_4_0_0;
            }
            anti-replay-window-size 4096;
        }
    }
    match-direction input;
}
    ipsec {
        proposal ipsec_proposal_ms_4_0_0 {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
        }
        policy ipsec_policy_ms_4_0_0 {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec_proposal_ms_4_0_0;
        }
    }
    ike {
        proposal ike_proposal_ms_4_0_0 {
            authentication-method pre-shared-keys;
            dh-group group2;
        }
        policy ike_policy_ms_4_0_0 {
            version 2;
            proposals ike_proposal_ms_4_0_0;
            pre-shared-key ascii-text "$9ABC123"; ## SECRET-DATA
        }
    }
```

```
user@router1# show services service-set
ipsec_ss_ms_4_0_01 {
    next-hop-service {
        inside-service-interface ms-4/0/0.1;
        outside-service-interface ms-4/0/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.0.1.1;
    }
    ipsec-vpn-rules vpn_rule_ms_4_0_01;
}
```

Configuring Router 2

Step-by-Step Procedure

1. Configure the interface properties such as family, service-domain, and unit.

```
user@router2# set interfaces ms-1/0/0 services-options inactivity-non-tcp-timeout 600
user@router2# set interfaces ms-1/0/0 unit 0 family inet
user@router2# set interfaces ms-1/0/0 unit 1 family inet
user@router2# set interfaces ms-1/0/0 unit 1 family inet6
user@router2# set interfaces ms-1/0/0 unit 1 service-domain inside
user@router2# set interfaces ms-1/0/0 unit 2 family inet
user@router2# set interfaces ms-1/0/0 unit 2 family inet6
user@router2# set interfaces ms-1/0/0 unit 2 service-domain outside
user@router2# set interfaces ge-2/0/0 unit 0 family inet adddress 10.0.1.2/30
```

2. Configure IPsec properties such as address, remote-gateway, policies, match-direction, protocol, replay window size, algorithm details, secrecy keys, proposal, authentication method, groups, and version.

```
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from source-address
    192.168.0.0/16
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 from destination-address
    172.16.0.0/16
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then remote-gateway 10.0.1.1
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ike-policy
    ike_policy_ms_5_2_0
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then dynamic ipsec-policy
    ipsec_policy_ms_5_2_0
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 term term11 then anti-replay-window-size
    4096
user@router2# set services ipsec-vpn rule vpn_rule_ms_5_2_01 match-direction input
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 protocol esp
```

```
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 authentication-algorithm
  hmac-sha1-96
user@router2# set services ipsec-vpn ipsec proposal ipsec_proposal_ms_5_2_0 encryption-algorithm 3des-cbc
user@router2# set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 perfect-forward-secrecy keys
  group2
user@router2# set services ipsec-vpn ipsec policy ipsec_policy_ms_5_2_0 proposals ipsec_proposal_ms_5_2_0
user@router2# set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 authentication-method
  pre-shared-keys
user@router2# set services ipsec-vpn ike proposal ike_proposal_ms_5_2_0 dh-group group2
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 version 2
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 proposals ike_proposal_ms_5_2_0
user@router2# set services ipsec-vpn ike policy ike_policy_ms_5_2_0 pre-shared-key ascii-text "$ABC123"
user@router2# set services ipsec-vpn establish-tunnels immediately
```

3. Configure a service set such as next-hop-service, and the ipsec-vpn-options.

```
user@router2# set services service-set ipsec_ss_ms_5_2_01 next-hop-service inside-service-interface
  ms-1/0/0.1
user@router2# set services service-set ipsec_ss_ms_5_2_01 next-hop-service outside-service-interface
  ms-1/0/0.2
user@router2# set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-options local-gateway 10.0.1.2
user@router2# set services service-set ipsec_ss_ms_5_2_01 ipsec-vpn-rules vpn_rule_ms_5_2_01
```

4. Configure routing options static route and the next hop.

```
user@router2# set routing-options static route 172.16.0.0/16 next-hop ms-1/0/0.1
```

Results

From the configuration mode of Router 2, confirm your configuration by entering the **show interfaces**, **show services ipsec-vpn**, and **show services service-set** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router2# show interfaces
ms-1/0/0 {
    unit 0 {
        family inet;
    }
    unit 1 {
        family inet;
        family inet6;
```

```
        service-domain inside;
    }
    unit 2 {
        family inet;
        family inet6;
        service-domain outside;
    }
}
ge-2/0/0 {
    unit 0 {
        family inet {
            address 10.0.1.2/30;
        }
    }
}
```

```
user@router2# show services ipsec-vpn
rule vpn_rule_ms_5_2_01 {
    term term11 {
        from {
            source-address {
                192.168.0.0/16;
            }
            destination-address {
                172.16.0.0/16;
            }
        }
        then {
            remote-gateway 10.0.1.1;
            dynamic {
                ike-policy ike_policy_ms_5_2_0;
                ipsec-policy ipsec_policy_ms_5_2_0;
            }
            anti-replay-window-size 4096;
        }
    }
    match-direction input;
}
    ipsec {
        proposal ipsec_proposal_ms_5_2_0 {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
        }
```

```
        policy ipsec_policy_ms_5_2_0 {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec_proposal_ms_5_2_0;
        }
    }
    ike {
        proposal ike_proposal_ms_5_2_0 {
            authentication-method pre-shared-keys;
            dh-group group2;
        }
        policy ike_policy_ms_5_2_0 {
            version 2;
            proposals ike_proposal_ms_5_2_0;
            pre-shared-key ascii-text "$9ABC123"; ## SECRET-DATA
        }
    }
establish-tunnels immediately;
```

```
user@router2# show services service-set
ipsec_ss_ms_5_2_01 {
    next-hop-service {
        inside-service-interface ms-1/0/0.1;
        outside-service-interface ms-1/0/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.0.1.2;
    }
    ipsec-vpn-rules vpn_rule_ms_5_2_01;
}
```

```
user@router2 #show routing-options
static {
    route 172.16.0.0/16 next-hop ms-1/0/0.1;
}
```

Verification

IN THIS SECTION

Verifying Tunnel Creation

Purpose

Verify that Dynamic End Points are created.

Action

Run the following command on Router 1:

`user@router1 >`**show services ipsec-vpn ipsec security-associations detail**

```
Service set: ipsec_ss_ms_4_0_01, IKE Routing-instance: default

  Rule: vpn_rule_ms_4_0_01, Term: term11, Tunnel index: 1
  Local gateway: 10.0.1.1, Remote gateway: 10.0.1.2
  IPSec inside interface: ms-4/0/0.1, Tunnel MTU: 1500
  Local identity: ipv4_subnet(any:0,[0..7]=172.16.0.0/16)
  Remote identity: ipv4_subnet(any:0,[0..7]=192.168.0.0/16)

    Direction: inbound, SPI: 112014862, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 24556 seconds
    Hard lifetime: Expires in 25130 seconds
    Anti-replay service: Enabled, Replay window size: 4096

    Direction: outbound, SPI: 1469281276, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 24556 seconds
    Hard lifetime: Expires in 25130 seconds
    Anti-replay service: Enabled, Replay window size: 4096
```

Meaning

The output shows that the IPSec SAs are up on the router with their state as Installed. The IPSec tunnel is up and ready to send traffic over the tunnel.

Verifying Traffic Flow Through the DEP Tunnel

Purpose

Verify traffic flow across the newly-created DEP tunnel.

Action

Run the following command on Router 2:

```
user@router2> show services ipsec-vpn ipsec statistics
```

```
PIC: ms-1/0/0, Service set: ipsec_ss_ms_5_2_01

ESP Statistics:
  Encrypted bytes:           153328
  Decrypted bytes:           131424
  Encrypted packets:           2738
  Decrypted packets:           2738
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

Verifying IPsec Security Associations for the Service Set

Purpose

Verify that the security associations configured for the service set are functioning correctly.

Action

Run the following command on Router 2:

```
user@router2> show services ipsec-vpn ipsec security-associations ipsec_ss_ms_5_2_01
```

```
Service set: ipsec_ss_ms_5_2_01, IKE Routing-instance: default

  Rule: vpn_rule_ms_5_2_01, Term: term11, Tunnel index: 1
  Local gateway: 10.0.1.2., Remote gateway: 10.0.1.1
  IPSec inside interface: ms-1/0/0.1, Tunnel MTU: 1500
    Direction SPI         AUX-SPI     Mode       Type     Protocol
    inbound   1612447024  0           tunnel     dynamic  ESP
    outbound  1824720964  0           tunnel     dynamic  ESP
```

Example: Configuring a Route-based IPSec Tunnel from an ACX device to an SRX device

IN THIS SECTION

This example shows how to configure a route-based IPsec tunnel on ACX devices, and contains the following sections:

Requirements

This example uses the following hardware and software components:

- ACX1100-AC router
- SRX Series device
- Junos OS Release 15.1X54-D50 and later.

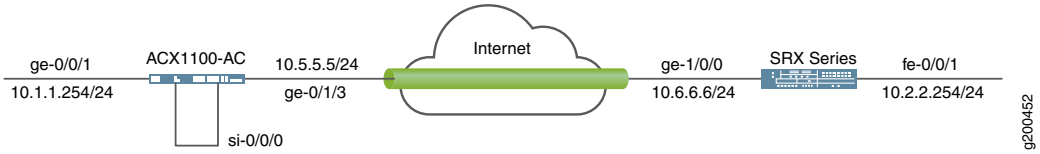
Overview

Junos OS enables you to configure route-based IPsec tunnel between two private networks. In this example, you configure a route-based IPsec tunnel between two private networks with ACX1100-AC router on one end and a SRX Series device on the other end. This example only describes the required CLI configurations for configuring IPsec tunnel on an ACX1100-AC router.

For configuring IPsec tunnel on a SRX Series device, see Example: Configuring a Route-Based VPN and VPN User Guide for Security Devices.

Figure 36 on page 738 shows an example of a route-based IPsec tunnel topology.

Figure 36: Route-based IPsec Tunnel Topology



Configuration

IN THIS SECTION

- Configure IPsec Tunnel on ACX1100-AC Router. | **738**

Configure IPsec Tunnel on ACX1100-AC Router.

CLI Quick Configuration

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

```
set chassis fpc 0 pic 0 tunnel-services bandwidth 1g
set chassis fpc 0 service-package bundle-nat-ipsec
set interfaces si-0/0/0 unit 0 family inet
set interfaces si-0/0/0 unit 1 family inet
set interfaces si-0/0/0 unit 1 service-domain inside
set interfaces si-0/0/0 unit 2 family inet
```

```
set interfaces si-0/0/0 unit 2 service-domain outside
set services ipsec-vpn ike proposal ike_standard authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_standard dh-group group2
set services ipsec-vpn ike proposal ike_standard authentication-algorithm sha1
set services ipsec-vpn ike proposal ike_standard encryption-algorithm 3des-cbc
set services ipsec-vpn ike proposal ike_standard lifetime-seconds 3600
set services ipsec-vpn ike policy CORE_policy proposals ike_standard
set services ipsec-vpn ike policy CORE_policy pre-shared-key ascii-text "$9$0xJZ1EyM87s2alK2aZU.mO1R"
set services ipsec-vpn ipsec proposal ipsec_standard protocol esp
set services ipsec-vpn ipsec proposal ipsec_standard authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec_standard encryption-algorithm aes-128-cbc
set services ipsec-vpn ipsec proposal ipsec_standard lifetime-seconds 600
set services ipsec-vpn ipsec policy ipsec_standard perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec policy ipsec_standard proposals ipsec_standard
set services service-set ss-rule-1 next-hop-service inside-service-interface si-0/0/0.1
set services service-set ss-rule-1 next-hop-service outside-service-interface si-0/0/0.2
set services service-set ss-rule-1 ipsec-vpn-options local-gateway 10.5.5.5
set services service-set ss-rule-1 ipsec-vpn-rules ipsec-rule-1
set services ipsec-vpn rule ipsec-rule-1 term 1 from source-address 0.0.0.0/0
set services ipsec-vpn rule ipsec-rule-1 term 1 from destination-address 0.0.0.0/0
set services ipsec-vpn rule ipsec-rule-1 term 1 then remote-gateway 10.6.6.6
set services ipsec-vpn rule ipsec-rule-1 term 1 then dynamic ike-policy CORE_policy
set services ipsec-vpn rule ipsec-rule-1 term 1 then dynamic ipsec-policy ipsec_standard
set services ipsec-vpn rule ipsec-rule-1 match-direction input
set services ipsec-vpn establish-tunnels immediately
set routing-options static route 10.2.2.0/24 next-hop si-0/0/0.1
set interfaces ge-0/0/0 description Unused
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.254/24
set interfaces ge-0/1/0 description Unused
set interfaces ge-0/1/1 description Unused
set interfaces ge-0/1/2 description Unused
set interfaces ge-0/1/3 description to_Internet
set interfaces ge-0/1/3 mtu 1514
set interfaces ge-0/1/3 unit 0 family inet address 10.5.5.5/24
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure IPsec tunnel on an ACX1100-AC router, you need to:

1. Create and configure a service interface.

```
[edit ]
```

```
user@host# set chassis fpc 0 pic 0 tunnel-services bandwidth 1g
user@host# set chassis fpc 0 service-package bundle-nat-ipsec
user@host# set interfaces si-0/0/0 unit 0 family inet
user@host# set interfaces si-0/0/0 unit 1 family inet
user@host# set interfaces si-0/0/0 unit 1 service-domain inside
user@host# set interfaces si-0/0/0 unit 2 family inet
user@host# set interfaces si-0/0/0 unit 2 service-domain outside
```

2. Create IPsec and IKE security associations.

```
[edit ]
user@host# set services ipsec-vpn ike proposal ike_standard authentication-method pre-shared-keys
user@host# set services ipsec-vpn ike proposal ike_standard dh-group group2
user@host# set services ipsec-vpn ike proposal ike_standard authentication-algorithm sha1
user@host# set services ipsec-vpn ike proposal ike_standard encryption-algorithm 3des-cbc
user@host# set services ipsec-vpn ike proposal ike_standard lifetime-seconds 3600
user@host# set services ipsec-vpn ike policy CORE_policy proposals ike_standard
user@host# set services ipsec-vpn ike policy CORE_policy pre-shared-key ascii-text
   "$9$0xJZ1EyM87s2alK2aZU.mO1R"
user@host# set services ipsec-vpn ipsec proposal ipsec_standard protocol esp
user@host# set services ipsec-vpn ipsec proposal ipsec_standard authentication-algorithm hmac-sha1-96
user@host# set services ipsec-vpn ipsec proposal ipsec_standard encryption-algorithm aes-128-cbc
user@host# set services ipsec-vpn ipsec proposal ipsec_standard lifetime-seconds 600
user@host# set services ipsec-vpn ipsec policy ipsec_standard perfect-forward-secrecy keys group2
user@host# set services ipsec-vpn ipsec policy ipsec_standard proposals ipsec_standard
```

3. Create a service set to define a selected traffic.

```
[edit ]
user@host# set services service-set ss-rule-1 next-hop-service inside-service-interface si-0/0/0.1
user@host# set services service-set ss-rule-1 next-hop-service outside-service-interface si-0/0/0.2
user@host# set services service-set ss-rule-1 ipsec-vpn-options local-gateway 10.5.5.5
user@host# set services service-set ss-rule-1 ipsec-vpn-rules ipsec-rule-1
user@host# set services ipsec-vpn rule ipsec-rule-1 term 1 from source-address 0.0.0.0/0
user@host# set services ipsec-vpn rule ipsec-rule-1 term 1 from destination-address 0.0.0.0/0
user@host# set services ipsec-vpn rule ipsec-rule-1 term 1 then remote-gateway 10.6.6.6
user@host# set services ipsec-vpn rule ipsec-rule-1 term 1 then dynamic ike-policy CORE_policy
user@host# set services ipsec-vpn rule ipsec-rule-1 term 1 then dynamic ipsec-policy ipsec_standard
user@host# set services ipsec-vpn rule ipsec-rule-1 match-direction input
user@host# set services ipsec-vpn establish-tunnels immediately
```

4. Establish routes to send traffic to a service plane.

```
[edit ]
user@host# set routing-options static route 10.2.2.0/24 next-hop si-0/0/0.1
```

5. Create network interfaces.

```
[edit ]
user@host# set interfaces ge-0/0/0 description Unused
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.254/24
user@host# set interfaces ge-0/1/0 description Unused
user@host# set interfaces ge-0/1/1 description Unused
user@host# set interfaces ge-0/1/2 description Unused
user@host# set interfaces ge-0/1/3 description to_Internet
user@host# set interfaces ge-0/1/3 mtu 1514
user@host# set interfaces ge-0/1/3 unit 0 family inet address 10.5.5.5/24
```

6. Commit the configuration.

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

RELATED DOCUMENTATION

- IPsec for ACX Series Overview | 635
- Configuring Security Associations | 639
- Configuring IPsec Proposals | 680
- Configuring IKE Proposals | 665
- Service Sets | 697
- Configuring IPsec Service Sets | 698

CHAPTER 36

Enhancing Security with Static IPSec over VRF

IN THIS CHAPTER

Example: Configuring Statically Assigned IPsec Tunnels over a VRF Instance

IN THIS SECTION

This example shows how to configure a statically assigned IPsec tunnel over a VRF instance, and contains the following sections:

Requirements

This example uses the following hardware and software components:

- M Series, MX Series, or T Series router that is configured as a provider edge router.
- Junos OS Release 9.4 and later.

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Junos OS enables you to configure statically assigned IPsec tunnels on Virtual Routing and Forwarding (VRF) instances. Ability to configure IPsec tunnels on VRF instances enhances network segmentation and

security. You can have multiple customer tunnels configured on the same PE router over VRF instances. Each VRF instance acts as logical router with an exclusive routing table.

Configuration

IN THIS SECTION

This example shows the configuration of an IPsec tunnel over a VRF instance on a provider edge router, and provides step-by-step instructions for completing the required configuration.

This section contains:

Configuring the Provider Edge Router

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-0/3/0 unit 0 family inet address 10.6.6.6/32
set interfaces ge-1/1/0 description "teller ge-0/1/0"
set interfaces ge-1/1/0 unit 0 family inet address 10.21.1.1/16
set interfaces ms-1/2/0 unit 0 family inet address 10.7.7.7/32
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set policy-options policy-statement vpn-export then community add vpn-community
set policy-options policy-statement vpn-export then accept
set policy-options policy-statement vpn-import term a from community vpn-community
set policy-options policy-statement vpn-import term a then accept
set policy-options community vpn-community members target:100:20
set routing-instances vrf instance-type vrf
set routing-instances vrf interface ge-0/3/0.0
set routing-instances vrf interface ms-1/2/0.1
set routing-instances vrf route-distinguisher 192.168.0.1:1
set routing-instances vrf vrf-import vpn-import
set routing-instances vrf vrf-export vpn-export
```

```
set routing-instances vrf routing-options static route 10.0.0.0/0 next-hop ge-0/3/0.0
set routing-instances vrf routing-options static route 10.11.11.1/32 next-hop ge-0/3/0.0
set routing-instances vrf routing-options static route 10.8.8.1/32 next-hop ms-1/2/0.1
set services ipsec-vpn ipsec proposal demo_ipsec_proposal protocol esp
set services ipsec-vpn ipsec proposal demo_ipsec_proposal authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal demo_ipsec_proposal encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy demo_ipsec_policy perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec policy demo_ipsec_policy proposals demo_ipsec_proposal
set services ipsec-vpn ike proposal demo_ike_proposal authentication-method pre-shared-keys
set services ipsec-vpn ike proposal demo_ike_proposal dh-group group2
set services ipsec-vpn ike policy demo_ike_policy proposals demo_ike_proposal
set services ipsec-vpn ike policy demo_ike_policy pre-shared-key ascii-text juniperkey
set services ipsec-vpn rule demo-rule term demo-term then remote-gateway 10.21.2.1
set services ipsec-vpn rule demo-rule term demo-term then dynamic ike-policy demo_ike_policy
set services ipsec-vpn rule demo-rule match-direction input
set services service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-service-set ipsec-vpn-options local-gateway 10.21.1.1
set services service-set demo-service-set ipsec-vpn-rules demo-rule
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure a statically assigned IPsec tunnel on a VRF instance:

1. Configure the interfaces. In this step, you configure two Ethernet (**ge**) interfaces, one services interface (**ms-**), and also the service-domain properties for the logical interfaces of the services interface. Note that the logical interface that is marked as the inside interface applies the configured service on the traffic, whereas the one that is marked as the outside interface acts as the egress point for the traffic on which the inside interface has applied the service.

```
[edit interfaces]
user@PE1# set ge-0/3/0 unit 0 family inet address 10.6.6.6/32
user@PE1# set ge-1/1/0 description "teller ge-0/1/0"
user@PE1# set ge-1/1/0 unit 0 family inet address 10.21.1.1/16
user@PE1# set ms-1/2/0 unit 0 family inet address 10.7.7.7/32
user@PE1# set ms-1/2/0 unit 1 family inet
user@PE1# set ms-1/2/0 unit 1 service-domain inside
user@PE1# set ms-1/2/0 unit 2 family inet
user@PE1# set ms-1/2/0 unit 2 service-domain outside
```

2. Configure a routing policy to specify route import and export criteria for the VRF instance. The import and export policies defined in this step are referenced from the routing-instance configuration in the next step.

```
[edit policy-options]
user@PE1# set policy-statement vpn-export then community add vpn-community
user@PE1# set policy-statement vpn-export then accept
user@PE1# set policy-statement vpn-import term a from community vpn-community
user@PE1# set policy-statement vpn-import term a then accept
user@PE1# set community vpn-community members target:100:20
```

3. Configure a routing instance and specify the routing-instance type as **vrf**. Apply the import and export policies defined in the previous step to the routing instance, and specify a static route to send the IPsec traffic to the inside interface (**ms-1/2/0.1**) configured in the first step.

```
[edit routing-instance]
user@PE1# set vrf instance-type vrf
user@PE1# set vrf interface ge-0/3/0.0
user@PE1# set vrf interface ms-1/2/0.1
user@PE1# set vrf route-distinguisher 192.168.0.1:1
user@PE1# set vrf vrf-import vpn-import
user@PE1# set vrf vrf-export vpn-export
user@PE1# set vrf routing-options static route 10.0.0.0/0 next-hop ge-0/3/0.0
user@PE1# set vrf routing-options static route 10.11.11.1/32 next-hop ge-0/3/0.0
user@PE1# set vrf routing-options static route 10.8.8.1/32 next-hop ms-1/2/0.1
```

4. Configure IKE and IPsec proposals and policies, and a rule to apply the IKE policy on the incoming traffic..

> **NOTE:** By default, Junos OS uses IKE policy version 1.0. Junos OS Release 11.4 and later also support IKE policy version 2.0 which you must configure at **[edit services ipsec-vpn ike policy policy-name pre-shared]**.

```
[edit services]
user@PE1# set ipsec-vpn ipsec proposal demo_ipsec_proposal protocol esp
user@PE1# set ipsec-vpn ipsec proposal demo_ipsec_proposal authentication-algorithm hmac-sha1-96
user@PE1# set ipsec-vpn ipsec proposal demo_ipsec_proposal encryption-algorithm 3des-cbc
user@PE1# set ipsec-vpn ipsec policy demo_ipsec_policy perfect-forward-secrecy keys group2
user@PE1# set ipsec-vpn ipsec policy demo_ipsec_policy proposals demo_ipsec_proposal
```

```
user@PE1# set ipsec-vpn ike proposal demo_ike_proposal authentication-method pre-shared-keys
user@PE1# set ipsec-vpn ike proposal demo_ike_proposal dh-group group2
user@PE1# set ipsec-vpn ike policy demo_ike_policy proposals demo_ike_proposal
user@PE1# set ipsec-vpn ike policy demo_ike_policy pre-shared-key ascii-text juniperkey
user@PE1# set ipsec-vpn rule demo-rule term demo-term then remote-gateway 10.21.2.1
user@PE1# set ipsec-vpn rule demo-rule term demo-term then dynamic ike-policy demo_ike_policy
user@PE1# set ipsec-vpn rule demo-rule match-direction input
```

5. Configure a next-hop style service set. Note that you must configure the inside and outside interfaces that you configured in the first step as the **inside-service-interface** and **outside-service-interface** respectively.

```
[edit services]
user@PE1# set service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
user@PE1# set service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
user@PE1# set service-set demo-service-set ipsec-vpn-options local-gateway 10.21.1.1
user@PE1# set service-set demo-service-set ipsec-vpn-rules demo-rule
```

6. Commit the configuration.

```
[edit]
user@PE1# commit
```

Results

From the configuration mode of Router 1, confirm your configuration by entering the **show interfaces**, **show policy-options**, **show routing-instances**, **show services ipsec-vpn**, and **show services service-set** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show interfaces
...
    ms-1/2/0 {
        unit 0 {
            family inet {
                address 10.7.7.7/32;
            }
        }
        unit 1 {
            family inet;
```

```
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
    }
    ge-0/3/0 {
        unit 0 {
            family inet {
                address 10.6.6.6/32;
            }
        }
    }
    ge-1/1/0 {
        description "teller ge-0/1/0";
        unit 0 {
            family inet {
                address 10.21.1.1/16;
            }
        }
    }
...
```

```
user@PE1# show policy-options
    policy-statement vpn-export {
        then {
            community add vpn-community;
            accept;
        }
    }
    policy-statement vpn-import {
        term a {
            from community vpn-community;
            then accept;
        }
    }
    community vpn-community members target:100:20;
```

```
user@PE1# show routing-instances
vrf {
    instance-type vrf;
    interface ge-0/3/0.0;
```

```
    interface ms-1/2/0.1;
    route-distinguisher 192.168.0.1:1;
    vrf-import vpn-import;
    vrf-export vpn-export;
    routing-options {
        static {
            route 10.0.0.0/0 next-hop ge-0/3/0.0;
            route 10.11.11.1/32 next-hop ge-0/3/0.0;
            route 10.8.8.1/32 next-hop ms-1/2/0.1;
        }
    }
}
```

```
user@PE1# show services ipsec-vpn
ipsec-vpn {
    rule demo-rule {
        term demo-term {
            then {
                remote-gateway 10.21.2.1;
                dynamic {
                    ike-policy demo_ike_policy;
                }
            }
        }
        match-direction input;
    }
    ipsec {
        proposal demo_ipsec_proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
        }
        policy demo_ipsec_policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals demo_ipsec_proposal;
        }
    }
    ike {
        proposal demo_ike_proposal {
            authentication-method pre-shared-keys;
            dh-group group2;
        }
```

```
        policy demo_ike_policy {
            proposals demo_ike_proposal;
            pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
        }
    }
}
```

```
user@PE1# show services service-set demo-service-set
    next-hop-service {
        inside-service-interface ms-1/2/0.1;
        outside-service-interface ms-1/2/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.21.1.1;
    }
    ipsec-vpn-rules demo-rule;
```

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | 618
- Configuring Security Associations | 639
- Configuring IPsec Proposals | 680
- Configuring IKE Proposals | 665

CHAPTER 37

Dynamically Assigning Tunnels Using Junos VPN Site Secure

IN THIS CHAPTER

Configuring Dynamic Endpoints for IPsec Tunnels

IPsec tunnels can also be established using *dynamic peer* security gateways, in which the remote ends of tunnels do not have a statically assigned IP address. Since the remote address is not known and might be pulled from an address pool each time the remote host reboots, establishment of the tunnel relies on using IKE **main** mode with either preshared global keys or digital certificates that accept any remote identification value. Both policy-based and link-type tunnels are supported:

- Policy-based tunnels used shared mode.
- Link-type or routed tunnels use dedicated mode. Each tunnel allocates a services interface from a pool of interfaces configured for the dynamic peers. Routing protocols can be configured to run on these services interfaces to learn routes over the IPsec tunnel that is used as a link in this scenario.

This section includes the following topics:

Authentication Process

The remote (dynamic peer) initiates the negotiations with the local (Juniper Networks) router. The local router uses the default IKE and IPsec policies to match the proposals sent by the remote peer to negotiate the security association (SA) values. Implicit proposals contain a list of all the supported transforms that the local router expects from all the dynamic peers.

If preshared key authentication is used, the preshared key is global for a service set. When seeking the preshared key for the peer, the local router matches the peer's source address against any explicitly configured preshared keys in that service set. If a match is not found, the local router uses the global preshared key for authentication.

Phase 2 of the authentication matches the *proxy identities* of the protected hosts and networks sent by the peer against a list of configured proxy identities. The accepted proxy identity is used to create the dynamic rules for encrypting the traffic. You can configure proxy identities by including the **allowed-proxy-pair** statement in the IKE access profile. If no entry matches, the negotiation is rejected.

If you do not configure the **allowed-proxy-pair** statement, the default value **ANY(0.0.0.0/0)-ANY** is applied, and the local router accepts any proxy identities sent by the peer. Both IPv4 and IPv6 addresses are accepted, but you must configure all IPv6 addresses manually.

Once the phase 2 negotiation completes successfully, the router builds the dynamic rules and inserts the reverse route into the routing table using the accepted proxy identity.

Implicit Dynamic Rules

After successful negotiation with the dynamic peer, the key management process (kmd) creates a dynamic rule for the accepted phase 2 proxy and applies it on the local AS or Multiservices PIC. The source and destination addresses are specified by the accepted proxy. This rule is used to encrypt traffic directed to one of the end hosts in the phase 2 proxy identity.

The dynamic rule includes an **ipsec-inside-interface** value, which is the interface name assigned to the dynamic tunnel. The **source-address** and **destination-address** values are accepted from the proxy ID. The **match-direction** value is **input** for next-hop-style service sets.

> **NOTE:** You do not configure this rule; it is created by the key management process (kmd).

Rule lookup for static tunnels is unaffected by the presence of a dynamic rule; it is performed in the order configured. When a packet is received for a service set, static rules are always matched first.

Dynamic rules are matched after the rule match for static rules has failed.

Response to dead peer detection (DPD) hello messages takes place the same way with dynamic peers as with static peers. Initiating DPD hello messages from dynamic peers is not supported.

Reverse Route Insertion

Static routes are automatically inserted into the route table for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created based on the remote proxy network and mask sent by the peer and is inserted in the relevant route table after successful phase 1 and phase 2 negotiations.

The route preference for each static reverse route is 1. This value is necessary to avoid conflict with similar routes that might be added by the routing protocol process (rpd).

No routes are added if the accepted remote proxy address is the default (**0.0.0.0/0**). In this case you can run routing protocols over the IPsec tunnel to learn routes and add static routes for the traffic you want to be protected over this tunnel.

For next-hop-style service sets, the reverse routes include next hops pointing to the locations specified by the **inside-service-interface** statement.

The route table in which to insert these routes depends on where the **inside-service-interface** location is listed. If these interfaces are present in a VPN routing and forwarding (VRF) instance, then routes are added to the corresponding VRF table; otherwise, the routes are added to **inet.0**.

> **NOTE:** Reverse route insertion takes place only for tunnels to dynamic peers. These routes are added only for next-hop-style service sets.

Configuring an IKE Access Profile

You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set. Alternatively, you can include the **ike-policy** statement to reference an IKE policy you define with either specific identification values or a wildcard (the **any-remote-id** option). You configure the IKE policy at the **[edit services ipsec-vpn ike]** hierarchy level.

The IKE tunnel profile specifies all the information needed to complete the IKE negotiation. Each protocol has its own statement hierarchy within the client statement to configure protocol-specific attribute value pairs, but only one client configuration is allowed for each profile. The following is the configuration at the **[edit access]** hierarchy level; for more information on access profiles, see the *Junos OS Administration Library*.

```
[edit access]
profile profile-name {
    client * {
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text key-string | hexadecimal key-string);
            ike-policy policy-name;
            interface-id <string-value>;
            ipsec-policy ipsec-policy;
        }
    }
}
```

NOTE: For dynamic peers, the Junos OS supports the IKE main mode with either the preshared key method of authentication or an IKE access profile that uses a local digital certificate.

- In preshared key mode, the IP address is used to identify a tunnel peer to get the preshared key information. The **client** value * (wildcard) means that configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.
- In digital certificate mode, the IKE policy defines which remote identification values are allowed.

The following statements make up the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer's network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

  By default, **remote 0.0.0.0/0 local 0.0.0.0/0** is used if no values are configured. Both IPv4 and IPv6 address formats are supported in this configuration, but there are no default IPv6 addresses. You must specify even **0::0/0**.

- **pre-shared-key**—Key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key is known to both ends through an out-of-band secure mechanism. You can configure the value either in **hexadecimal** or **ascii-text** format. It is a mandatory value.

- **ike-policy**—Policy that defines the remote identification values corresponding to the allowed dynamic peers; can contain a wildcard value **any-remote-id** for use in dynamic endpoint configurations only.

- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical services interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Referencing the IKE Access Profile in a Service Set

To complete the configuration, you need to reference the IKE access profile configured at the **[edit access]** hierarchy level. To do this, include the **ike-access-profile** statement at the **[edit services service-set *name* ipsec-vpn-options]** hierarchy level:

```
[edit services service-set name]
ipsec-vpn-options {
    local-gateway address;
    ike-access-profile profile-name;
}
next-hop-service {
    inside-service-interface interface-name;
    outside-service-interface interface-name;
}
```

The **ike-access-profile** statement must reference the same name as the **profile** statement you configured for IKE access at the **[edit access]** hierarchy level. You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.

All interfaces referenced by the **inside-service-interface** statement within a service set must belong to the same VRF instance.

Configuring the Interface Identifier

You can configure an interface identifier for a group of dynamic peers, which specifies which adaptive services logical interface(s) take part in the dynamic IPsec negotiation. By assigning the same interface identifier to multiple logical interfaces, you can create a pool of interfaces for this purpose. To configure an interface identifier, include the **ipsec-interface-id** statement and the **dedicated** or **shared** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* dial-options]** hierarchy level:

```
[edit interfaces interface-name unit logical-unit-number dial-options]
ipsec-interface-id identifier;
(dedicated | shared);
```

Specifying the interface identifier in the **dial-options** statement makes this logical interface part of the pool identified by the **ipsec-interface-id** statement.

> **NOTE:** Only one interface identifier can be specified at a time. You can include the **ipsec-interface-id** statement or the **l2tp-interface-id** statement, but not both.

If you configure **shared** mode, it enables one logical interface to be shared across multiple tunnels. The **dedicated** statement specifies that the logical interface is used in a dedicated mode, which is necessary when you are configuring an IPsec link-type tunnel. You must include the **dedicated** statement when you specify an **ipsec-interface-id** value.

Default IKE and IPsec Proposals

The software includes implicit default IKE and IPsec proposals to match the proposals sent by the dynamic peers. The values are shown in Table 27 on page 755; if more than one value is shown, the first value is the default.

> **NOTE:** RSA certificates are not supported with dynamic endpoint configuration.

Table 27: Default IKE and IPsec Proposals for Dynamic Negotiations

Statement Name	Values
Implicit IKE Proposal	
authentication-method	**pre-shared keys**
dh-group	**group1**, **group2**, **group5**, **group14**
authentication-algorithm	**sha1**, **md5**, **sha-256**
encryption-algorithm	**3des-cbc**, **des-cbc**, **aes-128**, **aes-192**, **aes-256**
lifetime-seconds	**3600** seconds
Implicit IPsec Proposal	
protocol	**esp**, **ah**, **bundle**
authentication-algorithm	**hmac-sha1-96**, **hmac-md5-96**

Table 27: Default IKE and IPsec Proposals for Dynamic Negotiations *(continued)*

Statement Name	Values
encryption-algorithm	**3des-cbc**, **des-cbc**, **aes-128**, **aes-192**, **aes-256**
lifetime-seconds	**28,800** seconds (8 hours)

Distributing Endpoint IPsec Tunnels Among Services Interfaces

Starting in Junos OS Release 16.2R1, you can distribute IPsec tunnels with dynamic endpoints among multiple MS-MICs or among multiple service PICs of an MS-MPC. You configure tunnel distribution by configuring a next-hop IPsec service set for each service PIC's multiservices (ms-) interface. Starting in Junos OS Release 17.1R1, you can also distribute IPsec tunnels with dynamic endpoints among aggregated multiservices (AMS) interfaces of MS-MICs or MS-MPCs by configuring a next-hop IPsec service set for each AMS interface.

You can later add service PIC hardware to the MX Series router and include the service PIC in the tunnel distribution by simply adding another service set, without needing to change the configuration of the IPsec peers.

To configure tunnel distribution, perform the following steps when configuring dynamic endpoint IPsec tunnels:

- Configure a next-hop IPsec service set for each services interface or AMS interface used by the dynamic endpoint IPsec tunnel (see "Referencing the IKE Access Profile in a Service Set" on page 754). All of the service sets must:
  - Use the same type of services interface—either multiservices (ms-) interfaces or AMS (ams-) interfaces.
  - Have an interface in the **outside-service** statement that is in the same VPN routing and forwarding (VRF) instance as the interfaces in the other service sets.
  - Have the same **local-gateway** IP address.
  - Have the same **ike-access-profile** name.
- When configuring the interface identifier (see "Configuring the Interface Identifier" on page 754), the **ipsec-interface-id *identifier*** must be configured:
  - Only under interfaces that appear in the **inside-service-set** statements of the service sets.
  - With **dedicated** for all the interfaces, or with **shared** for all the interfaces.
  - Under no more than one shared unit of an interface.
  - Only under interfaces configured with **service-domain inside**.
  - Only under interfaces that are in the same VRF.

Release History Table

Release	Description
17.1	Starting in Junos OS Release 17.1R1, you can also distribute IPsec tunnels with dynamic endpoints among aggregated multiservices (AMS) interfaces of MS-MICs or MS-MPCs by configuring a next-hop IPsec service set for each AMS interface.
16.2	Starting in Junos OS Release 16.2R1, you can distribute IPsec tunnels with dynamic endpoints among multiple MS-MICs or among multiple service PICs of an MS-MPC. You configure tunnel distribution by configuring a next-hop IPsec service set for each service PIC's multiservices (ms-) interface.

RELATED DOCUMENTATION

- Configuring IKE Policies | **671**
- Configuring IPsec Rules | **688**
- Configuring IKE Proposals | **665**
- Configuring IPsec Proposals | **680**
- Configuring Security Associations | **639**

Requesting for and Installing a Digital Certificates on Your Router

IN THIS SECTION

A digital certificate is an electronic means for verifying your identity through a trusted third party, known as a certificate authority (CA). Alternatively, you can use a self-signed certificate to attest to your identity. The CA server you use can be owned and operated by an independent CA or by your own organization, in which case you become your own CA. If you use an independent CA, you must contact them for the addresses of their CA and certificate revocation list (CRL) servers (for obtaining certificates and CRLs) and for the information they require when submitting personal certificate requests. When you are your own CA, you determine this information yourself. The Public Key Infrastructure (PKI) provides an infrastructure for digital certificate management.

Requesting a Digital Certificate—Manual Process

To obtain digital certificates manually, you must configure a CA profile, generate a private-public key pair, create a local certificate, and load the certificates on the router. After loading the certificates, they can be referenced in your IPsec-VPN configuration.

This procedure shows how you can configure a CA profile:

1. Configure a CA profile:

```
user@R2# set security pki ca-profile entrust ca-identity entrust enrollment url
  http://ca-1.example.com/cgi-bin/pkiclient.exe
```

   After you commit this configuration. The configuration on Router 2 must contain the following:

```
[edit]
security {
    pki {
        ca-profile entrust {
            ca-identity entrust;
            enrollment {
                url http://ca-1.example.com/cgi-bin/pkiclient.exe;
            }
        }
    }
}
```

2. Certificate revocation list (CRL) verification is enabled by default. You can optionally specify the Lightweight Access Directory (LDAP) server where the CA stores the CRL. The certificate typically includes a certificate distribution point (CDP), which contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically. In this example, the LDAP URL is specified, which overrides the location provided in the certificate:

```
user@R2# set security pki ca-profile entrust revocation-check crl url
  ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase
```

   After you commit this configuration. The configuration on Router 2 must contain the following:

```
[edit]
security pki ca-profile entrust {
    revocation-check {
        crl {
            url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
```

```
    }
  }
}
```

3. After you configure the CA profile, request a CA certificate from the trusted CA. In this example, the certificate is enrolled online and installed into the router automatically.

   `user@R2>` **request security pki ca-certificate enroll ca-profile entrust**

```
Received following certificates:
  Certificate: C=us, O=juniper
    Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

> **NOTE:** If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or website download), you can install it with the **request security pki ca-certificate load** command.

4. Next, you must generate a private-public key pair before you can create a local certificate.

   `user@R2>` **request security pki generate-key-pair certificate-id local-entrust2**

```
Generated key pair local-entrust2, key size 1024 bits
```

   When the key pair is available, generate a local certificate request and send it to the CA for processing.

   `user@R2>` **request security pki generate-certificate-request**

```
certificate-id local-entrust2 domain-name router2.example.com
filename entrust-req2 subject cn=router2.example.com
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
```

```
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ70fO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

NOTE: You can request the creation and installation of a local certificate online with the **request security pki local-certificate enroll** command.

5. The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the router and load the certificate.

   `user@R2>` **request security pki local-certificate load filename /tmp/router2-cert certificate-id local-entrust2**

```
Local certificate local-entrust2 loaded successfully
```

NOTE: The name of the file sent to you by the CA might not match the name of the certificate identifier. However, the **certificate-id** name must always match the name of the key pair you generated for the router.

RELATED DOCUMENTATION

Example: IKE Dynamic SA Configuration with Digital Certificates | **790**

Example: Configuring Dynamically Assigned Policy Based Tunnels

IN THIS SECTION

This example shows how to configure dynamically assigned policy-based tunnels and contains the following sections.

Requirements

This example uses the following hardware and software components:

- Three M Series, MX Series or T Series routers.
- Junos OS Release 9.4 or later.

Overview and Topology

An IPsec policy for dynamic endpoints defines a combination of security parameters (IPsec proposals) used during IPsec negotiation between dynamic peer security gateways, in which the remote ends of tunnels do not have a statically assigned IP address.

A policy based VPN is a configuration with a specific VPN tunnel referenced in a policy which acts as a Tunnel. You use a Policy-based VPN if the remote VPN device is a non-Juniper device and if you must access only one subnet or one network at the remote site, across the VPN.

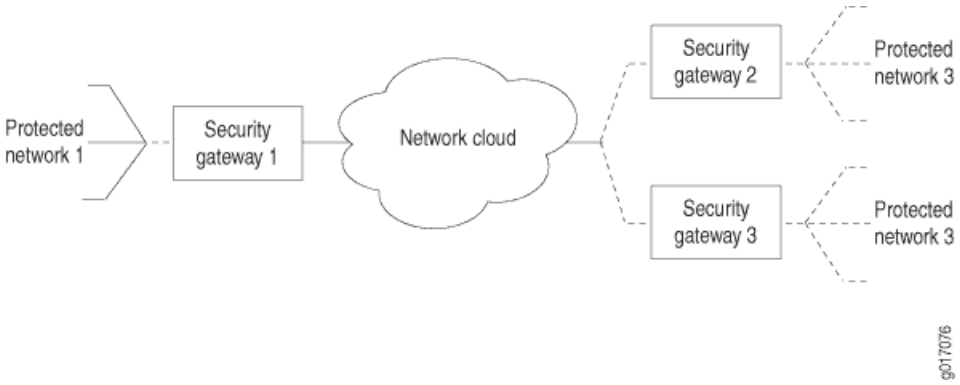
This example explains the IPsec dynamic endpoint tunneling topology as shown in Figure 37 on page 762.

Before you configure dynamically assigned tunnels, be sure you have:

- A local network N-1 connected to a security gateway SG-1. The exit points must have a Juniper Networks router to terminate the static and dynamic peer endpoints. The tunnel termination address on SG-1 is 10.1.1.1 and the local network address is 172.16.1.0/24.
- Two remote peer routers that obtain addresses from an ISP pool and run an RFC-compliant IKE. The remote network N-2 has the address 172.16.2.0/24 and is connected to the security gateway SG-2 with

the tunnel termination address 10.2.2.2. The remote network N-3 has the address 172.16.3.0/24 and is connected to the security gateway SG-3 with the tunnel termination address 10.3.3.3.

Figure 37: IPsec Dynamic Endpoint Tunneling Topology



Configuration

IN THIS SECTION

To configure dynamically assigned policy based tunnels, perform these tasks:

> **NOTE:** The interface types shown in this example are for indicative purpose only. For example, you can use **so-** interfaces instead of **ge-** and **sp-** instead of **ms-**.

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, of SG1 router.

Configuring Interfaces

```
set interfaces ms-0/0/0 unit 0 family inet
set interfaces ms-0/0/0 unit 1 family inet
set interfaces ms-0/0/0 unit 1 service-domain inside
set interfaces ms-0/0/0 unit 1 dial-options ipsec-interface-id demo-ipsec-interface-id
set interfaces ms-0/0/0 unit 1 dial-options mode shared
set interfaces ms-0/0/0 unit 2 family inet
set interfaces ms-0/0/0 unit 2 service-domain outside
```

Configuring Access Profile

```
set access profile demo-access-profile client * ike allowed-proxy-pair remote 172.16.2.0/24 local
  172.16.1.0/24
set access profile demo-access-profile client * ike allowed-proxy-pair remote 172.16.3.0/24 local
  172.16.1.0/24
set access profile demo-access-profile client * ike ascii-text keyfordynamicpeers
set access profile demo-access-profile client * ike interface-id demo-ipsec-interface-id
```

Configuring Service Set

```
set services service-set demo-service-set next-hop-service inside-service-interface ms-0/0/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-0/0/0.2
```

Configuring IPsec Properties

```
set services ipsec-vpn ipsec proposal ipsec_proposal_demo1 protocol esp
set services ipsec-vpn ipsec proposal ipsec_proposal_demo1 authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec_proposal_demo1 encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy demo2 perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec policy demo2 proposals ipsec_proposal_demo1
set services ipsec-vpn ike proposal ike_proposal_demo1 authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike_proposal_demo1 dh-group group2
set services ipsec-vpn ike policy ike_policy_demo1 version 2
set services ipsec-vpn ike policy ike_policy_demo1 proposals ike_proposal_demo1
set services ipsec-vpn ike policy ike_policy_demo1 pre-shared-key ascii-text keyfordemo1
```

Configuring Routing Instances

```
set routing-instances demo-vrf instance-type vrf
set routing-instances demo-vrf ms-0/0/0.1
set routing-instances demo-vrf ms-0/0/0.2
```

Configuring a Next-Hop SG1 Service-Set

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy.

1. Configure the interfaces.

```
[edit interfaces]
user@router1# set interfaces ms-0/0/0 unit 0 family inet
user@router1# set interfaces ms-0/0/0 unit 1 family inet
user@router1# set interfaces ms-0/0/0 unit 1 service-domain inside
user@router1# set interfaces ms-0/0/0 unit 1 dial-options ipsec-interface-id demo-ipsec-interface-id
user@router1# set interfaces ms-0/0/0 unit 1 dial-options mode shared
user@router1# set interfaces ms-0/0/0 unit 2 family inet
user@router1# set interfaces ms-0/0/0 unit 2 service-domain outside
```

2. Configure the access profile.

```
[edit access]
user@router1# set profile demo-access-profile client * ike allowed-proxy-pair remote 172.16.2.0/24 local
   172.16.1.0/24
user@router1# set profile demo-access-profile client * ike ascii-text keyfordynamicpeers
user@router1# set profile demo-access-profile client * ike interface-id demo-ipsec-interface-id
```

3. Configure the services set.

```
[edit services]
user@router1# set service-set demo-service-set next-hop-service inside-service-interface ms-0/0/0.1
user@router1# set service-set demo-service-set next-hop-service outside-service-interface ms-0/0/0.2
```

4. Configure the IPsec properties.

```
[edit services ipsec-vpn]
```

```
user@router1#set ipsec proposal ipsec_proposal_demo1 protocol esp
user@router1#set ipsec proposal ipsec_proposal_demo1 authentication-algorithm hmac-sha1-96
user@router1#set ipsec proposal ipsec_proposal_demo1 encryption-algorithm 3des-cbc
user@router1#set ipsec policy demo2 perfect-forward-secrecy keys group2
user@router1#set ipsec policy demo2 proposals ipsec_proposal_demo1
user@router1#set ike proposal ike_proposal_demo1 authentication-method pre-shared-keys
user@router1#set ike proposal ike_proposal_demo1 dh-group group2
user@router1#set ike policy ike_policy_demo1 version 2
user@router1#set ike policy ike_policy_demo1 proposals ike_proposal_demo1
user@router1#set ike policy ike_policy_demo1 pre-shared-key ascii-text keyfordemo1
```

5. Configure the routing instances.

```
[edit routing-instances]
user@router1# set demo-vrf instance-type vrf
user@router1# set demo-vrf ms-0/0/0.1
user@router1# set demo-vrf ms-0/0/0.2
```

Results

From configuration mode of Router 1, confirm your configuration by entering the **show interfaces**, **show access**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
interfaces {
    ms-0/0/0 {
        unit 0 {
            family inet;
        }
        unit 1 {
            family inet;
            service-domain inside;
            dial-options {
                ipsec-interface-id demo-ipsec-interface-id;
                mode shared;
            }
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
```

```
    }
}
access {
    profile demo-access-profile client * {
        ike {
            allowed-proxy-pair {
                remote 172.16.2.0/24 local 172.16.1.0/24; #Set for Network 2 connected to Network 1
                remote 172.16.3.0/24 local 172.16.1.0/24; #Set for Network 3 connected to Network 1
            }
            pre-shared-key {
                ascii-text keyfordynamicpeers;
            }
            interface-id demo-ipsec-interface-id;
        }
    }
}
services {
    service-set demo-service-set {
        next-hop-service {
            inside-service-interface ms-0/0/0.1;
            outside-service-interface ms-0/0/0.2;
        }
        ipsec-vpn-options {
            local-gateway 1.1.1.1;
            ike-access-profile demo-access-profile;
        }
    }
    ipsec-vpn {
        ipsec {
            proposal ipsec_proposal_demo1 {
                protocol esp;
                authentication-algorithm hmac-sha1-96;
                encryption-algorithm 3des-cbc;
            }
            policy demo2 {
                perfect-forward-secrecy {
                    keys group2;
                }
                proposals ipsec_proposal_demo1;
            }
        }
        ike {
            proposal ike_proposal_demo1 {
                authentication-method pre-shared-keys;
```

```
            dh-group group2;
          }
          policy ike_policy_demo1 {
            version 2;
            proposals ike_proposal_demo1;
            pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
          }
        }
      }
    }
    routing-instances {
      demo-vrf {
        instance-type vrf;
        interface ms-0/0/0.1;
        interface ms-0/0/0.2;
      }
    }
```

Verification

Verifying That the Next-Hop SG1 Service Set with Policy-Based Tunnels Is Created

Purpose

Verify that the next-hop SG1 service set with policy-based tunnels is created.

Action

From operational mode, enter the **show route** command.

`user@router1>` **show route**

```
demo-vrf.inet.0: .... # Routing instance
172.11.0.0/24 *[Static/1]..
 > via ms-0/0/0.1
 172.12.0.0/24 *[Static/1]..
> via ms-0/0/0.1
```

From operational mode, enter the **show services ipsec-vpn ipsec security-associations detail**

`user@router1>`**show services ipsec-vpn ipsec security-associations detail**

```
rule: junos-dynamic-rule-0
term: term-0
```

```
local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
remote-gateway-address: 10.2.2.2 #Tunnel termination address on SG-2
source-address : 0.0.0.0/0
destination-address : 0.0.0.0/0
ipsec-inside-interface: ms-0/0/0.1
term: term-1
local-gateway-address : 10.1.1.1 #Tunnel termination address on SG-1
remote-gateway-address: 10.3.3.3 #Tunnel termination address on SG-3
source-address : 0.0.0.0/0
destination-address : 0.0.0.0/0
IPsec Properties
ipsec-inside-interface: ms-0/0/0.1
match-direction: input
```

Meaning

The **show services ipsec-vpn ipsec security-associations detail** command output shows the properties that you configured.

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | **618**
- Configuring Security Associations | **639**
- Configuring IPsec Policies | **685**
- Configuring IKE Policies | **671**
- Tracing Junos VPN Site Secure Operations | **710**

Example: Configuring IKE Dynamic SAs

IN THIS SECTION

This example shows how to configure IKE dynamic SAs and contains the following sections.

Requirements

This example uses the following hardware and software components:

- Four M Series, MX Series, or T Series routers with multiservices interfaces installed in them.
- Junos OS Release 9.4 or later.

No special configuration beyond device initiation is required before you can configure this feature.

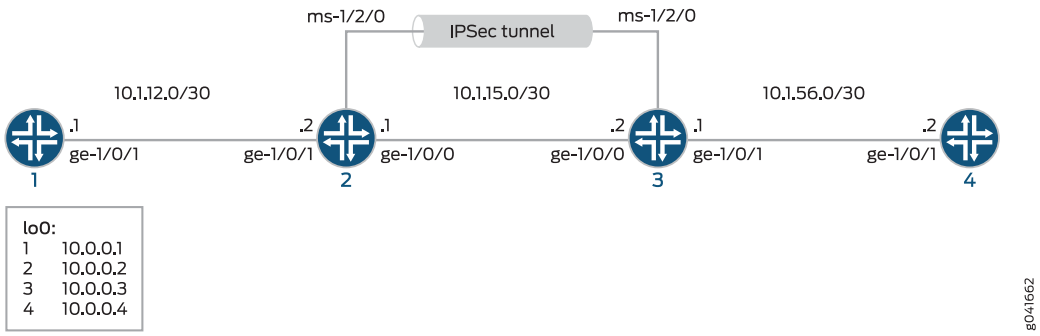
Overview and Topology

A security association (SA) is a simplex connection that enables two hosts to securely communicate with each other by means of IPsec.

Dynamic SAs are best suited for large-scale, geographically distributed networks where manual distribution, maintenance, and tracking of keys are difficult tasks. Dynamic SAs are configured with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. A dynamic SA includes one or more proposals that allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

Figure 38 on page 769 shows an IPsec topology that contains a group of four routers. This configuration requires Routers 2 and 3 to establish an IPsec tunnel by using an IKE dynamic SA, enhanced authentication, and encryption. Routers 1 and 4 provide basic connectivity and are used to verify that the IPsec tunnel is operational.

Figure 38: IKE Dynamic SAs



NOTE: When you do not specify an IKE proposal, an IPsec proposal, and an IPsec policy on a MultiServices PIC, the Junos OS defaults to the highest level of encryption and authentication. As a result, the default authentication protocol is ESP, the default authentication mode is HMAC-SHA1-96, and the default encryption mode is 3DES-CBC.

Configuration

IN THIS SECTION

To configure IKE dynamic SA, perform these tasks:

NOTE: The interface types shown in this example are for indicative purpose only. For example, you can use **so-** interfaces instead of **ge-** and **sp-** instead of **ms-**.

Configuring Router 1

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, of Router 1.

```
set interfaces ge-0/0/0 description "to R2 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.12.2/30
set interfaces lo0 unit 0 family inet address 10.0.0.1/32
set routing-options router-id 10.0.0.1
set protocols ospf area 0.0.0.0 interface ge-0/0/0
set protocols ospf area 0.0.0.0 interface lo0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router 1 for OSPF connectivity with Router 2:

1. Configure an Ethernet interface and a loopback interface.

```
[edit interfaces]
user@router1# set ge-0/0/0 description "to R2 ge-0/0/0"
user@router1# set ge-0/0/0 unit 0 family inet address 10.1.12.2/30
user@router1# set lo0 unit 0 family inet address 10.0.0.1/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit interfaces]
user@router1# set ospf area 0.0.0.0 interface ge-0/0/0.0
user@router1# set ospf area 0.0.0.0 interface lo0.0
```

3. Configure the router ID.

```
[edit routing-options]
user@router1# set router-id 10.0.0.1
```

4. Commit the configuration.

```
[edit]
user@router1# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router1# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R2 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
```

```
        }
      }
    }
    lo0 {
      unit 0 {
        family inet {
          address 10.0.0.1/32;
        }
      }
    }
}
```

```
user@router1# show protocols ospf
protocols {
    ospf {
      area 0.0.0.0 {
        interface ge-0/0/0.0;
        interface lo0.0;
      }
    }
}
```

```
user@router1# show routing-options
routing-options {
    router-id 10.0.0.1;
}
```

Configuring Router 2

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, of Router 2.

```
set interfaces ge-0/0/0 description "to R1 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.12.1/30
set interfaces ge-0/0/1 description "to R3 ge-0/0/1"
set interfaces ge-0/0/1 unit 0 family inet address 10.1.15.1/30
set interfaces ms-1/2/0 services-options syslog host local services info
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
```

```
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.2/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set routing-options router-id 10.0.0.2
set services ipsec-vpn rule rule-ike term term-ike then remote-gateway 10.1.15.2
set services ipsec-vpn rule rule-ike term term-ike then dynamic ike-policy ike-demo-policy
set services ipsec-vpn rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
set services ipsec-vpn rule match-direction input
set services ipsec-vpn ike proposal ike-demo-proposal authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike-demo-proposal dh-group group2
set services ipsec-vpn ike policy ike-demo-policy pre-shared proposals demo-proposal
set services ipsec-vpn ike policy ike-demo-policy pre-shared pre-shared-key ascii-text keyfordemo
set services ipsec-vpn ipsec proposal ipsec-demo-proposal protocol esp
set services ipsec-vpn ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec proposals ipsec-demo-proposal
set services service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.1
set services service-set demo-service-set ipsec-vpn-rules rule-ike
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF connectivity and IPsec tunnel parameters on Router 2:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), a loopback interface, and a multiservices interface (ms-1/2/0).

```
[edit interfaces]
user@router2# set ge-0/0/0 description "to R1 ge-0/0/0"
user@router2# set ge-0/0/0 unit 0 family inet address 10.1.12.1/30
user@router2# set ge-0/0/1 description "to R3 ge-0/0/1"
user@router2# set ge-0/0/1 unit 0 family inet address 10.1.15.1/30
user@router2# set ms-1/2/0 services-options syslog host local services info
user@router2# set ms-1/2/0 unit 0 family inet
user@router2# set ms-1/2/0 unit 1 family inet
user@router2# set ms-1/2/0 unit 1 service-domain inside
user@router2# set ms-1/2/0 unit 2 family inet
```

```
user@router2# set ms-1/2/0 unit 2 service-domain outside
user@router2# set lo0 unit 0 family inet address 10.0.0.2/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit protocols]
user@router2# set ospf area 0.0.0.0 interface ge-0/0/0.0
user@router2# set ospf area 0.0.0.0 interface lo0.0
user@router2# set ospf area 0.0.0.0 interface ms-1/2/0.1
```

3. Configure the router ID.

```
[edit routing-options]
user@router2# set router-ID 10.0.0.2
```

4. Configure an IPsec rule. In this step, you configure an IPsec rule, specify manual SA parameters, such as the remote gateway address, authentication and encryption properties, and so on.

> **NOTE:** By default, Junos OS uses IKE policy version 1.0. Junos OS Release 11.4 and later also support IKE policy version 2.0 which you must configure at **[edit services ipsec-vpn ike policy *policy-name* pre-shared]**.

```
[edit services ipsec-vpn]
user@router2# set rule rule-ike term term-ike then remote-gateway 10.1.15.2
user@router2# set rule rule-ike term term-ike then dynamic ike-policy ike-demo-policy
user@router2# set rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
user@router2# set rule match-direction input
user@router2# set ike proposal ike-demo-proposal authentication-method pre-shared-keys
user@router2# set ike proposal ike-demo-proposal dh-group group2
user@router2# set ike policy ike-demo-policy pre-shared proposals demo-proposal
user@router2# set ike policy ike-demo-policy pre-shared pre-shared-key ascii-text keyfordemo
user@router2# set ipsec proposal ipsec-demo-proposal protocol esp
user@router2# set ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
user@router2# set ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
user@router2# set ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
user@router2# set ipsec proposals ipsec-demo-proposal
```

5. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router2# set service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
user@router2# set service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
user@router2# set service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.1
user@router2# set service-set demo-service-set ipsec-vpn-rules rule-ike
```

6. Commit the configuration.

```
[edit]
user@router2# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router1# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R1 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.1/30;
            }
        }
    }
    ge-0/0/1 {
        description "To R3 ge-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    ms-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
```

```
            }
          }
        }
        unit 0 {
          family inet;
        }
        unit 1 {
          family inet;
          service-domain inside;
        }
        unit 2 {
          family inet;
          service-domain outside;
        }
    }
    lo0 {
        unit 0 {
          family inet {
            address 10.0.0.2/32;
          }
        }
    }
}
```

```
user@router2# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface lo0.0;
            interface ms-1/2/0.1;
        }
    }
}
```

```
user@router2# show routing-options
routing-options {
    router-id 10.0.0.2;
}
```

```
user@router2# show services
services {
```

```
    ipsec-vpn {
        rule rule-ike {
            term term-ike {
                then {
                    remote-gateway 10.1.15.2;
                    dynamic {
                        ike-policy ike-demo-policy;
                        ipsec-policy ipsec-demo-policy;
                    }
                }
            }
            match-direction input;
        }
        ike {
            proposal ike-demo-proposal {
                authentication-method pre-shared-keys;
                dh-group group2;
            }
            policy ike-demo-policy {
                proposals demo-proposal;
                pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
            }
        }
        ipsec {
        proposal ipsec-demo-proposal {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
        }
        policy ipsec-demo-policy {
            perfect-forward-secrecy {
                keys group2;
            }
            proposals ipsec-demo-proposal;
        }
    }
}
service-set demo-service-set {
    next-hop-service {
        inside-service-interface ms-1/2/0.1;
        outside-service-interface ms-1/2/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.1.15.1;
```

```
    }
    ipsec-vpn-rules rule-ike;
}
service-set demo-service-set {
    next-hop-service {
        inside-service-interface ms-1/2/0.1;
        outside-service-interface ms-1/2/0.2;
    }
    ipsec-vpn-options {
        local-gateway 10.1.15.2;
    }
    ipsec-vpn-rules rule-ike;
}
```

Configuring Router 3

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, of Router 3.

```
set interfaces ge-0/0/0 description "to R4 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.56.1/30
set interfaces ge-0/0/1 description "to R2 ge-0/0/1"
set interfaces ge-0/0/1 unit 0 family inet address 10.1.15.2/30
set interfaces ms-1/2/0 services-options syslog host local services info
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.3/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set routing-options router-id 10.0.0.3
set services ipsec-vpn rule rule-ike term term-ike then remote-gateway 10.1.15.1
set services ipsec-vpn rule rule-ike term term-ike then dynamic ike-policy ike-demo-policy
set services ipsec-vpn rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
set services ipsec-vpn rule match-direction input
set services ipsec-vpn ike proposal ike-demo-proposal authentication-method pre-shared-keys
set services ipsec-vpn ike proposal ike-demo-proposal dh-group group2
set services ipsec-vpn ike policy ike-demo-policy pre-shared proposals demo-proposal
set services ipsec-vpn ike policy ike-demo-policy pre-shared pre-shared-key ascii-text keyfordemo
```

```
set services ipsec-vpn ipsec proposal ipsec-demo-proposal protocol esp
set services ipsec-vpn ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec proposals ipsec-demo-proposal
set services service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.2
set services service-set demo-service-set ipsec-vpn-rules rule-ike
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF connectivity and IPsec tunnel parameters on Router 3:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), a loopback interface, and a multiservices interface (ms-1/2/0).

```
[edit interfaces]
user@router3# set ge-0/0/0 description "to R4 ge-0/0/0"
user@router3# set ge-0/0/0 unit 0 family inet address 10.1.56.1/30
user@router3# set ge-0/0/1 description "to R2 ge-0/0/1"
user@router3# set ge-0/0/1 unit 0 family inet address 10.1.15.2/30
user@router3# set ms-1/2/0 services-options syslog host local services info
user@router3# set ms-1/2/0 unit 0 family inet
user@router3# set ms-1/2/0 unit 1 family inet
user@router3# set ms-1/2/0 unit 1 service-domain inside
user@router3# set ms-1/2/0 unit 2 family inet
user@router3# set ms-1/2/0 unit 2 service-domain outside
user@router3# set lo0 unit 0 family inet address 10.0.0.3/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit protocols]
user@router3# set ospf area 0.0.0.0 interface ge-0/0/0.0
user@router3# set ospf area 0.0.0.0 interface lo0.0
user@router3# set ospf area 0.0.0.0 interface ms-1/2/0.1
```

3. Configure a router ID.

```
[edit routing-options]
```

```
user@router3# set router-id 10.0.0.3
```

4. Configure an IPsec rule. In this step, you configure an IPsec rule and specify manual SA parameters, such as the remote gateway address, authentication and encryption properties, and so on.

```
[edit services ipsec-vpn]
user@router3# set rule rule-ike term term-ike then remote-gateway 10.1.15.1
user@router3# set rule rule-ike term term-ike then dynamic ike-policy ike-demo-policy
user@router3# set rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
user@router3# set rule match-direction input
user@router3# set ike proposal ike-demo-proposal authentication-method pre-shared-keys
user@router3# set ike proposal ike-demo-proposal dh-group group2
user@router3# set ike policy ike-demo-policy pre-shared proposals demo-proposal
user@router3# set ike policy ike-demo-policy pre-shared pre-shared-key ascii-text keyfordemo
user@router3# set ipsec proposal ipsec-demo-proposal protocol esp
user@router3# set ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
user@router3# set ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
user@router3# set ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
user@router3# set ipsec proposals ipsec-demo-proposal
```

5. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router3# set service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
user@router3# set service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
user@router3# set service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.2
user@router3# set service-set demo-service-set ipsec-vpn-rules rule-ike
```

6. Commit the configuration.

```
[edit]
user@router3# commit
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router3# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R4 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    ge-0/0/1 {
        description "To R2 ge-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    ms-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
                }
            }
        }
        unit 0 {
            family inet {
            }
            unit 1 {
                family inet;
                service-domain inside;
            }
            unit 2 {
                family inet;
                service-domain outside;
            }
        }
        lo0 {
            unit 0 {
                family inet {
                    address 10.0.0.3/32;
                }
            }
```

```
    }
  }
}
```

```
user@router3# show protocols ospf
protocols {
  ospf {
    area 0.0.0.0 {
      interface ge-0/0/0.0;
      interface lo0.0;
      interface ms-1/2/0.1;
    }
  }
}
```

```
user@router3# show routing-options
routing-options {
  router-id 10.0.0.3;
}
```

```
user@router3# show services
services {
  ipsec-vpn {
    rule rule-ike {
      term term-ike {
        then {
          remote-gateway 10.1.15.1;
          dynamic {
            ike-policy ike-demo-policy;
            ipsec-policy ipsec-demo-policy;
          }
        }
      }
      match-direction input;
    }
    ike {
      proposal ike-demo-proposal {
        authentication-method pre-shared-keys;
        dh-group group2;
      }
      policy ike-demo-policy {
        proposals demo-proposal;
```

```
            pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
        }
    }
    ipsec {
    proposal ipsec-demo-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
    }
    policy ipsec-demo-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-demo-proposal;
    }
  }
}
```

Configuring Router 4

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, of Router 4.

```
set interfaces ge-0/0/0 description "to R3 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.56.2/30
set interfaces lo0 unit 0 family inet address 10.0.0.4/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options router-id 10.0.0.4
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To set up OSPF connectivity with Router 4

1. Configure the interfaces. In this step, you configure an Ethernet interface (ge-1/0/1) and a loopback interface.

```
user@router4# set interfaces ge-0/0/0 description "to R3 ge-0/0/0"
user@router4# set interfaces ge-0/0/0 unit 0 family inet address 10.1.56.2/30
```

```
user@router4# set interfaces lo0 unit 0 family inet address 10.0.0.4/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
user@router4# set protocols ospf area 0.0.0.0 interface ge-0/0/0
user@router4# set protocols ospf area 0.0.0.0 interface lo0.0
```

3. Configure the router ID.

```
[edit routing-options]
user@router4# set router-id 10.0.0.4
```

Results

From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router4# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R3 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}
```

```
user@router4# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
```

```
            interface ge-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

```
user@router4# show routing-options
routing-options {
    router-id 10.0.0.4;
}
```

Verification

Verifying Your Work on Router 1

Purpose

Verify proper operation of Router 1.

Action

From operational mode, enter **ping 10.1.56.2** command to the ge-0/0/0 interface on Router 4 to send traffic across the IPsec tunnel

`user@router1>`**ping 10.1.56.2**

```
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

Meaning

The output shows that Router 1 is able to reach Router 4 over the IPsec tunnel.

Verifying Your Work on Router 2

Purpose

Verify that the IKE SA negotiation is successful.

Action

From operational mode, enter the **show services ipsec-vpn ike security-associations** command.

```
user@router2>show services ipsec-vpn ike security-associations
```

```
Remote Address State Initiator cookie Responder cookie Exchange type
10.1.15.2 Matured 03075bd3a0000003 4bff26a5c7000003 Main
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the MultiServices PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

From operational mode, enter the **show services ipsec-vpn ipsec security-associations detail** command.

```
user@router2> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: demo-service-set
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Direction: inbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling through the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

From operational mode, enter the **show services ipsec-vpn statistics** command.

```
user@router2> show services ipsec-vpn ipsec statistics
```

```
PIC: ms-1/2/0, Service set: demo-service-set
ESP Statistics:
Encrypted bytes: 2248
Decrypted bytes: 2120
Encrypted packets: 27
Decrypted packets: 25
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Meaning

The **show services ipsec-vpn ipsec security-associations detail** command output shows the SA properties that you configured.

The **show services ipsec-vpn ipsec statistics** command output shows the traffic flow over the IPsec tunnel.

Verifying Your Work on Router 3

Purpose

Verify that the IKE SA negotiation is successful on Router 3.

Action

From operational mode, enter the **show services ipsec-vpn ike security-associations** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

`user@router3>`**show services ipsec-vpn ike security-associations**

```
Remote Address State Initiator cookie Responder cookie Exchange type
10.1.15.1 Matured 03075bd3a0000003 4bff26a5c7000003 Main
```

To verify that the IPsec SA is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

From operational mode, enter the **show services ipsec-vpn ipsec security-associations detail** command.

`user@router3>`**show services ipsec-vpn ipsec security-associations detail**

```
Service set: demo-service-set
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Direction: inbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling through the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

From operational mode, enter the **show services ipsec-vpn ike security-associations** command.

`user@router3>`**show services ipsec-vpn ipsec statistics**

```
PIC: ms-1/2/0, Service set: demo-service-set
ESP Statistics:
Encrypted bytes: 2120
Decrypted bytes: 2248
Encrypted packets: 25
Decrypted packets: 27
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

Meaning

The **show services ipsec-vpn ipsec security-associations detail** command output shows the SA properties that you configured.

The **show services ipsec-vpn ipsec statistics** command output shows the traffic flow over the IPsec tunnel.

Verifying Your Work on Router 4

Purpose

Verify that that the IKE SA negotiation is successful.

Action

From operational mode, enter **ping 10.1.12.2** command to the ge-0/0/0 interface on Router 1 to send traffic across the IPsec tunnel.

```
user@router4>ping 10.1.12.2
```

```
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

To confirm that traffic travels through the IPsec tunnel, issue the **traceroute** command to the ge-0/0/0 interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPsec tunnel through the adaptive services IPsec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the ge-0/0/0 interface on Router 1.

From operational mode, enter the **traceroute 10.1.12.2**.

```
user@router4>traceroute 10.1.12.2
```

```
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
1 10.1.15.2 (10.1.15.2) 0.987 ms 0.630 ms 0.563 ms
2 10.0.0.2 (10.0.0.2) 1.194 ms 1.058 ms 1.033 ms
3 10.1.12.2 (10.1.12.2) 1.073 ms 0.949 ms 0.932 ms
```

Meaning

The **ping 10.1.12.2** output shows that Router 4 is able to reach Router 1 over the IPsec tunnel.

The **traceroute 10.1.12.2** output shows that traffic travels the IPsec tunnel.

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | 618
- Configuring Security Associations | 639
- Configuring IKE Proposals | 665
- Configuring IKE Policies | 671
- Example: Configuring Manual SAs | 646

Example: IKE Dynamic SA Configuration with Digital Certificates

IN THIS SECTION

This example shows how to configure IKE dynamic SA with digital certificates and contains the following sections.

Requirements

This example uses the following hardware and software components:

- Four M Series, MX Series, or T Series routers with multiservices interfaces installed in them.
- Junos OS Release 9.4 or later.

Before you configure this example you must request a CA certificate, create a local certificate, and load these digital certificates into the router. For details, see "Requesting for and Installing a Digital Certificates on Your Router" on page 757

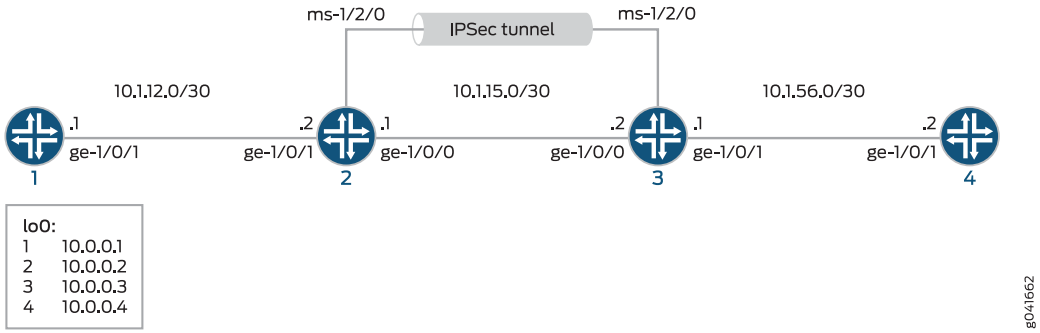
Overview

A security association (SA) is a simplex connection that enables two hosts to securely communicate with each other using IPsec. This example explains IKE dynamic SA configuration with digital certificates. The use of digital certificates provides additional security to your IKE tunnel. Using default values in the Services PIC, you do not need to configure an IPsec proposal or IPsec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the IKE proposal and local certificate in an IKE policy, and apply the CA profile to the service set.

Figure 39 on page 791 shows an IPsec topology containing a group of four routers. This configuration requires Routers 2 and 3 to establish an IKE-based IPsec tunnel by using digital certificates in place of preshared keys. Routers 1 and 4 provide basic connectivity and are used to verify that the IPsec tunnel is operational.

Topology

Figure 39: MS PIC IKE Dynamic SA Topology Diagram



Configuration

IN THIS SECTION

To configure IKE dynamic SA with digital certificates, perform these tasks:

NOTE: The interface types shown in this example are for indicative purpose only. For example, you can use **so-** interfaces instead of **ge-** and **sp-** instead of **ms-**.

Configuring Router 1

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, of Router 1.

```
set interfaces ge-0/0/0 description "to R2 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.12.2/30
set interfaces lo0 unit 0 family inet address 10.0.0.1/32
set routing-options router-id 10.0.0.1
set protocols ospf area 0.0.0.0 interface ge-0/0/0
set protocols ospf area 0.0.0.0 interface lo0.0
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure Router 1 for OSPF connectivity with Router 2:

1. Configure an Ethernet interface and the loopback interface.

```
[edit interfaces]
user@router1# set ge-0/0/0 description "to R2 ge-0/0/0"
user@router1# set ge-0/0/0 unit 0 family inet address 10.1.12.2/30
user@router1# set lo0 unit 0 family inet address 10.0.0.1/32
```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

```
[edit protocols]
user@router1# set ospf area 0.0.0.0 interface ge-0/0/0.0
user@router1# set ospf area 0.0.0.0 interface lo0.0
```

3. Configure the router ID.

```
[edit routing-options]
```

```
user@router1# set router-id 10.0.0.1
```

4. Commit the configuration.

```
[edit]
user@router1# commit
```

Results

From the configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R2 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
}
```

```
user@router1# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

```
user@router1# show routing-options
routing-options {
    router-id 10.0.0.1;
}
```

Configuring Router 2

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, of Router 2.

```
set interfaces ge-0/0/0 description "to R1 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.12.1/30
set interfaces ge-0/0/1 description "to R3 ge-0/0/1"
set interfaces ge-0/0/1 unit 0 family inet address 10.1.15.1/30
set interfaces ms-1/2/0 services-options syslog host local services info
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.2/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set routing-options router-id 10.0.0.2
set services ipsec-vpn rule rule-ike term term-ike then remote-gateway 10.1.15.2
set services ipsec-vpn rule rule-ike term term-ike then dynamic ike-policy ike-digital-certificates
set services ipsec-vpn rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
set services ipsec-vpn rule match-direction input
set services ipsec-vpn ike proposal ike-demo-proposal authentication-method rsa-signatures
set services ipsec-vpn ike policy ike-digital-certificates proposals ike-demo-proposal
set services ipsec-vpn ike policy ike-digital-certificates local-id fqdn router2.example.com
set services ipsec-vpn ike policy ike-digital-certificates local-certificate local-entrust2
set services ipsec-vpn ike policy ike-digital-certificates remote-id fqdn router3.example.com
set services ipsec-vpn ipsec proposal ipsec-demo-proposal protocol esp
set services ipsec-vpn ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec proposals ipsec-demo-proposal
set services ipsec-vpn establish-tunnels immediately
set services service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
```

```
set services service-set demo-service-set ipsec-vpn-options trusted-ca entrust
set services service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.1
set services service-set demo-service-set ipsec-vpn-rules rule-ike
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure OSPF connectivity and IPsec tunnel parameters on Router 2:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), the loopback interface and a multiservices interface (ms-1/2/0).

   ```
   [edit interfaces]
   user@router2# set ge-0/0/0 description "to R1 ge-0/0/0"
   user@router2# set ge-0/0/0 unit 0 family inet address 10.1.12.1/30
   user@router2# set ge-0/0/1 description "to R3 ge-0/0/1"
   user@router2# set ge-0/0/1 unit 0 family inet address 10.1.15.1/30
   user@router2# set ms-1/2/0 services-options syslog host local services info
   user@router2# set ms-1/2/0 unit 0 family inet
   user@router2# set ms-1/2/0 unit 1 family inet
   user@router2# set ms-1/2/0 unit 1 service-domain inside
   user@router2# set ms-1/2/0 unit 2 family inet
   user@router2# set ms-1/2/0 unit 2 service-domain outside
   user@router2# set lo0 unit 0 family inet address 10.0.0.2/32
   ```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

   ```
   [edit protocols]
   user@router2# set ospf area 0.0.0.0 interface ge-0/0/0.0
   user@router2# set ospf area 0.0.0.0 interface lo0.0
   user@router2# set ospf area 0.0.0.0 interface ms-1/2/0.1
   ```

3. Configure the router ID.

   ```
   [edit routing-options]
   user@router2# set router-ID 10.0.0.2
   ```

4. Configure an IKE proposal and policy. To enable an IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal proposal-name authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the

local-certificate statement at the **[edit services ipsec-vpn ike policy policy-name]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

> **NOTE:** For information about creating and installing digital certificates, see "Requesting for and Installing a Digital Certificates on Your Router" on page 757

```
[edit services ipsec-vpn]
user@router2# set ike proposal ike-demo-proposal authentication-method rsa-signatures
user@router2# set ike policy ike-digital-certificates proposals ike-demo-proposal
user@router2# set ike policy ike-digital-certificates local-id fqdn router2.example.com
user@router2# set ike policy ike-digital-certificates local-certificate local-entrust2
user@router2# set ike policy ike-digital-certificates remote-id fqdn router3.example.com
```

5. Configure an IPsec proposal and policy. Also, set the **established-tunnels** knob to **immediately**.

```
[edit services ipsec-vpn]
user@router2# set ipsec proposal ipsec-demo-proposal protocol esp
user@router2# set ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
user@router2# set ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
user@router2# set ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
user@router2# set ipsec proposals ipsec-demo-proposal
user@router2# set establish-tunnels immediately
```

6. Configure an IPsec rule.

```
[edit services ipsec-vpn]
user@router2# set rule rule-ike term term-ike then remote-gateway 10.1.15.2
user@router2# set rule rule-ike term term-ike then dynamic ike-policy ike-digital-certificates
user@router2# set rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
user@router2# set rule match-direction input
```

7. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router2# set service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
user@router2# set service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
```

```
user@router2# set service-set demo-service-set ipsec-vpn-options trusted-ca entrust
user@router2# set service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.1
user@router2# set service-set demo-service-set ipsec-vpn-rules rule-ike
```

8. Commit the configuration.

```
[edit]
user@router2# commit
```

Results

From the configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router2# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R1 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.1/30;
            }
        }
    }
    ge-0/0/1 {
        description "To R3 ge-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    ms-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
                }
            }
        }
        unit 0 {
            family inet;
```

```
        }
        unit 1 {
            family inet;
            service-domain inside;
        }
        unit 2 {
            family inet;
            service-domain outside;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.2/32;
            }
        }
    }
}
```

```
user@router2# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface lo0.0;
            interface ms-1/2/0.1;
        }
    }
}
```

```
user@router2# show routing-options
routing-options {
    router-id 10.0.0.2;
}
```

```
user@router2# show services
services {
    ipsec-vpn {
        rule rule-ike {
            term term-ike {
                then {
                    remote-gateway 10.1.15.2;
```

```
            dynamic {
                ike-policy ike-digital-certificates;
                ipsec-policy ipsec-demo-policy
            }
        }
    }
    match-direction input;
}
ike {
    proposal ike-demo-proposal {
        authentication-method rsa-signatures;
    }
    policy ike-digital-certificates {
        proposals ike-demo-proposal;
        local-id fqdn router2.example.com;
        local-certificate local-entrust2;
        remote-id fqdn router3.example.com;
    }
}
ipsec {
    proposal ipsec-demo-proposal {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
    }
    policy demo-policy {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals ipsec-demo-proposal;
    }
    establish-tunnels immediately;
}
service-set service-set-dynamic-demo-service-set {
    next-hop-service {
        inside-service-interface ms-1/2/0.1;
        outside-service-interface ms-1/2/0.2;
    }
    ipsec-vpn-options {
        trusted-ca entrust;
        local-gateway 10.1.15.1;
    }
    ipsec-vpn-rules rule-ike;
}
```

```
    }
}
```

Configuring Router 3

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, of Router 3.

```
set interfaces ge-0/0/0 description "to R4 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.56.1/30
set interfaces ge-0/0/1 description "to R2 ge-0/0/1"
set interfaces ge-0/0/1 unit 0 family inet address 10.1.15.2/30
set interfaces ms-1/2/0 services-options syslog host local services info
set interfaces ms-1/2/0 unit 0 family inet
set interfaces ms-1/2/0 unit 1 family inet
set interfaces ms-1/2/0 unit 1 service-domain inside
set interfaces ms-1/2/0 unit 2 family inet
set interfaces ms-1/2/0 unit 2 service-domain outside
set interfaces lo0 unit 0 family inet address 10.0.0.3/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set protocols ospf area 0.0.0.0 interface ms-1/2/0.1
set routing-options router-id 10.0.0.3
set services ipsec-vpn rule rule-ike term term-ike then remote-gateway 10.1.15.1
set services ipsec-vpn rule rule-ike term term-ike then dynamic ike-policy ike-digital-certificates
set services ipsec-vpn rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
set services ipsec-vpn rule match-direction input
set services ipsec-vpn ike proposal ike-demo-proposal authentication-method rsa-signatures
set services ipsec-vpn ike policy ike-digital-certificates proposals ike-demo-proposal
set services ipsec-vpn ike policy ike-digital-certificates local-id fqdn router3.example.com
set services ipsec-vpn ike policy ike-digital-certificates local-certificate local-entrust3
set services ipsec-vpn ike policy ike-digital-certificates remote-id fqdn router2.example.com
set services ipsec-vpn ipsec proposal ipsec-demo-proposal protocol esp
set services ipsec-vpn ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
set services ipsec-vpn ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
set services ipsec-vpn ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
set services ipsec-vpn ipsec proposals ipsec-demo-proposal
set services ipsec-vpn establish-tunnels immediately
set services service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
set services service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
set services service-set demo-service-set ipsec-vpn-options trusted-ca entrust
set services service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.2
```

```
set services service-set demo-service-set ipsec-vpn-rules rule-ike
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

> **NOTE:** If the IPsec peers do not have a symmetrical configuration containing all the necessary components, they cannot establish a peering relationship. You need to request a CA certificate, create a local certificate, load these digital certificates into the router, and reference them in your IPsec configuration. For information about digital certification, see "Requesting for and Installing a Digital Certificates on Your Router" on page 757

To configure OSPF connectivity and IPsec tunnel parameters on Router 3:

1. Configure interface properties. In this step, you configure two Ethernet interfaces (ge-1/0/0 and ge-1/0/1), the loopback interface, and a multiservices interface (ms-1/2/0).

```
[edit interfaces]
user@router3# set ge-0/0/0 description "to R4 ge-0/0/0"
user@router3# set ge-0/0/0 unit 0 family inet address 10.1.56.1/30
user@router3# set ge-0/0/1 description "to R2 ge-0/0/1"
user@router3# set ge-0/0/1 unit 0 family inet address 10.1.15.2/30
user@router3# set ms-1/2/0 services-options syslog host local services info
user@router3# set ms-1/2/0 unit 0 family inet
user@router3# set ms-1/2/0 unit 1 family inet
user@router3# set ms-1/2/0 unit 1 service-domain inside
user@router3# set ms-1/2/0 unit 2 family inet
user@router3# set ms-1/2/0 unit 2 service-domain outside
user@router3# set lo0 unit 0 family inet address 10.0.0.3/32
```

2. Specify the OSPF area, associate the interfaces with the OSPF area.

```
[edit protocols]
user@router3# set ospf area 0.0.0.0 interface ge-0/0/0.0
user@router3# set ospf area 0.0.0.0 interface lo0.0
user@router3# set ospf area 0.0.0.0 interface ms-1/2/0.1
```

3. Configure a router ID.

```
[edit routing-options]
user@router3# set router-id 10.0.0.3
```

4. Configure an IKE proposal and policy. To enable an IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal proposal-name authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy policy-name]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set service-set-name ipsec-vpn-options]** hierarchy level.

   NOTE: For information about creating and installing digital certificates, see "Requesting for and Installing a Digital Certificates on Your Router" on page 757

```
[edit services ipsec-vpn]
user@router3# set ike proposal ike-demo-proposal authentication-method rsa-signatures
user@router3# set ike policy ike-digital-certificates proposals ike-demo-proposal
user@router3# set ike policy ike-digital-certificates local-id fqdn router2.example.com
user@router3# set ike policy ike-digital-certificates local-certificate local-entrust2
user@router3# set ike policy ike-digital-certificates remote-id fqdn router3.example.com
```

5. Configure an IPsec proposal. Also, set the **established-tunnels** knob to **immediately**.

```
[edit services ipsec-vpn]
user@router3# set ipsec proposal ipsec-demo-proposal protocol esp
user@router3# set ipsec proposal ipsec-demo-proposal authentication-algorithm hmac-sha1-96
user@router3# set ipsec proposal ipsec-demo-proposal encryption-algorithm 3des-cbc
user@router3# set ipsec policy ipsec-demo-policy perfect-forward-secrecy keys group2
user@router3# set ipsec proposals ipsec-demo-proposal
user@router3# set establish-tunnels immediately
```

6. Configure an IPsec rule.

```
[edit services ipsec-vpn]
user@router3# set rule rule-ike term term-ike then remote-gateway 10.1.15.2
user@router3# set rule rule-ike term term-ike then dynamic ike-policy ike-digital-certificates
user@router3# set rule rule-ike term term-ike then dynamic ipsec-policy ipsec-demo-policy
user@router3# set rule match-direction input
```

7. Configure a next-hop style service set, specify the local-gateway address, and associate the IPsec VPN rule with the service set.

```
[edit services]
user@router3# set service-set demo-service-set next-hop-service inside-service-interface ms-1/2/0.1
user@router3# set service-set demo-service-set next-hop-service outside-service-interface ms-1/2/0.2
user@router3# set service-set demo-service-set ipsec-vpn-options trusted-ca entrust
user@router3# set service-set demo-service-set ipsec-vpn-options local-gateway 10.1.15.2
user@router3# set service-set demo-service-set ipsec-vpn-rules rule-ike
```

8. Commit the configuration.

```
[edit]
user@router3# commit
```

Results

From the configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, **show routing-options**, and **show services** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router3# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R4 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    ge-0/0/1 {
        description "To R2 ge-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    ms-1/2/0 {
        services-options {
            syslog {
                host local {
```

```
            services info;
          }
        }
      }
      unit 0 {
        family inet {
        }
        unit 1 {
          family inet;
          service-domain inside;
        }
        unit 2 {
          family inet;
          service-domain outside;
        }
      }
      lo0 {
        unit 0 {
          family inet {
            address 10.0.0.3/32;
          }
        }
      }
    }
}
```

```
user@router3# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface lo0.0;
            interface ms-1/2/0.1;
        }
    }
}
```

```
user@router3# show routing-options
routing-options {
    router-id 10.0.0.3;
}
```

```
user@router3# show services
services {
    ipsec-vpn {
        rule rule-ike {
            term term-ike {
                then {
                    remote-gateway 10.1.15.1;
                    dynamic {
                        ike-policy ike-digital-certificates;
                        ipsec-policy ipsec-demo-policy
                    }
                }
            }
            match-direction input;
        }
        ike {
            proposal ike-demo-proposal {
                authentication-method rsa-signatures;
            }
            policy ike-digital-certificates {
                proposals ike-demo-proposal;
                local-id fqdn router3.example.com;
                local-certificate local-entrust3;
                remote-id fqdn router2.example.com;
            }
        }
        ipsec {
            proposal ipsec-demo-proposal {
                protocol esp;
                authentication-algorithm hmac-sha1-96;
                encryption-algorithm 3des-cbc;
            }
            policy demo-policy {
                perfect-forward-secrecy {
                    keys group2;
                }
                proposals ipsec-demo-proposal;
            }
            establish-tunnels immediately;
        }
        service-set service-set-dynamic-demo-service-set {
            next-hop-service {
                inside-service-interface ms-1/2/0.1;
                outside-service-interface ms-1/2/0.2;
```

```
        }
        ipsec-vpn-options {
            trusted-ca entrust;
            local-gateway 10.1.15.2;
        }
        ipsec-vpn-rules rule-ike;
    }
  }
}
```

Configuring Router 4

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, of Router 4.

```
set interfaces ge-0/0/0 description "to R3 ge-0/0/0"
set interfaces ge-0/0/0 unit 0 family inet address 10.1.56.2/30
set interfaces lo0 unit 0 family inet address 10.0.0.4/32
set protocols ospf area 0.0.0.0 interface ge-0/0/0.0
set protocols ospf area 0.0.0.0 interface lo0.0
set routing-options router-id 10.0.0.4
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To set up OSPF connectivity with Router 4

1. Configure the interfaces. In this step, you configure an Ethernet interface (ge-1/0/1) and the loopback interface.

   ```
   [edit interfaces]
   user@router4# set ge-0/0/0 description "to R3 ge-0/0/0"
   user@router4# set ge-0/0/0 unit 0 family inet address 10.1.56.2/30
   user@router4# set lo0 unit 0 family inet address 10.0.0.4/32
   ```

2. Specify the OSPF area and associate the interfaces with the OSPF area.

   ```
   [edit protocols]
   user@router4# set ospf area 0.0.0.0 interface ge-0/0/0
   ```

```
user@router4# set ospf area 0.0.0.0 interface lo0.0
```

3. Configure the router ID.

```
[edit routing-options]
user@router4# set router-id 10.0.0.4
```

Results

From the configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols ospf**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration

```
user@router4# show interfaces
interfaces {
    ge-0/0/0 {
        description "To R3 ge-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.4/32;
            }
        }
    }
}
```

```
user@router4# show protocols ospf
protocols {
    ospf {
        area 0.0.0.0 {
            interface ge-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

```
user@router4# show routing-options
routing-options {
    router-id 10.0.0.4;
}
```

Verification

Verifying Your Work on Router 1

Purpose

On Router 1, verify ping command to the so-0/0/0 interface on Router 4 to send traffic across the IPsec tunnel.

Action

From operational mode, enter **ping 10.1.56.2**.

```
user@router1>ping 10.1.56.2
```

```
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

If you ping the loopback address of Router 4, the operation succeeds because the address is part of the OSPF network configured on Router 4.

```
user@router1>ping 10.0.0.4
```

```
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=62 time=1.318 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=62 time=1.084 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=62 time=3.260 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.084/1.887/3.260/0.975 ms
```

Verifying Your Work on Router 2

Purpose

To verify that matched traffic is being diverted to the bidirectional IPsec tunnel, view the IPsec statistics:

Action

From operational mode, enter the **show services ipsec-vpn ipsec statistics**.

```
user@router2>show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-dynamic-demo-service-set
ESP Statistics:
Encrypted bytes: 162056
Decrypted bytes: 161896
Encrypted packets: 2215
Decrypted packets: 2216
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command:

From operational mode, enter the **show services ipsec-vpn ike security-associations**

```
user@router2> show services ipsec-vpn ike security-associations
```

```
Remote Address State Initiator cookie Responder cookie Exchange type
10.1.15.2 Matured d82610c59114fd37 ec4391f76783ef28 Main
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the Services PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

From operational mode, enter the **show services ipsec-vpn ipsec security-associations detail**

```
user@router2> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-demo-service-set
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
IPsec inside interface: sp-1/2/0.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 857451461, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 9052 seconds
Hard lifetime: Expires in 9187 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 1272330309, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 9052 seconds
Hard lifetime: Expires in 9187 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To display the digital certificates that are used to establish the IPsec tunnel, issue the show services ipsec-vpn certificates command:

From operational mode, enter the **show services ipsec-vpn certificates**

```
user@router2> show services ipsec-vpn certificates
```

```
Service set: service-set-dynamic-demo-service-set, Total entries: 3
Certificate cache entry: 3
Flags: Non-root Trusted
Issued to: router3.example.com, Issued by: juniper
Alternate subject: router3.example.com
Validity:
Not before: 2005 Nov 21st, 23:33:58 GMT
Not after: 2008 Nov 22nd, 00:03:58 GMT
Certificate cache entry: 2
Flags: Non-root Trusted
Issued to: router2.example.com, Issued by: juniper
Alternate subject: router2.example.com
Validity:
Not before: 2005 Nov 21st, 23:28:22 GMT
Not after: 2008 Nov 21st, 23:58:22 GMT
Certificate cache entry: 1
Flags: Root Trusted
```

```
Issued to: juniper, Issued by: juniper
Validity:
Not before: 2005 Oct 18th, 23:54:22 GMT
Not after: 2025 Oct 19th, 00:24:22 GMT
```

To display the CA certificate, issue the show security pki ca-certificate detail command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

From operational mode, enter the **show security pki ca-certificate detail**

`user@router2>` **show security pki ca-certificate detail**

```
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 9235
Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us
Validity:
Not before: 2005 Oct 18th, 23:54:22 GMT
Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
04:47:08:07:de:17:23:13
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925c
Issuer:
```

```
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us, Common name: First Officer
Validity:
Not before: 2005 Oct 18th, 23:55:59 GMT
Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
da:eb:10:27:bd:46:34:33
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us, Common name: First Officer
Validity:
Not before: 2005 Oct 18th, 23:55:59 GMT
Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
```

```
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
```

To display the local certificate request, issue the show security pki certificate-request command:

From operational mode, enter the **show security pki certificate-request**

```
user@router2> show security pki certificate-request
```

```
Certificate identifier: local-entrust2
Issued to: router2.example.com
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```

To display the local certificate, issue the show security pki local-certificate command:

From operational mode, enter the **show security pki local-certificate**

```
user@router2> show security pki local-certificate
```

```
Certificate identifier: local-entrust2
Issued to: router2.example.com, Issued by: juniper
Validity:
Not before: 2005 Nov 21st, 23:28:22 GMT
Not after: 2008 Nov 21st, 23:58:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```

Verifying Your Work on Router 3

Purpose

To verify that matched traffic is being diverted to the bidirectional IPsec tunnel, view the IPsec statistics:

Action

From operational mode, enter the **show services ipsec-vpn ipsec statistics**.

```
user@router3>show services ipsec-vpn ipsec statistics
```

```
PIC: sp-1/2/0, Service set: service-set-dynamic-demo-service-set
ESP Statistics:
Encrypted bytes: 161896
Decrypted bytes: 162056
Encrypted packets: 2216
Decrypted packets: 2215
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the show services ipsec-vpn ike security-associations command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

From operational mode, enter the **show services ipsec-vpn ike security-associations**.

`user@router3>`**show services ipsec-vpn ike security-associations**

```
Remote Address State Initiator cookie Responder cookie Exchange type
10.1.15.1 Matured d82610c59114fd37 ec4391f76783ef28 Main
```

To verify that the IPsec SA is active, issue the show services ipsec-vpn ipsec security-associations detail command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

From operational mode, enter the **show services ipsec-vpn ipsec security-associations detail**.

`user@router3>`**show services ipsec-vpn ipsec security-associations detail**

```
Service set: service-set-dynamic-demo-service-set
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
IPsec inside interface: sp-1/2/0.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 1272330309, AUX-SPI: 0
```

```
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 7219 seconds
Hard lifetime: Expires in 7309 seconds
Anti-replay service: Enabled, Replay window size: 64
Direction: outbound, SPI: 857451461, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 7219 seconds
Hard lifetime: Expires in 7309 seconds
Anti-replay service: Enabled, Replay window size: 64
```

To display the digital certificates that are used to establish the IPsec tunnel, issue the show services ipsec-vpn certificates command:

From operational mode, enter the **show services ipsec-vpn certificates**.

```
user@router3>show services ipsec-vpn certificates
```

```
Service set: service-set-dynamic-demo-service-set, Total entries: 3
Certificate cache entry: 3
Flags: Non-root Trusted
Issued to: router3.example.com, Issued by: juniper
Alternate subject: router3.example.com
Validity:
Not before: 2005 Nov 21st, 23:33:58 GMT
Not after: 2008 Nov 22nd, 00:03:58 GMT
Certificate cache entry: 2
Flags: Non-root Trusted
Issued to: router2.example.com, Issued by: juniper
Alternate subject: router2.example.com
Validity:
Not before: 2005 Nov 21st, 23:28:22 GMT
Not after: 2008 Nov 21st, 23:58:22 GMT
Certificate cache entry: 1
Flags: Root Trusted
Issued to: juniper, Issued by: juniper
Validity:
Not before: 2005 Oct 18th, 23:54:22 GMT
Not after: 2025 Oct 19th, 00:24:22 GMT
```

To display the CA certificate, issue the show security pki ca-certificate detail command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

From operational mode, enter the **show security pki ca-certificate detail**.

```
user@router3>show security pki ca-certificate detail
```

```
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 9235
Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us
Validity:
Not before: 2005 Oct 18th, 23:54:22 GMT
Not after: 2025 Oct 19th, 00:24:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
04:47:08:07:de:17:23:13
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925c
Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us, Common name: First Officer
Validity:
Not before: 2005 Oct 18th, 23:55:59 GMT
Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
```

```
c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
da:eb:10:27:bd:46:34:33
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Key encipherment
Certificate identifier: entrust
Certificate version: 3
Serial number: 4355 925b
Issuer:
Organization: juniper, Country: us
Subject:
Organization: juniper, Country: us, Common name: First Officer
Validity:
Not before: 2005 Oct 18th, 23:55:59 GMT
Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
C=us, O=juniper, CN=CRL1
http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
```

To display the local certificate request, issue the show security pki certificate-request command:

From operational mode, enter the **show security pki certificate-request**.

```
user@router3>show security pki certificate-request
```

```
Certificate identifier: local-entrust3
Issued to: router3.example.com
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```

To display the local certificate, issue the show security pki local-certificate command:

From operational mode, enter the **show security pki local-certificate**.

```
user@router3>show security pki local-certificate
```

```
Certificate identifier: local-entrust3
Issued to: router3.example.com, Issued by: juniper
Validity:
Not before: 2005 Nov 21st, 23:33:58 GMT
Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
```

Verifying Your Work on Router 4

Purpose

On Router 4, issue a ping command to the so-0/0/0 interface on Router 1 to send traffic across the IPsec tunnel.

Action

From operational mode, enter **ping 10.1.12.2**.

```
user@router4>ping 10.1.12.2
```

```
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
```

```
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

The final way you can confirm that traffic travels over the IPsec tunnel is by issuing the traceroute command to the so-0/0/0 interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPsec tunnel through the adaptive services IPsec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the so-0/0/0 interface on Router 1.

From operational mode, enter the **traceroute 10.1.12.2**.

```
user@router4>traceroute 10.1.12.2
```

```
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
1 10.1.15.2 (10.1.15.2) 0.987 ms 0.630 ms 0.563 ms
2 10.0.0.2 (10.0.0.2) 1.194 ms 1.058 ms 1.033 ms
3 10.1.12.2 (10.1.12.2) 1.073 ms 0.949 ms 0.932 ms
```

RELATED DOCUMENTATION

- Understanding Junos VPN Site Secure | **618**
- Configuring Security Associations | **639**
- Configuring IKE Proposals | **665**
- Configuring IKE Policies | **671**
- Example: Configuring IKE Dynamic SAs | **768**
- Example: Configuring Manual SAs | **646**
- Requesting for and Installing a Digital Certificates on Your Router | **757**

PART 7

Alleviating Congestion and Controlling Service Using CoS

CHAPTER 38

Class of Service Overview

IN THIS CHAPTER

Class of Service Overview

The CoS configuration available for the M Series and MX Series-based service cards enables you to configure Differentiated Services (DiffServ) code point (DSCP) marking and forwarding-class assignment for packets transiting the service cards-service PICs. The M Series and MX Series-based service cards include Multiservices PIC, MS-MIC, MS-MPC, MS-DPC, and Adaptive Services PIC. You can configure the CoS service alongside the stateful firewall and NAT services, using a similar rule structure. The component structures are described in detail in the *Class of Service User Guide (Routers and EX9200 Switches)*.

Standards for Differentiated Services are described in the following documents:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*

> **NOTE:** CoS BA classification is not supported on services interfaces. The CoS configuration is available only for NAT and stateful firewall services. The CoS configuration does not work with other services that run on the service cards such as IPsec.

RELATED DOCUMENTATION

Restrictions and Cautions for CoS Configuration on Services Interfaces | 822

Configuring CoS Rules | 823

Configuring CoS Rule Sets | 830

Examples: Configuring CoS on Services Interfaces | 830

CHAPTER 39

Class of Service Configuration Overview

IN THIS CHAPTER

Restrictions and Cautions for CoS Configuration on Services Interfaces

The following restrictions and cautions apply to CoS configuration on services interfaces:

- You must configure at least one stateful firewall rule or NAT rule on the service set. Otherwise, CoS does not work.
- The services interfaces do not support scheduling, only DiffServ marking and queue assignment. You must configure scheduling at the **[edit class-of-service]** hierarchy level on the output interface or fabric.
- In the default configuration, queues 1 and 2 receive 0 percent bandwidth. If packets will be assigned to these queues, you must configure a scheduling map.
- You must issue a **commit full** command before using custom forwarding-class names in the configuration.
- Only the Junos standard DiffServ names can be used in the configuration. Custom names are not recognized.
- On M Series routers, you can configure rewrite rules that change packet headers and attach the rules to output interfaces. These rules might overwrite the DSCP marking configured on a MultiServices PIC. It is important to keep this adverse effect in mind and use care when creating system-wide configurations.

  For example, knowing that the MultiServices PIC can mark packets with any ToS or DSCP value and the output interface is restricted to only eight DSCP values, rewrite rules on the output interface condense the mapping from 64 to 8 values with overall loss of granularity. In this case, you have the following options:

  - Remove the rewrite rules from the output interface.
  - Configure the output interface to include the most important mappings.

RELATED DOCUMENTATION

Configuring CoS Rules

IN THIS SECTION

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

```
[edit services cos]
rule rule-name {
    match-direction (input | output | input-output);
    term term-name {
        from {
            application-sets set-name;
            applications [ application-names ];
            destination-address address;
            destination-prefix-list list-name <except>;
            source-address address;
            source-prefix-list list-name <except>;
        }
        then {
            application-profile profile-name;
            dscp (alias | bits);
            forwarding-class class-name;
            syslog;
```

```
            reflexive; | revert; | reverse {
                application-profile profile-name;
                dscp (alias | bits);
                forwarding-class class-name;
                syslog;
            }
        }
    }
}
```

Each CoS rule consists of a set of terms, similar to a filter configured at the **[edit firewall]** hierarchy level. 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.

Apply the CoS rule to a service set at the **[edit services]** hierarchy level:

```
[edit services]
service-set service-set-name {
    cos-rules [cos-rule-name];
    }
```

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

Configuring Match Direction for CoS Rules

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

```
match-direction (input | output | input-output);
```

If you configure **match-direction input-output**, bidirectional rule creation is allowed.

The match direction is used with respect to the traffic flow through the Multiservices PIC, MS-MIC, or MS-MPC. When a packet is sent to the PIC, direction information is carried along with it.

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, MS-MIC, or MS-MPC. 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 Multiservices PIC, MS-MIC,

or MS-MPC, the packet direction is output. For more information on inside and outside interfaces, see "Configuring Service Sets to be Applied to Services Interfaces" on page 9.

On the Multiservices PIC, MS-MIC, or MS-MPC, 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 CoS Rules

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

```
from {
    application-sets set-name;
    applications [ application-names ];
    destination-address address;
    destination-prefix-list list-name <except>;
    source-address address;
    source-prefix-list list-name <except>;
}
```

The source address and destination address can be either IPv4 or IPv6. You can use either the source address or the destination address as a match condition, in the same way that you would configure a firewall filter; for more information, see the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

Alternatively, you can specify a list of source or destination prefixes by configuring 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 CoS rule. For an example, see "Examples: Configuring Stateful Firewall Rules" on page 553.

If you omit the **from** term, the router accepts all traffic and the default protocol handlers take effect:

- User Datagram Protocol (UDP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) create a bidirectional flow with a predicted reverse flow.
- IP creates a unidirectional flow.

You can also include application protocol definitions you have configured at the **[edit applications]** hierarchy level; for more information, see "Configuring Application Properties" on page 502.

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

Configuring Actions in CoS Rules

IN THIS SECTION

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

```
[edit services cos rule rule-name term term-name]
then {
   application-profile profile-name;
   dscp (alias | bits);
   forwarding-class class-name;
   syslog;
   reflexive; | revert; | reverse {
      application-profile profile-name;
      dscp (alias | bits);
      forwarding-class class-name;
      syslog;
   }
}
```

The principal CoS actions are as follows:

- **dscp**—Causes the packet to be marked with the specified DiffServ code point (DSCP) value or alias.
- **forwarding-class**—Causes the packet to be assigned to the specified forwarding class.

For detailed information about DSCP values and forwarding classes, see "Examples: Configuring CoS on Services Interfaces" on page 830 or the *Class of Service User Guide (Routers and EX9200 Switches)*.

You can optionally set the configuration to record information in the system logging facility by including the **syslog** statement at the **[edit services cos rule *rule-name* term *term-name* then]** hierarchy level. This statement overrides any **syslog** setting included in the service set or interface default configuration.

For information about some additional CoS actions, see the following sections:

Configuring Application Profiles for Use as CoS Rule Actions

You can optionally define one or more application profiles for inclusion in CoS actions. To configure application profiles, include the **application-profile** statement at the **[edit services cos]** hierarchy level:

```
[edit services cos]
application-profile profile-name {
    ftp {
        data {
            dscp (alias | bits);
            forwarding-class class-name;
        }
    }
    sip {
        video {
            dscp (alias | bits);
            forwarding-class class-name;
        }
        voice {
            dscp (alias | bits);
            forwarding-class class-name;
        }
    }
}
```

The **application-profile** statement includes two main components and three traffic types: **ftp** with the **data** traffic type and **sip** with the **video** and **voice** traffic types. You can set the appropriate **dscp** and **forwarding-class** values for each component within the application profile.

> **NOTE:** The **ftp** and **sip** statements are not supported on Juniper Network MX Series 3D Universal Edge Routers.

You can apply the application profile to a CoS configuration by including it at the **[edit services cos rule *rule-name* term *term-name* then]** hierarchy level.

Configuring Reflexive, Revert, and Reverse CoS Rule Actions

CoS services are unidirectional. It might be necessary to specify different treatments for flows in opposite directions.

Regardless of whether a packet matches the input, output or input-output direction, flows in both directions are created. A forward, reverse, or forward-and-reverse CoS action is associated with each flow. Bear in mind that the flow in the reverse direction might end up having a CoS action associated with it that you have not specifically configured.

To control the direction in which service is applied, as distinct from the direction in which the rule match is applied, you can configure the (**reflexive | revert | reverse**) statement at the **[edit services cos rule *rule-name* term *term-name* then]** hierarchy level:

```
[edit services cos rule rule-name term term-name then]
reflexive; | revert; | reverse {
    application-profile profile-name;
    dscp (alias | bits);
    forwarding-class class-name;
    syslog;
}
```

The three actions are mutually exclusive:

- **reflexive** causes the CoS rule actions to be applied to flows in the reverse direction as well as to flows in the matching direction.
- Starting with Junos OS Release 16.1R5 and Junos OS Release 17.4R1, **revert** stores the DSCP and forwarding class of a packet that is received in the match direction of the rule and then applies that DSCP and forwarding class to packets that are received in the reverse direction of the same session.
- **reverse** allows you to define the CoS behavior for flows in the reverse direction.

If you omit the statement, data flows inherit the CoS behavior of the forward control flow.

Configuring CoS Session Creation When Packet Received in Non-Matching Direction

Starting with Junos OS Release 16.1R5 and Junos OS Release 17.4R1, you can configure a service set to create a CoS session even if a packet is first received in the wrong match direction for a CoS rule that is assigned to the service set. This results in the CoS rule values being applied as soon as a packet in the correct match direction is received. To configure this capability, include the **match-rules-on-reverse-flow** at the **[edit services service-set *service-set-name* cos-options]** hierarchy level:

```
[edit services service-set service-set-name cos-options]
match-rules-on-reverse-flow;
```

Example: Configuring CoS Rules

The following example shows a CoS configuration containing two rules, one for input matching on a specified application set and the other for output matching on a specified source address:

```
[edit services]
cos {
   rule my-cos-rule {
      match-direction input-output;
      term term1 {
         from {
            source-address 10.1.3.2/32;
            application-set sip;
         }
         then {
            dscp ef;
            syslog;
         }
      }
      term term2 {
         from {
            destination-address 10.2.3.2;
            applications http;
         }
         then {
            dscp af21;
         }
      }
   }
}
```

Release History Table

Release	Description
16.1R5	Starting with Junos OS Release 16.1R5 and Junos OS Release 17.4R1, **revert** stores the DSCP and forwarding class of a packet that is received in the match direction of the rule and then applies that DSCP and forwarding class to packets that are received in the reverse direction of the same session.
16.1R5	Starting with Junos OS Release 16.1R5 and Junos OS Release 17.4R1, you can configure a service set to create a CoS session even if a packet is first received in the wrong match direction for a CoS rule that is assigned to the service set.

RELATED DOCUMENTATION

- Class of Service Overview | 821
- Restrictions and Cautions for CoS Configuration on Services Interfaces | 822
- Configuring CoS Rule Sets | 830
- Examples: Configuring CoS on Services Interfaces | 830

Configuring CoS Rule Sets

The **rule-set** statement defines a collection of CoS 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 cos]** 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, the packet is dropped by default.

RELATED DOCUMENTATION

- Class of Service Overview | 821
- Restrictions and Cautions for CoS Configuration on Services Interfaces | 822
- Configuring CoS Rules | 823
- Examples: Configuring CoS on Services Interfaces | 830

Examples: Configuring CoS on Services Interfaces

To make settings consistent across Juniper Networks routers, you configure many CoS settings at the **[edit class-of-service]** hierarchy level to be used on services interfaces. When you commit this configuration along with what you configure at the **[edit services cos]** hierarchy level, these properties are applied to the Multiservices PIC, MS-MIC, or MS-MPC.

The following configuration examples at the **[edit class-of-service]** hierarchy level can be applied on services interfaces. For more information, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

> **NOTE:** The first two configurations, mapping forwarding-class name to forwarding-class ID and mapping forwarding-class name to queue number, are mutually exclusive.

Mapping Forwarding-Class Name to Forwarding-Class ID

Map forwarding-class names to forwarding-class IDs:

```
[edit class-of-service]
forwarding-classes {
    forwarding-class fc0 0;
    forwarding-class fc1 0;
    forwarding-class fc2 1;
    forwarding-class fc3 1;
    forwarding-class fc4 2;
    forwarding-class fc5 2;
    forwarding-class fc6 3;
    forwarding-class fc7 3;
    forwarding-class fc8 4;
    forwarding-class fc9 4;
    forwarding-class fc10 5;
    forwarding-class fc11 5;
    forwarding-class fc12 6;
    forwarding-class fc13 6;
    forwarding-class fc14 7;
    forwarding-class fc15 7;
}
```

Mapping Forwarding-Class Name to Queue Number

Map forwarding-class names to queue numbers:

```
[edit class-of-service]
forwarding-classes {
    queue 0 be;
    queue 1 ef;
```

```
        queue 2 af;
        queue 3 nc;
        queue 4 ef1;
        queue 5 ef2;
        queue 6 af1;
        queue 7 nc1;
    }
```

Mapping Diffserv Code Point Aliases to DSCP Bits

Map alias names to DSCP bit values. The aliases then can be used instead of the DSCP bits in adaptive services configurations.

```
    [edit class-of-service]
    code-point-aliases {
        (dscp | dscp-ipv6 | exp | ieee-802.1 | inet-precedence) {
            alias | bits;
        }
    }
```

Here is an example:

```
code-point-aliases {
    dscp {
        my1 110001;
        my2 101110;
        be 000001;
        cs7 110000;
    }
}
```

RELATED DOCUMENTATION

- Class of Service Overview | 821
- Restrictions and Cautions for CoS Configuration on Services Interfaces | 822
- Configuring CoS Rules | 823
- Configuring CoS Rule Sets | 830

CHAPTER 40

Configuring Class of Service on LSQ Interfaces

IN THIS CHAPTER

Link Services Configuration for Junos Interfaces

This topic provides links to topics explaining link services configuration for the following interface types:

- For information about configuring LSQ interface redundancy across multiple routers using SONET APS interfaces, see "Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS" on page 908
- For information about configuring LSQ interface redundancy in a single router using SONET APS interfaces, see "Configuring LSQ Interface Redundancy in a Single Router Using SONET APS" on page 911
- For information about configuring LSQ interface redundancy in a single router using Virtual Interfaces, see "Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces" on page 912
- For information about configuring CoS scheduling queues on Logical LSQ interfaces, see "Configuring CoS Scheduling Queues on Logical LSQ Interfaces" on page 834
- For information about configuring CoS fragmentation by forwarding class on LSQ interfaces, see"Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces" on page 839
- For information about reserving bundle bandwidth for Link-Layer overhead on LSQ interfaces, see "Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces" on page 926
- For information about configuring multiclass MLPPP on LSQ interfaces, see "Configuring Multiclass MLPPP on LSQ Interfaces" on page 927
- For information about oversubscribing interface bandwidth on LSQ interfaces, see "Oversubscribing Interface Bandwidth on LSQ Interfaces" on page 845

- For information about configuring guaranteed minimum rate on LSQ interfaces, see "Configuring Guaranteed Minimum Rate on LSQ Interfaces" on page 851
- For information about configuring link services and CoS on services PICs, see"Configuring Link Services and CoS on Services PICs" on page 841
- For information about configuring LSQ interfaces as NxT1 or NxE1 bundles using MLPPP, see"Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP" on page 932
- For information about configuring LSQ interfaces as NxT1 or NxE1 bundles using FRF.16, see"Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16" on page 938
- For information about configuring LSQ interfaces for single fractional T1 or E1 interfaces using MLPPP and LFI, see "Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI" on page 946
- For information about configuring LSQ interfaces for single fractional T1 or E1 interfaces using FRF.12, see "Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12" on page 952
- For information about configuring LSQ interfaces as NxT1 or NxE1 bundles using FRF.15, see "Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15" on page 945
- For information about configuring LSQ interfaces for T3 links configured for compressed RTP over MLPPP, see "Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP" on page 961
- For information about configuring LSQ interfaces as T3 or OC3 bundles using FRF.12, see "Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12" on page 963
- For information about configuring LSQ interfaces for ATM2 IQ interfaces using MLPPP, see "Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP" on page 965

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | 905

Configuring CoS Scheduling Queues on Logical LSQ Interfaces

For link services IQ (**lsq-**) interfaces, you can specify a scheduler map for each logical unit. A logical unit represents either an MLPPP bundle or a DLCI configured on a FRF.16 bundle. The scheduler is applied to the traffic sent to an AS or Multiservices PIC running the Layer 2 link services package.

If you configure a scheduler map on a bundle, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port*]** hierarchy level. If you configure a scheduler map on an FRF.16 DLCI, you

must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-*fpc/pic/port:channel*]** hierarchy level. For more information, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

If you need latency guarantees for multiclass or LFI traffic, you must use channelized IQ PICs for the constituent links. With non-IQ PICs, because queueing is not done at the channelized interface level on the constituent links, latency-sensitive traffic might not receive the type of service that it should. Constituent links from the following PICs support latency guarantees:

- Channelized E1 IQ PIC
- Channelized OC3 IQ PIC
- Channelized OC12 IQ PIC
- Channelized STM1 IQ PIC
- Channelized T3 IQ PIC

For scheduling queues on a logical interface, you can configure the following scheduler map properties at the **[edit class-of-service schedulers]** hierarchy level:

- **buffer-size**—The queue size; for more information, see "Configuring Scheduler Buffer Size" on page 836.
- **priority**—The transmit priority (low, high, strict-high); for more information, see "Configuring Scheduler Priority" on page 836.
- **shaping-rate**—The subscribed transmit rate; for more information, see "Configuring Scheduler Shaping Rate" on page 837.
- **drop-profile-map**—The random early detection (RED) drop profile; for more information, see "Configuring Drop Profiles" on page 837.

When you configure MLPPP and FRF.12 on M Series and T Series routers, you should configure a single scheduler with non-zero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ interface (**lsq**) and to each constituent link.

When you configure FRF.16 on M Series and T Series routers, you can assign a single scheduler map to the link services IQ interface (**lsq**) and to each link services IQ DLCI, or you can assign different scheduler maps to the various DLCIs of the bundle, as shown in "Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16" on page 942. For the constituent links of an FRF.16 bundle, you do not need to configure a custom scheduler. Because LFI and multiclass are not supported for FRF.16, the traffic from each constituent link is transmitted from queue 0. This means you should allow most of the bandwidth to be used by queue 0. The default scheduler transmission rate and buffer size percentages for queues 0 through 3 are 95, 0, 0, and 5 percent, respectively. This default scheduler sends all user traffic to queue 0 and all network-control traffic to queue 3, and therefore it is well suited to the behavior of FRF.16. You can configure a custom scheduler that explicitly replicates the 95, 0, 0, and 5 percent queuing behaviors, and apply it to the constituent links.

> **NOTE:** On T Series and M320 routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

For link services IQ interfaces (**lsq**), these scheduling properties work as they do in other PICs, except as noted in the following sections.

> **NOTE:** On T Series and M320 routers, **lsq** interfaces do not support DiffServ code point (DSCP) and DSCP-IPv6 rewrite markers.

Configuring Scheduler Buffer Size

You can configure the scheduler buffer size in three ways: as a temporal value, as a percentage, and as a remainder. On a single logical interface (MLPPP or a FRF.16 DLCI), each queue can have a different buffer size.

If you specify a temporal value, the queuing algorithm starts dropping packets when it queues more than a computed number of bytes. This number is computed by multiplying logical interface speed by the temporal value. For MLPPP bundles, logical interface speed is equal to the bundle bandwidth, which is the sum of constituent link speeds minus link-layer overhead. For MLFR FRF.16 DLCIs, logical interface speed is equal to bundle bandwidth multiplied by the DLCI shaping rate. In all cases, the maximum temporal value is limited to 200 milliseconds.

Buffer size percentages are implicitly converted into temporal values by multiplying the percentage by 200 milliseconds. For example, buffer size specified as **buffer-size percent 20** is the same as a 40-millisecond temporal delay. The link services IQ implementation guarantees 200 milliseconds of buffer delay for all interfaces with T1 and higher speeds. For slower interfaces, it guarantees one second of buffer delay.

The queueing algorithm evenly distributes leftover bandwidth among all queues that are configured with the **buffer-size remainder** statement. The queuing algorithm guarantees enough space in the transmit buffer for two MTU-sized packets.

Configuring Scheduler Priority

The transmit priority of each queue is determined by the scheduler and the forwarding class. Each queue receives a guaranteed amount of bandwidth specified with the scheduler **transmit-rate** statement.

Configuring Scheduler Shaping Rate

You use the shaping rate to set the percentage of total bundle bandwidth that is dedicated to a DLCI. For link services IQ DLCIs, only percentages are accepted, which allows adjustments in response to dynamic changes in bundle bandwidth—for example, when a link goes up or down. This means that absolute shaping rates are not supported on FRF.16 bundles. Absolute shaping rates are allowed for MLPPP and MLFR bundles only.

For scheduling between DLCIs in a MLFR FRF.16 bundle, you can configure a shaping rate for each DLCI. A shaping rate is expressed as a percentage of the aggregate bundle bandwidth. Shaping rate percentages for all DLCIs within a bundle can add up to 100 percent or less. Leftover bandwidth is distributed equally to DLCIs that do not have the **shaping-rate** statement included at the **[edit class-of-service interfaces lsq-*fpc*/*pic*/*port*:*channel* unit *logical-unit-number*]** hierarchy level. If none of the DLCIs in an MLFR FRF.16 bundle specify a DLCI scheduler, the total bandwidth is evenly divided across all DLCIs.

> **NOTE:** For FRF.16 bundles on link services IQ interfaces, only shaping rates based on percentage are supported.

Configuring Drop Profiles

You can configure random early detection (RED) on LSQ interfaces as in other CoS scenarios. To configure RED, include one or more drop profiles and attach them to a scheduler for a particular forwarding class. For more information about RED profiles, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

The LSQ implementation performs tail RED. It supports a maximum of 256 drop profiles per PIC. Drop profiles are configurable on a per-queue, per-loss-priority, and per-TCP-bit basis.

You can attach scheduler maps with configured RED drop profiles to any LSQ logical interface: an MLPPP bundle, an FRF.15 bundle, or an FRF.16 DLCI. Different queues (forwarding classes) on the same logical interface can have different associated drop profiles.

The following example shows how to configure a RED profile on an LSQ interface:

```
[edit]
class-of-service {
   drop-profiles {
      drop-low {
         # Configure suitable drop profile for low loss priority
         ...
      }
      drop-high {
```

```
            # Configure suitable drop profile for high loss priority
            ...
        }
    }
    scheduler-maps {
        schedmap {
            # Best-effort queue will use be-scheduler
            # Other queues may use different schedulers
            forwarding-class be scheduler be-scheduler;
            ...
        }
    }
    schedulers {
        be-scheduler {
            # Configure two drop profiles for low and high loss priority
            drop-profile-map loss-priority low protocol any drop-profile drop-low;
            drop-profile-map loss-priority high protocol any drop-profile drop-high;
            # Other scheduler parameters (buffer-size, priority,
            # and transmit-rate) are already supported.
            ...
        }
    }
    interfaces {
        lsq-1/3/0.0 {
            # Attach a scheduler map (that includes RED drop profiles)
            # to a LSQ logical interface.
            scheduler-map schedmap;
        }
    }
}
```

NOTE: The RED profiles should be applied only on the LSQ bundles and not on the egress links that constitute the bundle.

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | **905**
- Configuring Link Services and CoS on Services PICs | **841**
- Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces | **839**

Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces

For link services IQ (**lsq-**) interfaces, you can specify fragmentation properties for specific forwarding classes. Traffic on each forwarding class can be either multilink encapsulated (fragmented and sequenced) or nonencapsulated (hashed with no fragmentation). By default, traffic in all forwarding classes is multilink encapsulated.

When you do not configure fragmentation properties for the queues on MLPPP interfaces, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number* fragment-threshold]** hierarchy level is the fragmentation threshold for all forwarding classes within the MLPPP interface. For MLFR FRF.16 interfaces, the fragmentation threshold you set at the **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options fragment-threshold]** hierarchy level is the fragmentation threshold for all forwarding classes within the MLFR FRF.16 interface.

If you do not set a maximum fragment size anywhere in the configuration, packets are still fragmented if they exceed the smallest maximum transmission unit (MTU) or maximum received reconstructed unit (MRRU) of all the links in the bundle. A nonencapsulated flow uses only one link. If the flow exceeds a single link, then the forwarding class must be multilink encapsulated, unless the packet size exceeds the MTU/MRRU.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the MRRU by including the **mrru** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see *Configuring MRRU on Multilink and Link Services Logical Interfaces*.

To configure fragmentation properties on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            (fragment-threshold bytes | no-fragmentation);
            multilink-class number;
        }
    }
}
```

To set a per-forwarding class fragmentation threshold, include the **fragment-threshold** statement in the fragmentation map. This statement sets the maximum size of each multilink fragment.

To set traffic on a queue to be nonencapsulated rather than multilink encapsulated, include the **no-fragmentation** statement in the fragmentation map. This statement specifies that an extra fragmentation header is not prepended to the packets received on this queue and that static link load balancing is used to ensure in-order packet delivery.

For a given forwarding class, you can include either the **fragment-threshold** or **no-fragmentation** statement; they are mutually exclusive.

You use the **multilink-class** statement to map a forwarding class into a multiclass MLPPP (MCML). For a given forwarding class, you can include either the **multilink-class** or **no-fragmentation** statement; they are mutually exclusive. For more information about MCML, see "Configuring Multiclass MLPPP on LSQ Interfaces" on page 927.

To associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI, include the **fragmentation-map** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
[edit class-of-service interfaces]
lsq-fpc/pic/port {
    unit logical-unit-number { # Multilink PPP
    fragmentation-map map-name;
}
lsq-fpc/pic/port:channel { # MLFR FRF.16
unit logical-unit-number {
    fragmentation-map map-name;
}
```

For configuration examples, see the following topics:

- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP on page 932
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16 on page 938
- Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI on page 946
- Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12 on page 952
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15 on page 945
- Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP on page 961
- Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12 on page 963
- Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP on page 965

For Link Services PIC link services (**ls-**) interfaces, fragmentation maps are not supported. Instead, you enable LFI by including the **interleave-fragments** statement at the **[edit interfaces *interface-name* unit**

logical-unit-number] hierarchy level. For more information, see *Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces*.

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | **905**
- Configuring Link Services and CoS on Services PICs | **841**
- Configuring CoS Scheduling Queues on Logical LSQ Interfaces | **834**
- Link Services Configuration for Junos Interfaces | **833**

Configuring Link Services and CoS on Services PICs

To configure link services and CoS on an AS or Multiservices PIC, you must perform the following steps:

1. Enable the Layer 2 service package. You enable service packages per PIC, not per port. When you enable the Layer 2 service package, the entire PIC uses the configured package. To enable the Layer 2 service package, include the **service-package** statement at the **[edit chassis fpc *slot-number* pic *pic-number* adaptive-services]** hierarchy level, and specify **layer-2**:

   ```
   [edit chassis fpc slot-number pic pic-number adaptive-services]
   service-package layer-2;
   ```

   For more information about AS or Multiservices PIC service packages, see *Enabling Service Packages* and "Layer 2 Service Package Capabilities and Interfaces" on page 905.

2. Configure a multilink PPP or FRF.16 bundle by combining constituent links into a virtual link, or bundle.

   Configuring an MLPPP Bundle

   To configure an MLPPP bundle, configure constituent links and bundle properties by including the following statements in the configuration:

   ```
   [edit interfaces interface-name unit logical-unit-number]
   encapsulation ppp;
   family mlppp {
      bundle lsq-fpc/pic/port.logical-unit-number;
   }
   [edit interfaces lsq-fpc/pic/port unit logical-unit-number]
   drop-timeout milliseconds;
   ```

```
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
   address address;
}
```

For more information about these statements, see the *Link and Multilink Services Interfaces User Guide for Routing Devices*.

Configuring an MLFR FRF.16 Bundle

To configure an MLFR FRF.16 bundle, configure constituent links and bundle properties by including the following statements in the configuration:

```
[edit chassis fpc slot-number pic slot-number]
mlfr-uni-nni-bundles number;
[edit interfaces interface-name ]
encapsulation multilink-frame-relay-uni-nni;
unit logical-unit-number {
   family mlfr-uni-nni {
      bundle lsq-fpc/pic/port:channel;
   }
}
```

For more information about the **mlfr-uni-nni-bundles** statement, see the *Junos OS Administration Library*. MLFR FRF.16 uses channels as logical units.

For MLFR FRF.16, you must configure one end as data circuit-terminating equipment (DCE) by including the following statements at the **[edit interfaces lsq-*fpc*/*pic*/*port*:*channel*]** hierarchy level.

```
encapsulation multilink-frame-relay-uni-nni;
dce;
mlfr-uni-nni-options {
   acknowledge-retries number;
   acknowledge-timer milliseconds;
   action-red-differential-delay (disable-tx | remove-link);
   drop-timeout milliseconds;
   fragment-threshold bytes;
   hello-timer milliseconds;
```

```
    link-layer-overhead percent;
    lmi-type (ansi | itu);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 number;
    t392 number;
    yellow-differential-delay milliseconds;
}
unit logical-unit-number {
    dlci dlci-identifier;
    family inet {
        address address;
    }
}
```

For more information about MLFR UNI NNI properties, see *Link and Multilink Services Interfaces User Guide for Routing Devices*.

3. To configure CoS components for each multilink bundle, enable per-unit scheduling on the interface, configure a scheduler map, apply the scheduler to each queue, configure a fragmentation map, and apply the fragmentation map to each bundle. Include the following statements:

```
[edit interfaces]
lsq-fpc/pic/port {
    per-unit-scheduler; # Enables per-unit scheduling on the bundle
}
[edit class-of-service]
interfaces {
    lsq-fpc/pic/port { # Multilink PPP
    unit logical-unit-number {
        scheduler-map map-name; # Applies scheduler map to each queue
    }
}
lsq-fpc/pic/port:channel { # MLFR FRF.16
unit logical-unit-number {
    # Scheduler map provides scheduling information for
    # the queues within a single DLCI.
    scheduler-map map-name;
    shaping-rate percent percent;
}
```

```
forwarding-classes {
   queue queue-number class-name priority (high | low);
}
scheduler-maps {
   map-name {
      forwarding-class class-name scheduler scheduler-name;
   }
}
schedulers {
   scheduler-name {
      buffer-size (percent percentage | remainder | temporal microseconds);
      priority priority-level;
      transmit-rate (percent percentage | rate | remainder) <exact>;
   }
}
fragmentation-maps {
   map-name {
      forwarding-class class-name {
         fragment-threshold bytes;
         no-fragmentation;
      }
   }
}
```

Associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI by including the following statements at the **[edit class-of-service]** hierarchy level:

```
interfaces {
   lsq-fpc/pic/port {
      unit logical-unit-number { # Multilink PPP
      fragmentation-map map-name;
   }
}
lsq-fpc/pic/port:channel { # MLFR FRF.16
unit logical-unit-number {
   fragmentation-map map-name;
}
```

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | 905

Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS | 908

Configuring LSQ Interface Redundancy in a Single Router Using SONET APS | 911
Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912
Link Services Configuration for Junos Interfaces | 833

Oversubscribing Interface Bandwidth on LSQ Interfaces

The term *oversubscribing interface bandwidth* means configuring shaping rates (peak information rates [PIRs]) so that their sum exceeds the interface bandwidth.

On Channelized IQ PICs, Gigabit Ethernet IQ PICs, and FRF.16 link services IQ (**lsq-**) interfaces on AS and Multiservices PICs, you can oversubscribe interface bandwidth. The logical interfaces (and DLCIs within an FRF.16 bundle) can be oversubscribed when there is leftover bandwidth. The oversubscription is limited to the configured PIR. Any unused bandwidth is distributed equally among oversubscribed logical interfaces or DLCIs.

For networks that are not likely to experience congestion, oversubscribing interface bandwidth improves network utilization, thereby allowing more customers to be provisioned on a single interface. If the actual data traffic does not exceed the interface bandwidth, oversubscription allows you to sell more bandwidth than the interface can support.

We recommend avoiding oversubscription in networks that are likely to experience congestion. Be careful not to oversubscribe a service by too much, because this can cause degradation in the performance of the router during congestion. When you configure oversubscription, some output queues can be starved if the actual data traffic exceeds the physical interface bandwidth. You can prevent degradation by using statistical multiplexing to ensure that the actual data traffic does not exceed the interface bandwidth.

> **NOTE:** You cannot oversubscribe interface bandwidth when you configure traffic shaping using the method described in *Applying Scheduler Maps and Shaping Rate to DLCIs and VLANs*.

When configuring oversubscription for FRF.16 bundle interfaces, you can assign traffic control profiles that apply on a physical interface basis. When you apply traffic control profiles to FRF.16 bundles at the *logical* interface level, member link interface bandwidth is underutilized when there is a small proportion of traffic or no traffic at all on an individual DLCI. Support for traffic control features on the FRF.16 bundle physical interface level addresses this limitation.

To configure oversubscription of an interface, perform the following steps:

1. Include the **shaping-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]
shaping-rate (percent percentage | rate);
```

NOTE: When configuring oversubscription for FRF.16 bundle interfaces on a physical interface basis, you *must* specify **shaping-rate** as a percentage.

On LSQ interfaces, you can configure the shaping rate as a percentage.

On IQ and IQ2 interfaces, you can configure the shaping rate as an absolute rate from 1000 through 6,400,000,000,000 bits per second.

Alternatively, you can configure a shaping rate for a logical interface and oversubscribe the physical interface by including the **shaping-rate** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level. However, with this configuration approach, you cannot independently control the delay-buffer rate, as described in Step 2.

NOTE: For channelized and Gigabit Ethernet IQ interfaces, the **shaping-rate** and **guaranteed-rate** statements are mutually exclusive. You cannot configure some logical interfaces to use a shaping rate and others to use a guaranteed rate. This means there are no service guarantees when you configure a PIR. For these interfaces, you can configure either a PIR or a committed information rate (CIR), but not both.

This restriction does not apply to Gigabit Ethernet IQ2 PICs or link services IQ (LSQ) interfaces on AS or Multiservices PICs. For LSQ and Gigabit Ethernet IQ2 interfaces, you can configure both a PIR and a CIR on an interface. For more information about CIRs, see "Configuring Guaranteed Minimum Rate on LSQ Interfaces" on page 851.

2. Optionally, you can base the delay buffer calculation on a delay-buffer rate. To do this, include the **delay-buffer-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

   NOTE: When configuring oversubscription for FRF.16 bundle interfaces on a physical interface basis, you *must* specify **delay-buffer-rate** as a percentage.

   ```
   [edit class-of-service traffic-control-profiles profile-name]
   delay-buffer-rate (percent percentage | rate);
   ```

The delay-buffer rate overrides the shaping rate as the basis for the delay-buffer calculation. In other words, the shaping rate or scaled shaping rate is used for delay-buffer calculations only when the delay-buffer rate is not configured.

For LSQ interfaces, if you do not configure a delay-buffer rate, the guaranteed rate (CIR) is used to assign buffers. If you do not configure a guaranteed rate, the shaping rate (PIR) is used in the undersubscribed case, and the scaled shaping rate is used in the oversubscribed case.

On LSQ interfaces, you can configure the delay-buffer rate as a percentage.

On IQ and IQ2 interfaces, you can configure the delay-buffer rate as an absolute rate from 1000 through 6,400,000,000,000 bits per second.

The actual delay buffer is based on the calculations described in the *Class of Service User Guide (Routers and EX9200 Switches)*. For an example showing how the delay-buffer rates are applied, see "Examples: Oversubscribing an LSQ Interface" on page 848.

Configuring large buffers on relatively low-speed links can cause packet aging. To help prevent this problem, the software requires that the sum of the delay-buffer rates be less than or equal to the port speed.

This restriction does not eliminate the possibility of packet aging, so you should be cautious when using the **delay-buffer-rate** statement. Though some amount of extra buffering might be desirable for burst absorption, delay-buffer rates should not far exceed the service rate of the logical interface.

If you configure delay-buffer rates so that the sum exceeds the port speed, the configured delay-buffer rate is not implemented for the last logical interface that you configure. Instead, that logical interface receives a delay-buffer rate of zero, and a warning message is displayed in the CLI. If bandwidth becomes available (because another logical interface is deleted or deactivated, or the port speed is increased), the configured delay-buffer-rate is reevaluated and implemented if possible.

If you do not configure a delay-buffer rate or a guaranteed rate, the logical interface receives a delay-buffer rate in proportion to the shaping rate and the remaining delay-buffer rate available. In other words, the delay-buffer rate for each logical interface with no configured delay-buffer rate is equal to:

```
(remaining delay-buffer rate * shaping rate) / (sum of shaping rates)
```

The remaining delay-buffer rate is equal to:

```
(interface speed) – (sum of configured delay-buffer rates)
```

3. To assign a scheduler map to the logical interface, include the **scheduler-map** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

```
[edit class-of-service traffic-control-profiles profile-name]
scheduler-map map-name;
```

For information about configuring schedulers and scheduler maps, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

4. Optionally, you can enable large buffer sizes to be configured. To do this, include the **q-pic-large-buffer** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level:

   ```
   [edit chassis fpc slot-number pic pic-number]
   q-pic-large-buffer;
   ```

   If you do not include this statement, the delay-buffer size is more restricted. We recommend restricted buffers for delay-sensitive traffic, such as voice traffic. For more information, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

5. To enable scheduling on logical interfaces, include the **per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

   ```
   [edit interfaces interface-name ]
   per-unit-scheduler;
   ```

   When you include this statement, the maximum number of VLANs supported is 768 on a single-port Gigabit Ethernet IQ PIC. On a two-port Gigabit Ethernet IQ PIC, the maximum number is 384.

6. To enable scheduling for FRF.16 bundles physical interfaces, include the **no-per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

   ```
   [edit interfaces interface-name]
   no-per-unit-scheduler;
   ```

7. To apply the traffic-scheduling profile to the logical interface, include the **output-traffic-control-profile** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

   ```
   [edit class-of-service interfaces interface-name unit logical-unit-number]
   output-traffic-control-profile profile-name;
   ```

   You cannot include the **output-traffic-control-profile** statement in the configuration if any of the following statements are included in the logical interface configuration: **scheduler-map**, **shaping-rate**, **adaptive-shaper**, or **virtual-channel-group**.

   For a table that shows how the bandwidth and delay buffer are allocated in various configurations, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

Examples: Oversubscribing an LSQ Interface

Oversubscribing an LSQ Interface with Scheduling Based on the Logical Interface

Apply a traffic-control profile to a logical interface representing a DLCI on an FRF.16 bundle.

```
interfaces {
    lsq-1/3/0:0 {
        per-unit-scheduler;
        unit 0 {
            dlci 100;
        }
        unit 1 {
            dlci 200;
        }
    }
}
class-of-service {
    traffic-control-profiles {
        tc_0 {
            shaping-rate percent 100;
            guaranteed-rate percent 60;
            delay-buffer-rate percent 80;
        }
        tc_1 {
            shaping-rate percent 80;
            guaranteed-rate percent 40;
        }
    }
    interfaces {
        lsq-1/3/0 {
            unit 0 {
                output-traffic-control-profile tc_0;
            }
            unit 1 {
                output-traffic-control-profile tc_1;
            }
        }
    }
}
```

Oversubscribing an LSQ Interface with Scheduling Based on the Physical Interface

Apply a traffic-control profile to the physical interface representing an FRF.16 bundle:

```
interfaces {
    lsq-0/2/0:0 {
        no-per-unit-scheduler;
        encapsulation multilink-frame-relay-uni-nni;
        unit 0 {
            dlci 100;
            family inet {
                address 18.18.18.2/24;
            }
        }
    }
class-of-service {
    traffic-control-profiles {
        rlsq_tc {
            scheduler-map rlsq;
            shaping-rate percent 60;
            delay-buffer-rate percent 10;
        }
    }
    interfaces {
        lsq-0/2/0:0 {
            output-traffic-control-profile rlsq_tc;
        }
    }
}
scheduler-maps {
    rlsq {
        forwarding-class best-effort scheduler rlsq_scheduler;
        forwarding-class expedited-forwarding scheduler rlsq_scheduler1;
    }
}
schedulers {
    rlsq_scheduler {
        transmit-rate percent 20;
        priority low;
    }
    rlsq_scheduler1 {
        transmit-rate percent 40;
        priority high;
    }
}
```

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | 905

Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces | 926

Configuring Guaranteed Minimum Rate on LSQ Interfaces | 851

Link Services Configuration for Junos Interfaces | 833

Configuring Guaranteed Minimum Rate on LSQ Interfaces

On Gigabit Ethernet IQ PICs, Channelized IQ PICs, and FRF.16 link services IQ (LSQ) interfaces on AS and Multiservices PICs, you can configure guaranteed bandwidth, also known as a committed information rate (CIR). This allows you to specify a guaranteed rate for each logical interface. The guaranteed rate is a minimum. If excess physical interface bandwidth is available for use, the logical interface receives more than the guaranteed rate provisioned for the interface.

You cannot provision the sum of the guaranteed rates to be more than the physical interface bandwidth, or the bundle bandwidth for LSQ interfaces. If the sum of the guaranteed rates exceeds the interface or bundle bandwidth, the commit operation does not fail, but the software automatically decreases the rates so that the sum of the guaranteed rates is equal to the available bundle bandwidth.

To configure a guaranteed minimum rate, perform the following steps:

1. Include the **guaranteed-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

   ```
   [edit class-of-service traffic-control-profiles profile-name]
   guaranteed-rate (percent percentage | rate);
   ```

   On LSQ interfaces, you can configure the guaranteed rate as a percentage.

   On IQ and IQ2 interfaces, you can configure the guaranteed rate as an absolute rate from 1000 through 160,000,000,000 bits per second.

> **NOTE:** For channelized and Gigabit Ethernet IQ interfaces, the **shaping-rate** and **guaranteed-rate** statements are mutually exclusive. You cannot configure some logical interfaces to use a shaping rate and others to use a guaranteed rate. This means there are no service guarantees when you configure a PIR. For these interfaces, you can configure either a PIR or a committed information rate (CIR), but not both.
>
> This restriction does not apply to Gigabit Ethernet IQ2 PICs or link services IQ (LSQ) interfaces on AS or Multiservices PICs. For LSQ and Gigabit Ethernet IQ2 interfaces, you can configure both a PIR and a CIR on an interface. For more information about CIRs, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

2. Optionally, you can base the delay buffer calculation on a delay-buffer rate. To do this, include the **delay-buffer-rate** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

   ```
   [edit class-of-service traffic-control-profiles profile-name]
   delay-buffer-rate (percent percentage | rate);
   ```

   On LSQ interfaces, you can configure the delay-buffer rate as a percentage.

   On IQ and IQ2 interfaces, you can configure the delay-buffer rate as an absolute rate from 1000 through 160,000,000,000 bits per second.

   The actual delay buffer is based on the calculations described in tables in the *Class of Service User Guide (Routers and EX9200 Switches)*. For an example showing how the delay-buffer rates are applied, see "Example: Configuring Guaranteed Minimum Rate" on page 854.

   If you do not include the **delay-buffer-rate** statement, the delay-buffer calculation is based on the guaranteed rate, the shaping rate if no guaranteed rate is configured, or the scaled shaping rate if the interface is oversubscribed.

   If you do not specify a shaping rate or a guaranteed rate, the logical interface receives a minimal delay-buffer rate and minimal bandwidth equal to 4 MTU-sized packets.

   You can configure a rate for the delay buffer that is higher than the guaranteed rate. This can be useful when the traffic flow might not require much bandwidth in general, but in some cases can be bursty and therefore needs a large buffer.

   Configuring large buffers on relatively low-speed links can cause packet aging. To help prevent this problem, the software requires that the sum of the delay-buffer rates be less than or equal to the port speed. This restriction does not eliminate the possibility of packet aging, so you should be cautious when using the **delay-buffer-rate** statement. Though some amount of extra buffering might be desirable for burst absorption, delay-buffer rates should not far exceed the service rate of the logical interface.

If you configure delay-buffer rates so that the sum exceeds the port speed, the configured delay-buffer rate is not implemented for the last logical interface that you configure. Instead, that logical interface receives a delay-buffer rate of 0, and a warning message is displayed in the CLI. If bandwidth becomes available (because another logical interface is deleted or deactivated, or the port speed is increased), the configured delay-buffer-rate is reevaluated and implemented if possible.

If the guaranteed rate of a logical interface cannot be implemented, that logical interface receives a delay-buffer rate of 0, even if the configured delay-buffer rate is within the interface speed. If at a later time the guaranteed rate of the logical interface can be met, the configured delay-buffer rate is reevaluated and if the delay-buffer rate is within the remaining bandwidth, it is implemented.

If any logical interface has a configured guaranteed rate, all other logical interfaces on that port that do not have a guaranteed rate configured receive a delay-buffer rate of 0. This is because the absence of a guaranteed rate configuration corresponds to a guaranteed rate of 0 and, consequently, a delay-buffer rate of 0.

3. To assign a scheduler map to the logical interface, include the **scheduler-map** statement at the **[edit class-of-service traffic-control-profiles *profile-name*]** hierarchy level:

   ```
   [edit class-of-service traffic-control-profiles profile-name]
   scheduler-map map-name;
   ```

   For information about configuring schedulers and scheduler maps, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

4. To enable large buffer sizes to be configured, include the **q-pic-large-buffer** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level:

   ```
   [edit chassis fpc slot-number pic pic-number]
   q-pic-large-buffer;
   ```

   If you do not include this statement, the delay-buffer size is more restricted. For more information, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

5. To enable scheduling on logical interfaces, include the **per-unit-scheduler** statement at the **[edit interfaces *interface-name*]** hierarchy level:

   ```
   [edit interfaces interface-name ]
   per-unit-scheduler;
   ```

   When you include this statement, the maximum number of VLANs supported is 767 on a single-port Gigabit Ethernet IQ PIC. On a two-port Gigabit Ethernet IQ PIC, the maximum number is 383.

6. To apply the traffic-scheduling profile to the logical interface, include the output-traffic-control-profile statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number*]** hierarchy level:

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
output-traffic-control-profile profile-name;
```

Example: Configuring Guaranteed Minimum Rate

Two logical interface units, **0** and **1**, are provisioned with a guaranteed minimum of 750 Kbps and 500 Kbps, respectively. For logical unit **1**, the delay buffer is based on the guaranteed rate setting. For logical unit **0**, a delay-buffer rate of 500 Kbps is specified. The actual delay buffers allocated to each logical interface are 2 seconds of 500 Kbps. The 2-second value is based on the following calculation:

```
delay-buffer-rate < [8 x 64 Kbps]): 2 seconds of delay-buffer-rate
```

For more information about this calculation, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

```
chassis {
    fpc 3 {
        pic 0 {
            q-pic-large-buffer;
        }
    }
}
interfaces {
    t1-3/0/1 {
        per-unit-scheduler;
    }
}
class-of-service {
    traffic-control-profiles {
        tc-profile3 {
            guaranteed-rate 750k;
            scheduler-map sched-map3;
            delay-buffer-rate 500k; # 500 Kbps is less than 8 x 64 Kbps
        }
        tc-profile4 {
            guaranteed-rate 500k; # 500 Kbps is less than 8 x 64 Kbps
            scheduler-map sched-map4;
        }
    }
    interface t1-3/0/1 {
        unit 0 {
            output-traffic-control-profile tc-profile3;
```

```
        }
        unit 1 {
            output-traffic-control-profile tc-profile4;
        }
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | **905**
- Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces | **926**
- Oversubscribing Interface Bandwidth on LSQ Interfaces | **845**
- Link Services Configuration for Junos Interfaces | **833**

8

PART

Configuring Inter-Chassis MS-MPC and MS-MIC Redundancy for NAT and Stateful Firewall

CHAPTER 41

Configuring Inter-Chassis MS-MPC and MS-MIC Redundancy for NAT and Stateful Firewall (Release 16.1 and later)

IN THIS CHAPTER

Configuring Inter-chassis MS-MPC and MS-MIC Redundancy for NAT and Stateful Firewall Overview (Release 16.1 and later)

NOTE: This topic applies to Junos OS release 16.1 and higher. (For Junos OS release 15.1 and earlier, see "Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier)" on page 888).

Carrier-grade NAT (CGN) and stateful firewall deployments can use a dual-chassis implementation to provide a redundant data path and redundancy for key components in the router. Although intra-chassis high availability can be used in an MX Series device by employing the AMS interfaces, this method only deals locally with service PIC and full MS-MPC or MS-MIC card failures. If for any reason traffic is switched to a backup router due to some other failure in the router, the session state from the Service PICs is lost.

Inter-chassis high availability offers a more robust solution by preserving the session state of NAT and stateful firewalls from the services PICs. This technology is a primary-secondary model, not an active-active cluster. Traffic to be serviced by the services PICs that are configured for inter-chassis high availability only flows through the MX Series device that is currently the master in the pair.

To configure interchassis redundancy for NAT and stateful firewall, you configure:

1. Stateful synchronization, which replicates the session state from the services PICs on the master chassis to the backup chassis. For more information, see "Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)" on page 858.
2. The service redundancy daemon, which allows mastership switchover to occur based on a monitored event. Most operators would not want to employ stateful synchronization without also implementing the service redundancy daemon. For more information, see "Service Redundancy Daemon Overview" on page 875

Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)

> **NOTE:** This topic applies to Junos OS release 16.1 and higher. (For Junos OS release 15.1 and earlier, see "Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier)" on page 888).

Stateful synchronization synchronizes long-lived sessions between the master and backup MX Series chassis in the high availability pair. By default, long lived sessions are stateful firewall, NAT, and IDS sessions that have been active on the services PIC for 180 seconds, though you can configure this to be a higher or lower value. Stateful firewall sessions, NAT sessions, and IDS sessions are the session types that can be synchronized.

Inter-chassis high availability works with ms- service interfaces configured on MS-MIC or MS-MPC interface cards. An ms- interface unit other than unit 0 must be configured with the **ip-address-owner service-plane** option.

The following NAT translation types and sessions support stateful synchronization:

- basic-nat44
- dynamic-nat44
- napt-44
- napt-44 with endpoint-independent mapping (EIM), or endpoint-independent filters (EIF)

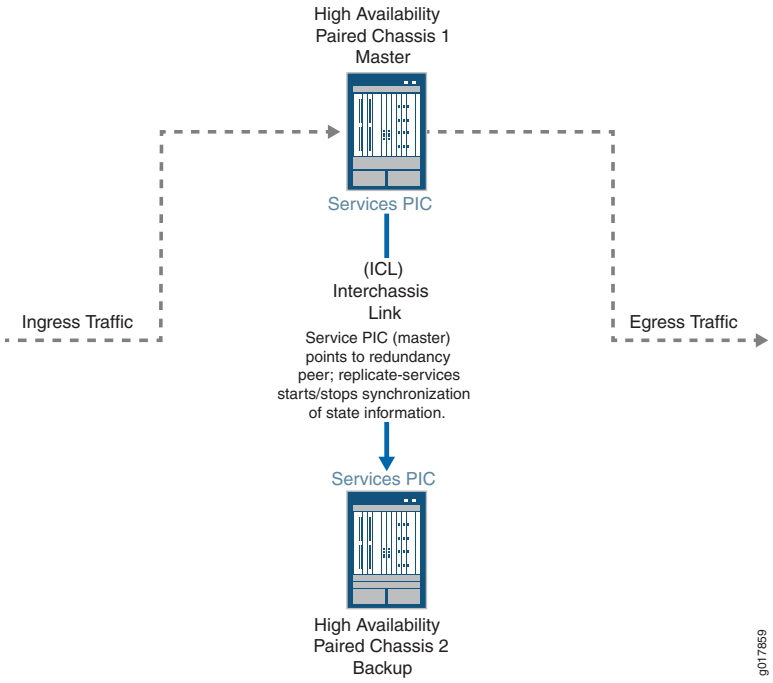
- dnat-44
- twice-nat
- stateful-nat64

The following restrictions apply:

- Replicating state information for the port block allocation (PBA), endpoint-independent mapping (EIM), or endpoint-independent filters (EIF) features is not supported.
- When configuring a service set for NAT or stateful firewall that belongs to a stateful synchronization setup, - the NAT and stateful firewall configurations for the service set must be identical on both MX Series devices.
- Application Layer Gateway (ALG) sessions do not support stateful synchronization.

Figure 40 on page 859 shows the inter-chassis high availability topology.

Figure 40: Stateful Sync Topology



RELATED DOCUMENTATION

Configuring Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) (Release 16.1 and later) | **860**

Configuring Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) (Release 16.1 and later)

NOTE: This topic applies to Junos OS release 16.1 and higher. (For Junos OS release 15.1 and earlier, see "Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier)" on page 888).

To configure stateful synchronization inter-chassis high availability for stateful firewall and NAPT44 on MS-MIC or MS-MPC service PICs, perform the following configuration steps on each chassis of the high availability pair.

1. Configure the services ms- interface.

   a. Specify the IPv4 address of the local services card. This address is used by the TCP channel between the HA pairs.

      ```
      [edit interfaces interface-name redundancy-options]
      user@host# set redundancy-local data-address address
      ```

      When you configure the other chassis, this is the address you use for the **redundancy-peer ipaddress**.

   b. Specify the IPv4 address of the remote services card. This address is used by the TCP channel between the HA pairs.

      ```
      [edit interfaces interface-name redundancy-options]
      user@host# set redundancy-peer ipaddress address
      ```

      When you configure the other chassis, this is the address you use for the **redundancy-local data-address**.

   c. Configure the length of time that the flow remains active for replication, in seconds.

      ```
      [edit interfaces interface-name redundancy-options]
      user@host# set replication-threshold seconds
      ```

   d. Configure a unit other than 0 with the **ip-address-owner service-plane** option.

      ```
      [edit interfaces interface-name]
      user@host# set unit logical-unit-number ip-address-owner service-plane
      ```

   e. For the unit configured with the **ip-address-owner service-plane** option, assign the IPv4 address of the local services card that you configured with the **redundancy-local data-address** option.

      ```
      [edit interfaces interface-name unit logical-unit-number]
      user@host# set family inet addressaddress
      ```

   f. Configure the inside and outside interface units, which are used by the next-hop service set. Use different unit numbers for the inside and outside units, and do not use 0 or the unit number used with the **ip-address-owner service-plane** option.

      ```
      [edit]
      user@host# set interfaces interface-name unit logical-unit-number family inet
      user@host# set interfaces interface-name unit logical-unit-number service-domain inside
      user@host# set interfaces interface-name unit logical-unit-number family inet
      user@host# set interfaces interface-name unit logical-unit-number service-domain outside
      ```

2. Configure the next-hop service set that contains the NAT rules or stateful firewall rules. The service set must be configured identically on each chassis of the high availability pair. The NAT rules and stateful firewall rules must also be configured identically on each chassis.

3. For ease of management, we recommend you create a special routing instance with **instance-type vrf** to host the HA synchronization traffic between the MX Series high availability pair. Then specify the name of the special routing instance to apply to the HA synchronization traffic between the high availability pair.

   ```
   [edit interfaces interface-name redundancy-options]
   user@host# set routing-instance instance-name
   ```

4. Repeat these steps for the other chassis of the high availability pair.

RELATED DOCUMENTATION

Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later) | 858

Example: Inter-Chassis Stateful Synchronization for Long-Lived NAT and Stateful Firewall Flows (MS-MIC, MS-MPC) (Release 16.1 and later)

IN THIS SECTION

This example shows how to configure inter-chassis high availability for NAT services.

Requirements

This example uses the following hardware and software components:

- Two MX480 routers with MS-MPC line cards
- Junos OS Release 16.1 or later

Overview

Two MX Series routers are identically configured to facilitate stateful failover for NAT services in case of a chassis failure.

Configuration

IN THIS SECTION

To configure inter-chassis high availability for this example, perform these tasks:

CLI Quick Configuration

To quickly configure this example on the routers, copy the following commands and paste them into the router terminal window after removing line breaks and substituting interface information specific to your site.

NOTE: The following configuration is for chassis 1.

```
[edit]
```

```
set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.2
set interfaces ms-4/0/0 redundancy-options redundancy-local data-address 5.5.5.1
set interfaces ms-4/0/0 redundancy-options routing-instance HA
set interfaces ms-4/0/0 redundancy-options replication-threshold 180
set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.1/32
set interfaces ms-4/0/0 unit 20 family inet
set interfaces ms-4/0/0 unit 20 service-domain inside
set interfaces ms-4/0/0 unit 30 family inet
set interfaces ms-4/0/0 unit 30 service-domain outside
set interfaces ge-2/0/0 vlan-tagging
set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.1/24
set policy-options policy-statement dummy term 1 then reject
set routing-instances HA instance-type vrf
set routing-instances HA interface ge-2/0/0.0
set routing-instances HA interface ms-4/0/0.10
set routing-instances HA route-distinguisher 1:1
set routing-instances HA vrf-import dummy
set routing-instances HA vrf-export dummy
set routing-instances HA routing-options static route route 5.5.5.1/32 next-hop ms-4/0/0.10
set routing-instances HA routing-options static route route 5.5.5.2/32 next-hop 20.1.1.2
set routing-options static-route 100.100.100.0/24 next-hop ms-4/0/0.20
set services nat pool p2 address 32.0.0.0/24
set services nat pool p2 port automatic random-allocation
set services nat pool p2 address-allocation round-robin
set services nat rule r2 match-direction input
set services nat rule r2 term t1 from source-address 129.0.0.0/8
set services nat rule r2 term t1 from source-address 128.0.0.0/8
set services nat rule r2 term t1 then translated source-pool p2
set services nat rule r2 term t1 then translated translation-type napt-44
set services nat rule r2 term t1 then translated address-pooling paired
set services nat rule r2 term t1 then syslog
set services service-set ss2 nat-rules r2
set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
set services service-set ss2 syslog host local class session-logs
set services service-set ss2 syslog host local class nat-logs
```

NOTE: The following configuration is for chassis 2. NAT and service set information must be identical for chassis 1 and 2.

```
set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.1
set interfaces ms-4/0/0 redundancy-options redundancy-local data-address 5.5.5.2
set interfaces ms-4/0/0 redundancy-options routing-instance HA
set interfaces ms-4/0/0 redundancy-options replication-threshold 180
set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.2/32
set interfaces ms-4/0/0 unit 20 family inet
set interfaces ms-4/0/0 unit 20 service-domain inside
set interfaces ms-4/0/0 unit 30 family inet
set interfaces ms-4/0/0 unit 30 service-domain outside
set interfaces ge-2/0/0 vlan-tagging
set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.2/24
set policy-options policy-statement dummy term 1 then reject
set routing-instances HA instance-type vrf
set routing-instances HA interface ge-2/0/0.0
set routing-instances HA interface ms-4/0/0.10
set routing-instances HA route-distinguisher 1:1
set routing-instances HA vrf-import dummy
set routing-instances HA vrf-export dummy
set routing-instances HA routing-options static route 5.5.5.2/32 next-hop ms-4/0/0.10
set routing-instances HA routing-options static route 5.5.5.1/32 next-hop 20.1.1.1
set routing-options static-route 100.100.100.0/24 next-hop ms-4/0/0.20
set services nat pool p2 address 32.0.0.0/24
set services nat pool p2 port automatic random-allocation
set services nat pool p2 address-allocation round-robin
set services nat rule r2 match-direction input
set services nat rule r2 term t1 from source-address 129.0.0.0/8
set services nat rule r2 term t1 from source-address 128.0.0.0/8
set services nat rule r2 term t1 then translated source-pool p2
set services nat rule r2 term t1 then translated translation-type napt-44
set services nat rule r2 term t1 then translated address-pooling paired
set services nat rule r2 term t1 then syslog
set services service-set ss2 nat-rules r2
set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
set services service-set ss2 syslog host local class session-logs
set services service-set ss2 syslog host local class nat-logs
```

Configuring Interfaces for Chassis 1

Step-by-Step Procedure

The interfaces for each of the HA pair of routers are configured identically with the exception of the following service PIC options:

- The **redundancy-options redundancy-peer ipaddress *address*** must be different on each chassis *and* must point to the **redundancy-options redundancy-local data-address *data-address*** on the peer chassis.
- The **unit *unit-number* family inet address *address*** of a unit, other than 0, that contains the **ip-address-owner service-plane** option must be different on each chassis.

To configure interfaces:

1. Configure the redundant service PIC on chassis 1.

```
[edit interfaces}
user@host# set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.2
user@host# set interfaces ms-4/0/0 redundancy-options redundancy-local data-address 5.5.5.1
user@host# set interfaces ms-4/0/0 redundancy-options routing-instance HA
user@host# set interfaces ms-4/0/0 redundancy-options replication-threshold 180
user@host# set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
user@host# set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.1/32
user@host# set interfaces ms-4/0/0 unit 20 family inet
user@host# set interfaces ms-4/0/0 unit 20 service-domain inside
user@host# set interfaces ms-4/0/0 unit 30 family inet
user@host# set interfaces ms-4/0/0 unit 30 service-domain outside
```

2. Configure the interfaces for chassis 1 that are used as interchassis links for synchronization traffic.

```
user@host# set interfaces ge-2/0/0 vlan-tagging
user@host# set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.1/24
```

3. Configure remaining interfaces as needed.

Results

`user@host#` **show interfaces**

```
ge-2/0/0 {
    vlan-tagging;
    unit 0 {
        vlan-id 100;
        family inet {
             address 20.1.1.1/24;
```

```
        }
    }
}
ms-4/0/0 {
    redundancy-options {
        redundancy-peer {
            address 5.5.5.2;
        }
        redundancy-local {
            data-address 5.5.5.1;
        }
        routing-instance HA;
    }
    unit 10 {
        ip-address-owner service-plane;
        family inet {
            address 5.5.5.1/32;
        }
    }
    unit 20 {
        family inet;
        family inet6;
        service-domain inside;
    }
    unit 30 {
        family inet;
        family inet6;
        service-domain outside;
    }
}
```

Configure Routing Information for HA Synchronization Traffic Between MX Series Routers for Chassis 1

Step-by-Step Procedure

Detailed routing configuration is not included for this example. A routing instance is required for the HA synchronization traffic between the chassis as follows:

To configure the routing instances for chassis 1:

1. Specify a dummy policy statement. This statement is referenced in the routing instance configuration.

   ```
   user@host# set policy-options policy-statement dummy term 1 then reject
   ```

2. Specify the options for the routing instance.

```
user@host# set routing-instances HA instance-type vrf
user@host# set routing-instances HA interface ge-2/0/0.0
user@host# set routing-instances HA interface ms-4/0/0.10
user@host# set routing-instances HA route-distinguisher 1:1
user@host# set policy-options policy-statement dummy term 1 then reject
user@host# set routing-instances HA vrf-import dummy
user@host# set routing-instances HA vrf-export dummy
@user@host# set routing-instances HA routing-options static route 5.5.5.1/32 next-hop ms-4/0/0.10
user@host# set routing-instances HA routing-options static route 5.5.5.2/32 next-hop 20.1.1.2
```

3. Specify the next-hop traffic to which the service set is applied.

```
user@host# set routing-options static-route 100.100.100.0/24 next-hop ms-4/0/0.20
```

Results

`@user@host#` **show routing-instances**

```
HA {
    instance-type vrf;
    interface ge-2/0/0.0;
    interface ms-4/0/0.10;
    route-distinguisher 1:1;
    vrf-import dummy;
    vrf-export dummy;
    routing-options {
        static {
            route 5.5.5.1/32 next-hop ms-4/0/0.10;
            route 5.5.5.2/32 next-hop 20.1.1.2;
        }
    }
}
```

Configuring NAT for Chassis 1

Step-by-Step Procedure

Configure NAT identically on both routers.

To configure NAT:

1. Specify NAT pool and rule information..

```
user@host# set services nat pool p2 address 32.0.0.0/24
user@host# set services nat pool p2 port automatic random-allocation
user@host# set services nat pool p2 address-allocation round-robin
user@host# set services nat rule r2 match-direction input
user@host# set services nat rule r2 term t1 from source-address 129.0.0.0/8
user@host# set services nat rule r2 term t1 from source-address 128.0.0.0/8
user@host# set services nat rule r2 term t1 then translated source-pool p2
user@host# set services nat rule r2 term t1 then translated translation-type napt-44
user@host# set services nat rule r2 term t1 then translated address-pooling paired
user@host# set services nat rule r2 term t1 then syslog
```

Results

`user@host#` **show services nat**

```
nat {
    pool p2 {
        address 32.0.0.0/24;
        port {
            automatic {
                random-allocation;
            }
        }
        address-allocation round-robin;
    }
    rule r2 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    129.0.0.0/8;
                    128.0.0.0/8;
                }
            }
            then {
                translated {
                    source-pool p2;
                    translation-type {
                        napt-44;
                    }
                    address-pooling paired;
                }
                syslog;
```

```
            }
        }
    }
}
```

Configuring the Service Set

Step-by-Step Procedure

Configure the service set identically on both routers. To configure the service set:

1. (Optional) Service sets are replicated by default. To exclude a service set from replication using the following option.

   ```
   user@host# set services service-set ss2 replicate-services disable-replication-capability
   ```

2. Configure references to NAT rules for the service set.

   ```
   user@host# set services service-set ss2 nat-rules r2
   ```

3. Configure next-hop service interface on the MS-PIC.

   ```
   user@host# set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
   user@host# set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
   ```

4. Configure desired logging options.

   ```
   user@host# set services service-set ss2 syslog host local class session-logs
   user@host# set services service-set ss2 syslog host local class nat-logs
   ```

Results

`user@host#` **show services service-set ss2**

```
syslog {
   host local {
        class {
            session-logs;
            inactive:
            nat-logs;
```

```
        }
    }
    replicate-services {
        replication-threshold 180;
        inactive: disable-replication-capability;
    }
    nat-rules r2;
    next-hop-service {
        inside-service-interface ms-3/0/0.20;
        outside-service-interface ms-3/0/0.30;
    }
}
```

Configuring Interfaces for Chassis 2

Step-by-Step Procedure

The interfaces for each of the HA pair of routers are configured identically with the exception of the following service PIC options:

- **redundancy-options redundancy-peer ipaddress *address***
- **unit *unit-number* family inet address *address*** of a unit, other than 0, that contains the **ip-address-owner service-plane** option

1. Configure the redundant service PIC on chassis 2.

   The **redundancy-peer ipaddress** points to the address of the unit (unit 10) on ms-4/0/0 on chassis on chassis 1 that contains the **ip-address-owner service-plane** statement.

   ```
   [edit interfaces}
   set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.1
   user@host# set interfaces ms-4/0/0 redundancy-options redundancy-local data-address 5.5.5.2
   user@host# set interfaces ms-4/0/0 redundancy-options replication-threshold 180
   user@host# set interfaces ms-4/0/0 redundancy-options routing-instance HA
   user@host# set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
   user@host# set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.2/32
   user@host# set interfaces ms-4/0/0 unit 20 family inet
   user@host# set interfaces ms-4/0/0 unit 20 service-domain inside
   user@host# set interfaces ms-4/0/0 unit 30 family inet
   user@host# set interfaces ms-4/0/0 unit 30 service-domain outside
   ```

2. Configure the interfaces for chassis 2 that are used as interchassis links for synchronization traffic

```
user@host# set interfaces ge-2/0/0 vlan-tagging
user@host# set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.2/24
```

3. Configure remaining interfaces for chassis 2 as needed.

Results

`user@host#` **show interfaces**

```
ms-4/0/0 {
    redundancy-options {
        redundancy-peer {
            address 5.5.5.1;
        }
        redundancy-local {
            data-address 5.5.5.2;
        }
        routing-instance HA;
    }
    unit 0 {
        family inet;
    }
    unit 10 {
        ip-address-owner service-plane;
        family inet {
            address 5.5.5.2/32;
        }
    }
}
ge-2/0/0 {
    vlan-tagging;
    unit 0 {
        vlan-id 100;
        family inet {
             address 20.1.1.2/24;
        }
    }
    unit 10 {
        vlan-id 10;
        family inet {
            address 2.10.1.2/24;
        }
```

```
    }
}
```

Configure Routing Information for HA Synchronization Traffic Between MX Series Routers for Chassis 2

Step-by-Step Procedure

Detailed routing configuration is not included for this example. A routing instance is required for the HA synchronization traffic between the two chassis and is included here.

- Configure routing instances for chassis 2.

```
user@host# set routing-instances HA instance-type vrf
user@host# set routing-instances HA interface ge-2/0/0.0
user@host# set routing-instances HA interface ms-4/0/0.10
user@host# set routing-instances HA route-distinguisher 1:1
user@host# set policy-options policy-statement dummy term 1 then reject
user@host# set routing-instances HA vrf-import dummy
user@host# set routing-instances HA vrf-export dummy
user@host# set routing-instances HA routing-options static route 5.5.5.2/32 next-hop ms-4/0/0.10
user@host# set routing-instances HA routing-options static route 5.5.5.1/32 next-hop 20.1.1.1
user@host# set routing-options static-route 100.100.100.0/24 next-hop ms-4/0/0.20
```

NOTE: The following configuration steps are *identical* to the steps shown for chassis 1.

- Configuring NAT
- Configuring the Service Set

Results

`@user@host#` **show services routing-instances**

```
HA {
    instance-type vrf;
    interface xe-2/2/0.0;
    interface ms-4/0/0.10;
    route-distinguisher 1:1;
    vrf-import dummy;
    vrf-export dummy;
    routing-options {
        static {
```

```
            route 5.5.5.2/32 next-hop ms-4/0/0.10;
            route 5.5.5.1/32 next-hop 20.1.1.1;
        }
    }
}
```

RELATED DOCUMENTATION

> Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later) | **858**

Service Redundancy Daemon Overview

IN THIS SECTION

Introduction to the Service Redundancy Daemon

- The service redundancy daemon (srd) provides configurable events that can decide when redundancy occurs across multiple gateways on MX Series routers with MS-MPCs and MS-MICs. This enables you to manage mastership switchovers based on a monitored event. You can configure redundancy based on monitored events, including:
  - Link down events.
  - FPC and PIC reboots.

- Routing protocol daemon (rpd) aborts and restarts.
- Peer gateway events, including requests to acquire or release mastership, or to broadcast warnings.

Service Redundancy Daemon Components

The following configurable components control srd processing:

- **Redundancy Event**—A monitored critical event that triggers the srd to acquire or release mastership for redundancy peers, or to trigger warning-only events, and to add or delete signal routes. Monitored events include interface or link down events, rpd events, and acquire or release mastership events from peers.
- **Redundancy Policy**—A policy that defines the set of actions taken when a redundancy event occurs. Available actions include acquisition or release of mastership, and addition or deletion of signal routes.
- **Redundancy Set**—A collection of one or more service sets with a common redundancy policy or policies. A redundancy set applies to two or more system gateways. Only one of the gateways is master and the peer or peers are standby at any time. Redundancy policies define the actions to be taken for a redundancy set when the srd detects a triggering event.
- **Redundancy Group**—A one-to-one relationship exists between a redundancy set and a redundancy group. One redundancy set can be part of only one redundancy group.
- **Signal routes**—Static routes that are added or deleted by the srd based on mastership state changes.
- **Routing Policies**—Policies that are configured to advertise routes based on the existence or non-existence of signal routes using the **if-route-exists** condition.
- **VRRP (Virtual Router Redundancy Protocol) route tracking**—TA standard Junos OS VRRP feature, but optional srd component, that tracks whether a reachable route exists in the routing table of the routing instance included in the configuration and dynamically changes the priority of the VRRP group based on the reachability of the tracked route, triggering a new master router election. The route to be tracked is a signal route.

Service Redundancy Daemon Constraints

The following constraints apply to srd processing configurations:

- A one-to-one relationship exists between a redundancy set and a redundancy group. One redundancy set can be part of only one redundancy group.
- One redundancy policy can be part of only one redundancy set, but one redundancy set can have multiple redundancy policies. For example, redundancy set RS1 can include redundancy policies RP1 and RP2. Redundancy policies RP1 and RP2 cannot be included in redundancy sets other than RS1.

- One redundancy event can be part of only one redundancy policy, but one redundancy policy can have multiple redundancy events. For example, redundancy policy RP1 can include redundancy events RE1 and RE2. Redundancy events RE1 and RE2 cannot be included in redundancy policies other than RP1.
- One monitored interface or link can be part of only one redundancy event, but one redundancy event can have multiple monitored interfaces.
- One service set can be part of only one redundancy set, but one redundancy set may have multiple service sets.
- If gateway 1, the chassis that is configured with the lower IP address, is the master chassis and you deactivate SRD on it, a switchover to gateway 2 occurs. If gateway 2, the chassis that is configured with the higher IP address, is the master chassis and you deactivate SRD on it, a switchover does not occur.
- A particular redundancy-set can be active on only one gateway, but not all redundancy sets have to be active on the same gateway. For example, redundancy set A can be active on gateway 1 while redundancy set B is active on gateway 2.

Service Redundancy Daemon Operation

The srd operates as follows:

1. The srd runs on the Routing Engine. It continuously monitors configured redundancy events.
2. When a redundancy event is detected, the srd:
    a. Adds or removes signal routes specified in the redundancy policy.
    b. Switches services to the next preferred standby gateway.
    c. Updates stateful sync roles as needed.
3. Resulting route changes cause:
    a. The routing policy connected to this route to advertise routes differently.
    b. VRRP to change advertised priorities.

To summarize the switchover process:

1. A critical event occurs.
2. srd adds or removes a signal route.
3. A routing policy advertises routes differently. VRRP changes advertised priorities.
4. Services switch over to the next preferred standby gateway.
5. Stateful synchronization is updated accordingly.

NOTE: The order of routing priorities must match the order of services mastership.

RELATED DOCUMENTATION

Configuring the Service Redundancy Daemon | 878

Configuring the Service Redundancy Daemon

IN THIS SECTION

Before you configure srd processing, we recommend that you be familiar with *Configuring ICCP for MC-LAG*, which explains peer relationships between gateways that are enabled to exchange master and standby roles.

You use the following configuration statements:

- **redundancy-policy** at the **[edit policy-options]** hierarchy level
- **redundancy-event** at the **[edit event-options]** hierarchy level
- **redundancy-set** at the **[edit services]** hierarchy level

The actions to be performed when configured redundancy events occur are defined in redundancy policies. Redundancy polices are associated with redundancy sets; they are analogous to rules associated with service sets. Redundancy sets are associated to redundancy groups by redundancy group IDs. Redundancy group details are defined by the underlying Inter-Chassis Communication Protocol daemon (iccpd) configuration. Service sets and redundancy sets are associated through the **redundancy-sets** statement in service sets configuration.

In the procedures that follow, redundancy events that are configured and associated with a redundancy policy. The redundancy policy is associated with a redundancy set to take appropriate action of mastership-release or mastership-acquire. If an event is associated with a policy that takes the mastership-release action, srd checks whether the redundancy peer's state is ready or warned. If the standby is in a warned state, then the mastership-release action fails. You can restore the health check and manually execute the release-mastership action.

To release mastership in any case, you can either configure the policy action as **release-mastership-force** or use the **request services redundancy-set *redundancy-set* redundancy-event *redundancy-event* trigger force** command in the operational CLI. Even if your configuration specifies the **release-mastership-force** option, using the **request services redundancy-set *redundancy-set* redundancy-event *redundancy-event* trigger force** CLI command takes precedence and mastership is released. Similarly, if a redundancy event is configured with a policy with an acquire-mastership action, then srd checks the local redundancy set state. In the case of a wait state, the action fails unless you use the **request services redundancy-set *redundancy-set* redundancy-event *redundancy-event* trigger force** CLI command. We recommend that you determine why health checks fail and take action to correct the failure. After that, when the redundancy set state returns to STANDBY, then this mastership change action succeeds.

A particular redundancy-set can be active on only one gateway, but not all redundancy sets have to be active on the same gateway. For example, redundancy set A can be active on gateway 1 while redundancy set B is active on gateway 2.

To configure srd, perform the following configuration tasks in the recommended sequence. Configurations are shown for two gateways for which mastership may change.

Configuring Redundancy Events

To configure redundancy events:

1. Configure any link-down redundancy events for the master gateway.

   ```
   [edit services]
   user@gateway1# set event-options redundancy-event event-name monitor link-down interface-name
   ```

   For example:

   ```
   [edit services]
   user@gateway1# set event-options redundancy-event RELS_MSHIP_CRIT_EV monitor link-down ms-2/3/0.0
   user@gateway1# set event-options redundancy-event RELS_MSHIP_CRIT_EV monitor link-down xe-3/0/0.0
   ```

2. Configure any process redundancy events for the master gateway.

   ```
   [edit services]
   ```

```
user@gateway1# set event-options redundancy-event event-name monitor process routing restart
```

For example:

```
[edit services]
user@gateway1# set event-options redundancy-event RELS_MSHIP_CRIT_EV monitor process routing
  restart
```

3. Configure any link-down redundancy events for the standby gateway.

```
[edit services]
user@gateway2# set event-options redundancy-event event-name monitor link-down interface-name
```

For example:

```
[edit services]
user@gateway2# set event-options redundancy-event WARN_EV monitor link-down ms-2/3/0.0
user@gateway2# set event-options redundancy-event WARN_EV monitor link-down xe-3/0/0.0
```

4. Configure any process redundancy events for the standby gateway.

```
[edit services]
user@gateway2# set event-options redundancy-event event-name monitor process routing restart
```

For example:

```
[edit services]
user@gateway2# set event-options redundancy-event WARN_EV monitor process routing restart
```

5. Configure any peer redundancy events for the standby gateway.

```
[edit services]
user@gateway2# set event-options redundancy-event event-name monitor peer (mastership-acquire |
  mastership-release)
```

For example:

```
[edit services]
user@gateway2# set event-options redundancy-event PEER_MSHIP_ACQU_EV monitor peer
  mastership-acquire
```

```
user@gateway2# set event-options redundancy-event PEER_MSHIP_RELS_EV monitor peer
  mastership-release
```

Configuring Redundancy Policies

Service redundancy policies specify actions triggered by monitored redundancy events.

To configure redundancy policies:

1. Specify a redundancy policy and redundancy event for the master gateway. Follow the same steps for the standby gateway.

   ```
   user@gateway1# edit policy-options redundancy-policy policy-name redundancy-events [event-list] then
   ```

2. Specify an action of acquiring or releasing mastership.

   ```
   [edit policy-options redundancy-policy policy-name redundancy-events [event-list then]
   user@gateway1# set acquire-mastership
   ```

   or

   ```
   [edit policy-options redundancy-policy policy-name redundancy-events [event-list then]
   user@gateway1# set (release-mastership | release-mastership-force)
   ```

3. (Optional) Specify an action of adding a static route.

   ```
   [edit policy-options redundancy-policy policy-name redundancy-events [event-list then]
   user@gateway1# set add-static-route destination (receive | next-hop next-hop) routing-instance routing-instance
   ```

   BEST PRACTICE: We recommend using the **receive** option.

4. (Optional) Specify an action of deleting a static route.

   ```
   [edit policy-options redundancy-policy policy-name redundancy-events [event-list then]
   user@gateway1# set delete-static-route destination routing-instance routing-instance
   ```

The following example demonstrates configuring redundancy policies for two peer gateways:

```
user@gateway1# edit policy-options redundancy-policy ACQU_MSHIP_POL redundancy-events
   ACQU_MSHIP_MANUAL_EV then

[edit policy-options redundancy-policy ACQU_MSHIP_POL redundancy-event ACQU_MSHIP_MANUAL_EV
   then]
user@gateway1# set acquire-mastership add-static-route 10.45.45.0/24 receive routing-instance SGI-PRIVATE

user@gateway1# top
user@gateway1# edit policy-options redundancy-policy RELS_MSHIP_POL redundancy-events
   PEER_MSHIP_ACQU_EV then

[edit policy-options redundancy-policy RELS_MSHIP_POL redundancy-events PEER_MSHIP_ACQU_EV then]
user@gateway1# set release-mastership-force delete-static-route 10.45.45.0/24 receive routing-instance
   SGI-PRIVATE
```

```
user@gateway2# edit policy-options redundancy-policy RELS_MSHIP_POL redundancy-events
   PEER_MSHIP_ACQU_EV then

[edit policy-options redundancy-policy ACQU_MSHIP_POL redundancy-events ACQU_MSHIP_MANUAL_EV
   then]
user@gateway2# set release-mastership-force add-static-route 10.45.45.0/24 receive routing-instance
   SGI-PRIVATE
user@gateway2# top
user@gateway2# edit policy-options redundancy-policy ACQU_MSHIP_POL redundancy-events
   PEER_MSHIP_RELS_EV then

[edit policy-options redundancy-policy ACQU_MSHIP_POL redundancy-events PEER_MSHIP_RELS_EV then]
user@gateway2# set acquire-mastership delete-static-route 10.45.45.0/24 receive routing-instance SGI-PRIVATE
user@gateway2# top
user@gateway2# edit policy-options redundancy-policy WARN_POL redundancy-events WARN_EV then

[edit policy-options redundancy-policy WARN_POL redundancy-events WARN_EV then]
user@gateway2# set broadcast-warning
```

Configuring Redundancy Set and Group

The redundancy group IDs that srd uses are associated with those configured for the ICCP daemon (iccpd) through the existing ICCP configuration hierarchy by using the same redundancy group ID in the configuration of the services redundancy group.

```
iccp {
 local-ip-addr 1.1.1.1;
 peer 2.2.2.2 {
  redundancy-group-id-list 1;
  liveness-detection {
   minimum-interval 1000;
  }
 }
}
```

To configure redundancy sets:

1. Specify redundancy set and group for the master gateway.

   ```
   [edit services]
   user@gateway1# set redundancy-set redundancy-set redundancy-group redundancy-group
   ```

   For example:

   ```
   [edit services]
   user@gateway1# set redundancy-set 1 redundancy-group 1
   ```

2. Specify redundancy policies for the redundancy set.

   ```
   [edit services]
   user@gateway1# set redundancy-set redundancy-set redundancy-policy [redundancy-policy-list]
   ```

   For example:

   ```
   [edit services]
   user@gateway1# set redundancy-set 1 redundancy-policy ACQU_MSHIP_POL RELS_MSHIP_POL WARN_POL
   ```

3. Specify redundancy set and group for the peer gateway.

```
[edit services]
user@gateway2# set redundancy-set redundancy-set redundancy-group redundancy-group
```

For example:

```
user@gateway2# set redundancy-set 1 redundancy-group 1
```

4. Specify redundancy policies for the redundancy set.

```
[edit services]
user@gateway2# set redundancy-set redundancy-set redundancy-policy [redundancy-policy-list]
```

For example:

```
[edit services]
user@gateway1# set redundancy-set 1 redundancy-policy [ACQU_MSHIP_POL RELS_MSHIP_POL
  WARN_POL]
```

Configuring Routing Policies Supporting Redundancy

To configure routing policies that support redundancy:

1. At the **[edit policy-options condition]** hierarchy level, use the **if-route-exists** configuration statement to set a condition based on the existence of signal routes that requires redundancy-related routing changes. Specify the routing table that is used.

```
[edit policy-options condition condition-name}
user@gateway# set if-route-exists signal-route table routing-table
```

For example:

```
[edit policy-options condition switchover-route-exists]
user@gateway# set if-route-exists 10.45.45.0/24 table bgp1_table
```

2. At the **[edit policy-options policy-statement *statement-name*]** hierarchy level, specify routing changes based on the condition indicating the existence of the signal route. For BGP, routing changes typically include change to local-preference and as-path-prepend values.

   a. To change local-preference, specify **local-preference** in the **then** clause of the policy statement.

```
[edit policy-options policy-statement policy-name]
user@gateway# set term term from protocol [protocol variables] prefix-list prefix-list condition
    condition-name then local-preference preference-value accept
```

For example:

```
[edit policy-options policy-statement ha-export-v6-policy]
user@gateway# set term update-local-pref from protocol static bgp prefix-list ipv4-default-route condition
    switchover-route-exists then local-preference 350 accept
```

b. To change **as-path-prepend** values, specify **as-path-prepend** in the **then** clause of the policy statement.

```
[edit policy-options policy-statement policy-name]
user@gateway# set term term from prefix-list prefix-list condition condition-name then as-path-prepend
    [as-prepend-values] next-hop self accept
```

For example:

```
[edit policy-options policy-statement ha-export-v6-policy
user@gateway# set term update-as-prepend prefix-list ipv6-default-route condition
    switchover-route-exists then as-path-prepend "64674 64674 64674 64674" next-hop self accept
```

Configuring Service Sets

Specify stateful synchronization of services for a service set.

1. Specify the service set and redundancy set.

```
[edit]
user@gateway1# set services service-set service-set-name redundancy-set-id redundancy-set
```

For example:

```
[edit]
user@gateway1# set services service-set CGN4_SP-7-0-0 redundancy-set-id 1
```

RELATED DOCUMENTATION

Service Redundancy Daemon Overview | 875

Using Service Redundancy Daemon Scripts to View and Change the Status of a Gateway

You can determine the status of a gateway, disable or enable all the interfaces on the gateway, or pull services-related MIB information from the gateway by running service redundancy daemon (srd) scripts.

Before you can use these scripts, you must enable them:

- Enable the srd scripts.

```
[edit]
user@host# set system scripts op file sdg-inservice.slax
user@host# set system scripts op file sdg-oos.slax
user@host# set system scripts op file services-oids.slax
user@host# set system scripts op file srd-status.slax
user@host# set system scripts op max-datasize 512m
```

Use the srd scripts as the root user:

- Disable all the interfaces on the MX series router and power off the MS-MPC cards.
  a. Ensure that all local redundancy sets are in standby mode.

```
root@host> show services redundancy-group
```

  b. Run the **sdg-oos** script.

```
root@host> op sdg-oos
```

- Enable all the interfaces on the MX series router and power on the MS-MPC cards.

```
root@host> op sdg-inservice
```

- Check the service state of a gateway.

```
root@host> op srd-status
```

- Pull services-related MIB information from the gateway.

```
root@host> op services-oids
```

RELATED DOCUMENTATION

Service Redundancy Daemon Overview | 875

CHAPTER 42

Configuring Inter-Chassis Stateful Synchronization for NAT and Stateful Firewall (Release 15.1 and earlier)

IN THIS CHAPTER

Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier)

IN THIS SECTION

NOTE: This topic applies to Junos OS release 15.1 and earlier. (For Junos OS release 16.1 and higher, see "Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)" on page 858.)

Inter-chassis high availability supports stateful synchronization of services using a switchover to a backup services PIC on a different chassis. This topic applies to Junos OS release 15.1 and earlier. (For Junos OS release 16.1 and higher, see "Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later)" on page 858.) The feature is described in the following topics:

Inter-Chassis High Availability for Stateful Firewall and NAPT44 Overview (MS-MIC, MS-MPC)

Carrier-grade NAT (CGN) deployments can use dual-chassis implementations to provide a redundant data path and redundancy for key components in the router. Although intra-chassis high availability can be used in dual-chassis environments, it deals only with service PIC failures. If traffic is switched to a backup router due to some other failure in the router, state is lost. Inter-chassis high availability preserves state and provides redundancy using fewer service PICs than intra-chassis high availability. Only long-lived flows are synchronized between the master and backup chassis in the high availability pair. The service PICs do not replicate state until an explicit CLI command, **request services redundancy (synchronize | no-synchronize)**, is issued to start or stop the state replication. Stateful firewall, NAPT44, and APP state information can be synchronized.

> **NOTE:** When both the master and backup PICs are up, replication starts immediately when the **request services redundancy command** is issued.

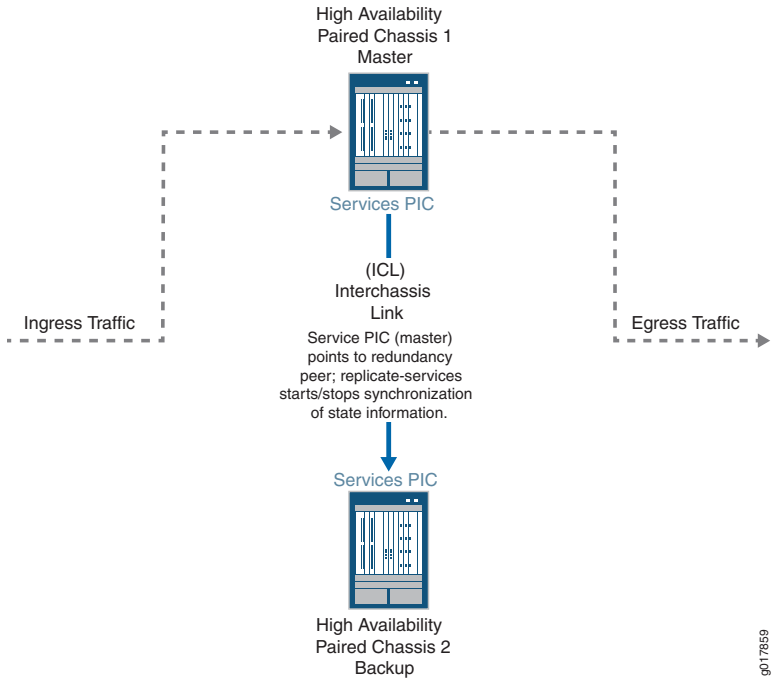
In order to use Inter-chassis high availability, you must use service sets configured for next-hop service interfaces. Inter-chassis high availability works with ms- service interfaces configured on MS-MIC or MS-MPC interface cards. A unit other than unit 0 must be configured with the **ip-address-owner service-plane** option.

The following restrictions apply:

- NAPT44 is the only translation type supported.
- Checkpointing is not supported for ALGs, PBA port block allocation (PBA), endpoint- independent mapping (EIM), or endpoint- independent filters (EIF).

Figure 41 on page 890 shows the inter-chassis high availability topology.

Figure 41: Inter-Chassis High Availability Topology



SEE ALSO

Configuring Inter-Chassis High Availability for Stateful Firewall and NAPT44 (MS-MPC, MS-MIC) | 890

Configuring Inter-Chassis High Availability for Stateful Firewall and NAPT44 (MS-MPC, MS-MIC)

To configure inter-chassis availability for stateful firewall and NAPT44 on MS-MIC or MS-MPC service PICS, perform the following configuration steps on each chassis of the high availability pair:

1. At the **[edit interfaces *interface-name* redundancy-options]** hierarchy level, set the **ipaddress** for the **redundancy-peer**. This IPv4 address specifies one of the hosted IP addresses of the remote PIC. This address is used by the TCP channel between the HA pairs.

   [edit interfaces *interface-name* **redundancy-options**]
   user@host# **set redundancy-peer ipaddress *ipaddress***

NOTE: When you enable or disable high availability of MS-MICs or MS-MPCs by configuring or removing the primary and backup adaptive services PICs by using the **redundancy-options redundancy-peer ipaddress *address*** statement at the **[edit interfaces *interface-name*]** hierarchy level, the configuration change is treated as a catastrophic event for each service-set that refers to the affected interface at the **[edit services service-set *name* interface-service service-interface *interface-name*]** hierarchy level. A catastrophic event at the service-set level has the effect of deactivating the service set, applying the change, and then reactivating the service set.

2. Specify the name of a special routing instance, or VRF, you want applied to the HA synchronization traffic between the high availability pair.

```
[edit interfaces interface-name redundancy-options]
user@host# set routing-instance instance-name
```

3. For the service set defining an interface that is a member of the high availability pair, configure the service replication options using the **replicate-services** option.

```
[edit services service-set service-set-name replicate-services]
user@host# set replication-threshold threshold-value
stateful-firewall
nat
```

SEE ALSO

Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier) | 888

Example: Inter-Chassis Stateful High Availability for NAT and Stateful Firewall (MS-MIC, MS-MPC) | 892

Example: Inter-Chassis Stateful High Availability for NAT and Stateful Firewall (MS-MIC, MS-MPC)

IN THIS SECTION

This example shows how to configure inter-chassis high availability for stateful firewall and NAT services.

Requirements

This example uses the following hardware and software components:

- Two MX480 routers with MS-MPC line cards
- Junos OS Release 13.3 or later

Overview

Two MX 3D routers are identically configured to facilitate stateful failover for firewall and NAT services in case of a chassis failure.

Configuration

IN THIS SECTION

To configure inter-chassis high availability for this example, perform these tasks:

CLI Quick Configuration

To quickly configure this example on the routers, copy the following commands and paste them into the router terminal window after removing line breaks and substituting interface information specific to your site.

NOTE: The following configuration is for chassis 1.

```
[edit]
set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.2
set interfaces ms-4/0/0 redundancy-options routing-instance HA
set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.1/32
set interfaces ms-4/0/0 unit 20 family inet
set interfaces ms-4/0/0 unit 20 service-domain inside
set interfaces ms-4/0/0 unit 30 family inet
set interfaces ms-4/0/0 unit 30 service-domain outside
set interfaces ge-2/0/0 vlan-tagging
set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.1/24
set routing-instances HA instance-type vrf
set routing-instances HA interface ge-2/0/0.0
set routing-instances HA interface ms-4/0/0.10
set routing-instances HA route-distinguisher 1:1
set policy-options policy-statement dummy term 1 then reject
set routing-instances HA vrf-import dummy
set routing-instances HA vrf-export dummy
set routing-instances HA routing-options static route route 5.5.5.1/32 next-hop ms-4/0/0.10
set routing-instances HA routing-options static route route 5.5.5.2/32 next-hop 20.1.1.2
set services nat pool p2 address 32.0.0.0/24
set services nat pool p2 port automatic random-allocation
set services nat pool p2 address-allocation round-robin
set services nat rule r2 match-direction input
set services nat rule r2 term t1 from source-address 129.0.0.0/8
set services nat rule r2 term t1 from source-address 128.0.0.0/8
set services nat rule r2 term t1 then translated source-pool p2
set services nat rule r2 term t1 then translated translation-type napt-44
set services nat rule r2 term t1 then translated address-pooling paired
set services nat rule r2 term t1 then syslog
set services stateful-firewall rule r2 match-direction input
set services stateful-firewall rule r2 term t1 from source-address any-unicast
set services stateful-firewall rule r2 term t1 then accept
set services stateful-firewall rule r2 term t1 then syslog
set services service-set ss2 replicate-services replication-threshold 180
set services service-set ss2 replicate-services stateful-firewall
```

```
set services service-set ss2 replicate-services nat
set services service-set ss2 stateful-firewall-rules r2
set services service-set ss2 nat-rules r2
set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
set services service-set ss2 syslog host local class session-logs
set services service-set ss2 syslog host local class stateful-firewall-logs
set services service-set ss2 syslog host local class nat-logs
```

NOTE: The following configuration is for chassis 2. The NAT, stateful firewall, and service-set information must be identical for chassis 1 and 2.

```
set interfaces ms-4/0/0 redundancy-options routing-instance HA
set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.2/32
set interfaces ms-4/0/0 unit 20 family inet
set interfaces ms-4/0/0 unit 20 service-domain inside
set interfaces ms-4/0/0 unit 30 family inet
set interfaces ms-4/0/0 unit 30 service-domain outside
set interfaces ge-2/0/0 vlan-tagging
set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.2/24
set routing-instances HA instance-type vrf
set routing-instances HA interface ge-2/0/0.0
set routing-instances HA interface ms-4/0/0.10
set routing-instances HA route-distinguisher 1:1
set routing-instances HA vrf-import dummy
set routing-instances HA vrf-export dummy
set routing-instances HA routing-options static route 5.5.5.2/32 next-hop ms-4/0/0.10
set routing-instances HA routing-options static route 5.5.5.1/32 next-hop 20.1.1.1
set services nat pool p2 address 32.0.0.0/24
set services nat pool p2 port automatic random-allocation
set services nat pool p2 address-allocation round-robin
set services nat rule r2 match-direction input
set services nat rule r2 term t1 from source-address 129.0.0.0/8
set services nat rule r2 term t1 from source-address 128.0.0.0/8
set services nat rule r2 term t1 then translated source-pool p2
set services nat rule r2 term t1 then translated translation-type napt-44
set services nat rule r2 term t1 then translated address-pooling paired
set services nat rule r2 term t1 then syslog
set services stateful-firewall rule r2 match-direction input
set services stateful-firewall rule r2 term t1 from source-address any-unicast
```

```
set services stateful-firewall rule r2 term t1 then accept
set services stateful-firewall rule r2 term t1 then syslog
set services service-set ss2 replicate-services replication-threshold 180
set services service-set ss2 replicate-services stateful-firewall
set services service-set ss2 replicate-services nat
set services service-set ss2 stateful-firewall-rules r2
set services service-set ss2 nat-rules r2
set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
set services service-set ss2 syslog host local class session-logs
set services service-set ss2 syslog host local class stateful-firewall-logs
set services service-set ss2 syslog host local class nat-logs
```

Configuring Interfaces for Chassis 1.

Step-by-Step Procedure

The interfaces for each of the HA pair of routers are configured identically with the exception of the following service PIC options:

- **redundancy-options redundancy-peer ipaddress *address***
- **unit *unit-number* family inet address *address*** of a unit, other than 0, that contains the **ip-address-owner service-plane** option

To configure interfaces:

1. Configure the redundant service PIC on chassis 1.

```
[edit interfaces}
user@host# set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.2
user@host# set interfaces ms-4/0/0 redundancy-options routing-instance HA
user@host# set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
user@host# set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.1/32
user@host# set interfaces ms-4/0/0 unit 20 family inet
user@host# set interfaces ms-4/0/0 unit 20 service-domain inside
user@host# set interfaces ms-4/0/0 unit 30 family inet
user@host# set interfaces ms-4/0/0 unit 30 service-domain outside
```

2. Configure the interfaces for chassis 1 that are used as interchassis links for synchronization traffic.

```
user@host# set interfaces ge-2/0/0 vlan-tagging
user@host# set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.1/24
```

3. Configure remaining interfaces as needed.

Results

`user@host#` **show interfaces**

```
ge-2/0/0 {
                vlan-tagging;
        unit 0 {
            vlan-id 100;
            family inet {
                 address 20.1.1.1/24;
            }
        }
            }
ms-4/0/0 {
        redundancy-options {
            redundancy-peer {
                ipaddress 5.5.5.2;
            }
            routing-instance HA;
        }
        unit 10 {
            ip-address-owner service-plane;
            family inet {
                address 5.5.5.1/32;
            }
        }
        unit 20 {
            family inet;
            family inet6;
            service-domain inside;
        }
        unit 30 {
            family inet;
            family inet6;
            service-domain outside;
        }
            }
}
```

Configure Routing Information for Chassis 1

Step-by-Step Procedure

Detailed routing configuration is not included for this example. A routing instance is required for the HA synchronization traffic between the chassis as follows:

- Configure routing instances for Chassis 1.

```
user@host# set routing-instances HA instance-type vrf
user@host# set routing-instances HA interface ge-2/0/0.0
user@host# set routing-instances HA interface ms-4/0/0.10
user@host# set routing-instances HA route-distinguisher 1:1
user@host# set policy-options policy-statement dummy term 1 then reject
user@host# set routing-instances HA vrf-import dummy
user@host# set routing-instances HA vrf-export dummy
user@host# set routing-instances HA routing-options static route route 5.5.5.1/32 next-hop ms-4/0/0.10
user@host# set routing-instances HA routing-options static route route 5.5.5.2/32 next-hop 20.1.1.2
```

Results

`user@host#` **show routing-instances**

```
HA {
        instance-type vrf;
        interface ge-2/0/0.0;
        interface ms-4/0/0.10;
        route-distinguisher 1:1;
        vrf-import dummy;
        vrf-export dummy;
        routing-options {
            static {
                route 5.5.5.1/32 next-hop ms-4/0/0.10;
                route 5.5.5.2/32 next-hop 20.1.1.2;
                            }
        }
    }
```

Configuring NAT and Stateful Firewall for Chassis 1

Step-by-Step Procedure

Configure NAT and stateful firewall identically on both routers. To configure NAT and stateful firewall:

1. Configure NAT as needed.

```
user@host# set services nat pool p2 address 32.0.0.0/24
user@host# set services nat pool p2 port automatic random-allocation
```

```
user@host# set services nat pool p2 address-allocation round-robin
user@host# set services nat rule r2 match-direction input
user@host# set services nat rule r2 term t1 from source-address 129.0.0.0/8
user@host# set services nat rule r2 term t1 from source-address 128.0.0.0/8
user@host# set services nat rule r2 term t1 then translated source-pool p2
user@host# set services nat rule r2 term t1 then translated translation-type napt-44
user@host# set services nat rule r2 term t1 then translated address-pooling paired
user@host# set services nat rule r2 term t1 then syslog
```

2. Configure stateful firewall as needed.

```
user@host# set services stateful-firewall rule r2 match-direction input
user@host# set services stateful-firewall rule r2 term t1 from source-address any-unicast
user@host# set services stateful-firewall rule r2 term t1 then accept
user@host# set services stateful-firewall rule r2 term t1 then syslog
```

Results

`user@host#` **show services nat**

```
nat {
        pool p2 {
            address 32.0.0.0/24;
            port {
                automatic {
                    random-allocation;
                }
            }
            address-allocation round-robin;
        }
        rule r2 {
            match-direction input;
            term t1 {
                from {
                    source-address {
                        129.0.0.0/8;
                        128.0.0.0/8;
                    }
                }
                then {
                    translated {
                        source-pool p2;
```

```
                        translation-type {
                            napt-44;
                        }
                        address-pooling paired;
                    }
                    syslog;
                }
            }
        }
    }
}
```

`user@host` **show services stateful-firewell**

```
rule r2 {
    match-direction input;
    term t1 {
        from {
            source-address {
                any-unicast;
            }
        }
        then {
            accept;
            syslog;
        }
    }
}
```

Configuring the Service Set

Step-by-Step Procedure

Configure the the service set identically on both routers. To configure the service set:

1. Configure the service set replication options.

   user@host# **set services service-set ss2 replicate-services replication-threshold 180**
   user@host# **set services service-set ss2 replicate-services stateful-firewall**
   user@host# **set services service-set ss2 replicate-services nat**

2. Configure references to NAT and stateful firewall rules for the service set.

```
user@host# set services service-set ss2 stateful-firewall-rules r2
user@host# set services service-set ss2 nat-rules r2
```

3. Configure next-hop service interface on the MS-PIC.

```
user@host# set services service-set ss2 next-hop-service inside-service-interface ms-4/0/0.20
user@host# set services service-set ss2 next-hop-service outside-service-interface ms-4/0/0.30
```

4. Configure desired logging options.

```
user@host# set services service-set ss2 syslog host local class session-logs
user@host# set services service-set ss2 syslog host local class stateful-firewall-logs
user@host# set services service-set ss2 syslog host local class nat-logs
```

Results

`user@host#` **show services service-set ss2**

```
syslog {
            host local {
                class {
                    session-logs;
                    inactive: stateful-firewall-logs;
                    nat-logs;
                }
            }
        }
        replicate-services {
            replication-threshold 180;
            stateful-firewall;
            nat;
        }
        stateful-firewall-rules r2;
        inactive: nat-rules r2;
        next-hop-service {
            inside-service-interface ms-3/0/0.20;
            outside-service-interface ms-3/0/0.30;
        }
    }
```

Configuring Interfaces for Chassis 2

Step-by-Step Procedure

The interfaces for each of the HA pair of routers are configured identically with the exception of the following service PIC options:

- **redundancy-options redundancy-peer ipaddress *address***
- **unit *unit-number* family inet address *address*** of a unit, other than 0, that contains the **ip-address-owner service-plane** option

1. Configure the redundant service PIC on chassis 2.

   The **redundancy-peer ipaddress** points to the address of the unit (unit 10) on ms-4/0/0 on chassis on chassis 1 that contains the **ip-address-owner service-plane** statement.

   ```
   [edit interfaces}
   set interfaces ms-4/0/0 redundancy-options redundancy-peer ipaddress 5.5.5.1
   user@host# set interfaces ms-4/0/0 redundancy-options routing-instance HA
   user@host# set interfaces ms-4/0/0 unit 10 ip-address-owner service-plane
   user@host# set interfaces ms-4/0/0 unit 10 family inet address 5.5.5.2/32
   user@host# set interfaces ms-4/0/0 unit 20 family inet
   user@host# set interfaces ms-4/0/0 unit 20 service-domain inside
   user@host# set interfaces ms-4/0/0 unit 30 family inet
   user@host# set interfaces ms-4/0/0 unit 30 service-domain outside
   ```

2. Configure the interfaces for chassis 2 that are used as interchassis links for synchronization traffic

   ```
   user@host# set interfaces ge-2/0/0 vlan-tagging
   user@host# set interfaces ge-2/0/0 unit 0 vlan-id 100 family inet address 20.1.1.2/24
   ```

3. Configure remaining interfaces for chassis 2 as needed.

Results

`user@host#` **show interfaces**

```
ms-4/0/0 {
        redundancy-options {
            redundancy-peer {
                ipaddress 5.5.5.1;
            }
            routing-instance HA;
```

```
        }
        unit 0 {
            family inet;
        }
        unit 10 {
            ip-address-owner service-plane;
            family inet {
                address 5.5.5.2/32;
            }
        }
ge-2/0/0 {
        vlan-tagging;
        unit 0 {
            vlan-id 100;
            family inet {
                 address 20.1.1.2/24;
            }
        }
        unit 10 {
            vlan-id 10;
            family inet {
                address 2.10.1.2/24;
            }
```

Configure Routing Information for Chassis 2

Step-by-Step Procedure

Detailed routing configuration is not included for this example. A routing instance is required for the HA synchronization traffic between the two chassis and is included here.

- Configure routing instances for chassis 2.

```
user@host# set routing-instances HA instance-type vrf
user@host# set routing-instances HA interface ge-2/0/0.0
user@host# set routing-instances HA interface ms-4/0/0.10
user@host# set routing-instances HA route-distinguisher 1:1
user@host# set policy-options policy-statement dummy term 1 then reject
user@host# set routing-instances HA vrf-import dummy
user@host# set routing-instances HA vrf-export dummy
user@host# set routing-instances HA routing-options static route 5.5.5.2/32 next-hop ms-4/0/0.10
user@host# set routing-instances HA routing-options static route 5.5.5.1/32 next-hop 20.1.1.1
```

NOTE: The following configuration steps are *identical* to the steps shown for chassis 1.

- Configuring NAT and Stateful Firewall
- Configuring the Service Set

Results

`user@host#` **show services routing-instances**

```
HA {
        instance-type vrf;
        interface xe-2/2/0.0;
        interface ms-4/0/0.10;
        route-distinguisher 1:1;
        vrf-import dummy;
        vrf-export dummy;
        routing-options {
            static {
                route 5.5.5.2/32 next-hop ms-4/0/0.10;
                route 5.5.5.1/32 next-hop 20.1.1.1;
            }
        }
```

SEE ALSO

Inter-Chassis High Availability for Stateful Firewall and NAPT44 Overview (MS-MIC, MS-MPC) | **889**

Configuring Inter-Chassis High Availability for Stateful Firewall and NAPT44 (MS-MPC, MS-MIC) | **890**

9

PART

Configuring Interface Redundancy and Bundling on LSQ Interfaces

CHAPTER 43

Overview

IN THIS CHAPTER

Layer 2 Service Package Capabilities and Interfaces

As described in *Enabling Service Packages*, you can configure the AS or Multiservices PIC and the internal ASM in the M7i platform to use either the Layer 2 or the Layer 3 service package.

When you enable the Layer 2 service package, the AS or Multiservices PIC supports *link services*. On the AS or Multiservices PIC and the ASM, link services include the following:

- Junos CoS components—"Configuring CoS Scheduling Queues on Logical LSQ Interfaces" on page 834 describes how the Junos CoS components work on link services IQ (**lsq**) interfaces. For detailed information about Junos CoS components, see the *Class of Service User Guide (Routers and EX9200 Switches)*.
- Data compression using the compressed Real-Time Transport Protocol (CRTP) for use in voice over IP (VoIP) transmission.

  NOTE: On LSQ interfaces, all multilink traffic for a single bundle is sent to a single processor. If CRTP is enabled on the bundle, it adds overhead to the CPU. Because T3 network interfaces support only one link per bundle, make sure you configure a fragmentation map for compressed traffic on these interfaces and specify the **no-fragmentation** option. For more information, see "Configuring Delay-Sensitive Packet Interleaving" on page 1028 and "Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces" on page 839.

- Link fragment interleaving (LFI) on Frame Relay links using FRF.12 end-to-end fragmentation—The standard for FRF.12 is defined in the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*.
- LFI on Multilink Point-to-Point Protocol (MLPPP) links.
- Multilink Frame Relay (MLFR) end-to-end (FRF.15)—The standard for FRF.15 is defined in the specification FRF.15, *End-to-End Multilink Frame Relay Implementation Agreement*.

- Multilink Frame Relay (MLFR) UNI NNI (FRF.16)—The standard for FRF.16 is defined in the specification FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*.
- MLPPP—The standard for MLPPP is defined in the specification RFC 1990, *The PPP Multilink Protocol (MP)*.
- Multiclass extension to MLPPP—The standard is defined in the specification RFC 2686, *The Multi-Class Extension to Multi-Link PPP*.

For the LSQ interface on the AS or Multiservices PIC, the configuration syntax is almost the same as for Multilink and Link Services PICs. The primary difference is the use of the interface-type descriptor **lsq** instead of **ml** or **ls**. When you enable the Layer 2 service package on the AS or Multiservices PIC, the following interfaces are automatically created:

```
gr-fpc/pic/port
ip-fpc/pic/port
lsq-fpc/pic/port
lsq-fpc/pic/port:0
...
lsq-fpc/pic/port:N
mt-fpc/pic/port
pd-fpc/pic/port
pe-fpc/pic/port
sp-fpc/pic/port
vt-fpc/pic/port
```

Interface types **gr**, **ip**, **mt**, **pd**, **pe**, and **vt** are standard tunnel interfaces that are available on the AS or Multiservices PIC whether you enable the Layer 2 or the Layer 3 service package. These tunnel interfaces function the same way for both service packages, except that the Layer 2 service package does not support some tunnel functions, as shown in Table 5 on page 24. For more information about tunnel interfaces, see *Tunnel and Encryption Services Interfaces User Guide for Routing Devices*.

NOTE: Interface type **sp** is created because it is needed by the Junos OS. For the Layer 2 service package, the **sp** interface is not configurable, but you should not disable it.

Interface type **lsq-*fpc/pic/port*** is the physical link services IQ interface (**lsq**). Interface types **lsq-*fpc/pic/port*:0** through **lsq-*fpc/pic/port*:*N*** represent FRF.16 bundles. These interface types are created when you include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc *slot-number* pic *pic-number*]** hierarchy level. For more information, see "Configuring CoS Scheduling Queues on Logical LSQ Interfaces" on page 834.

NOTE: On DS0, E1, or T1 interfaces in LSQ bundles, you can configure the **bandwidth** statement, but the router does not use the bandwidth value if the interfaces are included in an MLPPP or MLFR bundle. The bandwidth is calculated internally according to the time slots, framing, and byte-encoding of the interface. For more information about these properties, see the *Junos OS Network Interfaces Library for Routing Devices*.

CHAPTER 44

Configuring Interface Redundancy with SONET APS and Virtual Interfaces

IN THIS CHAPTER

Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS

IN THIS SECTION

Link services IQ (**lsq-**) interfaces that are paired with SONET PICs can use the Automatic Protection Switching (APS) configuration already available on SONET networks to provide failure recovery. SONET APS provides stateless failure recovery, if it is configured on SONET interfaces in separate chassis and each SONET PIC is paired with an AS or Multiservices PIC in the same chassis. If one of the following conditions for APS failure is met, the associated SONET PIC triggers recovery to the backup circuit and its associated AS or Multiservices PIC. The failure conditions are:

- Failure of Link Services IQ PIC
- Failure of FPC that hosts the Link Services IQ PIC
- Failure of Packet Forwarding Engine
- Failure of chassis

The guidelines for configuring SONET APS are described in the *Junos OS Network Interfaces Library for Routing Devices*.

The following sections describe how to configure failover properties:

Configuring the Association between LSQ and SONET Interfaces

To configure the association between AS or Multiservices PICs hosting link services IQ interfaces and the SONET interfaces, include the **lsq-failure-options** statement at the **[edit interfaces]** hierarchy level:

```
lsq-fpc/pic/port {
    lsq-failure-options {
        no-termination-request;
        [ trigger-link-failure interface-name ];
    }
}
```

For example, consider the following network scenario:

- Primary router includes interfaces **oc3-0/2/0** and **lsq-1/1/0**.
- Backup router includes interfaces **oc3-2/2/0** and **lsq-3/2/0**.

Configure SONET APS, with **oc3-0/2/0** as the working circuit and **oc3-2/2/0** as the protect circuit. Include the **trigger-link-failure** statement to extend failure to the LSQ PICs:

```
interfaces lsq-1/1/0 {
    lsq-failure-options {
        trigger-link-failure oc3-0/2/0;
    }
}
```

NOTE: You must configure the **lsq-failure-options** statement on the primary router only. The configuration is not supported on the backup router.

To inhibit the router from sending PPP termination-request messages to the remote host if the Link Services IQ PIC fails, include the **no-termination-request** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* lsq-failure-options]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port lsq-failure-options]
no-termination-request;
```

This functionality is supported on link PICs as well. To inhibit the router from sending PPP termination-request messages to the remote host if a link PIC fails, include the **no-termination-request** statement at the **[edit interfaces *interface-name* ppp-options]** hierarchy level.

```
[edit interfaces interface-name ppp-options]
no-termination-request;
```

The **no-termination-request** statement is supported only with MLPPP and SONET APS configurations and works with PPP, PPP over Frame Relay, and MLPPP interfaces only, on the following PICs:

- Channelized OC3 IQ PICs
- Channelized OC12 IQ PICs
- Channelized STM1 IQ PICs
- Channelized STM4 IQ PICs

Configuring SONET APS Interoperability with Cisco Systems FRF.16

Juniper Networks routers configured with APS might not interoperate correctly with Cisco FRF.16. To enable interoperation, include the **cisco-interoperability** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* mlfr-uni-nni-bundle-options]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port mlfr-uni-nni-bundle-options]
cisco-interoperability send-lip-remove-link-for-link-reject;
```

The **send-lip-remove-link-for-link-reject** option prompts the router to send a Link Integrity Protocol remove link when it receives an add-link rejection message.

Restrictions on APS Redundancy for LSQ Interfaces

The following restrictions apply to LSQ failure recovery:

- It applies only to Link Services IQ PICs installed in M Series routers, except for M320 routers.
- You must configure the **failure-options** statement on physical LSQ interfaces, not on MLFR channelized units.
- The Link Services IQ PICs must be associated with SONET link PICs. The paired PICs can be installed on different routers or in the same router; in other words, both interchassis and intrachassis recovery are supported
- Failure recovery is stateless; as a result, route flapping and loss of link state is expected in interchassis recovery, requiring PPP renegotiation. In intrachassis recovery, no impact on traffic is anticipated with Routing Engine failover, but PIC failover results in PPP renegotiation.

- The switchover is not revertive: when the original hardware is restored to service, traffic does not automatically revert back to it.
- Normal APS switchover and PIC-triggered APS switchover can be distinguished only by checking the system log messages.

> **NOTE:** When an AS PIC experiences persistent back pressure as a result of high traffic volume for 3 seconds, the condition triggers an automatic core dump and reboot of the PIC to help clear the blockage. A system log message at level LOG_ERR is generated. This mechanism applies to both Layer 2 and Layer 3 service packages.

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | **905**

Configuring LSQ Interface Redundancy in a Single Router Using SONET APS | **911**

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | **912**

Configuring Link Services and CoS on Services PICs | **841**

Link Services Configuration for Junos Interfaces | **833**

Configuring LSQ Interface Redundancy in a Single Router Using SONET APS

Stateless switchover from one Link Services IQ PIC to another within the same router can be configured by using the SONET APS mechanism described in "Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS" on page 908. Each Link Services IQ PIC must be associated with a specified SONET link PIC within the same router.

> **NOTE:** For complete intrachassis recovery, including recovery from Routing Engine failover, graceful Routing Engine switchover (GRES) must be enabled on the router. For more information, see the *Junos OS Administration Library*.

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces

IN THIS SECTION

You can configure failure recovery on M Series, MX Series, and T Series routers that have multiple AS or Multiservices PICs and DPCs with **lsq-** interfaces by specifying a virtual LSQ redundancy (**rlsq**) interface in which the primary Link Services IQ PIC is active and a secondary PIC is on standby. If the primary PIC fails, the secondary PIC becomes active, and all LSQ processing is transferred to it. To determine which PIC is currently active, issue the **show interfaces redundancy** command.

NOTE: This configuration does not require the use of SONET APS for failover. Network interfaces that do not support SONET can be used, such as T1 or E1 interfaces.

The following sections provide more information:

Configuring Redundant Paired LSQ Interfaces

The physical interface type **rlsq** specifies the pairings between primary and secondary **lsq** interfaces to enable redundancy. To configure a backup **lsq** interface, include the **redundancy-options** statement at the **[edit interfaces rlsq*number*]** hierarchy level:

```
[edit interfaces rlsqnumber]
```

```
redundancy-options {
    (hot-standby | warm-standby);
    primary lsq-fpc/pic/port;
    secondary lsq-fpc/pic/port;
}
```

For the **rlsq** interface, ***number*** can be from 0 through 1023. If the primary **lsq** interface fails, traffic processing switches to the secondary interface. The secondary interface remains active even after the primary interface recovers. If the secondary interface fails and the primary interface is active, processing switches to the primary interface.

The **hot-standby** option is used with one-to-one redundancy configurations, in which one working PIC is supported by one backup PIC. It is supported with MLPPP, CRTP, FRF.15, and FRF.16 configurations for the LSQ interface to achieve an uninterrupted LSQ service. It sets the requirement for the failure detection and recovery time to be less than 5 seconds. The behavior is revertive, but you can manually switch between the primary and secondary PICs by issuing the **request interfaces (revert | switchover) rlsq*number*** operational mode command. It also provides a switch over time of 5 seconds and less for FRF.15 and a maximum of 10 seconds for FRF.16.

The **warm-standby** option is used with redundancy configurations in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected.

Certain combinations of **hot-standby** and **warm-standby** configuration are not permitted and result in a configuration error. The following examples are permitted:

- Interface **rlsq0** configured with **primary lsq-0/0/0** and **warm-standby**, in combination with interface **rlsq0:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:0**, in combination with interface **rlsq0:1** configured with **primary lsq-0/0/0:1**

The following example combinations are not permitted:

- Interface **rlsq0** configured with **primary lsq-0/0/0** and **hot-standby**, in combination with interface **rlsq0:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:0**, in combination with interface **rlsq1:0** configured with **primary lsq-0/0/0:0**
- Interface **rlsq0:0** configured with **primary lsq-0/0/0:1**, in combination with interface **rlsq1:1** configured with **primary lsq-0/0/0:1**
- Interface **rlsq0** configured with **primary lsq-0/0/0**, in combination with interface **rlsq1** configured with **primary lsq-0/0/0**

In addition, the same physical interface cannot be reused as the primary interface for more than one **rlsq** interface, nor can any of the associated logical interfaces. For example, primary interface **lsq-0/0/0** cannot be reused in another **rlsq** interface as **lsq-0/0/0:0**.

Restrictions on Redundant LSQ Interfaces

Link Services IQ PIC failure occurs under the following conditions:

- The primary PIC fails to boot. In this case, the **rlsq** interface does not come up and manual intervention is necessary to reboot or replace the PIC, or to rename the primary PIC to the secondary one in the **rlsq** configuration.
- If the following conditions are not met when configuring an **rlsq** interface:
  - The unit number allocated to the **rlsq** interface is less than the number of Multilink Frame Relay user-to-network interface network-to-network interface (UNI-NNI) (FRF.16) bundles allocated on the Link Services PIC.
  - Data-link connection identifier (DLCI) is configured for the **rlsq** interface.

  If these conditions are not met, the **rlsq** interface does not boot. When you issue the **show interfaces redundancy** command, the state of the **rlsq** interface is indicated as **Waiting for primary MS PIC**.
- The primary PIC becomes active and then fails. The secondary PIC automatically takes over processing.
- A failover to the secondary PIC takes place. The secondary PIC then fails. If the primary PIC has been restored to active state, processing switches to it.
- The FPC that contains the Link Services IQ PIC fails.

The following constraints apply to redundant LSQ configurations:

- We recommend that primary and secondary PICs be configured in two different FPCs (in chassis other than M10i routers).
- You cannot configure a Link Services IQ PIC with explicit bundle configurations and as a constituent of an **rlsq** interface.
- Redundant LSQ configurations provide full GRES support. (You must configure GRES at the **[edit chassis]** hierarchy level; see the *Junos OS Administration Library*.
- If you configure the **redundancy-options** statement with the **hot-standby** option, the configuration must include one **primary** interface value and one **secondary** interface value.
- Since the same interface name is used for **hot-standby** and **warm-standby**, if you modify the configuration to change this attribute, it is recommended that you first deactivate the interface, commit the new configuration, and then reactivate the interface.
- You cannot make changes to an active **redundancy-options** configuration. You must deactivate the **rlsq*number*** interface configuration, change it, and reactivate it.

- The **rlsq*number*** configuration becomes active only if the primary interface is active. When the configuration is first activated, the primary interface must be active; if not, the **rlsq** interface waits until the primary interface comes up.
- You cannot modify the configuration of **lsq** interfaces after they have been included in an active **rlsq** interface.
- All the operational mode commands that apply to **rsp** interfaces also apply to **rlsq** interfaces. You can issue **show** commands for the **rlsq** interface or the primary and secondary **lsq** interfaces. However, statistics on the link interfaces are not carried over following a Routing Engine switchover.
- The **rlsq** interfaces also support the **lsq-failure-options** configuration, discussed in "Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS" on page 908. If the primary and secondary Link Services IQ PICs fail and the **lsq-failure-options** statement is configured, the configuration triggers a SONET APS switchover.
- Redundant LSQ configurations that require MLPPP Multilink Frame Relay (FRF.15 and FRF.16) are supported only with the **warm-standby** option.
- Redundant LSQ support is extended to ATM network interfaces.
- Channelized interfaces are used with FRF-16 bundles, for example **rlsq0:0**. The **rlsq** number and its constituents, the **primary** and **secondary** interfaces, must match for the configuration to be valid: either all must be channelized, or none. For an example of an FRF.16 configuration, see "Configuring LSQ Interface Redundancy for an FRF.16 Bundle" on page 922.
- When you configure a channelized **rlsq** interface, you must use a channel index number from 0 through 254.

> **NOTE:** Adaptive Services and Multiservices PICs in layer-2 mode (running Layer 2 services) are not rebooted when a MAC flow-control situation is detected.

Configuring Link State Replication for Redundant Link PICs

Link state replication, also called *interface preservation*, is an addition to the SONET Automatic Protection Switching (APS) functionality that helps promote redundancy of the link PICs used in LSQ configurations.

Link state replication provides the ability to add two sets of links, one from the active (working) SONET PIC and the other from the backup (protect) SONET PIC to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without causing a link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation. For more information about SONET APS configurations, see the *Junos OS Network Interfaces Library for Routing Devices*.

To configure link state replication, include the **preserve-interface** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level on both network interfaces:

```
edit interfaces interface-name sonet-options aps]
preserve-interface;
```

The following constraints apply to link PIC redundancy:

- APS functionality must be available on the SONET PICs and the interface configurations must be identical on both ends of the link. Any configuration mismatch causes the commit operation to fail.
- This feature is supported only with LSQ and SONET APS-enabled link PICs, including Channelized OC3, Channelized OC12, and Channelized STM1 intelligent queuing (IQ) PICs.
- Link state replication supports MLPPP and PPP over Frame Relay (**frame-relay-ppp**) encapsulation, and fully supports GRES.
- Enabling the interface or protocol traceoptions with a large number of MLPPP links can trigger Link Control Protocol (LCP) renegotiation during the link switchover time.

  NOTE: This renegotiation is more likely to take place for configurations with back-to-back Juniper Networks routers than in networks in which a Juniper Networks router is connected to an add/drop multiplexer (ADM).

- In general, networks that connect a Juniper Networks router to an ADM allow faster MLPPP link switchover than those with back-to-back Juniper Networks routers. The MLPPP link switchover time difference may be significant, especially for networks with a large number of MLPPP links.
- An aggressive LCP keepalive timeout configuration can lead to LCP renegotiation during the MLPPP link switchover. By default, the LCP keepalive timer interval is 10 seconds and the consecutive link down count is 3. The MLPPP links start LCP negotiation only after a timeout of 30 seconds. Lowering these configuration values may trigger one or more of the MLPPP links to renegotiate during the switchover time.

  NOTE: LCP renegotiation is more likely to take place for configurations with back-to-back Juniper Networks routers than in networks in which a Juniper Networks router is connected to an ADM.

As an example, the following configuration shows the link state replication configuration between the ports **coc3-1/0/0** and c**oc3-2/0/0**.

```
interfaces {
    coc3-1/0/0 {
        sonet-options {
```

```
            aps {
                preserve-interface;
                working-circuit aps-group-1;
            }
        }
    }
    coc3-2/0/0 {
        sonet-options {
            aps {
                preserve-interface;
                protect-circuit aps-group-1;
            }
        }
    }
}
```

Examples: Configuring Redundant LSQ Interfaces for Failure Recovery

Configuring LSQ Interface Redundancy for MLPPP

The following configuration shows that **lsq-1/1/0** and **lsq-1/3/0** work as a pair and the redundancy type is **hot-standby**, which sets the requirement for the failure detection and recovery time to be less than 5 seconds:

```
interfaces rlsq0 {
    redundancy-options {
        primary lsq-1/1/0;
        secondary lsq-1/3/0;
        hot-standby; #either hot-standby or warm-standby is supported
    }
}
```

The following example shows a related MLPPP configuration:

NOTE: MLPPP protocol configuration is required for this configuration.

```
interfaces {
    t1-/1/2/0 {
        unit 0 {
            family mlppp {
                bundle rlsq0.0;
            }
        }
    }
    rlsq0 {
        unit 0 {
            family inet {
                address 30.1.1.2/24;
            }
        }
    }
}
```

The following example shows a related CoS configuration:

```
class-of-service {
    interfaces {
        rlsq0 {
            unit * {
                fragmentation-maps fr-map1;
            }
        }
    }
}
```

The following example shows a complete link state replication configuration for MLPPP. This example uses two bundles, each with four T1 links. The first four T1 links (**t1-*:1** through **t1-*:4**) form the first bundle and the last four T1 links (**t1-*:5** through **t1-*:8**) form the second bundle. To minimize the duplication in the configuration, this example uses the **[edit groups]** statement; for more information, see the *Junos OS Administration Library*. This type of configuration is not required; it simplifies the task and minimizes duplication.

```
groups {
    ml-partition-group {
        interfaces {
            <coc3-*> {
                partition 1 oc-slice 1 interface-type coc1;
            }
            <coc1-*> {
```

```
            partition 1-8 interface-type t1;
          }
        }
      }
      ml-bundle-group-1 {
        interfaces {
          <t1-*:"[1-4]"> {
            encapsulation ppp;
            unit 0 {
              family mlppp {
                bundle lsq-0/1/0.0;
              }
            }
          }
        }
      }
      ml-bundle-group-2 {
        interfaces {
          <t1-*:"[5-8]"> {
            encapsulation ppp;
            unit 0 {
              family mlppp {
                bundle lsq-0/1/0.1;
              }
            }
          }
        }
      }
    }
    interfaces {
      lsq-0/1/0 {
        unit 0 {
          encapsulation multilink-ppp;
          family inet {
            address 1.1.1.1/32 {
              destination 1.1.1.2;
            }
          }
        }
        unit 1 {
          encapsulation multilink-ppp;
          family inet {
            address 1.1.2.1/32 {
              destination 1.1.2.2;
```

```
            }
        }
    }
}
coc3-1/0/0 {
    apply-groups ml-partition-group;
    sonet-options {
        aps {
            preserve-interface;
            working-circuit aps-group-1;
        }
    }
}
coc1-1/0/0:1 {
    apply-groups ml-partition-group;
}
t1-1/0/0:1:1 {
    apply-groups ml-bundle-group-1;
}
t1-1/0/0:1:2 {
    apply-groups ml-bundle-group-1;
}
t1-1/0/0:1:3 {
    apply-groups ml-bundle-group-1;
}
t1-1/0/0:1:4 {
    apply-groups ml-bundle-group-1;
}
t1-1/0/0:1:5 {
    apply-groups ml-bundle-group-2;
}
t1-1/0/0:1:6 {
    apply-groups ml-bundle-group-2;
}
t1-1/0/0:1:7 {
    apply-groups ml-bundle-group-2;
}
t1-1/0/0:1:8 {
    apply-groups ml-bundle-group-2;
}
coc3-2/0/0 {
    apply-groups ml-partition-group;
    sonet-options {
        aps {
```

```
            preserve-interface;
            protect-circuit aps-group-1;
          }
        }
      }
      coc1-2/0/0:1 {
        apply-groups ml-partition-group;
      }
      t1-2/0/0:1:1 {
        apply-groups ml-bundle-group-1;
      }
      t1-2/0/0:1:2 {
        apply-groups ml-bundle-group-1;
      }
      t1-2/0/0:1:3 {
        apply-groups ml-bundle-group-1;
      }
      t1-2/0/0:1:4 {
        apply-groups ml-bundle-group-1;
      }
      t1-2/0/0:1:5 {
        apply-groups ml-bundle-group-2;
      }
      t1-2/0/0:1:6 {
        apply-groups ml-bundle-group-2;
      }
      t1-2/0/0:1:7 {
        apply-groups ml-bundle-group-2;
      }
      t1-2/0/0:1:8 {
        apply-groups ml-bundle-group-2;
      }
    }
```

Configuring LSQ Interface Redundancy for an FRF.15 Bundle

The following example shows a configuration for an FRF.15 bundle:

```
interfaces rlsq0 {
  redundancy-options {
```

```
        primary lsq-1/2/0;
        secondary lsq-1/3/0;
        warm-standby; #either hot-standby or warm-standby is supported
    }
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 30.1.1.1/24;
        }
    }
}
```

Configuring LSQ Interface Redundancy for an FRF.16 Bundle

The following example shows a configuration for an FRF.16 bundle:

```
interfaces rlsq0:0 {
    dce;
    encapsulation multilink-frame-relay-uni-nni;
    redundancy-options {
        primary lsq-1/2/0:0;
        secondary lsq-1/3/0:0;
        warm-standby; #either hot-standby or warm-standby is supported
    }
    unit 0 {
        dlci 1000;
        family inet {
            address 50.1.1.1/24;
        }
    }
}
```

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | **905**

Configuring LSQ Interface Redundancy Across Multiple Routers Using SONET APS | **908**

Configuring LSQ Interface Redundancy in a Single Router Using SONET APS | **911**

CHAPTER 45

Enabling Bundling on LSQ Interfaces

IN THIS CHAPTER

Inline MLPPP for WAN Interfaces Overview

Inline Multilink PPP (MLPPP), Multilink Frame Relay (FRF.16), and Multilink Frame Relay End-to-End (FRF.15) for time-division multiplexing (TDM) WAN interfaces provide bundling services through the Packet Forwarding Engine without requiring a PIC or Dense Port Concentrator (DPC).

Traditionally, bundling services are used to bundle multiple low-speed links to create a higher bandwidth pipe. This combined bandwidth is available to traffic from all links and supports link fragmentation and interleaving (LFI) on the bundle, reducing high priority packet transmission delay.

This support includes multiple links on the same bundle as well as multiclass extension for MLPPP. Through this service you can enable bundling services without additional DPC slots to support Service DPC and free up the slots for other MICs.

NOTE: MLPPP is not supported on MX Series Virtual Chassis.

Starting in Junos OS Release 15.1, you can configure inline MLPPP interfaces on MX80, MX104, MX240, MX480, and MX960 routers with Channelized E1/T1 Circuit Emulation MICs. A maximum of up to eight inline MLPPP interface bundles are supported on Channelized E1/T1 Circuit Emulation MICs, similar to the support for inline MLPPP bundles on other MICs with which they are compatible.

Configuring inline MLPPP for WAN interfaces benefits the following services:

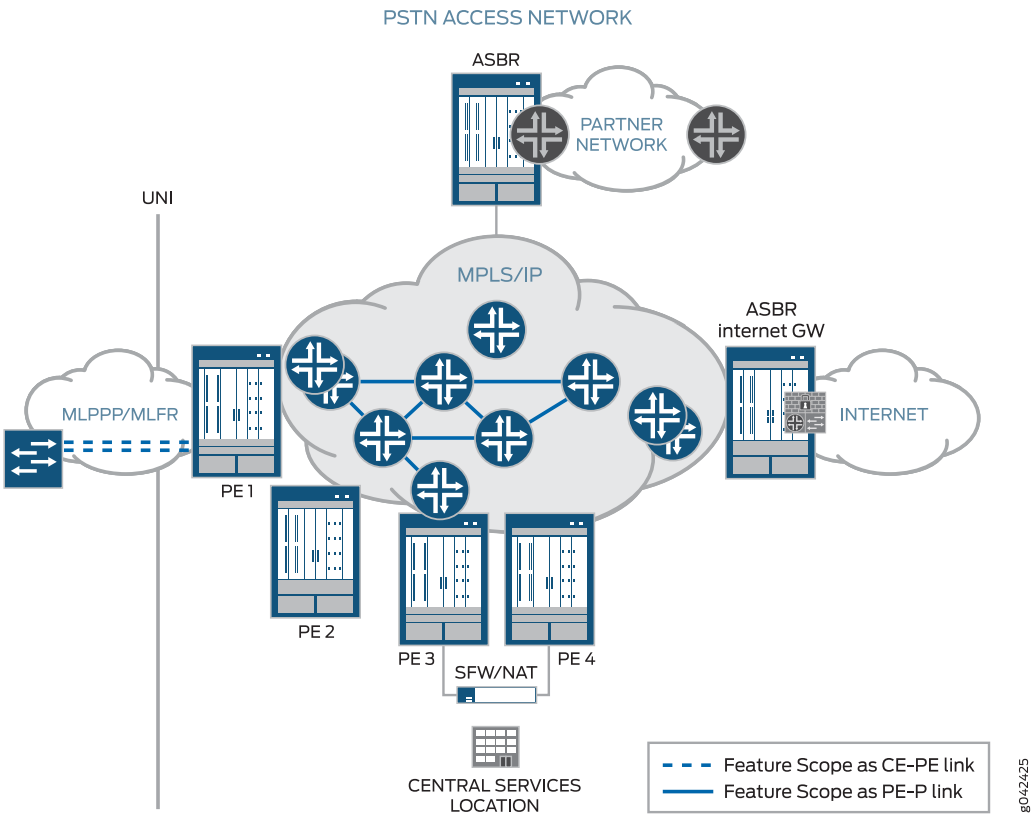
- CE-PE link for Layer 3 VPN and DIA service with public switched telephone networks (PSTN)-based access networks.
- PE-P link when PSTN is used for MPLS networks.

This feature is used by the following service providers:

- Service providers that use PSTN to offer Layer 3 VPN and DIA service with PSTN-based access networks to medium or large business customers.
- Service providers with SONET-based core networks.

The following figure illustrates the scope of this feature:

Figure 42: Inline MLPPP for WAN Interfaces



For connecting many smaller sites in VPNs, bundling the TDM circuits together with MLPPP/MLFR technology is the *only* way to offer higher bandwidth and link redundancy.

MLPPP enables you to bundle multiple PPP links into a single multilink bundle, and MLFR enables you to bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single multilink bundle. Multilink bundles provide additional bandwidth, load balancing, and redundancy by aggregating low-speed links, such as T1, E1, and serial links.

MLPPP is a protocol for aggregating multiple constituent links into one larger PPP bundle. MLFR allows you to aggregate multiple Frame Relay links by inverse multiplexing. MLPPP and MLFR provide service options between low-speed T1 and E1 services. In addition to providing additional bandwidth, bundling multiple links can add a level of fault tolerance to your dedicated access service. Because you can implement bundling across multiple interfaces, you can protect users against loss of access when a single interface fails.

To configure inline MLPPP for WAN interfaces, see:

- *Example: Configuring Inline MLPPP and Multilink Frame Relay End-to-End (FRF.15) for WAN Interfaces*
- *Example: Configuring Inline Multilink Frame Relay (FRF.16) for WAN Interfaces*

Release History Table

Release	Description
15.1	Starting in Junos OS Release 15.1, you can configure inline MLPPP interfaces on MX80, MX104, MX240, MX480, and MX960 routers with Channelized E1/T1 Circuit Emulation MICs.

RELATED DOCUMENTATION

Enabling Inline LSQ Services | **929**

Enabling MLPPP Link Fragmentation and Interleaving

Example: Configuring Multilink Frame Relay FRF.15

Example: Configuring Multilink Frame Relay FRF.16

Link and Multilink Services Interfaces User Guide for Routing Devices

Reserving Bundle Bandwidth for Link-Layer Overhead on LSQ Interfaces

Link-layer overhead can cause packet drops on constituent links because of bit stuffing on serial links. Bit stuffing is used to prevent data from being interpreted as control information.

By default, 4 percent of the total bundle bandwidth is set aside for link-layer overhead. In most network environments, the average link-layer overhead is 1.6 percent. Therefore, we recommend 4 percent as a safeguard. For more information, see RFC 4814, *Hash and Stuffing: Overlooked Factors in Network Device Benchmarking*.

For link services IQ (**lsq-**) interfaces, you can configure the percentage of bundle bandwidth to be set aside for link-layer overhead. To do this, include the **link-layer-overhead** statement:

```
link-layer-overhead percent;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]**
- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

You can configure the value to be from 0 percent through 50 percent.

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | **905**

Oversubscribing Interface Bandwidth on LSQ Interfaces | **845**

Configuring Guaranteed Minimum Rate on LSQ Interfaces | **851**

Link Services Configuration for Junos Interfaces | **833**

Configuring Multiclass MLPPP on LSQ Interfaces

For link services LSQ (**lsq-**) interfaces with MLPPP encapsulation, you can configure multiclass MLPPP (MCML). If you do not configure MCML, fragments from different classes cannot be interleaved. All fragments for a single packet must be sent before the fragments from another packet are sent. Nonfragmented packets can be interleaved between fragments of another packet to reduce latency seen by nonfragmented packets. In effect, latency-sensitive traffic is encapsulated as regular PPP traffic, and bulk traffic is encapsulated as multilink traffic. This model works as long as there is a single class of latency-sensitive traffic, and there is no high-priority traffic that takes precedence over latency-sensitive traffic. This approach to LFI, used on the Link Services PIC, supports only two levels of traffic priority, which is not sufficient to carry the four-to-eight forwarding classes that are supported by M Series and T Series routers. For more information about the Link Services PIC support of LFI, see *Configuring Delay-Sensitive Packet Interleaving on Link Services Logical Interfaces*.

NOTE: ACX Series routers do not support link fragmentation interleaving (LFI).

For link services LSQ interfaces only, you can configure MCML, as defined in RFC 2686, *The Multi-Class Extension to Multi-Link PPP*. MCML makes it possible to have multiple classes of latency-sensitive traffic that are carried over a single multilink bundle with bulk traffic. In effect, MCML allows different classes of traffic to have different latency guarantees. With MCML, you can map each forwarding class into a separate multilink class, thus preserving priority and latency guarantees.

NOTE: Configuring both LFI and MCML on the same bundle is not necessary, nor is it supported, because multiclass MLPPP represents a superset of functionality. When you configure multiclass MLPPP, LFI is automatically enabled.

The Junos OS implementation of MCML does not support compression of common header bytes, which is referred to in RFC 2686 as "prefix elision."

MCML greatly simplifies packet ordering issues that occur when multiple links are used. Without MCML, all voice traffic belonging to a single flow is hashed to a single link to avoid packet ordering issues. With MCML, you can assign voice traffic to a high-priority class, and you can use multiple links. For more information about voice services support on link services IQ interfaces (**lsq**), see "Configuring Services Interfaces for Voice Services" on page 1026.

To configure MCML on a link services IQ interface, you must specify how many multilink classes should be negotiated when a link joins the bundle, and you must specify the mapping of a forwarding class into an MCML class.

To specify how many multilink classes should be negotiated when a link joins the bundle, include the **multilink-max-classes** statement:

```
multilink-max-classes number;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

The number of multilink classes can be 1 through 8. The number of multilink classes for each forwarding class must not exceed the number of multilink classes to be negotiated.

> **NOTE:** In ACX Series routers, the multilink classes can be 1 through 4.

To specify the mapping of a forwarding class into a MCML class, include the **multilink-class** statement at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level:

```
[edit class-of-service fragmentation-maps map-name forwarding-class class-name]
multilink-class number;
```

The multilink class index number can be 0 through 7. The **multilink-class** statement and **no-fragmentation** statements are mutually exclusive.

> **NOTE:** In ACX Series routers, the multilink class index number can be 0 through 3. ACX Series routers do not support the **no-fragmentation** statement for fragmentation map.

To view the number of multilink classes negotiated, issue the **show interfaces lsq-*fpc/pic/port.logical-unit-number* detail** command.

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | **905**
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP | **932**
- Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP | **965**
- Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP | **961**
- Link Services Configuration for Junos Interfaces | **833**

Enabling Inline LSQ Services

Inline Multilink PPP (MLPPP), Multilink Frame Relay (FRF.16), and Multilink Frame Relay End-to-End (FRF.15) for time-division multiplexing (TDM) WAN interfaces provide bundling services through the Packet Forwarding Engine without requiring a PIC or Dense Port Concentrator (DPC).

Traditionally, bundling services are used to bundle multiple low-speed links to create a higher bandwidth pipe. This combined bandwidth is available to traffic from all links and supports link fragmentation and interleaving (LFI) on the bundle, reducing high priority packet transmission delay.

This support includes multiple links on the same bundle as well as multiclass extension for MLPPP. Through this service you can enable bundling services without additional DPC slots to support Service DPC and free up the slots for other MICs.

The inline LSQ logical interface (referred to as lsq-) is a virtual service logical interface that resides on the Packet Forwarding Engine to provide Layer 2 bundling services that do not need a service PIC. The naming convention is **lsq-slot/pic/0**.

> **NOTE:** Click here for a compatibility matrix of MICs currently supported by MPC1, MPC2, MPC3, MPC6, MPC8, and MPC9 on MX240, MX480, MX960, MX2008, MX2010, MX2020, and MX10003 routers.

A Type1 MPC has only one logical unit (LU); therefore only one LSQ logical interface can be created. When configuring a Type1 MPC, use PIC slot 0. Type2 MPC has two LUs; therefore two LSQ logical interfaces can be created. When configuring a Type2 MPC, use PIC slot 0 and slot 2.

Configure each LSQ logical interface with one loopback stream. This stream can be shaped like a regular stream, and is shared with other inline interfaces, such as the inline services (SI) interface.

To support FRF.16 bundles, create logical interfaces with the naming convention **lsq-slot/pic/0:*bundle_id***, where *bundle_id* can range from 0 to 254. You can configure logical interfaces created on the main LSQ logical interface as MLPPP or FRF.16.

Because SI and LSQ logical interfaces might share the same stream, and there could be multiple LSQ logical interfaces on that stream, any logical interface-related shaping is configured at the Layer 2 node instead of the Layer 1 node. As a result, when SI is enabled, instead of limiting the stream bandwidth to 1Gb or 10Gb based on the configuration, only the Layer 2 queue allocated for the SI interface is shaped at 1Gb or 10Gb.

For MLPPP and FRF.15, each LSQ logical interface is shaped based on the total bundle bandwidth (sum of member link bandwidths with control packet flow overhead) by configuring one unique Layer 3 node per bundle. Similarly, each FRF.16 logical interface is shaped based on total bundle bandwidth by configuring one unique Layer 2 node per bundle. FRF16 logical interface data-link connection identifiers (DLCIs) are mapped to Layer 3 nodes.

To enable inline LSQ services and create the **lsq-** logical interface for the specified PIC, specify the **multi-link-layer-2-inline** and **mlfr-uni-nni-bundles-inline** configuration statements.

```
[edit chassis fpc number pic number]
user@host# set multi-link-layer-2-inline
user@host# set mlfr-uni-nni-bundles-inline number
```

NOTE: On MX80 and MX104 routers that have a single Packet Forwarding Engine, you can configure the LSQ logical interface only on FPC 0 and PIC 0. The channelized card must be in slot FPC 0/0 for the corresponding bundle to work.

For example, to enable inline service for PIC 0 on a Type1 MPC on slot 1:

```
[edit chassis fpc 1 pic 0]
user@host# set multi-link-layer-2-inline
user@host# set mlfr-uni-nni-bundles-inline 1
```

As a result, logical interfaces lsq-1/0/0, and lsq-1/0/0:0 are created. The number of inline multilink frame relay user-to-network interface (UNI) and network-to-network interface (NNI) bundles is set to 1.

For example, to enable inline service for both PIC 0 and PIC 2 on Type2 MPC installed in slot 5:

```
[edit chassis fpc 5 pic 0]
user@host# set multi-link-layer-2-inline
user@host# set mlfr-uni-nni-bundles-inline 1

[edit chassis fpc 5 pic 2]
user@host# set multi-link-layer-2-inline
user@host# set mlfr-uni-nni-bundles-inline 1
```

As a result, logical interfaces lsq-5/0/0, lsq-5/0/0:0, lsq-5/0/0:1, lsq-5/2/0, lsq-5/2/0:0, and lsq-5/2/0:1 are created. The number of inline multilink frame relay user-to-network interface (UNI) and network-to-network interface (NNI) bundles is set to 1.

NOTE: The PIC number here is only used as an anchor to choose the correct LU to bind the inline LSQ interface. The bundling services are operational as long as the Packet Forwarding Engine to which it is bound is operational, even if the logical PIC is offline.

RELATED DOCUMENTATION

Inline MLPPP for WAN Interfaces Overview | 924

Inline MLPPP for WAN Interfaces Overview | 924

Link and Multilink Services Interfaces User Guide for Routing Devices

mlfr-uni-nni-bundles-inline | 1320
multi-link-layer-2-inline | 1323

Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP

To configure an *N*xT1 bundle using MLPPP, you aggregate *N* different T1 links into a bundle. The *N*xT1 bundle is called a logical interface, because it can represent, for example, a routing adjacency. To aggregate T1 links into a an MLPPP bundle, include the **bundle** statement at the **[edit interfaces t1-*fpc/pic/port* unit *logical-unit-number* family mlppp]** hierarchy level:

```
[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlppp]
bundle lsq-fpc/pic/port.logical-unit-number;
```

NOTE: Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-*fpc/pic/port* unit *logical-unit-number*]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

NOTE: ACX Series routers do not support drop-timeout and link-layer-overhead properties.

The logical link services IQ interface represents the MLPPP bundle. For the MLPPP bundle, there are four associated queues on M Series routers and eight associated queues on M320 and T Series routers. A

scheduler removes packets from the queues according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

For MLPPP, assign a single scheduler map to the link services IQ interface (**lsq**) and to each constituent link. The default schedulers for M Series and T Series routers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for MLPPP, you should configure a single scheduler with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ interface (**lsq**) and to each constituent link, as shown in "Example: Configuring an LSQ Interface as an NxT1 Bundle Using MLPPP" on page 935.

> **NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.
>
> If the member link belonging to one MLPP, MLFR, or MFR bundle interface is moved to another bundle interface, or the links are swapped between two bundle interfaces, a commit is required between the delete and add operations to ensure that the configuration is applied correctly.

If the bundle has more than one link, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-*fpc/pic/port*]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port]
per-unit-scheduler;
```

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
    t1-fpc/pic/port unit logical-unit-number {
        scheduler-map map-name;
    }
}
forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
```

```
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        priority priority-level;
        transmit-rate (rate | percent percentage | remainder) <exact>;
    }
}
```

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Class of Service User Guide (Routers and EX9200 Switches)*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated, independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            fragment-threshold bytes;
            multilink-class number;
            no-fragmentation;
        }
    }
}
```

For *N*xT1 bundles using MLPPP, the byte-wise load balancing used in multilink-encapsulated queues is superior to the flow-wise load balancing used in nonencapsulated queues. All other considerations are equal. Therefore, we recommend that you configure all queues to be multilink encapsulated. You do this by including the **fragment-threshold** statement in the configuration. If you choose to set traffic on a queue to be nonencapsulated rather than multilink encapsulated, include the **no-fragmentation** statement in the fragmentation map. You use the **multilink-class** statement to map a forwarding class into a multiclass MLPPP (MCML). For more information about MCML, see "Configuring Multiclass MLPPP on LSQ Interfaces" on page 927. For more information about fragmentation maps, see "Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces" on page 839.

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an MLPPP header. The MLPPP header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on one of the *N* different T1 links. The link is chosen on a packet-by-packet basis to balance the load across the various T1 links.

If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers. The outgoing link for each fragment is selected independently of all other fragments.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces lsq-*fpc/pic/port* unit *logical-unit-number*]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see *Configuring MRRU on Multilink and Link Services Logical Interfaces*.

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain PPP header. Because there is no MLPPP header, there is no sequence number information. Therefore, the software must take special measures to avoid packet reordering. To avoid packet reordering, the software places the packet on one of the *N* different T1 links. The link is determined by hashing the values in the header. For IP, the software computes the hash based on source address, destination address, and IP protocol. For MPLS, the software computes the hash based on up to five MPLS labels, or four MPLS labels and the IP header.

For UDP and TCP the software computes the hash based on the source and destination ports, as well as source and destination IP addresses. This guarantees that all packets belonging to the same TCP/UDP flow always pass through the same T1 link, and therefore cannot be reordered. However, it does not guarantee that the load on the various T1 links is balanced. If there are many flows, the load is usually balanced.

The *N* different T1 interfaces link to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from all the T1 links. If a packet has an MLPPP header, the sequence number field is used to put the packet back into sequence number order. If the packet has a plain PPP header, the software accepts the packet in the order in which it arrives and makes no attempt to reassemble or reorder the packet.

Example: Configuring an LSQ Interface as an NxT1 Bundle Using MLPPP

```
[edit chassis]
fpc 1 {
   pic 3 {
      adaptive-services {
         service-package layer-2;
```

```
        }
    }
}
[edit interfaces]
t1-0/0/0 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/3/0.1; # This adds t1-0/0/0 to the specified bundle.
        }
    }
}
t1-0/0/1 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/3/0.1;
        }
    }
}
lsq-1/3/0 {
    unit 1 { # This is the virtual link that concatenates multiple T1s.
    encapsulation multilink-ppp;
    drop-timeout 1000;
    fragment-threshold 128;
    link-layer-overhead 0.5;
    minimum-links 2;
    mrru 4500;
    short-sequence;
    family inet {
        address 10.2.3.4/24;
    }
}
[edit interfaces]
lsq-1/3/0 {
    per-unit-scheduler;
}
[edit class-of-service]
interfaces {
    lsq-1/3/0 { # multilink PPP constituent link
    unit 0 {
        scheduler-map sched-map1;
    }
}
```

```
t1-0/0/0 { # multilink PPP constituent link
unit 0 {
   scheduler-map sched-map1;
}
t1-0/0/1 { # multilink PPP constituent link
unit 0 {
   scheduler-map sched-map1;
}
forwarding-classes {
   queue 0 be;
   queue 1 ef;
   queue 2 af;
   queue 3 nc;
}
scheduler-maps {
   sched-map1 {
      forwarding-class af scheduler af-scheduler;
      forwarding-class be scheduler be-scheduler;
      forwarding-class ef scheduler ef-scheduler;
      forwarding-class nc scheduler nc-scheduler;
   }
}
schedulers {
   af-scheduler {
      transmit-rate percent 30;
      buffer-size percent 30;
      priority low;
   }
   be-scheduler {
      transmit-rate percent 25;
      buffer-size percent 25;
      priority low;
   }
   ef-scheduler {
      transmit-rate percent 40;
      buffer-size percent 40;
      priority strict-high; # voice queue
   }
   nc-scheduler {
      transmit-rate percent 5;
      buffer-size percent 5;
      priority high;
   }
}
```

```
fragmentation-maps {
   fragmap-1 {
      forwarding-class be {
         fragment-threshold 180;
      }
      forwarding-class ef {
         fragment-threshold 100;
      }
   }
}
[edit interfaces]
lsq-1/3/0 {
   unit 0 {
      fragmentation-map fragmap-1;
   }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | **905**
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16 | **938**
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15 | **945**
- Link Services Configuration for Junos Interfaces | **833**

Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16

To configure an *N*xT1 bundle using FRF.16, you aggregate *N* different T1 links into a bundle. The *N*xT1 bundle carries a potentially large number of Frame Relay PVCs, identified by their DLCIs. Each DLCI is called a logical interface, because it can represent, for example, a routing adjacency.

To aggregate T1 links into an FRF.16 bundle, include the **mlfr-uni-nni-bundles** statement at the **[edit chassis fpc *slot-number* pic *slot-number*]** hierarchy level and include the **bundle** statement at the **[edit interfaces t1-*fpc/pic/port* unit *logical-unit-number* family mlfr-uni-nni]** hierarchy level:

```
[edit chassis fpc slot-number pic slot-number]
mlfr-uni-nni-bundles number;

[edit interfaces t1-fpc/pic/port unit logical-unit-number family mlfr-uni-nni]
```

```
bundle lsq-fpc/pic/port:channel;
```

NOTE: Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-*fpc/pic/port:channel*]** hierarchy level:

```
[edit interfaces lsq- fpc/pic/port:channel]
encapsulation multilink-frame-relay-uni-nni;
dce;
mlfr-uni-nni-options {
    acknowledge-retries number;
    acknowledge-timer milliseconds;
    action-red-differential-delay (disable-tx | remove-link);
    drop-timeout milliseconds;
    fragment-threshold bytes;
    hello-timer milliseconds;
    link-layer-overhead percent;
    lmi-type (ansi | itu);
    minimum-links number;
    mrru bytes;
    n391 number;
    n392 number;
    n393 number;
    red-differential-delay milliseconds;
    t391 number;
    t392 number;
    yellow-differential-delay milliseconds;
}
unit logical-unit-number {
    dlci dlci-identifier;
    family inet {
        address address;
    }
}
```

The link services IQ channel represents the FRF.16 bundle. Four queues are associated with each DLCI. A scheduler removes packets from the queues according to a scheduling policy. On the link services IQ interface, you typically designate one queue to have strict priority. The remaining queues are serviced in proportion to weights you configure.

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high-priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Class of Service User Guide (Routers and EX9200 Switches)*.

If the bundle has more than one link, you must include the **per-unit-scheduler** statement at the **[edit interfaces lsq-*fpc/pic/port:channel*]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port:channel]
per-unit-scheduler;
```

For FRF.16, you can assign a single scheduler map to the link services IQ interface (**lsq**) and to each link services IQ DLCI, or you can assign different scheduler maps to the various DLCIs of the bundle, as shown in "Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16" on page 942.

For the constituent links of an FRF.16 bundle, you do not need to configure a custom scheduler. Because LFI and multiclass are not supported for FRF.16, the traffic from each constituent link is transmitted from queue 0. This means you should allow most of the bandwidth to be used by queue 0. For M Series and T Series routers, the default schedulers' transmission rate and buffer size percentages for queues 0 through 3 are 95, 0, 0, and 5 percent. These default schedulers send all user traffic to queue 0 and all network-control traffic to queue 3, and therefore are well suited to the behavior of FRF.16. If desired, you can configure a custom scheduler that explicitly replicates the 95, 0, 0, and 5 percent queuing behavior, and apply it to the constituent links.

NOTE: For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

If the member link belonging to one MLPP, MLFR, or MFR bundle interface is moved to another bundle interface, or the links are swapped between two bundle interfaces, a commit is required between the delete and add operations to ensure that the configuration is applied correctly.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
   lsq-fpc/pic/port:channel {
      unit logical-unit-number {
         scheduler-map map-name;
      }
   }
}
```

```
forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        priority priority-level;
        transmit-rate (rate | percent percentage | remainder) <exact>;
    }
}
```

To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            fragment-threshold bytes;
        }
    }
}
```

For FRF.16 traffic, only multilink encapsulated (fragmented and sequenced) queues are supported. This is the default queuing behavior for all forwarding classes. FRF.16 does not allow for nonencapsulated traffic because the protocol requires that all packets carry the fragmentation header. If a large packet is split into multiple fragments, the fragments must have consecutive sequential numbers. Therefore, you cannot include the **no-fragmentation** statement at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level for FRF.16 traffic. For FRF.16, if you want to carry voice or any other latency-sensitive traffic, you should not use slow links. At T1 speeds and above, the serialization delay is small enough so that you do not need to use explicit LFI.

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an FRF.16 header. The FRF.16 header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on one of the *N* different T1 links. The link is chosen on a packet-by-packet basis to balance the load across the various T1 links.

If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the

software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers. The outgoing link for each fragment is selected independently of all other fragments.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level. The MRRU is similar to the MTU but is specific to link services interfaces. By default, the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see *Configuring MRRU on Multilink and Link Services Logical Interfaces*.

The *N* different T1 interfaces link to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from all the T1 links. Because each packet has an FRF.16 header, the sequence number field is used to put the packet back into sequence number order.

Example: Configuring an LSQ Interface as an NxT1 Bundle Using FRF.16

Configure an *N*xT1 bundle using FRF.16 with multiple CoS scheduler maps:

```
[edit chassis fpc 1 pic 3]
adaptive-services {
    service-package layer-2;
}
mlfr-uni-nni-bundles 2; # Creates channelized LSQ interfaces/FRF.16 bundles.
[edit interfaces]
t1-0/0/0 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle lsq-1/3/0:1;
        }
    }
}
t1-0/0/1 {
    encapsulation multilink-frame-relay-uni-nni;
    unit 0 {
        family mlfr-uni-nni {
            bundle lsq-1/3/0:1;
        }
```

```
    }
}
lsq-1/3/0:1 { # Bundle link consisting of t1-0/0/0 and t1-0/0/1
per-unit-scheduler;
encapsulation multilink-frame-relay-uni-nni;
dce; # One end needs to be configured as DCE.
mlfr-uni-nni-bundle-options {
    drop-timeout 180;
    fragment-threshold 64;
    hello-timer 180;
    minimum-links 2;
    mrru 3000;
    link-layer-overhead 0.5;
}
unit 0 {
    dlci 26; # Each logical unit maps a single DLCI.
    family inet {
        address 10.2.3.4/24;
    }
}
unit 1 {
    dlci 42;
    family inet {
        address 10.20.30.40/24;
    }
}
unit 2 {
    dlci 69;
    family inet {
        address 10.20.30.40/24;
    }
}
[edit class-of-service]
scheduler-maps {
    sched-map-lsq0 {
        forwarding-class af scheduler af-scheduler-lsq0;
        forwarding-class be scheduler be-scheduler-lsq0;
        forwarding-class ef scheduler ef-scheduler-lsq0;
        forwarding-class nc scheduler nc-scheduler-lsq0;
    }
    sched-map-lsq1 {
        forwarding-class af scheduler af-scheduler-lsq1;
        forwarding-class be scheduler be-scheduler-lsq1;
        forwarding-class ef scheduler ef-scheduler-lsq1;
```

```
        forwarding-class nc scheduler nc-scheduler-lsq1;
    }
}
schedulers {
    af-scheduler-lsq0 {
        transmit-rate percent 60;
        buffer-size percent 60;
        priority low;
    }
    be-scheduler-lsq0 {
        transmit-rate percent 30;
        buffer-size percent 30;
        priority low;
    }
    ef-scheduler-lsq0 {
        transmit-rate percent 5;
        buffer-size percent 5;
        priority strict-high;
    }
    nc-scheduler-lsq0 {
        transmit-rate percent 5;
        buffer-size percent 5;
        priority high;
    }
    af-scheduler-lsq1 {
        transmit-rate percent 50;
        buffer-size percent 50;
        priority low;
    }
    be-scheduler-lsq1 {
        transmit-rate percent 30;
        buffer-size percent 30;
        priority low;
    }
    ef-scheduler-lsq1 {
        transmit-rate percent 15;
        buffer-size percent 15;
        priority strict-high;
    }
    nc-scheduler-lsq1 {
        transmit-rate percent 5;
        buffer-size percent 5;
        priority high;
    }
```

```
}
interfaces {
    lsq-1/3/0:1 { # MLFR FRF.16
    unit 0 {
        scheduler-map sched-map-lsq0;
    }
    unit 1 {
        scheduler-map sched-map-lsq1;
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | 905
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP | 932
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15 | 945
- Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP | 961
- Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.15

This example configures an ***N***xT1 bundle using FRF.15 on a link services IQ interface. FRF.15 is similar to FRF.12, as described in "Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12" on page 952. The difference is that FRF.15 supports multiple physical links in a bundle, whereas FRF.12 supports only one physical link per bundle. For the Junos OS implementation of FRF.15, you can configure one DLCI per physical link.

> **NOTE:** Link services IQ interfaces support both T1 and E1 physical interfaces. This example refers to T1 interfaces, but the configuration for E1 interfaces is similar.

```
[edit interfaces]
lsq-1/3/0 {
    per-unit-scheduler;
    unit 0 {
        dlci 69;
```

```
        encapsulation multilink-frame-relay-end-to-end;
    }
}
unit 1 {
    dlci 13;
    encapsulation multilink-frame-relay-end-to-end;
}
# First physical link
t1-1/1/0:1 {
    encapsulation frame-relay;
    unit 0 {
        family mlfr-end-to-end {
            bundle lsq-1/3/0.0;
        }
    }
}
# Second physical link
t1-1/1/0:2 {
    encapsulation frame-relay;
    unit 0 {
        family mlfr-end-to-end {
            bundle lsq-1/3/0.0;
        }
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | 905
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP | 932
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using FRF.16 | 938
- Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI

When you configure a single fractional T1 interface, it is called a logical interface, because it can represent, for example, a routing adjacency.

The logical link services IQ interface represents the MLPPP bundle. Four queues are associated with the logical interface. A scheduler removes packets from the queues according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

To configure a single fractional T1 interface using MLPPP and LFI, you associate one DS0 (fractional T1) interface with a link services IQ interface. To associate a fractional T1 interface with a link services IQ interface, include the **bundle** statement at the **[edit interfaces ds-*fpc/pic/port:channel* unit *logical-unit-number* family mlppp]** hierarchy level:

```
[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlppp]
bundle lsq-fpc/pic/port.logical-unit-number;
```

NOTE: Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-*fpc/pic/port* unit *logical-unit-number*]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-ppp;
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

For MLPPP, assign a single scheduler map to the link services IQ (**lsq**) interface and to each constituent link. The default schedulers for M Series and T Series routers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for MLPPP, you should configure a single scheduler with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign this scheduler to the link services IQ (**lsq**) interface and to each constituent link and to each constituent link, as shown in "Example: Configuring an LSQ Interface for a Fractional T1 Interface Using MLPPP and LFI" on page 950.

NOTE: For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
    ds-fpc/pic/port.channel {
        scheduler-map map-name;
    }
}
forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
}
schedulers {
    scheduler-name {
        buffer-size (percent percentage | remainder | temporal microseconds);
        priority priority-level;
        transmit-rate (rate | percent percentage | remainder) <exact>;
    }
}
```

For link services IQ interfaces, a strict-high-priority queue might starve all the other queues because traffic in a strict-high priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue receives infinite credits and does round-robin with high-priority queues, as described in the *Class of Service User Guide (Routers and EX9200 Switches)*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated, independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
   map-name {
      forwarding-class class-name {
         fragment-threshold bytes;
         no-fragmentation;
      }
   }
}
```

If you require the queue to transmit small packets with low latency, configure the queue to be nonencapsulated by including the **no-fragmentation** statement. If you require the queue to transmit large packets with normal latency, configure the queue to be multilink encapsulated by including the **fragment-threshold** statement. If you require the queue to transmit large packets with low latency, we recommend using a faster link and configuring the queue to be nonencapsulated. For more information about fragmentation maps, see "Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces" on page 839.

When a packet is removed from a multilink-encapsulated queue, it is fragmented. If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* unit *logical-unit-number*]** hierarchy level. The MRRU is similar to the MTU, but is specific to link services interfaces. By default the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see *Configuring MRRU on Multilink and Link Services Logical Interfaces*.

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an MLPPP header. The MLPPP header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on the fractional T1 link. Traffic from another queue might be interleaved between two fragments of the packet.

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain PPP header. The packet is then placed on the fractional T1 link as soon as possible. If necessary, the packet is placed between the fragments of a packet from another queue.

The fractional T1 interface links to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from the fractional T1 link. If a packet has an MLPPP header, the software assumes the packet is a fragment of a larger packet, and the fragment number field is used to reassemble the larger packet. If the packet has a plain PPP header, the software accepts the packet in the order in which it arrives, and the software makes no attempt to reassemble or reorder the packet.

Example: Configuring an LSQ Interface for a Fractional T1 Interface Using MLPPP and LFI

Configure a single fractional T1 logical interface:

```
[edit interfaces]
lsq-0/2/0 {
    per-unit-scheduler;
    unit 0 {
        encapsulation multilink-ppp;
        link-layer-overhead 0.5;
        family inet {
            address 10.40.1.1/30;
        }
    }
}
ct3-1/0/0 {
    partition 1 interface-type ct1;
}
ct1-1/0/0:1 {
    partition 1 timeslots 1-2 interface-type ds;
}
ds-1/0/0:1:1 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-0/2/0.0;
        }
    }
}
[edit class-of-service]
interfaces {
    ds-1/0/0:1:1 { # multilink PPP constituent link
    unit 0 {
        scheduler-map sched-map1;
    }
}
forwarding-classes {
    queue 0 be;
```

```
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
scheduler-maps {
    sched-map1 {
        forwarding-class af scheduler af-scheduler;
        forwarding-class be scheduler be-scheduler;
        forwarding-class ef scheduler ef-scheduler;
        forwarding-class nc scheduler nc-scheduler;
    }
}
schedulers {
    af-scheduler {
        transmit-rate percent 20;
        buffer-size percent 20;
        priority low;
    }
    be-scheduler {
        transmit-rate percent 20;
        buffer-size percent 20;
        priority low;
    }
    ef-scheduler {
        transmit-rate percent 50;
        buffer-size percent 50;
        priority strict-high; # voice queue
    }
    nc-scheduler {
        transmit-rate percent 10;
        buffer-size percent 10;
        priority high;
    }
}
fragmentation-maps {
    fragmap-1 {
        forwarding-class be {
            fragment-threshold 180;
        }
        forwarding-class ef {
            fragment-threshold 100;
        }
    }
}
```

```
[edit interfaces]
lsq-0/2/0 {
    unit 0 {
        fragmentation-map fragmap-1;
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | 905
- Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12 | 952
- Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12

To configure a single fractional T1 interface using FRF.16, you associate a DS0 interface with a link services IQ (**lsq**) interface. When you configure a single fractional T1, the fractional T1 carries a potentially large number of Frame Relay PVCs identified by their DLCIs. Each DLCI is called a logical interface, because it can represent, for example, a routing adjacency. To associate the DS0 interface with a link services IQ interface, include the **bundle** statement at the **[edit interfaces ds-*fpc/pic/port:channel* unit *logical-unit-number* family mlfr-end-to-end]** hierarchy level:

```
[edit interfaces ds-fpc/pic/port:channel unit logical-unit-number family mlfr-end-to-end]
bundle lsq-fpc/pic/port.logical-unit-number;
```

NOTE: Link services IQ interfaces support both T1 and E1 physical interfaces. These instructions apply to T1 interfaces, but the configuration for E1 interfaces is similar.

To configure the link services IQ interface properties, include the following statements at the **[edit interfaces lsq-*fpc/pic/port* unit *logical-unit-number*]** hierarchy level:

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number]
drop-timeout milliseconds;
encapsulation multilink-frame-relay-end-to-end;
```

```
fragment-threshold bytes;
link-layer-overhead percent;
minimum-links number;
mrru bytes;
short-sequence;
family inet {
    address address;
}
```

The logical link services IQ interface represents the FRF.12 bundle. Four queues are associated with each logical interface. A scheduler removes packets from the queues according to a scheduling policy. Typically, you designate one queue to have strict priority, and the remaining queues are serviced in proportion to weights you configure.

For FRF.12, assign a single scheduler map to the link services IQ interface (**lsq**) and to each constituent link. For M Series and T Series routers, the default schedulers, which assign 95, 0, 0, and 5 percent bandwidth for the transmission rate and buffer size of queues 0, 1, 2, and 3, are not adequate when you configure LFI or multiclass traffic. Therefore, for FRF.12, you should configure schedulers with nonzero percent transmission rates and buffer sizes for queues 0 through 3, and assign them to the link services IQ interface (**lsq**) and to each constituent link, as shown in "Examples: Configuring an LSQ Interface for a Fractional T1 Interface Using FRF.12" on page 955.

> **NOTE:** For M320 and T Series routers, the default scheduler transmission rate and buffer size percentages for queues 0 through 7 are 95, 0, 0, 5, 0, 0, 0, and 0 percent.

To configure and apply the scheduling policy, include the following statements at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
interfaces {
    ds-fpc/pic/port.channel {
        scheduler-map map-name;
    }
}
forwarding-classes {
    queue queue-number class-name;
}
scheduler-maps {
    map-name {
        forwarding-class class-name scheduler scheduler-name;
    }
```

```
}
schedulers {
   scheduler-name {
      buffer-size (percent percentage | remainder | temporal microseconds);
      priority priority-level;
      transmit-rate (rate | percent percentage | remainder) <exact>;
   }
}
```

For link services IQ interfaces, a strict-high-priority queue might starve the other three queues because traffic in a strict-high-priority queue is transmitted before any other queue is serviced. This implementation is unlike the standard Junos CoS implementation in which a strict-high-priority queue does round-robin with high-priority queues, as described in the *Class of Service User Guide (Routers and EX9200 Switches)*.

After the scheduler removes a packet from a queue, a certain action is taken. The action depends on whether the packet came from a multilink encapsulated queue (fragmented and sequenced) or a nonencapsulated queue (hashed with no fragmentation). Each queue can be designated as either multilink encapsulated or nonencapsulated, independently of the other. By default, traffic in all forwarding classes is multilink encapsulated. To configure packet fragmentation handling on a queue, include the **fragmentation-maps** statement at the **[edit class-of-service]** hierarchy level:

```
[edit class-of-service]
fragmentation-maps {
   map-name {
      forwarding-class class-name {
         fragment-threshold bytes;
         no-fragmentation;
      }
   }
}
```

If you require the queue to transmit small packets with low latency, configure the queue to be nonencapsulated by including the **no-fragmentation** statement. If you require the queue to transmit large packets with normal latency, configure the queue to be multilink encapsulated by including the **fragment-threshold** statement. If you require the queue to transmit large packets with low latency, we recommend using a faster link and configuring the queue to be nonencapsulated. For more information about fragmentation maps, see "Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces" on page 839.

When a packet is removed from a multilink-encapsulated queue, it is fragmented. If the packet exceeds the minimum link MTU, or if a queue has a fragment threshold configured at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, the software splits the packet into two or more fragments, which are assigned consecutive multilink sequence numbers.

If you do not include the **fragment-threshold** statement in the fragmentation map, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest MTU of all the links in the bundle.

Even if you do not set a maximum fragment size anywhere in the configuration, you can configure the maximum received reconstructed unit (MRRU) by including the **mrru** statement at the **[edit interfaces lsq-*fpc*/*pic*/*port* unit *logical-unit-number*]** hierarchy level. The MRRU is similar to the MTU but is specific to link services interfaces. By default, the MRRU size is 1500 bytes, and you can configure it to be from 1500 through 4500 bytes. For more information, see *Configuring MRRU on Multilink and Link Services Logical Interfaces*.

When a packet is removed from a multilink-encapsulated queue, the software gives the packet an FRF.12 header. The FRF.12 header contains a sequence number field, which is filled with the next available sequence number from a counter. The software then places the packet on the fractional T1 link. Traffic from another queue might be interleaved between two fragments of the packet.

When a packet is removed from a nonencapsulated queue, it is transmitted with a plain Frame Relay header. The packet is then placed on the fractional T1 link as soon as possible. If necessary, the packet is placed between the fragments of a packet from another queue.

The fractional T1 interface links to another router, which can be from Juniper Networks or another vendor. The router at the far end gathers packets from the fractional T1 link. If a packet has an FRF.12 header, the software assumes the packet is a fragment of a larger packet, and the fragment number field is used to reassemble the larger packet. If the packet has a plain Frame Relay header, the software accepts the packet in the order in which it arrives, and the software makes no attempt to reassemble or reorder the packet.

A whole packet from a nonencapsulated queue can be placed between fragments of a multilink-encapsulated queue. However, fragments from one multilink-encapsulated queue cannot be interleaved with fragments from another multilink-encapsulated queue. This is the intent of the specification FRF.12, *Frame Relay Fragmentation Implementation Agreement*. If fragments from two different queues were interleaved, the header fields might not have enough information to separate the fragments.

Examples: Configuring an LSQ Interface for a Fractional T1 Interface Using FRF.12

FRF.12 with Fragmentation and Without LFI

This example shows a 128 KB DS0 interface. There is one traffic stream on **ge-0/0/0**, which is classified into queue 0 (**be**). Packets are fragmented in the link services IQ (**lsq-**) interface according to the threshold configured in the fragmentation map.

```
[edit chassis]
fpc 0 {
    pic 3 {
        adaptive-services {
            service-package layer-2;
        }
    }
}
[edit interfaces]
ge-0/0/0 {
    unit 0 {
        family inet {
            address 20.1.1.1/24 {
                arp 20.1.1.2 mac 00.00.5e.00.53.56;
            }
        }
    }
}
ce1-0/2/0 {
    partition 1 timeslots 1-2 interface-type ds;
}
ds-0/2/0:1 {
    no-keepalives;
    dce;
    encapsulation frame-relay;
    unit 0 {
        dlci 100;
        family mlfr-end-to-end {
            bundle lsq-0/3/0.0;
        }
    }
}
lsq-0/3/0 {
    per-unit-scheduler;
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
        family inet {
            address 10.200.0.78/30;
        }
    }
}
fxp0 {
    unit 0 {
        family inet {
```

```
            address 172.16.1.162/24;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.1/32;
        }
    }
}
[edit class-of-service]
forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
interfaces {
    lsq-0/3/0 {
        unit 0 {
            fragmentation-map map1;
        }
    }
}
fragmentation-maps {
    map1 {
        forwarding-class {
            be {
                fragment-threshold 160;
            }
        }
    }
}
```

FRF.12 with Fragmentation and LFI

This example shows a 512 KB DS0 bundle and four traffic streams on **ge-0/0/0** that are classified into four queues. The fragment size is 160 for queue 0, queue 1, and queue 2. The voice stream on queue 3 has LFI configured.

```
[edit chassis]
fpc 0 {
    pic 3 {
        adaptive-services {
            service-package layer-2;
        }
    }
}
[edit interfaces]
ge-0/0/0 {
    unit 0 {
        family inet {
            address 20.1.1.1/24 {
                arp 20.1.1.2 mac 00.00.5e.00.53.56;
            }
        }
    }
    ce1-0/2/0 {
        partition 1 timeslots 1-8 interface-type ds;
    }
    ds-0/2/0:1 {
        no-keepalives;
        dce;
        encapsulation frame-relay;
        unit 0 {
            dlci 100;
            family mlfr-end-to-end {
                bundle lsq-0/3/0.0;
            }
        }
    }
    lsq-0/3/0 {
        per-unit-scheduler;
        unit 0 {
            encapsulation multilink-frame-relay-end-to-end;
            family inet {
                address 10.200.0.78/30;
            }
        }
    }
    [edit class-of-service]
    classifiers {
        inet-precedence ge-interface-classifier {
            forwarding-class be {
```

```
            loss-priority low code-points 000;
        }
        forwarding-class ef {
            loss-priority low code-points 010;
        }
        forwarding-class af {
            loss-priority low code-points 100;
        }
        forwarding-class nc {
            loss-priority low code-points 110;
        }
    }
}
forwarding-classes {
    queue 0 be;
    queue 1 ef;
    queue 2 af;
    queue 3 nc;
}
interfaces {
    lsq-0/3/0 {
        unit 0 {
            scheduler-map sched2;
            fragmentation-map map2;
        }
    }
    ds-0/2/0:1 {
        scheduler-map link-map2;
    }
    ge-0/0/0 {
        unit 0 {
            classifiers {
                inet-precedence ge-interface-classifier;
            }
        }
    }
}
scheduler-maps {
    sched2 {
        forwarding-class be scheduler economy;
        forwarding-class ef scheduler business;
        forwarding-class af scheduler stream;
        forwarding-class nc scheduler voice;
    }
```

```
    link-map2 {
        forwarding-class be scheduler link-economy;
        forwarding-class ef scheduler link-business;
        forwarding-class af scheduler link-stream;
        forwarding-class nc scheduler link-voice;
    }
}
fragmentation-maps {
    map2 {
        forwarding-class {
            be {
                fragment-threshold 160;
            }
            ef {
                fragment-threshold 160;
            }
            af {
                fragment-threshold 160;
            }
            nc {
                no-fragmentation;
            }
        }
    }
    schedulers {
        economy {
            transmit-rate percent 26;
            buffer-size percent 26;
        }
        business {
            transmit-rate percent 26;
            buffer-size percent 26;
        }
        stream {
            transmit-rate percent 35;
            buffer-size percent 35;
        }
        voice {
            transmit-rate percent 13;
            buffer-size percent 13;
        }
        link-economy {
            transmit-rate percent 26;
            buffer-size percent 26;
```

```
        }
        link-business {
            transmit-rate percent 26;
            buffer-size percent 26;
        }
        link-stream {
            transmit-rate percent 35;
            buffer-size percent 35;
        }
        link-voice {
            transmit-rate percent 13;
            buffer-size percent 13;
        }
      }
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | 905
- Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI | 946
- Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP

This example bundles a single T3 interface on a link services IQ interface with MLPPP encapsulation. Binding a single T3 interface to a multilink bundle allows you to configure compressed RTP (CRTP) on the T3 interface.

This scenario applies to MLPPP bundles only. The Junos OS does not currently support CRTP over Frame Relay. For more information, see “Configuring Services Interfaces for Voice Services” on page 1026.

There is no need to configure LFI at DS3 speeds, because the packet serialization delay is negligible.

```
[edit interfaces]
t3-0/0/0 {
    unit 0 {
        family mlppp {
```

```
            bundle lsq-1/3/0.1;
        }
    }
}
lsq-1/3/0.1 {
    encapsulation multilink-ppp;
}
compression {
    rtp {
        # cRTP parameters go here
        #
        port minimum 2000 maximum 64009;
    }
}
```

This configuration uses a default fragmentation map, which results in all forwarding classes (queues) being sent out with a multilink header.

To eliminate multilink headers, you can configure a fragmentation map in which all queues have the **no-fragmentation** statement at the **[edit class-of-service fragmentation-maps *map-name* forwarding-class *class-name*]** hierarchy level, and attach the fragmentation map to the **lsq-1/3/0.1** interface, as shown here:

```
[edit class-of-service]
fragmentation-maps {
    fragmap {
        forwarding-class {
            be {
                no-fragmentation;
            }
            af {
                no-fragmentation;
            }
            ef {
                no-fragmentation;
            }
            nc {
                no-fragmentation;
            }
        }
    }
}
interfaces {
    lsq-1/3/0.1 {
        fragmentation-map fragmap;
```

```
    }
}
```

RELATED DOCUMENTATION

- Layer 2 Service Package Capabilities and Interfaces | 905
- Configuring LSQ Interfaces as NxT1 or NxE1 Bundles Using MLPPP | 932
- Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using MLPPP and LFI | 946
- Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP | 965
- Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces as T3 or OC3 Bundles Using FRF.12

This example configures a clear-channel T3 or OC3 interface with multiple logical interfaces (DLCIs) on the link. In this scenario, each DLCI represents a customer. DLCIs are shaped at the egress PIC to a particular speed (*N*xDS0). This allows you to configure LFI using FRF.12 End-to-End Protocol on Frame Relay DLCIs.

To do this, first configure logical interfaces (DLCIs) on the physical interface. Then bundle the DLCIs, so that there is only one DLCI per bundle.

The physical interface must be capable of per-DLCI scheduling, which allows you to attach shaping rates to each DLCI. For more information, see the *Junos OS Network Interfaces Library for Routing Devices*.

To prevent fragment drops at the egress PIC, you must assign a shaping rate to the link services IQ logical interfaces and to the egress DLCIs. Shaping rates on DLCIs specify how much bandwidth is available for each DLCI. The shaping rate on link services IQ interfaces should match the shaping rate assigned to the DLCI that is associated with the bundle.

Egress interfaces also must have a scheduler map attached. The queue that carries voice should be strict-high-priority, while all other queues should be low-priority. This makes LFI possible.

This example shows voice traffic in the **ef** queue. The voice traffic is interleaved with bulk data. Alternatively, you can use multiclass MLPPP to carry multiple classes of traffic in different multilink classes, as described in "Configuring Multiclass MLPPP on LSQ Interfaces" on page 927.

```
[edit interfaces]
t3-0/0/0 {
    per-unit-scheduler;
    encapsulation frame-relay;
```

```
    unit 0 {
        dlci 69;
        family mlfr-end-to-end {
            bundle lsq-1/3/0.0;
        }
    }
    unit 1 {
        dlci 42;
        family mlfr-end-to-end {
            bundle lsq-1/3/0.1;
        }
    }
}
lsq-1/3/0 {
    unit 0 {
        encapsulation multilink-frame-relay-end-to-end;
    }
    fragment-threshold 320; # Multilink packets must be fragmented
}
unit 1 {
    encapsulation multilink-frame-relay-end-to-end;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched { # Scheduling parameters that apply to bundles on AS or Multiservices PICs.
    ...
}
pic-sched {
    # Scheduling parameters for egress DLCIs.
    # The voice queue should be strict-high priority.
    # All other queues should be low priority.
    ...
}
fragmentation-maps {
    fragmap {
        forwarding-class {
            ef {
                no-fragmentation;
            }
            # Voice is carried in the ef queue.
            # It is interleaved with bulk data.
        }
    }
```

```
}
interfaces {
    t3-0/0/0 {
        unit 0 {
            shaping-rate 512k;
            scheduler-map pic-sched;
        }
        unit 1 {
            shaping-rate 128k;
            scheduler-map pic-sched;
        }
    }
    lsq-1/3/0 { # Assign fragmentation and scheduling to LSQ interfaces.
    unit 0 {
        shaping-rate 512k;
        scheduler-map sched;
        fragmentation-map fragmap;
    }
    unit 1 {
        shaping-rate 128k;
        scheduler-map sched;
        fragmentation-map fragmap;
    }
}
```

For more information about how FRF.12 works with links services IQ interfaces, see "Configuring LSQ Interfaces for Single Fractional T1 or E1 Interfaces Using FRF.12" on page 952.

RELATED DOCUMENTATION

Layer 2 Service Package Capabilities and Interfaces | 905

Link Services Configuration for Junos Interfaces | 833

Configuring LSQ Interfaces for T3 Links Configured for Compressed RTP over MLPPP | 961

Configuring LSQ Interfaces for ATM2 IQ Interfaces Using MLPPP

This example configures an ATM2 IQ interface with MLPPP bundled with link services IQ interfaces. This allows you to configure LFI on ATM virtual circuits.

For this type of configuration, the ATM2 IQ interface must have LLC encapsulation.

The following ATM PICs are supported in this scenario:

- 2-port OC-3/STM1 ATM2 IQ
- 4-port DS3 ATM2 IQ

Virtual circuit multiplexed PPP over AAL5 is not supported. Frame Relay is not supported. Bundling of multiple ATM VCs into a single logical interface is not supported.

Unlike DS3 and OC3 interfaces, there is no need to create a separate scheduler map for the ATM PIC. For ATM, you define CoS components at the **[edit interfaces at-*fpc*/*pic*/*port* atm-options]** hierarchy level, as described in the *Junos OS Network Interfaces Library for Routing Devices*.

> **NOTE:** Do not configure RED profiles on ATM logical interfaces that are bundled. Drops do not occur at the ATM interface.

In this example, two ATM VCs are configured and bundled into two link services IQ bundles. A fragmentation map is used to interleave voice traffic with other multilink traffic. Because MLPPP is used, each link services IQ bundle can be configured for CRTP.

```
[edit interfaces]
at-1/2/0 {
    atm-options {
        vpi 0;
        pic-type atm2;
    }
    unit 0 {
        vci 0.69;
        encapsulation atm-mlppp-llc;
        family mlppp {
            bundle lsq-1/3/0.10;
        }
    }
    unit 1 {
        vci 0.42;
        encapsulation atm-mlppp-llc;
        family mlppp {
            bundle lsq-1/3/0.11;
        }
    }
}
lsq-1/3/0 {
    unit 10 {
        encapsulation multilink-ppp;
```

```
    }
    # Large packets must be fragmented.
    # You can specify fragmentation for each forwarding class.
    fragment-threshold 320;
    compression {
      rtp {
        port minimum 2000 maximum 64009;
      }
    }
}
unit 11 {
    encapsulation multilink-ppp;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched { # Scheduling parameters that apply to LSQ bundles on AS or Multiservices PICs.
    ...
}
fragmentation-maps {
    fragmap {
      forwarding-class {
        ef {
          no-fragmentation;
        }
      }
    }
}
interfaces { # Assign fragmentation and scheduling parameters to LSQ interfaces.
lsq-1/3/0 {
    unit 0 {
      shaping-rate 512k;
      scheduler-map sched;
      fragmentation-map fragmap;
    }
    unit 1 {
      shaping-rate 128k;
      scheduler-map sched;
      fragmentation-map fragmap;
    }
}
```

RELATED DOCUMENTATION

10

PART

Distributing Traffic Among Next-Hop Servers with Traffic Load Balancer

CHAPTER 46

Configuring Traffic Load Balancer

IN THIS CHAPTER

Traffic Load Balancer Overview

IN THIS SECTION

Traffic Load Balancing Support Summary

Table 28 on page 970 provides a summary of the traffic load balancing support on the MS-MPC and MS-MIC cards for Adaptive Services versus support on the MX-SPC3 security services card for Next Gen Services.

Table 28: Traffic Load Balancing Support Summary

	MS-MPC		MX-SPC3
Junos Release	< 16.1R6 & 18.2.R1	≥ 16.1R6 & 18.2R1	19.3R2
Max # of Instances per Chassis	32	2,000 / 32 in L2 DSR mode	2,000

Table 28: Traffic Load Balancing Support Summary *(continued)*

	MS-MPC		MX-SPC3
Max # of Virtual Services per Instance	32	32	32
Max # of virtual IP address per virtual service		1	1
Max # of Groups per Instances	32	32	32
Max # of Real-Services (Servers) per Group	255	255	255
Max # of groups per virtual service		1	1
Max # of Network Monitor Profiles per Group		2	2
Max # of HC's per security services per PIC/NPU in 5-sec's		4,000	1,250 – 19.3R2 10,000 – 20.1R1
Supported Health Check Protocols	ICMP, TCP, UDP, HTTP, SSL, Custom		ICMP, TCP, UDP, HTTP, SSL, Custom

Traffic Load Balancer Application Description

Traffic Load Balancer (TLB) is supported on MX Series routers with either of the Multiservices Modular Port Concentrator (MS-MPC), Multiservices Modular Interface Card (MS-MIC), or the MX Security Services Processing Card (MX-SPC3) and in conjunction with the Modular Port Concentrator (MPC) line cards supported on the MX Series routers as described in Table 29 on page 971.

NOTE: You cannot run Deterministic NAT and TLB simultaneously.

Table 29: TLB MX Series Router Platform Support Summary

TLB Mode	MX Platform Coverage
Multiservices Modular Port Concentrator (MS-MPC)	MX240, MX2480, MX960, MX2008, MX2010, MX2020

Table 29: TLB MX Series Router Platform Support Summary *(continued)*

TLB Mode	MX Platform Coverage
Multiservices Modular Interface Card (MS-MIC)	MX5, MX10, MX40, MX80, MX104, MX240, MX2480, MX960, MX2008, MX2010, MX2020
MX Security Services Processing Card (MX-SPC3)	MX240, MX480, MX960

- TLB enables you to distribute traffic among multiple servers.
- TLB employs an MS-MPC-based control plane and a data plane using the MX Series router forwarding engine.
- TLB uses an enhanced version of equal-cost multipath (ECMP). Enhanced ECMP facilitates the distribution of flows across groups of servers. Enhancements to native ECMP ensure that when servers fail, only flows associated with those servers are impacted, minimizing the overall network churn on services and sessions.
- TLB provides application-based health monitoring for up to 255 servers per group, providing Intelligent traffic steering based on health checking of server availability information. You can configure an aggregated multiservices (AMS) interface to provide one-to-one redundancy for MS-MPCs or Next Gen Services MX-SPC3 card used for server health monitoring.
- TLB applies its flow distribution processing to ingress traffic.
- TLB supports multiple virtual routing instances to provide improved support for large scale load balancing requirements.
- TLB supports static virtual-IP-address-to-real-IP-address translation, and static destination port translation during load balancing.

Traffic Load Balancer Modes of Operation

IN THIS SECTION

Traffic Load Balancer provides three modes of operation for the distribution of outgoing traffic and for handling the processing of return traffic.

Table 30 on page 973 summarizes the TLB support and which cards it's supported on.

Table 30: TLB Versus Security Service Cards Summary

Security Service Card	MS-MPC/MS-MIC	MX-SPC3
Translate	Yes	Yes
Transparent Layer 3 Direct Server Return	Yes	Yes
Transparent Layer 2 Direct Server Return	Yes	Not Supported

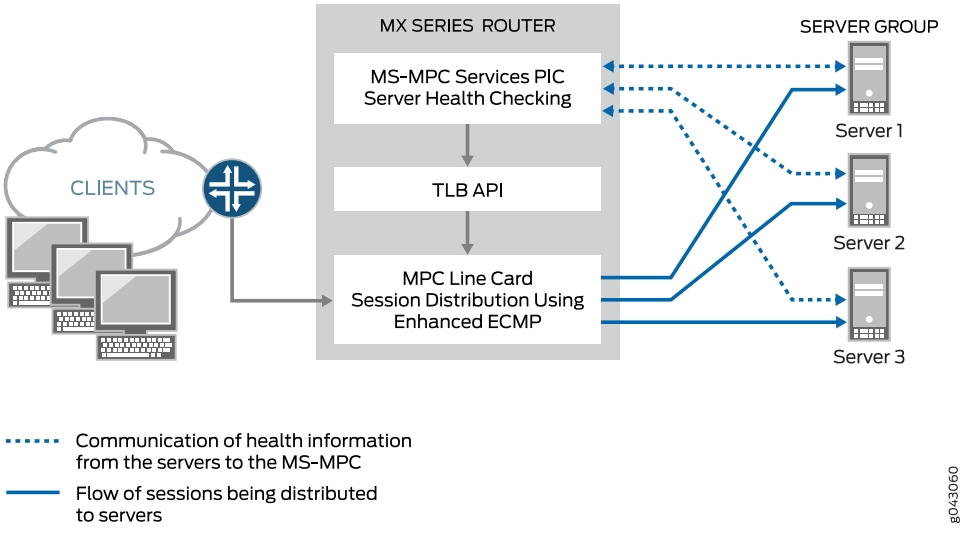
Transparent Mode Layer 2 Direct Server Return

When you use transparent mode Layer 2 direct server return (DSR):

- The PFE processes data.
- Load balancing works by changing the Layer 2 MAC of packets.
- An MS-MPC performs the network-monitoring probes.
- Real servers must be directly (Layer 2) reachable from the MX Series router.
- TLB installs a route and all the traffic over that route is load-balanced.
- TLB never modifies Layer 3 and higher level headers.

Figure 43 on page 973 shows the TLB topology for transparent mode Layer 2 DSR.

Figure 43: TLB Topology for Transparent Mode



Translated Mode

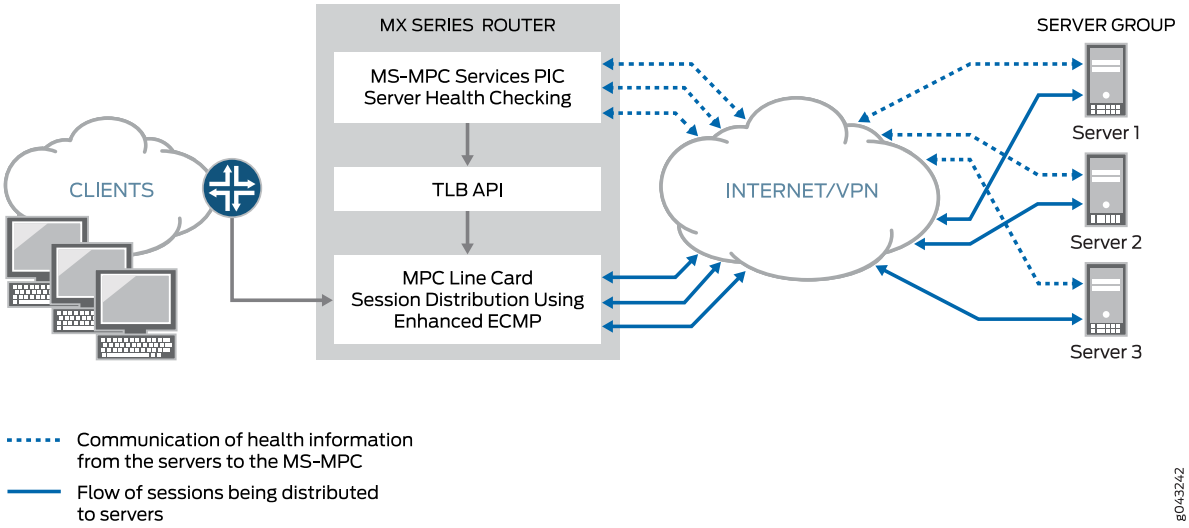
Translated mode provides greater flexibility than transparent mode Layer 2 DSR. When you choose translated mode:

- An MS-MPC performs the network-monitoring probes.
- The PFE performs stateless load balancing:
  - Data traffic directed to a virtual IP address undergoes translation of the virtual IP address to a real server IP address and translates the virtual port to a server listening port. Return traffic undergoes the reverse translation.
  - Client to virtual IP traffic is translated; the traffic is routed to reach its destination.
  - Server-to-client traffic is captured using implicit filters and directed to an appropriate load-balancing next hop for reverse processing. After translation, traffic is routed back to the client.
  - Two load balancing methods are available: random and hash. The random method is only for UDP traffic and provides quavms-random distribution. While not literally random, this mode provides fair distribution of traffic to an available set of servers. The hash method provides a hash key based on any combination of the source IP address, destination IP address, and protocol.

> **NOTE:** Translated mode processing is only available for IPv4-to-IPv4 and IPv6-to-IPv6 traffic.

Figure 44 on page 974 shows the TLB topology for translated mode.

Figure 44: TLB Topology for Translated Mode



Transparent Mode Layer 3 Direct Server Return

Transparent mode Layer 3 DSR load balancing distributes sessions to servers that can be a Layer 3 hop away. Traffic is returned directly to the client from the real-server.

Traffic Load Balancer Functions

TLB provides the following functions:

- TLB always distributes the *requests* for any flow. When you specify DSR mode, the response returns directly to the source. When you specify translated mode, reverse traffic is steered through implicit filters on server-facing interfaces.
- TLB supports hash-based load balancing or random load balancing.
- TLB enables you to configure servers offline to prevent a performance impact that might be caused by a rehashing for all existing flows. You can add a server in the administrative down state and use it later for traffic distribution by disabling the administrative down state. Configuring servers offline helps prevent traffic impact to other servers.
- When health checking determines a server to be down, only the affected flows are rehashed.
- When a previously down server is returned to service, all flows belonging to that server based on hashing return to it, impacting performance for the returned flows. For this reason, you can disable the automatic rejoining of a server to an active group. You can return servers to service by issuing the **request services traffic-load-balance real-service rejoin** operational command.

  > **NOTE:** NAT is not applied to the distributed flows.

- Health check monitoring application runs on an MS-MPC/NPU. This network processor unit (NPU) is not used for handling data traffic.
- TLB supports static virtual-IP-adddress-to-real-IP-address translation, and static destination port translation during load balancing.
- TLB provides multiple VRF support.

RELATED DOCUMENTATION

Interchassis High-Availability

Understanding AMS Interfaces

Traffic Load Balancer Application Components

Servers and Server Groups

TLB enables configuration of groups of up to 255 servers (referred to in configuration statements as *real services*) for use as alternate destinations for stateless session distribution. All servers used in server groups must be individually configured before assignment to groups. Load balancing uses hashing or randomization for session distribution. Users can add and delete servers to and from the TLB server distribution table and can also change the administrative status of a server.

> **NOTE:** TLB uses the session distribution next-hop API to update the server distribution table and retrieve statistics. *Applications do not have direct control on the server distribution table management. They can only influence changes indirectly through the add and delete services of the TLB API.*

Server Health Monitoring — Single Health Check and Dual Health Check

TLB supports TCP, HTTP, SSL Hello, and custom health check probes to monitor the health of servers in a group. You can use a single probe type for a server group, or a dual health check configuration that includes two probe types. The configurable health monitoring function resides on either an MX-SPC3 or an MS-MPC. By default, probe requests are sent every 5 seconds. Also by default, a real server is declared down only after five consecutive probe failures and declared up only after five consecutive probe successes.

Use a custom health check probe to specify the following:

- Expected string in the probe response
- String that is sent with the probe
- Server status to assign when the probe times out (up or down)
- Server status to assign when the expected response to the probe is received (up or down)
- Protocol — UDP or TCP

TLB provides *application stickiness*, meaning that server failures or changes do not affect traffic flows to other active servers. Changing a server's administrative state from up to down does not impact any active flows to remaining servers in the server distribution table. Adding a server or deleting a server from a group has some traffic impact for a length of time that depends on your configuration of the interval and retry parameters in the monitoring profile.

TLB provides two levels of server health monitoring:

- Single Health Check—One probe type is attached to a server group by means of the **network-monitoring-profile** configuration statement.

- TLB Dual Health Check (TLB-DHC)—Two probe types are associated with a server group by means of the **network-monitoring-profile** configuration statement. A server's status is declared based on the result of two health check probes. Users can configure up to two health check profiles per server group. If a server group is configured for dual health check, a real-service is declared to be UP only when both health-check probes are simultaneously UP; otherwise, a real-service is declared to be DOWN.

> **NOTE:**
> The following restrictions apply to AMS interfaces used for server health monitoring:
>
> - An AMS interface configured under a TLB instance uses its configured member interfaces exclusively for health checking of configured multiple real servers.
> - The member interfaces use unit 0 for single VRF cases, but can use units other than 1 for multiple VRF cases.
> - TLB uses the IP address that is configured for AMS member interfaces as the source IP address for health checks.
> - The member interfaces must be in the same routing instance as the interface used to reach real servers. This is mandatory for TLB server health-check procedures.

Virtual Services

The virtual service provides a virtual IP address (VIP) that is associated with the group of servers to which traffic is directed as determined by hash-based or random session distribution and server health monitoring. In the case of Layer2 DSR and Layer3 DSR, the special address 0.0.0.0 causes all traffic flowing to the forwarding instance to be load balanced.

The virtual service configuration includes:

- Mode—indicating how traffic is handled (translated or transparent).
- The group of servers to which sessions are distributed.
- The load balancing method.
- Routing instance and route metric.

> **BEST PRACTICE:** Although you can assign a virtual address of 0.0.0.0 in order to use default routing, we recommend using a virtual address that can be assigned to a routing instance set up specifically for TLB.

Traffic Load Balancer Configuration Limits

Traffic Load Balancer configuration limits are described in Table 31 on page 978.

Table 31: TLB Configuration Limits

Configuration Component	Configuration Limit
Maximum number of instances.	Starting in Junos OS Release 16.1R6 and Junos OS Release 18.2R1, the TLB application supports 2000 TLB instances for virtual services that use the direct-server-return or the translated mode. In earlier releases, the maximum number of instances is 32. If multiple virtual services are using the same server group, then all of those virtual services must use the same load balancing method to support 2000 TLB instances. For virtual services that use the layer2-direct-server-return mode, TLB supports only 32 TLB instances. To perform the same function as the layer2-direct-server-return mode and have support for 2000 TLB instances, you can use the direct-server-return mode and use a service filter with the skip action.
Maximum number of servers per group	255
Maximum number of virtual services per services PIC	32
Maximum number of health checks per services PIC in a 5-second interval	For MS-MPC services cards: 2000 For Next Gen Services mode and the MX-SPC3 services cards: 1250
Maximum number of groups per virtual service	1
Maximum number of virtual IP addresses per virtual service	1
Supported health checking protocols	ICMP, TCP, HTTP, SSL, Custom **NOTE:** ICMP health checking is supported only on MS-MPC services cards.

Release History Table

Release	Description
16.1R6	Starting in Junos OS Release 16.1R6 and Junos OS Release 18.2R1, the TLB application supports 2000 TLB instances for virtual services that use the direct-server-return or the translated mode.

RELATED DOCUMENTATION

Configuring TLB | 979

Configuring TLB

IN THIS SECTION

The following topics describe how to configure TLB. To create a complete application, you must also define interfaces and routing information. You can optionally define firewall filters and policy options in order to differentiate TLB traffic.

Loading the TLB Service Package

Load the TLB service package on each service PIC on which you want to run TLB.

> **NOTE:** For Next Gen Services and the MX-SPC3 services card, you do not need to load this package.

To load the TLB service package on a service PIC:

- Load the **jservices-traffic-dird** package.

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

For example:

```
[edit chassis fpc 3 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-traffic-dird
```

Configuring a TLB Instance Name

To configure a name for the TLB instance:

- At the **[edit services traffic-load-balance]** hierarchy level, identify the TLB instance name.

```
[edit services traffic-load-balance]
user@host# set instance instance-name
```

For example:

```
[edit services traffic-load-balance]
user@host# set instance tlb-instance1
```

Configuring Interface and Routing Information

To configure interface and routing information:

1. At the **[edit services traffic-load-balance instance *instance-name*]** hierarchy level, identify the service interface associated with this instance.

```
user@host# [edit services traffic-load-balance instance instance-name]
user@host# set interface interface-name
```

For example, on an MS-MPC:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set interface ms-1/0/0
```

For example, for Next Gen Services on an MX-SPC3:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set interface vms-1/0/0
```

2. Enable the routing of health-check packet responses from real servers to the service interface that you identified in Step 1.

```
[edit interfaces]
user@host# set interface-name unit 0 ip-address-owner service-plane
```

For example, on an MS-MPC:

```
[edit interfaces]
user@host# set ms-1/0/0 unit 0 ip-address-owner service-plane
```

For example, on an MX-SPC3:

```
[edit interfaces]
user@host# set vms-1/0/0 unit 0 ip-address-owner service-plane
```

3. Specify the client interface for which an implicit filter is defined to direct traffic in the forward direction. This is required only for translated mode.

```
user@host# [edit services traffic-load-balance instance instance-name]
user@host# set client-interface interface-name
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set client-interface ge-5/2/0.0
```

4. Specify the virtual routing instance used to route data traffic in the forward direction to servers. This is required for SLT and Layer 3 DSR; it is optional for Layer 2 DSR.

```
user@host# [edit services traffic-load-balance instance instance-name]
```

```
user@host# set server-vrf server-vrf
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set server-vrf server-vrf
```

5. Specify the server interface for which implicit filters are defined to direct return traffic to the client.

   NOTE: Implicit filters for return traffic are not used for DSR.

```
user@host# [edit services traffic-load-balance instance instance-name]
user@host# set server-interface server-interface
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set server-interface ge-5/2/1.0
```

6. (Optional) Specify the filter used to bypass health checking for return traffic.

```
user@host# [edit services traffic-load-balance instance instance-name]
user@host# set server-inet-bypass-filter server-inet-bypass-filter
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set server-inet-bypass-filter tlb-ipv4-bypass
```

7. Specify the virtual routing instance in which you want the data in the reverse direction to be routed to the clients.

```
user@host# [edit services traffic-load-balance instance instance-name]
user@host# set client-vrf client-vrf
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1]
user@host# set client-vrf client-vrf
```

NOTE: Virtual routing instances for routing data in the reverse direction are not used with DSR.

Configuring Servers

To configure servers for the TLB instance:

- Configure a logical name and IP address for each server to be made available for next-hop distribution.

  ```
  [edit services traffic-load-balance instance instance-name]
  user@host# set real-service real-service-name address server-ip-address
  ```

  For example:

  ```
  [edit services traffic-load-balance instance tlb-instance1]
  user@host# set real-service rs138 address 172.26.99.138
  user@host# set real-service rs139 address 172.26.99.139
  user@host# set real-service rs140 address 172.26.99.140
  ```

Configuring Network Monitoring Profiles

A network monitoring profile configures a health check probe, which you assign to a server group to which session traffic is distributed.

To configure a network monitoring profile:

1. Configure the type of probe to use for health monitoring — **icmp**, **tcp**, **http**, **ssl-hello**, or **custom**.

   > **NOTE:** **icmp** probes are supported only on MS-MPC cards.
   >
   > Next Gen Services and the MX-SPC3 do not support ICMP probes in this release.

   - For an ICMP probe:

     ```
     [edit services network-monitoring profile profile-name]
     user@host.com# set icmp
     ```

   - For a TCP probe:

     ```
     [edit services network-monitoring profile profile-name]
     user@host.com# set tcp port tcp-port-number
     ```

   - For an HTTP probe:

     ```
     [edit services network-monitoring profile profile-name]
     user@host.com# set http host hostname url url port http-port-number method (get | option)
     ```

   - For an SSL probe:

     ```
     [edit services network-monitoring profile profile-name]
     user@host.com# set ssl-hello port port ssl-version
     ```

   - For a custom probe:

     ```
     [edit services network-monitoring profile profile-name]
     user@host.com# set custom cmd priority default-real-service-status (down | up) expect (ascii | binary)
       receive-string port port real-service-action (down | up) send (ascii | binary) send-string
     ```

2. Configure the interval for probe attempts, in seconds (1 through 180).

   ```
   [edit services network-monitoring profile profile-name]
   ```

```
user@host.com# set probe-interval interval
```

For example:

```
[edit services network-monitoring profile profile1-icmp]
user@host.com# set probe-interval 2
```

3. Configure the number of failure retries, after which the real server is tagged as down.

```
[edit services network-monitoring profile profile-name]
user@host.com# set failure-retries number-of-retries
```

For example:

```
[edit services network-monitoring profile profile1-icmp]
user@host.com# set failure-retries 3
```

4. Configure the number of recovery retries, which is the number of successful probe attempts after which the server is declared up.

```
[edit services network-monitoring profile profile-name]
user@host.com# set recovery-retries number-of-retries
```

For example:

```
[edit services network-monitoring profile profile1-icmp]
user@host.com# set recovery-retries 1
```

Configuring Server Groups

Server groups consist of servers to which traffic is distributed by means of stateless, hash-based session distribution and server health monitoring.

To configure a server group:

1. Specify the names of one or more configured real servers.

```
[edit services traffic-load-balance instance instance-name groups group-name]
user@host.com# set real-services real-service-name, ...
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 groups tlb-group1]
user@host.com# set real-services [ rs138 rs139 rs140 ]
```

2. Configure the routing instance for the group when you do not want to use the default instance, **inet.0**.

```
[edit services traffic-load-balance instance instance-name groups group-name]
user@host.com# set routing-instance routing-instance-name
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 groups tlb-group1]
user@host.com# set routing-instance tlb-routing-instance1
```

3. (Optional) Disable the default option that allows a server to rejoin the group automatically when it comes up.

```
[edit services traffic-load-balance instance instance-name group group-name]
user@host.com# set real-service-rejoin-options no-auto-rejoin
```

4. (Optional) Configure the logical unit of the instance's service interface to use for health checking.
   a. Specify the logical unit.

```
[edit services traffic-load-balance instance instance-name group group-name]
user@host.com# set health-check-interface-subunit health-check-interface-subunit
```

   b. Enable the routing of health-check packet responses from real servers to the interface.

```
[edit interfaces]
user@host.com# set interface-name unit subunit ip-address-owner service-plane
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 group tlb-group1]
user@host.com# set health-check-interface-subunit 30
[edit interfaces]
user@host.com# set ms-1/0/0 unit 30 ip-address-owner service-plane
```

5. Configure one or two network monitoring profiles to be used to monitor the health of servers in this group.

```
[edit services traffic-load-balance instance instance-name groups group-name]
user@host.com# set network-monitoring-profile profile-name1 profile-name2
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 groups tlb-group1]
user@host.com# set network-monitoring-profile profile1-icmp profile2-http
```

Configuring Virtual Services

A virtual service provides an address that is associated with a the group of servers to which traffic is directed as determined by hash-based or random session distribution and server health monitoring. You may optionally specify filters and routing instances to steer traffic for TLB.

To configure a virtual service:

1. At the **[edit services traffic-load-balance instance *instance-name*]** hierarchy level, specify a non-zero address for the virtual service.

```
[edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
user@host# set address virtual-ip–address
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set address 192.0.2.11
```

2. Specify the server group used for this virtual service.

```
[edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
user@host# set group group-name
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set group tlb-group1
```

3. (Optional) Specify a routing instance for the virtual service. If you do not specify a routing instance, the default routing instance is used.

   ```
   [edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
   user@host# set routing-instance routing-instance
   ```

   For example:

   ```
   [edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
   user@host# set routing-instance msp-tproxy-server-vrf31
   ```

4. Specify the processing mode for the virtual service.

   ```
   [edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
   user@host# set mode (layer2-direct-server-return | direct-server-return | translated)
   ```

   For example:

   ```
   [edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
   user@host# set mode translated
   ```

5. (Optional) For a translated mode virtual service, enable the addition of the IP addresses for all the real servers in the group under the virtual service to the server-side filters. Doing this allows you to configure two virtual services with the same listening port and protocol on the same interface and VRF.

   ```
   [edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
   user@host# set include-real-server-ips-in-server-filter
   ```

6. (Optional) Specify a routing metric for the virtual service.

   ```
   [edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
   user@host# set routing-metric routing-metric
   ```

   For example:

   ```
   [edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
   user@host# set routing-metric 128
   ```

7. Specify the method used for load balancing. You can specify a hash method that provides a hash key based on any combination of the source IP address, destination IP address, and protocol, or you can specify **random**.

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set load-balancing-method (hash hash-key (source-ip | destination-ip | proto) | random)
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set load-balancing-method hash hash-key source-ip
```

or

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set load-balancing-method random
```

> **NOTE:** If you switch between the hash method and the random method for a virtual service, the statistics for the virtual service are lost.

8. For a translated mode virtual service, specify a service for translation, including a virtual-port, server-listening-port, and protocol.

```
[edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
user@host# set service service-name virtual-port virtual-port server-listening-port server-listening-port protocol
    (udp | tcp)
```

For example:

```
[edit services traffic-load-balance instance tlb-instance1 virtual-service virtual-service1]
user@host# set service fast-track-service virtual-port 1111 server-listening-port 22 protocol tcp
```

9. Commit the configuration.

```
[edit services traffic-load-balance instance instance-name virtual-service virtual-service-name]
user@host# commit
```

NOTE: In the absence of a client-interface configuration under the TLB instance, the implicit client filter (for VIP) is attached to the client-vrf configured under the TLB instance. In this case, the routing-instance under a translate mode virtual service cannot be the same as the client-vrf configured under the TLB instance. if it is, the commit fails.

Configuring Tracing for the Health Check Monitoring Function

To configure tracing options for the health check monitoring function:

1. Specify that you want to configure tracing options for the health check monitoring function.

```
[edit services network-monitoring]
user@host# edit traceoptions
```

2. (Optional) Configure the name of the file used for the trace output.

```
[edit services network-monitoring traceoptions]
user@host# set file file-name
```

3. (Optional) Disable remote tracing capabilities.

```
[edit services network-monitoring traceoptions]
user@host# set no-remote-trace
```

4. (Optional) Configure flags to filter the operations to be logged.

```
[edit services network-monitoring traceoptions]
user@host# set flag flag
```

Table 32 on page 990 describes the flags that you can include.

Table 32: Trace Flags

Flag	Support on MS-MPC and MX-SPC3 Cards	Description
all	MS-MPC and MX-SPC3	Trace all operations.
all-real-services	MX-SPC3	Trace all real services.

Table 32: Trace Flags *(continued)*

Flag	Support on MS-MPC and MX-SPC3 Cards	Description
config	MS-MPC and MX-SPC3	Trace traffic load balancer configuration events.
connect	MS-MPC and MX-SPC3	Trace traffic load balancer ipc events.
database	MS-MPC and MX-SPC3	Trace database events.
file-descriptor-queue	MS-MPC	Trace file descriptor queue events.
inter-thread	MS-MPC	Trace inter-thread communication events.
filter	MS-MPC and MX-SPC3	Trace traffic load balancer filter programming events.
health	MS-MPC and MX-SPC3	Trace traffic load balancer health events.
messages	MS-MPC and MX-SPC3	Trace normal events.
normal	MS-MPC and MX-SPC3	Trace normal events.
operational-commands	MS-MPC and MX-SPC3	Trace traffic load balancer show events.
parse	MS-MPC and MX-SPC3	Trace traffic load balancer parse events.
probe	MS-MPC and MX-SPC3	Trace probe events.
probe-infra	MS-MPC and MX-SPC3	Trace probe infra events.
route	MS-MPC and MX-SPC3	Trace traffic load balancer route events.
snmp	MS-MPC and MX-SPC3	Trace traffic load balancer SNMP events.
statistics	MS-MPC and MX-SPC3	Trace traffic load balancer statistics events.
system	MS-MPC and MX-SPC3	Trace traffic load balancer system events.

5. (Optional) Configure the level of tracing.

```
[edit services network-monitoring traceoptions]
user@host# set level (all |error | info | notice | verbose | warning)
```

6. (Optional) Configure tracing for a particular real server within a particular server group.

```
[edit services network-monitoring traceoptions]
user@host# set monitor monitor-object-name group-name group-name real-services-name real-service-name
```

7. (Optional) Starting in Junos OS Release 16.1R6 and 18.2R1, configure tracing for a particular virtual service and instance.

```
[edit services traffic-load-balance traceoptions]
user@host# set monitor monitor-object-name instance-name instance-name virtual-svc-name
   virtual-service-name
```

Release History Table

Release	Description
16.1R6	Starting in Junos OS Release 16.1R6 and 18.2R1, configure tracing for a particular virtual service and instance.

RELATED DOCUMENTATION

Traffic Load Balancer Overview | 970

PART 11

Enabling Load Balancing and High Availability Using Multiservices Interfaces

CHAPTER 47

Enabling Load Balancing and High Availability Using Multiservices Interfaces

IN THIS CHAPTER

Understanding Aggregated Multiservices Interfaces

IN THIS SECTION

This topic contains the following sections:

Aggregated Multiservices Interface

In Junos OS, you can combine multiple services interfaces to create a bundle of services interfaces that can function as a single interface. Such a bundle of interfaces is known as an *aggregated multiservices*

interface (AMS), and is denoted as ams*N* in the configuration, where *N* is a unique number that identifies an AMS interface (for example, ams0).

AMS configuration provides higher scalability, improved performance, and better failover and load-balancing options.

AMS configuration enables service sets to support multiple services PICs by associating an AMS bundle with a service set. An AMS bundle can have up to 24 services PICs as member interfaces and can distribute services among the member interfaces.

Member interfaces are identified as mams in the configuration. The chassisd process in routers that support AMS configuration creates a mams entry for every multiservices interface on the router.

Starting with Junos OS Release 16.2, an AMS interface can have up to 36 member interfaces. If you include more than 24 member interfaces, you must increase the service PIC boot timeout to 240 or 300 seconds for all service PICs. In Junos OS Release 16.1 and earlier, an AMS interface could have a maximum of 24 member interfaces.

Starting with Junos OS Release 17.1R1, AMS supports IPSec tunnel distribution for next-hop style service-sets. However, interface-style IPSec service sets are not supported.

Starting with Junos OS Release 19.2R1, you can use up to 60 PICs across different AMS bundles on a MX2020 router. The hard limit of maximum 36 member interfaces per AMS bundle still exists. However, in the chassis, there can be multiple AMS bundles such that 15 MS-MPC slots can be configured across these bundles.

When you configure services options at the ams interface level, the options apply to all member interfaces (mams) for the ams interface.

The options also apply to service sets configured on services interfaces corresponding to the ams interface's member interfaces. All settings are per PIC. For example, session-limit applies per member and not at an aggregate level.

NOTE: You cannot configure services options at both the ams (aggregate) and member-interface level. If services options are configured on ms-x/y/z or vms-x/y/z, they also apply to service sets on mams-x/y/z.

When you want services options settings to apply uniformly to all members, configure services options at the ams interface level. If you need different settings for individual members, configure services options at the member interface level.

NOTE: Per-member drop of traffic and per-member next-hop configuration is required for NAT64. For NAPT44, this per-member specification allows arbitrary hash keys, providing better load-balancing options to allow dynamic NAT operations to be performed. For NAT64, NAPT44, and dynamic NAT44, it is not possible to determine which member allocates the dynamic NAT address. To ensure that reverse flow packets arrive at the same member as the forward flow packets, pool-address-based routes are used to steer reverse flow packets.

NOTE: Until Junos OS Release 13.3, for every media logical interface on which services were configured (interface style services), a logical interface alias was internally created. This interface alias stores the topology chains for features that are performed on the logical interface after an input service was processed to avoid packet loops in the system. With interface aliases, the maximum number of logical interfaces supported with services was reduced to half the supported maximum number because each logical interface consumed two entries, namely, one for the interface itself and the other for the interface alias.

Starting in Junos OS Release 14.1R4, input interface aliases are not created for MS-MPCs and MS-MICs. As a result, the maximum number of logical interfaces that are supported with services PICs is equal to the maximum number supported on the system. After input service processing by MS-MPCs and MS-MICs, the services PIC sends the packet to the Packet Forwarding Engine on the multiservices (**ms-**) logical interface where the corresponding service is configured. Post-services are not supported on MS- MPCs and MS-MICs in Junos OS Release 13.2 and later.

NOTE: You cannot include MS-DPCs or other MS-PICs in an AMS configuration that contains MS-MICs or MS-MPCs as member interfaces.

NOTE: If you modify a NAT pool that is being used by a service set assigned to an AMS interface, you must deactivate and activate the service set before the NAT pool changes take effect.

By default, the traffic distribution over the member interfaces of an AMS interface happens in a round-robin fashion. You can also configure the following hash key values to regulate the traffic distribution: **source-ip**, **destination-ip** , and **protocol**. For services that require traffic symmetry, you must configure symmetrical hashing. Symmetrical hashing configuration ensures that both forward and reverse traffic is routed through the same member interface.

With basic NAT44, load balancing on AMS interfaces of MS-MICs and MS-MPCs does not work properly if the ingress hash key is source IP address and the egress hash key is destination IP address.

If the service set is applied on the Gigabit Ethernet or 10-Gigabit Ethernet interface that functions as the NAT inside interface, then the hash keys used for load balancing might be configured in such a way that the ingress key is set as destination IP address and the egress key is set as source IP address. Because the source IP address undergoes NAT processing, it is not available for hashing the traffic in the reverse direction. Therefore, load balancing does not happen on the same IP address and forward and reverse traffic does not map to the same PIC. With the hash keys reversed, load balancing occurs correctly.

With next-hop services, for forward traffic, the ingress key on the inside interface load -balances traffic, and for reverse traffic, the ingress key on the outside interface load -balances traffic or per-member next hops steer reverse traffic. With interface-style services, the ingress key load-balances forward traffic and the egress key load-balances forward traffic or per-member next hops steer reverse traffic. Forward traffic is traffic entering from the inner side of a service set and reverse traffic is traffic entering from the outer side of a service set. The forward key is the hash key used for the forward direction of traffic and the reverse key is the hash key used for the reverse direction of traffic (depends on whether it relates to interface services or next-hop services style.)

With stateful firewalls, you can configure the following combinations of forward and reverse keys for load balancing. In the following combinations presented for hash keys, FOR-KEY refers to the forward key, REV-KEY denotes the reverse key, SIP signifies source IP address, DIP signifies destination IP address, and PROTO refers to protocol such as IP.

- FOR-KEY: SIP, REV-KEY: DIP
- FOR-KEY: SIP,PROTO REV-KEY: DIP, PROTO
- FOR-KEY: DIP, REV-KEY: SIP
- FOR-KEY: DIP,PROTO REV-KEY: SIP, PROTO
- FOR-KEY: SIP,DIP REV-KEY: SIP, DIP
- FOR-KEY: SIP,DIP,PROTO REV-KEY: SIP, DIP,PROTO

With static NAT configured as basic NAT44 or destination NAT44, and with stateful firewall configured or not, if the forward direction of traffic must undergo NAT processing, configure the hash keys as follows:

- FOR-KEY: DIP, REV-KEY: SIP
- FOR-KEY: DIP,PROTO REV-KEY: SIP, PROTO

If the reverse direction of traffic must undergo NAT processing, configure the hash keys as follows:

- FOR-KEY: SIP, REV-KEY: DIP
- FOR-KEY: SIP,PROTO REV-KEY: DIP, PROTO

With dynamic NAT configured, and with stateful firewall configured or not, only the forward direction traffic can undergo NAT. The forward hash key can be any combination of SIP, DIP, and protocol, and the reverse hash key is ignored.

NOTE: The Junos OS AMS configuration supports IPv4 and IPv6 traffic.

IPv6 Traffic on AMS Interfaces Overview

Starting in Junos OS release 14.2R1, you can use AMS interfaces for IPv6 traffic. To configure IPv6 support for an AMS interface, include the **family inet6** statement at the **[edit interfaces *ams-interface-name* unit 1]** hierarchy level. When **family inet** and **family inet6** are set for an AMS interface subunit, the **hash-keys** is configured at service-set level for interface style and at IFL level for next-hop style.

When a member interface of an AMS bundle fails, traffic destined to the failed member is redistributed among the remaining active members. The traffic (flows or sessions) traversing through the existing active members is unaffected. If M members are currently active, the expected result is that only about 1/M fraction of the traffic (flows/sessions) is impacted because that amount of traffic is shifted from the failed member to remain active members. When the failed member interface comes back online, only a fraction of the traffic is redistributed to the new member. If N members are currently active, the expected result is that only about 1/(N+1) fraction of the traffic (flows/sessions) is impacted because that amount of traffic moves to the new restored member. The 1/M and 1/(N+1) values assume that the flows are uniformly distributed among members, because a packet-hash is used to load-balance and because traffic usually contains a typical random combination of IP addresses (or any other fields that are used as load-balancing keys).

Similar to IPv4 traffic, for IPv6 packets, an AMS bundle must contain members of only one services PIC type. Separate AMS bundles on the same router can contain members of different services PIC types (for example, two MS-MICs in ams0, and two MS-MPC PICs in ams1).

The number of flows distributed, in an ideal environment, can be 1/N in a best-case scenario when the Nth member goes up or down. However, this assumption considers that the hash keys load-balance the real or dynamic traffic. For example, consider a real-world deployment where member A is serving only one flow, whereas member B is serving 10 flows. If member B goes down, then the number of flows disrupted is 10/11. The NAT pool-split behavior is designed to utilize the benefits of the rehash-minimization feature. The splitting of a NAT pool is performed for dynamic NAT scenarios (dynamic NAT, NAT64, and NAPT44).

If the original and redistributed flows are defined as follows:

- Member-original-flows—The traffic mapped to a member when all members are up.
- Member-redistributed-flows—The additional traffic mapped to a member when some other member fails. These traffic flows might need to be rebalanced when member interfaces come up and go down.

With the preceding definitions of the original and redistributed flows for member interfaces, the following observations apply:

- The member-original-flows of a member stay intact as long as that member is up. Such flows are not impacted when other members move between the up and down states.
- The member-redistributed-flows of a member can change when other members go up or down. This change of flows occurs because these additional flows need to be rebalanced among all active members. Therefore, the member-redistributed-flow can vary a lot based on other members going down or up. Although it might seem that when a member goes down, the flows on active-members are preserved, and that when a member goes up, flows on active-members are not preserved in an effective way, this behavior is only because of static or hash-based rebalancing of traffic among active members.

The rehash-minimization feature handles the operational changes in a member interface status only (such as member offline or member Junos OS reset). It does not handle changes in configuration. For example, addition or deletion, or activation and deactivation, of member interfaces at the **[edit interfaces ams*N* load-balancing-options member-interface mams-a/b/0]** hierarchy level requires the member PICs to be bounced. Twice NAT or hairpinning is not supported, similar to IPv4 support for AMS interfaces.

Member Failure Options and High Availability Settings

Because multiple service interfaces are configured as part of an AMS bundle, AMS configuration also provides for failover and high availability support. You can either configure one of the member interfaces as a backup interface that becomes active when any one of the other member interfaces goes down, or configure the AMS in such a way that when one of the member interfaces goes down, the traffic assigned to that interface is shared across the active interfaces.

The **member-failure-options** configuration statement enables you to configure how to handle traffic when a member interface fails. One option is to redistribute the traffic immediately among the other member interfaces. However, redistribution of traffic involves recalculating the hash tags, and might cause some disruption in traffic on all the member interfaces.

The other option is to configure the AMS to drop all traffic that is assigned to the failed member interface. With this you can optionally configure an interval, **rejoin-timeout**, for the AMS to wait for the failed interface to come back online after which the AMS can redistribute the traffic among other member interfaces. If the failed member interface comes back online before the configured wait time, traffic continues unaffected on all member interfaces, including the interface that has come back online and resumed the operations.

You can also control the rejoining of the failed interface when it comes back online. If you do not include the **enable-rejoin** statement in the **member-failure-options** configuration, the failed interface cannot rejoin the AMS when it comes back online. In such cases, you can manually rejoin that to the AMS by executing the **request interfaces revert *interface-name*** operational mode command.

The **rejoin-timeout** and **enable-rejoin** statements enable you to minimize traffic disruptions when member interfaces flap.

> **NOTE:** When **member-failure-options** are not configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

The **high-availability-options** configuration enables you to designate one of the member interfaces as a backup interface. The backup interface does not participate in routing operations as long as it remains a backup interface. When a member interface fails, the backup interface handles the traffic assigned to the failed interface. When the failed interface comes back online, it becomes the new backup interface.

In a many-to-one configuration (N:1), a single backup interface supports all other member interfaces in the group. If any of the member interfaces fails, the backup interface takes over. In this stateless configuration, data is not synchronized between the backup interface and the other member interfaces.

Starting in Junos OS Release 16.1, in a one-to-one configuration, a single active interface is paired with a single backup interface. If the active interface fails, the backup interface does take over. Configurations using **member-failure-options** are not available for one-to-one (1:1) high availability configurations.

When both **member-failure-options** and **high-availability-options** are configured for an AMS, the **high-availability-options** configuration takes precedence over the **member-failure-options** configuration. If a second failure occurs before the failed interface comes back online to be the new backup, the **member-failure-options** configuration takes effect.

Warm Standby Redundancy

Starting in Junos OS Release 17.2R1, you can use the same services interface as the backup in multiple AMS interfaces, resulting in an N:1 warm standby option for MS-MPCs and MS-MICs.

Each warm standby AMS interface contains two members; one member is the service interface you want to protect, called the primary interface, and one member is the secondary (backup) interface. The primary interface is the active interface and the backup interface does not handle any traffic unless the primary interface fails.

To configure warm standby on an AMS interface, you use the **redundancy-options** statement. You cannot use the **load-balancing-options** statement in a warm standby AMS interface.

To switch from the primary interface to the secondary interface, issue the **request interface switchover ams*N*** command.

To revert to the primary interface from the secondary interface, issue the **request interface revert ams*N*** command.

Release History Table

Release	Description
19.2R1	Starting with Junos OS Release 19.2R1, you can use up to 60 PICs across different AMS bundles on a MX2020 router. The hard limit of maximum 36 member interfaces per AMS bundle still exists. However, in the chassis, there can be multiple AMS bundles such that 15 MS-MPC slots can be configured across these bundles.
17.2R1	Starting in Junos OS Release 17.2R1, you can use the same services interface as the backup in multiple AMS interfaces, resulting in an N:1 warm standby option for MS-MPCs and MS-MICs.
17.1	Starting with Junos OS Release 17.1R1, AMS supports IPSec tunnel distribution for next-hop style service-sets. However, interface-style IPSec service sets are not supported.
16.2	Starting with Junos OS Release 16.2, an AMS interface can have up to 36 member interfaces.
16.1	Starting in Junos OS Release 16.1, in a one-to-one configuration, a single active interface is paired with a single backup interface. If the active interface fails, the backup interface does take over.
14.2	Starting in Junos OS release 14.2R1, you can use AMS interfaces for IPv6 traffic.
14.1	Starting in Junos OS Release 14.1R4, input interface aliases are not created for MS-MPCs and MS-MICs.

Configuring Aggregated Multiservices Interfaces

The aggregated multiservices (AMS) interface configuration in Junos OS enables you to combine services interfaces from multiple PICs to create a bundle of interfaces that can function as a single interface. You identify the PIC that you want to act as the backup.

1. Create an aggregated multiservices interface and add member interfaces. Starting in Junos OS Release 19.3R2, an MX-SPC3 Next Gen Services AMS interface can have up to 16 member interfaces with a maximum of 8 MX-SPC3 services cards with up to 2 PICs on each card. Starting with Junos OS Release 16.2, an MS-MPC AMS interface can have up to 36 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface can have a maximum of 24 member interfaces.

   NOTE: The member interface format is **mams-*a*/*b*/0**, where *a* is the Flexible PIC Concentrator (FPC) slot number and *b* is the PIC slot number.

```
[edit interfaces]
user@host# set interface-name load-balancing-options member-interface mams-a/b/0
user@host# set interface-name load-balancing-options member-interface mams-a/b/0
```

For example on an MS-MPC, which can have up to four PICs:

```
[edit interfaces]
user@host# set ams1 load-balancing-options member-interface mams-1/1/0
user@host# set ams1 load-balancing-options member-interface mams-1/2/0
```

For example on an MX-SPC3, which can have up to two PICs:

```
[edit interfaces]
user@host# set ams1 load-balancing-options member-interface mams-1/0/0
user@host# set ams1 load-balancing-options member-interface mams-1/1/0
```

2. Configure logical units for the AMS interface.

```
[edit interfaces]
user@host# set interface-name unit logical-unit-number family family
user@host# set interface-name unit logical-unit-number family family
```

For example:

```
[edit interfaces]
user@host# set ams1 unit 1 family inet
user@host# set ams1 unit 2 family inet6
```

3. Configure member failure options.

```
[edit interfaces interface-name]
user@host# set load-balancing-options member-failure-options drop-member-traffic rejoin-timeout seconds
user@host# set load-balancing-options member-failure-options drop-member-traffic enable-rejoin
```

For example:

```
[edit interfaces ams1]
user@host# set load-balancing-options member-failure-options drop-member-traffic rejoin-timeout 1000
user@host# set load-balancing-options member-failure-options drop-member-traffic enable-rejoin
```

4. Configure the preferred backup.

```
[edit interfaces interface-name]
user@host# set load-balancing-options high-availability-options many-to-one preferred-backup
    preferred-backup
```

For example:

```
[edit interfaces ams1]
user@host# set load-balancing-options high-availability-options many-to-one preferred-backup mams-1/2/0
```

5. **NOTE:** This step is not applicable to the Next Gen Services MX-SPC3 services card in the MX240, MX480 or MX960 chassis.

If the AMS interface has more than 24 member interfaces, set the service PIC boot timeout value to 240 or 300 seconds for every services PIC on the MX Series router. We recommend that you use a value of 240.

NOTE: Starting with Junos OS Release 16.2, an AMS interface can have up to 36 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface could have a maximum of 24 member interfaces.

```
[edit interfaces interface-name multiservice-options]
user@host# set pic-boot-timeout (240 | 300);
```

For example:

```
[edit interfaces sp-1/1/0 multiservice-options]
user@host# set pic-boot-timeout 240
```

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, an MX-SPC3 Next Gen Services AMS interface can have up to 16 member interfaces with a maximum of 8 MX-SPC3 services cards with up to 2 PICs on each card.
16.2	Starting with Junos OS Release 16.2, an MS-MPC AMS interface can have up to 36 member interfaces.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces for Next Gen Services

Configuring Load Balancing on AMS Infrastructure

Configuring load balancing requires an aggregated multiservices (AMS) system. AMS involves grouping several services PICs together. An AMS configuration eliminates the need for separate routers within a system. The primary benefit of having an AMS configuration is the ability to support load balancing of traffic across multiple services PICs.

AMS is supported on the MS-MPC and MS-MIC. Starting in Junos OS Release 19.3R2, AMS interfaces are also supported on the MX-SPC3 if you are running Next Gen Services.

High availability (HA) is supported on AMS infrastructure on all MX Series 5G Universal Routing Platforms. AMS has several benefits:

- Support for configuring behavior if a services PIC that is part of the AMS configuration fails
- Support for specifying hash keys for each service set in either direction
- Support for adding routes to individual PICs within the AMS system

Configuring AMS Infrastructure

AMS supports load balancing across multiple service sets. All ingress or egress traffic for a service set can be load balanced across different services PICs. To enable load balancing, you have to configure an aggregate interface with existing services interfaces.

To configure failure behavior in AMS, include the **member-failure-options** statement:

```
[edit interfaces ams1]
load-balancing-options {
    member-failure-options {
        drop-member-traffic {
            rejoin-timeout rejoin-timeout;
        }
        redistribute-all-traffic {
            enable-rejoin;
        }
    }
}
```

If a PIC fails, you can configure the traffic to the failed PIC to be redistributed by using the **redistribute-all-traffic** statement at the **[edit interfaces *interface-name* load-balancing-options member-failure-options]** hierarchy level. If the **drop-member-traffic** statement is used, all traffic to the failed PIC is dropped. Both options are mutually exclusive.

> **NOTE:** If **member-failure-options** is not explicitly configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Only mams- interfaces (services interfaces that are part of AMS) can be aggregated. After an AMS interface has been configured, you cannot configure the individual constituent mams- interfaces. A mams- interface cannot be used as an ams interface (this is not applicable to Next Gen Services MX-SPC3). AMS supports IPv4 (**family inet**) and IPv6 (**family inet6**). You cannot configure addresses on an AMS interface. Network Address Translation (NAT) is the only application that runs on AMS infrastructure at this time.

> **NOTE:** You cannot configure unit 0 on an AMS interface.

To support multiple applications and different types of translation, AMS infrastructure supports configuring hashing for each service set. You can configure the hash keys separately for ingress and egress. The default configuration uses source IP, destination IP, and the protocol for hashing; incoming-interface for ingress and outgoing-interface for egress are also available.

> **NOTE:** When using AMS in a load-balanced setup for the NAT solution, the number of NAT IP addresses must be greater than or equal to the number of active mams-interfaces you have added to the AMS bundle.

Configuring High Availability

In an AMS system configured with high availability, a designated services PIC acts as a backup for other active PICs that are part of the AMS system in a many-to-one (N:1) backup configuration. In a N:1 backup configuration, one PIC is available as backup for all other active PICs. If any of the active PICs fail, the backup PIC takes over for the failed PIC. In an N:1 (stateless) backup configuration, traffic states and data structures are not synchronized between the active PICs and the backup PIC.

An AMS system also supports a one-to-one (1:1) configuration. In the case of 1:1 backup, a backup interface is paired with a single active interface. If the active interface fails, the backup interface takes over. In a 1:1 (stateful) configuration, traffic states and data structures are synchronized between the active PICs and the backup PIC. Stateful synchronization is required for high availability of IPsec connections. For IPsec connections, AMS supports 1:1 configuration only.

> **NOTE:** IPsec connections are not supported on the MX-SPC3 in this release.

High availability for load balancing is configured by adding the **high-availability-options** statement at the **[edit interfaces *interface-name* load-balancing-options]** hierarchy level.

To configure N:1 high availability, include the **high-availability-options** statement with the **many-to-one** option:

```
[edit interfaces ams1]
load-balancing-options {
    high-availability-options {
        many-to-one {
            preferred-backup preferred-backup;
        }
    }
}
```

Starting in Junos OS Release 16.1, you can configure stateful 1:1 high availability on an MS-MPC. To configure stateful 1:1 high availability, at the **[edit interfaces *interface-name* load-balancing-options]** hierarchy level, include the **high-availability-options** statement with the **one-to-one** option:

> **NOTE:** The Next Gen Services MX-SPC3 services card does not support AMS 1:1 high availability.

```
[edit interfaces ams1]
load-balancing-options {
```

```
    high-availability-options {
        one-to-one {
            preferred-backup preferred-backup;
        }
    }
}
```

Load Balancing Network Address Translation Flows

Network Address Translation (NAT) has been programmed as a plug-in and is a function of load balancing and high availability. The plug-in runs on AMS infrastructure. All flows for translation are automatically distributed to different services PICs that are part of the AMS infrastructure. In case of failure of an active services PIC, the configured backup PIC takes over the NAT pool resources of the failed PIC. The hashing method selected depends on the type of NAT. Using NAT on AMS infrastructure has a few limitations:

- NAT flows to failed PICs cannot be restored.
- There is no support for IPv6 flows.

  IPv6 address pools are not supported with AMS, however NAT64 is supported with AMS, so that IPv6 flows enters AMS.

  NAT64 is supported for Next Gen Services on the MX-SPC3 services card, there is no support of NAT66. IPv6 flows for different NAT services are supported except where the translation is required to be IPv6 to IPv6 or IPv4 to IPv6.
- Twice NAT is not supported for load balancing on MS-MPC cards.

  Twice NAT is supported for load balancing on the Next Gen Services MX-SPC3 services card.
- Deterministic NAT uses warm-standby AMS configuration and can distribute the load using multiple AMS bundles in warm-standby mode.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, AMS interfaces are also supported on the MX-SPC3 if you are running Next Gen Services.
16.1	Starting in Junos OS Release 16.1, you can configure stateful 1:1 high availability on an MS-MPC.

Configuring Warm Standby for Services Interfaces

You can configure an N:1 warm standby option for MS-MPCs, MS-MICs, and MX-SPC3s by creating multiple aggregated multiservices (AMS) interfaces, each of which contains the service interface you want to backup and the service interface that acts as the backup. The same backup service interface can be used in all these AMS interfaces. Starting in Junos OS Release 19.3R2, the N:1 warm standby option is also supported on the MX-SPC3 if you are running Next Gen Services.

To configure warm standby for services interfaces:

1. Create an AMS interface.

   ```
   [edit interfaces]
   user@host# set amsN
   ```

   The variable *N* is a unique number, such as 0 or 1.

2. Specify the primary service interface that you want to backup.

   ```
   [edit interfaces amsN]
   user@host# set redundancy-options primary mams-a/b/0
   ```

   The variable *a* is the FPC slot number and *b* is the PIC slot number for the primary service interface.

3. Specify the secondary service interface, which backs up the primary interface.

   ```
   [edit interfaces amsN]
   user@host# set redundancy-options secondary mams-a/b/0
   ```

   The variable *a* is the FPC slot number and *b* is the PIC slot number for the secondary service interface.

4. Repeat Steps 1 through 3 to create an AMS interface for each service interface that you want to backup. You can use the same secondary service interface in each AMS interface.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, the N:1 warm standby option is also supported on the MX-SPC3 if you are running Next Gen Services.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces | 994

Example: Configuring an Aggregated Multiservices Interface (AMS)

IN THIS SECTION

Hardware and Software Requirements

This example requires MX Series routers that have services interfaces installed in that and Junos OS Release 13.2 running on that.

Overview

The aggregated multiservices (AMS) interface configuration in Junos OS enables you to combine multiple services interfaces to create a bundle of interfaces that can function as a single interface. This example shows you how to configure an AMS interface, load-balancing options, member failure options, high availability settings on an AMS interface, and an interface-style service set configuration that uses the AMS interface.

> **NOTE:** You cannot include MS-DPCs or other multiservices PICs in an AMS configuration that contains MS-MICs or MS-MPCs as member interfaces.

An MS-PIC contains only one interface, whereas the MS-MPC contains four interfaces. To utilize the entire MS-MPC in a single AMS bundle, all the four member interfaces need to be assigned to that AMS bundle.

Keep the following points in mind for every member interface (XLP chip) needs to be part of the AMS interface bundle:

- XLP-based line cards from the same MPC can be part of multiple AMS bundles.
- Multiple XLP chips from several MPCs can also be part of a single bundle (up to eight member interfaces in an AMS bundle, depending on the deployment requirement).
- It is not necessary that all the XLP chips from the same MS-MPC must be part of the same AMS bundle. Some of the XLP chips can be part of an AMS bundle, while other XLP chips can be standalone **ms-** interfaces or need not be configured. However, the same XLP chip cannot be part of two different AMS interfaces at the same time. For example, each XLP chip from the same MS-MPC can be grouped into four different AMS bundles, based on the deployment needs.
- A maximum of up to eight member interfaces can be assigned to an AMS bundle.

For more information about AMS interfaces, see "Understanding Aggregated Multiservices Interfaces" on page 994.

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.

Adding Member Interfaces

```
set interfaces ams0 load-balancing-options member-interface mams-0/0/0
set interfaces ams0 load-balancing-options member-interface mams-0/1/0
set interfaces ams0 load-balancing-options member-interface mams-1/0/0
set interfaces ams0 load-balancing-options member-interface mams-1/1/0
set interfaces ams0 load-balancing-options member-interface mams-2/0/0
set interfaces ams0 load-balancing-options member-interface mams-2/1/0
```

Configuring Logical Units

```
set interfaces ams0 unit 1 family inet
```

Configuring Member Failure Options

```
set interfaces ams0 load-balancing-options member-failure-options drop-member-traffic rejoin-timeout
    300
set interfaces ams0 load-balancing-options member-failure-options drop-member-traffic enable-rejoin
```

Configuring High Availability Options

```
set interfaces ams0 load-balancing-options high-availability-options many-to-one preferred-backup
    mams-1/0/0
```

Configuring Service Set and Interface Services

```
set services service-set ams-ss1 interface-service service-interface ams0.1
set services service-set ams-ss1 interface-service load-balancing-options hash-keys ingress-key
    source-ip
set services service-set ams-ss1 interface-service load-balancing-options hash-keys egress-key
    destination-ip
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. Create an aggregated multiservices interface and add member interfaces.

   NOTE: You cannot configure the same mams to be part of two different AMS interfaces at the same time.

```
[edit]
user@router1# set interfaces ams0 load-balancing-options member-interface mams-0/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface mams-0/1/0
user@router1# set interfaces ams0 load-balancing-options member-interface mams-1/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface mams-1/1/0
user@router1# set interfaces ams0 load-balancing-options member-interface mams-2/0/0
user@router1# set interfaces ams0 load-balancing-options member-interface mams-2/1/0
```

2. Configure logical units for the AMS interface.

   NOTE: An AMS interface and its member interfaces cannot share the same logical interface units. For example, if one of the member interfaces has logical units 1 and 2 configured on it, you cannot configure logical units 1 and 2 for the AMS. Similarly, if you have configured logical units 3 and 4 on the AMS, you cannot configure those units on any of the member interfaces.

   ```
   [edit interfaces]
   user@router1# set ams0 unit 1 family inet
   ```

3. Configure member failure options.

   ```
   [edit interfaces ams0]
   user@router1# set load-balancing-options member-failure-options drop-member-traffic rejoin-timeout 300
   user@router1# set load-balancing-options member-failure-options drop-member-traffic enable-rejoin
   ```

   NOTE: This example shows the **drop-member-traffic** configuration. However, you if you would like to redistribute the traffic to other available members when one of the member interfaces goes down, you can include the **redistribute-all-traffic** statement instead of the **drop-member-traffic** statement.

   The default behavior, when the **member-failure-options** configuration is not included, is to drop member traffic with a rejoin timeout of 120 seconds.

4. Configure the high-availability options.

   ```
   [edit interfaces ams0]
   user@router1# set load-balancing-options high-availability-options many-to-one preferred-backup
     mams-1/0/0
   ```

5. Configure interface style services.

   ```
   [edit services]
   user@router1# set service-set ams-ss1 interface-service service-interface ams0.1
   ```

```
user@router1# set service-set ams-ss1 interface-service load-balancing-options hash-keys ingress-key
  source-ip
user@router1# set service-set ams-ss1 interface-service load-balancing-options hash-keys egress-key
  destination-ip
```

6. If you are done configuring the device, commit the configuration.

```
[edit]
user@router1# commit
```

Table 33: Key Configuration Statements Used in this Example

Statement	Description
member-interface	Adds a member interface (mams) to the AMS bundle.
drop-member-traffic	Specifies that all traffic to a member be dropped in case the member interface fails.
rejoin-timeout	Specifies the time interval, in seconds, for the AMS to wait before declaring a member interface down. If the failed member comes back online during this period, it can rejoin the AMS and resume traffic forwarding. The range is 0 through 1000 seconds.
enable-rejoin	Specifies whether a failed interface be allowed to rejoin the AMS when it comes back online. If this statement is not included in the configuration, you must manually add the interface to the AMS when the interface is back online.
preferred-backup	Designates a member interface as the floating backup.
interface-services	Specifies a service interface, an AMS interface in this example, to handle interface services.
hash-keys	Specifies the load-balancing hash keys. You can configure the following hash key values: **source-ip**, **destination-ip**, **iif** (incoming interface), **oif** (outgoing interface), and **protocol**. **NOTE:** For services that require traffic symmetry, you must configure symmetrical hashing. Symmetrical hashing configuration ensures that both forward and reverse traffic are routed through the same member interface.

Results

From the configuration mode, confirm your configuration by entering the **show interfaces ams0** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces ams0
load-balancing-options {
    member-interface mams-0/0/0;
    member-interface mams-0/1/0;
    member-interface mams-1/0/0;
    member-interface mams-1/1/0;
    member-interface mams-2/0/0;
    member-interface mams-2/1/0;
    member-failure-options {
        drop-member-traffic {
            rejoin-timeout 300;
            enable-rejoin;
        }
    }
    high-availability-options {
        many-to-one {
            preferred-backup mams-1/0/0;
        }
    }
}
    unit 1 {
        family inet;
    }
```

```
user@router1# show services
service-set ams-ss1 {
    interface-service {
        service-interface ams0.1;
        load-balancing-options {
            hash-keys {
                ingress-key source-ip;
                egress-key destination-ip;
            }
        }
    }
}
```

Verification

IN THIS SECTION

Confirm that the configuration is working properly.

Verifying the AMS Configuration

Purpose

Verify the AMS configuration and status of member interfaces.

Action

From operational mode, enter the **show** command.

```
user@router1> show interfaces load-balancing detail
```

```
Load-balancing interfaces detail
Interface        : ams0
  State          : Up
  Last change    : 00:01:28
  Member count   : 6
  HA Model       : Many-to-One
  Members        :
      Interface    Weight   State
      mams-0/0/0   10       Active
      mams-0/1/0   10       Active
      mams-1/0/0   10       Backup
      mams-1/1/0   10       Active
      mams-2/0/0   10       Active
      mams-2/1/0   10       Active
```

Meaning

Shows that **ams0** has six member interfaces with a many-to-one backup configuration. Of the six member interfaces, five are in active state and one, mams-1/0/0, is in backup state.

RELATED DOCUMENTATION

Example: Configuring Next-Hop Style Services on an Aggregated Multiservices Interface

IN THIS SECTION

Hardware and Software Requirements

MX Series routers with services interfaces installed and running Junos OS Release 13.2.

Overview

Starting with Release 13.2, Junos OS extends next-hop style services support to aggregated multiservices (AMS) interfaces. In releases earlier than 12.3, only interface style services configurations were supported on AMS interfaces.

The next-hop style services configuration on AMS interfaces is different from the interface style services configuration. For next-hop style services, the load-balancing hash keys are defined as part of the logical unit configuration of the AMS interface. For interface style services, the hash keys configuration falls under the service-set configuration.

This example explains the next-hop style services configuration on an AMS interface, and shows the verification steps to verify that the configuration is working correctly.

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.

Configuring an aggregated multiservices interface

```
set interfaces ams0 load-balancing-options member-interface mams-1/0/0
set interfaces ams0 load-balancing-options member-interface mams-1/1/0
set interfaces ams0 load-balancing-options member-interface mams-2/0/0
set interfaces ams0 load-balancing-options member-interface mams-2/1/0
set interfaces ams0 unit 1 family inet
set interfaces ams0 unit 1 service-domain inside
set interfaces ams0 unit 2 family inet
set interfaces ams0 unit 2 service-domain outside
```

Configuring Routing Instances that Use AMS interfaces

```
set routing-instances ri-internal instance-type virtual-router
set routing-instances ri-internal interface ge-0/0/2.0
set routing-instances ri-internal interface ams0.1
set routing-instances ri-internal routing-options static route 22.22.22.0/24 next-hop ams0.1
set routing-instances ri-external instance-type virtual-router
set routing-instances ri-external interface ge-2/0/6.0
set routing-instances ri-external interface ams0.2
set routing-instances ri-external routing-options static route 0.0.0.0/0 next-hop ams0.2
```

Configuring Hash Keys

```
set interfaces ams0 unit 1 load-balancing-options hash-keys ingress-key source-ip protocol
set interfaces ams0 unit 2 load-balancing-options hash-keys ingress-key destination-ip protocol
```

Configure Next Hop Services

```
set services service-set ams-test stateful-firewall-rules sfw1
set services service-set ams-test next-hop-service inside-service-interface ams0.1
set services service-set ams-test next-hop-service outside-service-interface ams0.2
```

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see "*Using the CLI Editor in Configuration Mode*" in the *CLI User Guide*.

1. Configure an aggregated multiservices interface and the load-balancing options.

```
[edit interfaces ams0]
user@router1# set load-balancing-options member-interface mams-1/0/0
user@router1# set load-balancing-options member-interface mams-1/1/0
user@router1# set load-balancing-options member-interface mams-2/0/0
user@router1# set load-balancing-options member-interface mams-2/1/0
user@router1# set unit 1 family inet
user@router1# set unit 1 service-domain inside
user@router1# set unit 2 family inet
user@router1# set unit 2 service-domain outside
```

2. Configure routing instances that use the aggregated multiservices interfaces configured in the first step.

```
[edit routing-instances]
user@router1# set ri-internal instance-type virtual-router
user@router1# set ri-internal interface ge-0/0/2.0
user@router1# set ri-internal interface ams0.1
user@router1# set ri-internal routing-options static route 22.22.22.0/24 next-hop ams0.1
user@router1# set ri-external instance-type virtual-router
user@router1# set ri-external interface ge-2/0/6.0
user@router1# set ri-external interface ams0.2
user@router1# set ri-external routing-options static route 0.0.0.0/0 next-hop ams0.2
```

3. Configure hash keys for the aggregated multiservices interfaces.

NOTE: Unlike in the interface-style configuration where hash keys are defined in the service-set configuration, for next-hop services, the hash keys are specified in the AMS configuration under the logical units.

```
[edit interfaces ams0]
user@router1# set unit 1 load-balancing-options hash-keys ingress-key source-ip protocol
user@router1# set unit 2 load-balancing-options hash-keys ingress-key destination-ip protocol
```

4. Configure next-hop style services under the service-set configuration.

```
[edit services service-set ams-test]
user@router1# set stateful-firewall-rules sfw1
user@router1# set next-hop-service inside-service-interface ams0.1
user@router1# set next-hop-service outside-service-interface ams0.2
```

5. Commit the configuration.

```
[edit]
user@router1# commit
```

Results

From the configuration mode, confirm your configuration by entering the **show interfaces ams0**, **show routing-instances**, and **show services service-set ams-test** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@router1# show interfaces ams0
load-balancing-options {
    member-interface mams-1/0/0;
    member-interface mams-1/1/0;
    member-interface mams-2/0/0;
    member-interface mams-2/1/0;
    member-failure-options {
        redistribute-all-traffic {
            enable-rejoin;
        }
    }
}
    unit 1 {
        family inet;
        service-domain inside;
        load-balancing-options {
            hash-keys {
                ingress-key [ source-ip protocol ];
            }
        }
    }
    unit 2 {
        family inet;
        service-domain outside;
        load-balancing-options {
            hash-keys {
                ingress-key [ destination-ip protocol ];
```

```
        }
      }
    }
```

```
user@router1# show routing-instances
ri-internal {
    instance-type virtual-router;
    interface ge-0/0/2.0;
    interface ams0.1
    routing-options {
        static {
            route 22.22.22.0/24 next-hop ams0.1;
        }
    }
}
    ri-external {
        instance-type virtual-router;
        interface ge-2/0/6.0;
        interface ams0.2
        routing-options {
            static {
                route 0.0.0.0/0 next-hop ams0.2;
            }
        }
    }
```

```
user@router1# show services service-set ams
stateful-firewall-rules sfw1;
next-hop-service {
    inside-service-interface ams0.1;
    outside-service-interface ams0.2;
}
```

RELATED DOCUMENTATION

Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

Understanding Aggregated Multiservices Interfaces | **994**

Example: Configuring Static Source Translation on AMS Infrastructure

This example shows a static source translation configured on an AMS interface. The flows will be load balanced across member interfaces with this example.

Configure the AMS interface **ams0** with load balancing options.

```
[edit interfaces ams0]
load-balancing-options {
member-interface mams-5/0/0;
member-interface mams-5/1/0;
}
unit 1 {
    family inet;
}
unit 2 {
    family inet;
}
```

Configure hashing for the service set for both ingress and egress traffic.

```
[edit services service-set ss1]
interface-service {
    service-interface ams0.1;
    load-balancing-options {
        hash-keys {
            ingress-key destination-ip;
            egress-key source-ip;
        }
    }
}
```

NOTE: Hashing is determined based on whether the service set is applied on the ingress or egress interface.

Configure two NAT pools because you have configured two member interfaces for the AMS interface.

```
[edit services]
nat {
    pool p1 {
        address-range low 20.1.1.80 high 20.1.1.80;
    }
pool p2 {
        address 20.1.1.81/32;
    }
}
```

Configure the NAT rule and translation.

```
[edit services]
nat {
    rule r1 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    20.1.1.2/32;
                }
            }
            then {
                translated {
                    source-pool p1;
                    translation-type {
                        basic-nat44;
                    }
                }
           }
        term t1 {
              from {
                  source-address {
                      40.1.1.2/32;
                  }
             }
             then {
                 translated {
                     source-pool p2;
```

```
                    translation-type {
                        basic-nat44;
                    }
                }
            }
        }
    }
```

NOTE: A similar configuration can be applied for translation types **dynamic-nat44** and **napt-44**. Twice NAT cannot run on AMS infrastructure at this time.

RELATED DOCUMENTATION

Configuring Load Balancing on AMS Infrastructure | **1004**

Understanding Aggregated Multiservices Interfaces | **994**

12

PART

Handling VoIP and Layer 2 Traffic

CHAPTER 48

Handling VoIP Traffic Using Voice Services

IN THIS CHAPTER

Voice Services Overview

Adaptive services interfaces include a voice services feature that allows you to specify interface type **lsq-*fpc/pic/port*** to accommodate voice over IP (VoIP) traffic. This interface uses compressed RTP (CRTP), which is defined in RFC 2508, *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*.

CRTP enables VoIP traffic to use low-speed links more effectively, by compressing the 40-byte IP/UDP/RTP header down to 2 to 4 bytes in most cases.

Voice services on the AS and MultiServices PICs support single-link PPP-encapsulated IPv4 traffic over the following physical interface types: ATM2, DS3, E1, E3, OC3, OC12, STM1, and T1, including the channelized versions of these interfaces.

Voice services do not require a separate service rules configuration.

Voice services also support LFI on Juniper Networks M Series Multiservice Edge routers, except the M320 router. For more information about configuring voice services, see "Configuring Services Interfaces for Voice Services" on page 1026.

For link services IQ interfaces (**lsq**) only, you can configure CRTP with multiclass MLPPP (MCML). MCML greatly simplifies packet ordering issues that occur when multiple links are used. Without MCML, all voice traffic belonging to a single flow is hashed to a single link in order to avoid packet ordering issues. With MCML, you can assign voice traffic to a high-priority class, and you can use multiple links. For more information about MCML support on link services IQ interfaces, see "Configuring Link Services and CoS on Services PICs" on page 841.

RELATED DOCUMENTATION

Configuring Services Interfaces for Voice Services

IN THIS SECTION

You define voice service properties such as compression by configuring statements and values for a voice services interface, specified by the interface type **lsq-**. You can include the following statements:

```
encapsulation mlppp;
family inet {
   address address;
}
compression {
   rtp {
      f-max-period number;
      maximum-contexts number <force>;
      port {
         minimum port-number;
         maximum port-number;
      }
      queues [ queue-numbers ];
   }
}
fragment-threshold bytes;
```

You can include these statements at the following hierarchy levels:

- **[edit interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**

The following sections provide detailed instructions for configuring for voice services on services interfaces:

Configuring the Logical Interface Address for the MLPPP Bundle

To configure the logical address for the MLPPP bundle, include the **address** statement:

```
address address {
    ...
}
```

You can configure this statement at the following hierarchy levels:

- **[edit interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number* family inet]**
- **[edit logical-systems *logical-system-name* interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number* family inet]**

address specifies an IP address for the interface. AS and Multiservices PICs support only IP version 4 (IPv4) addresses, which are therefore configured under the **family inet** statement.

For information on other addressing properties you can configure that are not specific to service interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

Configuring Compression of Voice Traffic

You can specify how a services interface handles voice traffic compression by including the **compression** statement:

```
compression {
    rtp {
        f-max-period number;
        maximum-contexts number <force>;
        port {
            minimum port-number;
            maximum port-number;
        }
        queues [ queue-numbers ];
    }
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**

The following statements configure the indicated compression properties:

- **f-max-period *number***—Sets the maximum number of compressed packets to insert between the transmission of full headers. If you do not include the statement, the default is 255 packets.
- **maximum-contexts *number* <force>**—Specifies the maximum number of RTP contexts to accept during negotiation. The optional **force** statement requires the PIC to use the value specified for maximum RTP contexts, regardless of the negotiated value. This option enables interoperation with Junos OS Releases that base the RTP context value on link speed.
- **port**, **minimum *port-number***, and **maximum *port-number***—Specify the lower and upper boundaries for a range of UDP destination port values on which RTP compression takes effect. Values for ***port-number*** can range from 0 through 65,535. RTP compression is applied to traffic transiting the ports within the specified range.
- **queues [*queue-numbers*]**—Specifies one or more of queues **q0**, **q1**, **q2**, and **q3** . RTP compression is applied to the traffic in the specified queues.

> **NOTE:** If you specify both a port range and one or more queues, compression takes place if either condition is met.

Configuring Delay-Sensitive Packet Interleaving

When you configure CRTP, the software automatically enables link fragmentation and interleaving (LFI). LFI reduces excessive delays by fragmenting long packets into smaller packets and interleaving them with real-time frames. This allows real-time and non-real-time data frames to be carried together on lower-speed links without causing excessive delays to the real-time traffic. When the peer interface receives the smaller fragments, it reassembles the fragments into their original packet. For example, short delay-sensitive packets, such as packetized voice, can race ahead of larger delay-insensitive packets, such as common data packets.

By default, LFI is always active when you include the **compression rtp** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level. You control the operation of LFI indirectly by setting the **fragment-threshold** statement on the same logical interface. For example, if you include the **fragment-threshold 256** statement at the **[edit interfaces *interface-name* unit *logical-unit-number*]** hierarchy level, all IP packets larger than 256 bytes are fragmented.

Example: Configuring Compression of Voice Traffic

Configure compression on a T1 interface with MLPPP encapsulation. Configure fragmentation for all IP packets larger than 128 bytes.

```
[edit interfaces]
t1-1/0/0 {
    unit 0 {
        family mlppp {
            bundle lsq-1/1/0.1;
        }
    }
}
lsq-1/1/0 {
    encapsulation mlppp;
    unit 1 {
        compression {
            rtp {
                port minimum 2000 maximum 64009;
            }
        }
        family inet {
            address 30.1.1.2/24;
        }
        fragment-threshold 128;
    }
}
```

RELATED DOCUMENTATION

- Voice Services Overview | 1025
- Configuring Encapsulation for Voice Services | 1029
- Configuring Network Interfaces for Voice Services | 1031
- Examples: Configuring Voice Services | 1032

Configuring Encapsulation for Voice Services

Voice services interfaces support the following logical interface encapsulation types:

- Multilink Point-to-Point Protocol (MLPPP), which is the default encapsulation

- ATM2 IQ MLPPP over AAL5 LLC
- Frame Relay PPP

For general information on encapsulation, see the *Junos OS Network Interfaces Library for Routing Devices*. You can also configure physical interface encapsulation on voice services interfaces.

To configure voice services encapsulation, include the **encapsulation** statement:

```
encapsulation type;
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]**

For voice services interfaces, the valid values for the ***type*** variable are **atm-mlppp-llc**, **frame-relay-ppp** or **multilink-ppp**.

You must also configure the physical interface with the corresponding encapsulation type, either Frame Relay or PPP. LSQ interfaces are supported by the following physical interface types: ATM2 IQ, DS3, E1, E3, OC3, OC12, STM1, and T1, including the channelized versions of these interfaces. For examples, see "Examples: Configuring Voice Services" on page 1032.

NOTE: The only protocol type supported with **frame-relay-ppp** encapsulation is **family mlppp**.

RELATED DOCUMENTATION

Voice Services Overview | **1025**

Configuring Services Interfaces for Voice Services | **1026**

Configuring Network Interfaces for Voice Services | **1031**

Examples: Configuring Voice Services | **1032**

Configuring Network Interfaces for Voice Services

IN THIS SECTION

To complete a voice services interface configuration, you need to configure the physical network interface with either MLPPP encapsulation and a voice services bundle or PPP encapsulation and a compression interface, as described in the following sections:

Configuring Voice Services Bundles with MLPPP Encapsulation

For voice services interfaces, you configure the link bundle as a channel. The physical interface is usually connected to networks capable of supporting MLPPP; the interface types supported for voice traffic are T1, E1, T3, E3, OC3, OC12, and STM1, including channelized versions of these interfaces.

> **NOTE:**
> For M Series routers and T Series routers, the following caveats apply:
>
> - Maximum supported throughput on the bundle interfaces is 45 Mbps.
> - Bundling of the logical interfaces under a T3 physical interface into the same or different bundles is not supported.

To configure a physical interface link for MLPPP, include the following statement:

```
bundle interface-name;
```

You can configure this statement at the following hierarchy levels:

- **[edit interfaces *interface-name* unit *logical-unit-number* family mlppp]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family mlppp]**

When you configure **family mlppp**, no other protocol configuration is allowed. For more information on link bundles, see *Configuring the Links in a Multilink or Link Services Bundle*.

Configuring the Compression Interface with PPP Encapsulation

To configure the physical interface for PPP encapsulation, you also need to specify the services interface to be used for voice compression: a Link Services IQ (**lsq-**) interface.

To configure the compression interface, include the **compression-device** statement:

```
compression-device interface-name;
```

You can configure this statement at the following hierarchy levels:

- **[edit interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**
- **[edit logical-systems *logical-system-name* interfaces (lsq | ls)-*fpc/pic/port* unit *logical-unit-number*]**

RELATED DOCUMENTATION

Voice Services Overview | **1025**

Configuring Services Interfaces for Voice Services | **1026**

Configuring Encapsulation for Voice Services | **1029**

Examples: Configuring Voice Services | **1032**

Examples: Configuring Voice Services

Configure voice services using a T1 physical interface and MLPPP bundle encapsulation:

```
[edit interfaces]
t1-0/2/0:1 {
    encapsulation ppp;
    unit 0 {
        family mlppp {
            bundle lsq-1/3/0.1;
        }
    }
}
lsq-1/3/0 {
    unit 1 {
        encapsulation mlppp;
        family inet {
            address 10.5.5.2/30;
```

```
        }
        compression {
            rtp {
                f-max-period 100;
                queues [ q1 q2 ];
                port {
                    minimum 16384;
                    maximum 32767;
                }
            }
        }
        fragment-threshold 128;
    }
}
```

Configure voice services using Frame Relay encapsulation without bundling:

```
[edit interfaces]
t1-1/0/0 {
    encapsulation frame-relay;
    unit 0 {
        dlci 100;
        encapsulation frame-relay-ppp;
        compression-device lsq-2/0/0.0;
    }
}
lsq-2/0/0 {
    unit 0 {
        compression {
            rtp {
                f-max-period 100;
                queues [ q1 q2 ];
                port {
                    minimum 16000;
                    maximum 32000;
                }
            }
        }
        family inet {
            address 10.1.1.1/32;
        }
    }
}
```

Configure voice services using an ATM2 physical interface (the corresponding class-of-service configuration is provided for illustration):

```
[edit interfaces]
at-1/2/0 {
    atm-options {
        vpi 0;
        pic-type atm2; # only ATM2 PICs are supported
    }
    unit 0 {
        vci 0.69;
        encapsulation atm-mlppp-llc;
        family mlppp {
            bundle lsq-1/3/0.10;
        }
    }
    unit 1 {
        vci 0.42;
        encapsulation atm-mlppp-llc;
        family mlppp {
            bundle lsq-1/3/0.11;
        }
    }
}
lsq-1/3/0 {
    unit 10 {
        encapsulation multilink-ppp;
    }
    # Large packets need to be fragmented.
    # Fragmentation can also be specified per forwarding class.
    fragment-threshold 320;
    compression {
        rtp {
            port minimum 2000 maximum 64009;
        }
    }
}
unit 11 {
    encapsulation multilink-ppp;
}
fragment-threshold 160;
[edit class-of-service]
scheduler-maps {
    sched {
        # Scheduling parameters apply to bundles on the AS or Multiservices PIC.
```

```
        # Unlike DS3/SONET interfaces, there is no need to create
        # a separate scheduler map for the ATM PIC. ATM defines
        # CoS constructs under the [edit interfaces at-fpc/pic/port] hierarchy.
        ...
    }
}
fragmentation-maps {
    fragmap {
        forwarding-class {
            ef {
                # In this example, voice is carried in the ef queue.
                # It is interleaved with bulk data.
                # Alternatively, you could use multiclass MLPPP to
                # carry multiple classes of traffic in different
                # multilink classes.
                no-fragmentation;
            }
        }
    }
}
interfaces {
    # Assign fragmentation and scheduling parameters to LSQ interfaces.
    lsq-1/3/0 {
        unit 0 {
            shaping-rate 512k;
            scheduler-map sched;
            fragmentation-map fragmap;
        }
        unit 1 {
            shaping-rate 128k;
            scheduler-map sched;
            fragmentation-map fragmap;
        }
    }
}
```

RELATED DOCUMENTATION

- Voice Services Overview | **1025**
- Configuring Services Interfaces for Voice Services | **1026**
- Configuring Encapsulation for Voice Services | **1029**
- Configuring Network Interfaces for Voice Services | **1031**

CHAPTER 49

Tunneling PPP Packets Across a Network Using Layer 2 Tunneling

IN THIS CHAPTER

Layer 2 Tunneling Protocol Overview

L2TP is defined in RFC 2661, *Layer Two Tunneling Protocol (L2TP)*.

L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end users and applications. It employs access profiles for group and individual user access, and uses authentication to establish secure connections between the two ends of each tunnel. Multilink PPP functionality is also supported.

The L2TP services are supported on the following routers only:

- M7i routers with AS PICs
- M10i routers with AS and MultiServices 100 PICs
- M120 routers with AS, MultiServices 100, and MultiServices 400 PICs
- On MX Series routers, the L2TP access concentrator (LAC) and L2TP network server (LNS) functions are supported only on MPCs; they are not supported on any services PIC or MS-DPC. For details about MPC support for L2TP, see the *MX Series Interface Module Reference*

For more information, see "L2TP Services Configuration Overview" on page 1037.

RELATED DOCUMENTATION

L2TP Services Configuration Overview

The statements for configuring L2TP services are found at the following hierarchy levels:

- **[edit services l2tp tunnel-group *group-name*]**

  The L2TP **tunnel-group** statement identifies an L2TP instance or L2TP server. Associated statements specify the local gateway address on which incoming tunnels and sessions are accepted, the Adaptive Services (AS) Physical Interface Card (PIC) that processes data for the sessions in this tunnel group, references to L2TP and PPP access profiles, and other attributes for configuring window sizes and timer values.

- **[edit interfaces sp-*fpc*/*pic*/*port* unit *logical-unit-number* dial-options]**

  The **dial-options** statement includes configuration for the **l2tp-interface-id** statement and the **shared**/**dedicated** flag. The interface identifier associates a user session with a logical interface. Sessions can use either shared or dedicated logical interfaces. To run routing protocols, a session must use a dedicated logical interface.

- **[edit access profile *profile-name* client *name* l2tp]**

  Tunnel profiles are defined at the **[edit access]** hierarchy level. Tunnel clients are defined with authentication, multilink negotiation and fragmentation, and other L2TP attributes in these profiles.

- **[edit access profile *profile-name* client *name* ppp]**

  User profiles are defined at the **[edit access]** hierarchy level. User clients are defined with authentication and other PPP attributes in these profiles. These client profiles are used when local authentication is specified.

- **[edit access radius-server *address*]**

  When you configure **authentication-order radius** at the **[edit access profile *profile-name*]** hierarchy level, you must configure a RADIUS service at the **[edit access radius-server]** hierarchy level.

NOTE: For more information about configuring properties at the **[edit access]** hierarchy level, see the *Junos OS Administration Library*. For information about L2TP LAC and LNS configurations on MX Series routers for subscriber access, see *L2TP for Subscriber Access Overview* in the *Junos Subscriber Access Configuration Guide*.

L2TP Minimum Configuration

To configure L2TP services, you must perform at least the following tasks:

- Define a tunnel group at the **[edit services l2tp]** hierarchy level with the following attributes:
  - **l2tp-access-profile**—Profile name for the L2TP tunnel.
  - **ppp-access-profile**—Profile name for the L2TP user.
  - **local-gateway**—Address for the L2TP tunnel.
  - **service-interface**—AS PIC interface for the L2TP service.
  - Optionally, you can configure **traceoptions** for debugging purposes.

The following example shows a minimum configuration for a tunnel group with trace options:

```
[edit services l2tp]
tunnel-group finance-lns-server {
    l2tp-access-profile westcoast_bldg_1_tunnel;
    ppp-access-profile westcoast_bldg_1;
    local-gateway {
        address 10.21.255.129;
    }
    service-interface sp-1/3/0;
}
traceoptions {
    flag all;
    filter {
        protocol udp;
        protocol l2tp;
        protocol ppp;
        protocol radius;
    }
}
```

- At the **[edit interfaces]** hierarchy level:
  - Identify the physical interface at which L2TP tunnel packets enter the router, for example **ge-0/3/0**.
  - Configure the AS PIC interface with **unit 0 family inet** defined for IP service, and configure another logical interface with **family inet** and the **dial-options** statement.

  The following example shows a minimum interfaces configuration for L2TP:

```
[edit interfaces]
ge-0/3/0 {
    unit 0 {
        family inet {
            address 10.58.255.129/28;
        }
    }
}
sp-1/3/0 {
    unit 0 {
        family inet;
    }
    unit 20 {
        dial-options {
            l2tp-interface-id test;
            shared;
        }
        family inet;
    }
}
```

- At the **[edit access]** hierarchy level:
  - Configure a tunnel profile. Each client specifies a unique L2TP Access Concentrator (LAC) name with an **interface-id** value that matches the one configured on the AS PIC interface unit; **shared-secret** is authentication between the LAC and the L2TP Network Server (LNS).
  - Configure a user profile. If RADIUS is used as the authentication method, it needs to be defined.
  - Define the RADIUS server with an IP address, port, and authentication data shared between the router and the RADIUS server.

> **NOTE:** When the L2TP Network Server (LNS) is configured with RADIUS authentication, the default behavior is to accept the preferred RADIUS-assigned IP address. Previously, the default behavior was to accept and install the nonzero peer IP address that came into the IP-Address option of the IPCP Configuration Request packet.

- Optionally, you can define a group profile for common attributes, for example **keepalive 0** to turn off keepalive messages.

The following example shows a minimum profiles configuration for L2TP:

```
[edit access]
group-profile westcoast_users {
    ppp {
        keepalive 0;
    }
}
profile westcoast_bldg_1_tunnel {
    client production {
        l2tp {
            interface-id test;
            shared-secret "$ABC123"; # SECRET-DATA
        }
        user-group-profile westcoast_users;
    }
}
profile westcoast_bldg_1 {
    authentication-order radius;
}
radius-server {
    192.168.65.63 {
        port 1812;
        secret "$ABC123"; # SECRET-DATA
    }
}
```

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- Configuring L2TP Tunnel Groups | **1041**
- Configuring the Identifier for Logical Interfaces that Provide L2TP Services | **1046**

Configuring L2TP Tunnel Groups

IN THIS SECTION

To establish L2TP service on a router, you need to identify an L2TP tunnel group and specify a number of values that define which access profiles, interface addresses, and other properties to use in creating a tunnel. To identify the tunnel group, include the **tunnel-group** statement at the **[edit services l2tp]** hierarchy level.

> **NOTE:** If you delete a tunnel group or mark it inactive, all L2TP sessions in that tunnel group are terminated. If you change the value of the **local-gateway address** or the **service-interface** statement, all L2TP sessions using those settings are terminated. If you change or delete other statements at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level, new tunnels you establish will use the updated values but existing tunnels and sessions are not affected.

This following sections explain how to configure L2TP tunnel groups:

Configuring Access Profiles for L2TP Tunnel Groups

To validate L2TP connections and session requests, you set up access profiles by configuring the **profile** statement at the **[edit access]** hierarchy level. You need to configure two types of profiles:

- L2TP tunnel access profile, which validates all L2TP connection requests to the specified local gateway address

- PPP access profile, which validates all PPP session requests through L2TP tunnels established to the local gateway address

For more information on configuring the profiles, see the *Junos OS Administration Library*. A profile example is included in "Examples: Configuring L2TP Services" on page 1049.

To associate the profiles with a tunnel group, include the **l2tp-access-profile** and **ppp-access-profile** statements at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
l2tp-access-profile profile-name;
ppp-access-profile profile-name;
```

Configuring the Local Gateway Address and PIC

When you configure an L2TP group, you must also define a local address for the L2TP tunnel connections and the AS PIC that processes the requests:

- To configure the local gateway IP address, include the **address** statement at the **[edit services l2tp tunnel-group *group-name* local-gateway]** hierarchy level:

  ```
  address address;
  ```

- To configure the AS PIC, include the **service-interface** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

  ```
  service-interface sp-fpc/pic/port;
  ```

You can optionally specify the logical unit number along with the service interface. If specified, the unit is used as a logical interface representing PPP sessions negotiated using this profile.

NOTE: If you change the local gateway address or the service interface configuration, all L2TP sessions using those settings are terminated.

Dynamic class-of-service (CoS) functionality is supported on L2TP LNS sessions or L2TP sessions with ATM VCs, as long as the L2TP session is configured to use an IQ2 PIC on the egress interface. For more information, see the *Class of Service User Guide (Routers and EX9200 Switches)*.

Configuring Window Size for L2TP Tunnels

You can configure the maximum window size for packet processing at each end of the L2TP tunnel:

- The receive window size limits the number of concurrent packets the server processes. By default, the maximum is 16 packets. To change the window size, include the **receive-window** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
receive-window packets;
```

- The maximum-send window size limits the other end's receive window size. The information is transmitted in the receive window size attribute-value pair. By default, the maximum is 32 packets. To change the window size, include the **maximum-send-window** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
maximum-send-window packets;
```

Configuring Timers for L2TP Tunnels

You can configure the following timer values that regulate L2TP tunnel processing:

- Hello interval—If the server does not receive any messages within a specified time interval, the router software sends a hello message to the tunnel's remote peer. By default, the interval length is 60 seconds. If you configure a value of 0, no hello messages are sent. To configure a different value, include the **hello-interval** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
hello-interval seconds;
```

- Retransmit interval—By default, the retransmit interval length is 30 seconds. To configure a different value, include the **retransmit-interval** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
retransmit-interval seconds;
```

- Tunnel timeout—If the server cannot send any data through the tunnel within a specified time interval, it assumes that the connection with the remote peer has been lost and deletes the tunnel. By default, the interval length is 120 seconds. To configure a different value, include the **tunnel-timeout** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
tunnel-timeout seconds;
```

Hiding Attribute-Value Pairs for L2TP Tunnels

Once an L2TP tunnel has been established and the connection authenticated, information is encoded by means of attribute-value pairs. By default, this information is not hidden. To hide the attribute-value pairs

once the shared secret is known, include the **hide-avps** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
hide-avps;
```

Configuring System Logging of L2TP Tunnel Activity

You can specify properties that control how system log messages are generated for L2TP services.

To configure interface-wide default system logging values, include the **syslog** statement at the **[edit services l2tp tunnel-group *group-name*]** hierarchy level:

```
syslog {
    host hostname {
        services severity-level;
        facility-override facility-name;
        log-prefix prefix-value;
    }
}
```

Configure the **host** statement with a hostname or IP address that specifies the system log target server. The hostname **local** directs system log messages to the Routing Engine. For external system log servers, the hostname must be reachable from the same routing instance to which the initial data packet (that triggered session establishment) is delivered. You can specify only one system logging hostname.

Table 34 on page 1044 lists the severity levels that you can specify in configuration statements at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Table 34: System Log Message Severity Levels

Severity Level	Description
any	Includes all severity levels
emergency	System panic or other condition that causes the router to stop functioning
alert	Conditions that require immediate correction, such as a corrupted system database
critical	Critical conditions, such as hard drive errors
error	Error conditions that generally have less serious consequences than errors in the emergency, alert, and critical levels

Table 34: System Log Message Severity Levels *(continued)*

Severity Level	Description
warning	Conditions that warrant monitoring
notice	Conditions that are not errors but might warrant special handling
info	Events or nonerror conditions of interest

We recommend setting the system logging severity level to **error** during normal operation. To monitor PIC resource usage, set the level to **warning**. To gather information about an intrusion attack when an intrusion detection system error is detected, set the level to **notice** for a specific service set. To debug a configuration or log Network Address Translation (NAT) events, set the level to **info**.

For more information about system log messages, see the System Log Explorer.

To use one particular facility code for all logging to the specified system log host, include the **facility-override** statement at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level:

```
facility-override facility-name;
```

The supported facilities include: **authorization**, **daemon**, **ftp**, **kernel**, **user**, and **local0** through **local7**.

To specify a text prefix for all logging to this system log host, include the **log-prefix** statement at the **[edit services l2tp tunnel-group *group-name* syslog host *hostname*]** hierarchy level:

```
log-prefix prefix-text;
```

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- Configuring the Identifier for Logical Interfaces that Provide L2TP Services | **1046**
- Tracing L2TP Operations | **1053**
- Examples: Configuring L2TP Services | **1049**

Configuring the Identifier for Logical Interfaces that Provide L2TP Services

You can configure L2TP services on adaptive services interfaces on M7i, M10i, M120, and MX Series routers only. You must configure the logical interface to be dedicated or shared. If a logical interface is dedicated, it can represent only one session at a time. A shared logical interface can have multiple sessions.

To configure the logical interface, include the **l2tp-interface-id** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* dial-options]** hierarchy level:

```
l2tp-interface-id name;
(dedicated | shared);
```

The **l2tp-interface-id** name configured on the logical interface must be replicated at the **[edit access profile *name*]** hierarchy level:

- For a user-specific identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* ppp]** hierarchy level.
- For a group identifier, include the **l2tp-interface-id** statement at the **[edit access profile *name* l2tp]** hierarchy level.

You can configure multiple logical interfaces with the same interface identifier, to be used as a pool for several users. For more information on configuring access profiles, see the *Junos OS Administration Library*.

> **NOTE:** If you delete the **dial-options** statement settings configured on a logical interface, all L2TP sessions running on that interface are terminated.

Example: Configuring Multilink PPP on a Shared Logical Interface

Multilink PPP is supported on either shared or dedicated logical interfaces. The following example can be used to configure many multilink bundles on a single shared interface:

```
interfaces {
    sp-1/3/0 {
        traceoptions {
            flag all;
        }
        unit 0 {
            family inet;
        }
        unit 20 {
```

```
            dial-options {
                l2tp-interface-id test;
                shared;
            }
            family inet;
        }
    }
}
access {
    profile t {
        client test {
            l2tp {
                interface-id test;
                multilink;
                shared-secret "$ABC123"; # SECRET-DATA
            }
        }
    }
    profile u {
        authentication-order radius;
    }
    radius-server {
        192.168.65.63 {
            port 1812;
            secret "$ABC123"; # SECRET-DATA
        }
    }
}
services {
    l2tp {
        tunnel-group 1 {
            l2tp-access-profile t;
            ppp-access-profile u;
            local-gateway {
                address 10.70.1.1;
            }
            service-interface sp-1/3/0;
        }
        traceoptions {
            flag all;
            debug-level packet-dump;
            filter {
                protocol l2tp;
                protocol ppp;
```

```
            protocol radius;
        }
    }
}
}
```

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- Configuring L2TP Tunnel Groups | **1041**
- Tracing L2TP Operations | **1053**
- Examples: Configuring L2TP Services | **1049**

AS PIC Redundancy for L2TP Services

L2TP services support AS PIC redundancy. To configure redundancy, you specify a redundancy services PIC (**rsp**) interface in which the primary AS PIC is active and a secondary AS PIC is on standby. If the primary AS PIC fails, the secondary PIC becomes active, and all service processing is transferred to it. If the primary AS PIC is restored, it remains in standby and does not preempt the secondary AS PIC; you need to manually restore the services to the primary PIC. To determine which PIC is currently active, issue the **show interfaces redundancy** command.

NOTE: On L2TP, the only service option supported is *warm standby*, in which one backup PIC supports multiple working PICs. Recovery times are not guaranteed, because the configuration must be completely restored on the backup PIC after a failure is detected. The tunnels and sessions are torn down upon switchover and need to be restarted by the LAC and PPP client, respectively. However, configuration is preserved and available on the new active PIC, although the protocol state needs to be reestablished.

As with the other AS PIC services that support warm standby, you can issue the **request interfaces (revert | switchover)** command to manually switch between primary and secondary L2TP interfaces.

For more information, see "Configuring AS or Multiservices PIC Redundancy" on page 29. For an example configuration, see "Examples: Configuring L2TP Services" on page 1049. For information on operational mode commands, see the CLI Explorer.

RELATED DOCUMENTATION

Examples: Configuring L2TP Services

Configure L2TP with multiple group and user profiles and a pool of logical interfaces for concurrent tunnel sessions:

```
[edit access]
address-pool customer_a {
   address 10.1.1.1/32;
}
address-pool customer_b {
   address-range low 10.2.2.1 high 10.2.3.2;
}
group-profile sunnyvale_users {
   ppp {
      framed-pool customer_a;
      idle-timeout 15;
      primary-dns 192.168.65.1;
      secondary-dns 192.168.65.2;
      primary-wins 192.168.65.3;
      secondary-wins 192.168.65.4;
      interface-id west;
   }
}
group-profile eastcoast_users {
   ppp {
      framed-pool customer_b;
      idle-timeout 20;
```

```
        primary-dns 192.168.65.5;
        secondary-dns 192.168.65.6;
        primary-wins 192.168.65.7;
        secondary-wins 192.168.65.8;
        interface-id east;
    }
}
group-profile sunnyvale_tunnel {
    l2tp {
        maximum-sessions-per-tunnel 100;
        interface-id west_shared;
    }
}
group-profile east_tunnel {
    l2tp {
        maximum-sessions-per-tunnel 125;
        interface-id east_shared;
    }
}
profile sunnyvale_bldg_1 {
    client white {
        chap-secret "$ABC123"; #            SECRET-DATA
        ppp {
            idle-timeout 22;
            primary-dns 192.168.65.1;
            framed-ip-address 10.12.12.12/32;
            interface-id east;
        }
        group-profile sunnyvale_users;
    }
    client blue {
        chap-secret "$ABC123"; #           SECRET-DATA
        group-profile sunnyvale_users;
    }
    authentication-order password;
}
profile sunnyvale_bldg_1_tunnel {
    client test {
        l2tp {
            shared-secret "$ABC123"; # SECRET-DATA
            maximum-sessions-per-tunnel 75;
            interface-id west_shared;
            ppp-authentication chap;
        }
```

```
        group-profile sunnyvale_tunnel;
    }
    client production {
        l2tp {
            shared-secret "$ABC123";
            ppp-authentication chap;
        }
        group-profile sunnyvale_tunnel;
    }
}
[edit services]
l2tp {
    tunnel-group finance-lns-server {
        l2tp-access-profile sunnyvale_bldg_1_tunnel;
        ppp-access-profile sunnyvale_bldg_1;
        local-gateway {
            address 10.1.117.3;
        }
        service-interface sp-1/3/0;
        receive-window 1500;
        maximum-send-window 1200;
        retransmit-interval 5;
        hello-interval 15;
        tunnel-timeout 55;
    }
    traceoptions {
        flag all;
    }
}
[edit interfaces sp-1/3/0]
unit0 {
    family inet;
}
unit 10 {
    dial-options {
        l2tp-interface-id foo-user;
        dedicated;
    }
    family inet;
}
unit 11 {
    dial-options {
        l2tp-interface-id east;
        dedicated;
```

```
    }
    family inet;
}
unit 12 {
    dial-options {
        l2tp-interface-id east;
        dedicated;
    }
    family inet;
}
unit 21 {
    dial-options {
        l2tp-interface-id west;
        dedicated;
    }
    family inet;
}
unit 30 {
    dial-options {
        l2tp-interface-id west_shared;
        shared;
    }
    family inet;
}
unit 40 {
    dial-options {
        l2tp-interface-id east_shared;
        shared;
    }
    family inet;
}
```

Configure L2TP redundancy:

```
interfaces {
    rsp0 {
        redundancy-options {
            primary sp-0/0/0;
            secondary sp-1/3/0;
        }
        unit 0 {
            family inet;
        }
        unit 11 {
```

```
        dial-options {
          l2tp-interface-id east_shared;
          shared;
        }
        family inet;
      }
    }
  }
```

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- Configuring L2TP Tunnel Groups | **1041**
- Configuring the Identifier for Logical Interfaces that Provide L2TP Services | **1046**
- Tracing L2TP Operations | **1053**

Tracing L2TP Operations

Tracing operations track all AS PIC operations and record them in a log file in the **/var/log** directory. By default, this file is named **/var/log/l2tpd**.

> **NOTE:** This topic refers to tracing L2TP LNS operations on M Series routers. To trace L2TP LAC operations on MX Series routers, see *Tracing L2TP Events for Troubleshooting*.

To trace L2TP operations, include the **traceoptions** statement at the **[edit services l2tp]** hierarchy level:

```
traceoptions {
  debug-level level;
  file <filename> <files number> <match regular-expression > <size maximum-file-size> <world-readable |
    no-world-readable>;
  filter {
    protocol name;
    user-name username;
  }
  flag flag;
```

```
    interfaces interface-name {
        debug-level severity;
        flag flag;
    }
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

You can specify the following L2TP tracing flags:

- **all**—Trace everything.
- **configuration**—Trace configuration events.
- **protocol**—Trace routing protocol events.
- **routing-socket**—Trace routing socket events.
- **rpd**—Trace routing protocol process events.

You can specify a trace level for PPP, L2TP, RADIUS, and User Datagram Protocol (UDP) tracing. To configure a trace level, include the **debug-level** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one of the following values:

- **detail**—Detailed debug information
- **error**—Errors only
- **packet-dump**—Packet decoding information

You can filter by protocol. To configure filters, include the **filter protocol** statement at the **[edit services l2tp traceoptions]** hierarchy level and specify one or more of the following protocol values:

- **ppp**
- **l2tp**
- **radius**
- **udp**

To implement filtering by protocol name, you must also configure either **flag protocol** or **flag all**.

You can also configure traceoptions for L2TP on a specific adaptive services interface. To configure per-interface tracing, include the **interfaces** statement at the **[edit services l2tp traceoptions]** hierarchy level:

```
interfaces interface-name {
    debug-level level;
    flag flag;
```

```
}
```

NOTE: Implementing traceoptions consumes CPU resources and affects the packet processing performance.

You can specify the **debug-level** and **flag** statements for the interface, but the options are slightly different from the general L2TP traceoptions. You specify the debug level as **detail**, **error**, or **extensive**, which provides complete PIC debug information. The following flags are available:

- **all**—Trace everything.
- **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
- **packet-dump**—Dump each packet's content based on debug level.
- **protocol**—Trace L2TP, PPP, and multilink handling.
- **system**—Trace packet processing on the PIC.

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**

L2TP Minimum Configuration | **1038**

Configuring L2TP Tunnel Groups | **1041**

Configuring the Identifier for Logical Interfaces that Provide L2TP Services | **1046**

Examples: Configuring L2TP Services | **1049**

PART 13

Configuration Statements and Operational Commands

CHAPTER 50

Configuration Statements

IN THIS CHAPTER

adaptive-services-pics

Syntax

```
adaptive-services-pics {
    traceoptions {
        file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced before Junos OS Release 7.4. The **file** option was added in Release 8.0.

Description

Define global services properties.

Options

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Tracing Services PIC Operations | 38

address (Interfaces)

Syntax

```
address address {
    ...
}
```

Hierarchy Level

[edit interfaces *interface-name* **unit** *logical-unit-number* **family** *family*],
[edit logical-systems *logical-system-name* interfaces *interface-name* **unit** *logical-unit-number* **family** *family*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the interface address.

Options

address—Address of the interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Network Interfaces Library for Routing Devices for other statements that do not affect services interfaces.

Configuring the Logical Interface Address for the MLPPP Bundle | **1027**

Junos OS Network Interfaces Library for Routing Devices

address (Services NAT Pool)

Syntax

```
address ip-prefix</prefix-length>;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The *ip-prefix* and */prefix-length* options were enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the NAT pool prefix value.

The subnet and broadcast addresses are not included in the list of usable IP addresses. For example, if you use 10.11.12.0/28 for the NAT pool prefix value, the addresses 10.11.12.0 (subnet address) and 10.11.12.15 (broadcast address) are not available.

Options

ip-prefix—Specify an IPv4 or IPv6 prefix value.

/prefix-length—(Optional) Specify an IPv4 or IPv6 prefix length.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101

address-allocation

Syntax

```
address-allocation round-robin;
```

Hierarchy Level

```
[edit services nat pool pool-name]
```

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.

Regardless of whether the round-robin method of allocation is addresses is enabled by using the **address-allocation round-robin** statement, round-robin allocation is enabled by default on MS-MICs and MS-MPCs.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Pools of Addresses and Ports for Network Address Translation Overview | 103

address-pooling

Syntax

```
address-pooling paired;
```

Hierarchy Level

[edit**services** nat **rule (Services NAT)** *rule-name* **term (Services NAT)** *term-name* **then (Services NAT) translated**]

Release Information
Statement introduced in JUNOS Release 10.1.

Description
Specify the NAT address pooling behavior.

Options
paired—Currently, the only valid setting specifies paired address pooling behavior.

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | **106**

address-range

Syntax

```
address-range low minimum-value high maximum-value;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
minimum-value and ***maximum-value*** options enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the NAT pool address range.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101

aggregation (IDS)

Syntax

```
aggregation {
    destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
    source-prefix prefix-value | source-prefix-ipv6 prefix-value;
}
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 17.1 on MS-MPCs.

Description

Configure the IDS rule session limits for individual destination or source subnets rather than individual addresses. This applies session limits to an aggregation of all attacks from or to a subnet of the specified length.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring IDS Rules on an MS-DPC | 583
- Configuring Protection Against Network Attacks on an MS-MPC | 601
- Understanding IDS on an MS-MPC | 597

allow-ip-options (Services Stateful Firewall)

Syntax

```
allow-ip-options [ values ];
```

Hierarchy Level

[edit services (Stateful Firewall) stateful-firewall **rule (Services Stateful Firewall)** *rule-name* **term (Services Stateful Firewall)** *term-name* **then (Services Stateful Firewall)**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure how the stateful firewall handles IP header information. This statement is optional.

Options

value—Can be a set or range of numeric values, or one or more of the following predefined option types. You can enter either the option name or its numeric equivalent.

Option Name	Numeric Value
any	**0**
ip-security	**130**
ip-stream	**8**
loose-source-route	**3**
route-record	**7**
router-alert	**148**
strict-source-route	**9**
timestamp	**4**

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in Stateful Firewall Rules | 550

allow-ip-options (IDS MS-MPC)

Syntax

```
allow-ip-options {
    any;
    loose-source-route;
    route-alert;
    route-record;
    security;
    stream-id;
    strict-source-route;
    timestamp;
}
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Specify the type of IPv4 options that the IDS rule permits in the IP header of a packet. If the packet includes an option that is not configured, the packet is blocked. If the packet includes a configured option whose length is an illegal value, the packet is dropped. This IDS rule can only be assigned to a service set on an MS-MPC.

Default

If you do not include the **allow-ip-options** statement, packets with any type of IPv4 option are blocked.

Options

any—Allow all IPv4 options.

loose-source-route—Allow the Loose Source Route option.

route-alert—Allow the Router Alert option.

route-record—Allow the Record Route option.

security—Allow the Security option.

stream-id—Allow the Stream ID option.

strict-source-route—Allow the Strict Source Route option.

timestamp—Allow the Time Stamp option.

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

allow-ipv6-extension-header (IDS MS-MPC)

Syntax

```
allow-ipv6-extension-header {
    ah;
    any;
    dstopts;
    esp;
    fragment;
    hop-by-hop;
    mobility;
    routing;
}
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Specify the type of IPv6 extension headers that the IDS rule permits in a packet. If the packet includes an extension header that is not configured, the packet is blocked. If the packet includes configured extension headers that are incorrect, the packet is dropped. This IDS rule can only be assigned to a service set on an MS-MPC.

Default

If you do not include the **allow-ipv6-extension-header** statement, packets with any type of extension header are blocked.

Options

ah—Allow Authentication Header extension header.

any—Allow all IPv6 extension headers.

dstopts—Allow Destination Options extension header.

esp—Allow Encapsulating Security Payload extension header.

fragment—Allow Fragment Header extension header.

hop-by-hop—Allow Hop-by-Hop Option extension header.

mobility—Allow Mobility Header extension header.

routing—Allow Routing Header extension header.

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | 601
Understanding IDS on an MS-MPC | 597

allow-multicast

Syntax

```
allow-multicast;
```

Hierarchy Level

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

Release Information
Statement introduced in Junos OS Release 8.0.

Description
Allow multicast traffic to be sent to the Adaptive Services or Multiservices PIC.

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

RELATED DOCUMENTATION

Enabling Services PICs to Accept Multicast Traffic | 25

allow-overlapping-nat-pools

Syntax

```
allow-overlapping-nat-pools;
```

Hierarchy Level

```
[edit services nat]
```

Release Information

Statement introduced with Junos OS Release 12.1.

Description

Specify that NAT source or destination pools can be shared between multiple service sets.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets for Network Address Translation | 117

anti-replay-window-size (Services IPsec VPN)

Syntax

```
anti-replay-window-size bits;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Specify the size of the IPsec antireplay window.

Options

bits—Size of the antireplay window, in bits.

Default: 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs)

Range: 64 through 4096 bits

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

anti-replay-window-size (Services Service Set)

Syntax

```
anti-replay-window-size bits;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Specify the size of the IPsec antireplay window. This statement is useful for dynamic endpoint tunnels for which you cannot configure the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement sets the antireplay window size for all the static tunnels within this service set. If a particular tunnel needs a specific value for antireplay window size, set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level. If antireplay check has to be disabled for a particular tunnel in this service set, set the **no-anti-replay** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

> **NOTE:** The **anti-replay-window-size** and **no-anti-replay** settings at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level override the settings specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

Options

bits—Size of the antireplay window, in bits.

Default: 64 bits (AS PICs), 128 bits (Multiservices PICs and DPCs)

Range: 64 through 4096 bits

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

Configuring IPsec Rules | 688

app-mapping-timeout

Syntax

app-mapping-timeout *app-mapping-timeout*;

Hierarchy Level

[edit **services** nat **pool** *nat-pool-name*]

Release Information

mapping-timeout statement introduced in JUNOS Release 12.3.

Description

Specify the duration for address pooling paired (AP-P) mappings that use the specified NAT pool. If this option is not configured and a timeout value is configured for **mapping-timeout**, the timeout value configured for **mapping-timeout** is used. If neither option is specified, the default value of 300 seconds is used.

Options

app-mapping-timeout—Lifetime of AP-P mappings in seconds.

Default: 300

Range: 120 through 864,000

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101

application

Syntax

```
application application-name {
    application-protocol protocol-name;
    child-inactivity-timeout seconds;
    destination-port port-number;
    gate-timeout seconds;
    icmp-code value;
    icmp-type value;
    inactivity-timeout value;
    protocol type;
    rpc-program-number number;
    snmp-command command;
    source-port port-number;
    ttl-threshold number;
    uuid hex-value;
}
```

Hierarchy Level

[edit **applications**],
[edit **applications application-set** *application-set-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure properties of an application and whether to include it in an application set.

Options

application-name—Identifier of the application.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

ALG Descriptions | 466

application-protocol

Syntax

```
application-protocol protocol-name;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
login options introduced in Junos OS Release 7.4.
ip option introduced in Junos OS Release 8.2.
ike-esp-nat option introduced in Junos OS Release 17.1.
ras option introduced in Junos OS Release 17.1.

Description

Identify the application protocol name. Application protocols are also called application layer gateways (ALGs).

Options

protocol-name—Name of the protocol. The following protocols are supported:

bootp—Bootstrap protocol

dce-rpc—DCE RPC

dce-rpc-portmap—DCE RPC portmap

dns—Domain Name Service

exec—Remote Execution Protocol

ftp—File Transfer Protocol

h323—H.323

icmp—ICMP

iiop—Internet Inter-ORB Protocol

ike-esp-nat—IKE ALG

ip—IP

login—Login

netbios—NetBIOS

netshow—NetShow

pptp—Point-to-Point Tunneling Protocol

ras—Gatekeeper RAS for H323

realaudio—RealAudio

rpc—RPC

rpc-portmap—RPC portmap

rtsp—Real Time Streaming Protocol

shell—Shell

sip—Session Initiation Protocol

snmp—SNMP

sqlnet—SQLNet

talk–Talk Program

tftp–Trivial File Transfer Protocol

traceroute—Traceroute

winframe—WinFrame

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

RELATED DOCUMENTATION

ALG Descriptions | **466**

Configuring Application Sets | **501**

Configuring Application Properties | **502**

Examples: Configuring Application Protocols | **524**

Verifying the Output of ALG Sessions | **525**

application-profile

Syntax

```
application-profile profile-name {
    ftp {
        data {
            dscp (alias | bits);
            forwarding-class class-name;
        }
    }
    sip {
        video {
            dscp (alias | bits);
            forwarding-class class-name;
        }
        voice {
            dscp (alias | bits);
            forwarding-class class-name;
        }
    }
}
```

Hierarchy Level

```
[edit services cos],
[edit services cos rule rule-name term term-name then],
[edit services cos rule rule-name term term-name then reverse]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define or apply a CoS application profile. When you apply a CoS application profile in a CoS rule, terminate the profile name with a semicolon (;).

Options

profile-name—Identifier for the application profile.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Application Profiles for Use as CoS Rule Actions | 827

application-set

Syntax

```
application-set application-set-name {
    application application-name;
}
```

Hierarchy Level

```
[edit applications]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure one or more applications to include in an application set.

Options

application-set-name—Identifier of an application set.

Required Privilege Level

system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

ALG Descriptions | 466

Configuring Application Sets | 501

Configuring Application Properties | 502

Examples: Configuring Application Protocols | 524

Verifying the Output of ALG Sessions | 525

application-sets (Services CoS)

Syntax

```
applications-sets set-name;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define one or more target application sets.

Options

set-name—Name of the target application set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions In CoS Rules | 825

application-sets (IDS MS-DPC)

Syntax

```
application-sets set-name;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more target application sets when using the MS-DPC.

Options

set-name—Name of the target application set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

application-sets (PCP)

Syntax

```
applications-sets set-name;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Define an application set to which the PCP rule applies. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

set-name—Name of the application set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

application-sets (Services NAT)

Syntax

```
applications-sets set-name;
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more target application sets.

Options

set-name—Name of the target application set.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

application-sets (Services Stateful Firewall)

Syntax

```
applications-sets set-name;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more target application sets.

Options

set-name—Name of the target application set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

applications (Services ALGs)

Syntax

```
applications { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define the applications used in services.

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

RELATED DOCUMENTATION

- ALG Descriptions | 466
- Configuring Application Sets | 501
- Configuring Application Properties | 502
- Examples: Configuring Application Protocols | 524
- Verifying the Output of ALG Sessions | 525

applications (Services CoS)

Syntax

```
applications [ application-name ];
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define one or more applications to which the CoS services apply.

Options

application-name—Name of the target application.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring Match Conditions In CoS Rules | 825

applications (IDS MS-DPC)

Syntax

```
applications [ application-name ];
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more applications to which IDS applies when using the MS-DPC.

Options

application-name—Name of the target application.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

applications (PCP)

Syntax

```
applications [ application-name ];
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Define one or more application protocols to which the PCP rule applies. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

application-name—Name of the application.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

applications (Services NAT)

Syntax

```
applications [ application-name ];
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more application protocols to which the NAT services apply.

Options

application-name—Name of the target application.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

applications (Services Stateful Firewall)

Syntax

```
applications [ application-name ];
```

Hierarchy Level

[edit services (Stateful Firewall) stateful-firewall **rule (Services Stateful Firewall)** *rule-name* **term (Services Stateful Firewall)** *term-name* **from (Services Stateful Firewall)**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define one or more applications to which the stateful firewall services apply.

Options

application-name—Name of the target application.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

authentication

Syntax

```
authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96 | hmac-sha-256-128);
    key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level

[edit services (IPsec VPN) ipsec-vpn **rule** *rule-name* **term** *term-name* **then manual direction** *direction*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure IPsec authentication parameters for a manual security association (SA).

Options

algorithm—Hash algorithm that authenticates packet data. The algorithm can be one of the following:

- **hmac-md5-96**—Produces a 128-bit digest.
- **hmac-sha1-96**—Produces a 160-bit digest.
- **hmac-sha-256-128**—Produces a 256-bit digest, truncated to 128 bits.

key—Type of authentication key. The key can be one of the following:

- **ascii-text key**—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
- **hexadecimal key**—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

authentication-algorithm (Services IKE)

Syntax

```
authentication-algorithm (md5 | sha1 | sha-256);
```

Hierarchy Level

```
[edit services ipsec-vpn ike proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
sha-256 option added in Junos OS Release 7.6.

Description

Configure the Internet Key Exchange (IKE) hash algorithm that authenticates packet data.

Options

md5—Produces a 128-bit digest.

sha1—Produces a 160-bit digest.

sha-256—Produces a 256-bit digest.

sha-384—Produces a 384-bit digest.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

authentication-algorithm (Services IPsec)

Syntax

```
authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
```

Hierarchy Level

[edit services ipsec-vpn **ipsec proposal** *ipsec-proposal-name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the IPsec hash algorithm that authenticates packet data.

NOTE: Keep the following points in mind when you configure the authentication algorithm in an IPsec proposal:

- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, an error occurs and the tunnel is not established in this scenario. For example, if one end of the tunnel contains router 1 configured with the authentication algorithm as hmac-sha- 256-128 and the other end of the tunnel contains router 2 configured with the authentication algorithm as hmac-md5-96, the VPN tunnel is not established.
- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, and when one end of the tunnel contains two IPsec proposals to check whether a less secure algorithm is selected or not, an error occurs and the tunnel is not established. For example, if you configure two authentication algorithms for an IPsec proposal as hmac-sha-256-128 and hmac-md5-96 on one end of the tunnel, router 1, and if you configure the algorithm for an IPsec proposal as hmac-md5-96 on the other end of the tunnel, router 2, the tunnel is not established and the number of proposals mismatch.
- When you configure two IPsec proposals at both ends of a tunnel, such as the **authentication-algorithm hmac-sha-256-128** and **authentication- algorithm hmac-md5-96** statements at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level on one of the tunnel, router 1 (with the algorithms in two successive statements to specify the order), and the **authentication-algorithm hmac-md5-96** and **authentication- algorithm hmac-sha-256-128** statements at the **[edit services ipsec-vpn ipsec proposal *proposal-name*]** hierarchy level on one of the tunnel, router 2 (with the algorithms in two successive statements to specify the order, which is the reverse order of router 1), the tunnel is established in this combination as expected because the number of proposals is the same on both ends and they contain the same set of algorithms. However, the authentication algorithm selected is hmac-md5-96 and not the stronger algorithm of hmac-sha-256-128. This method of selection of the algorithm occurs because the first matching proposal is selected. Also, for a default proposal, regardless of whether the router supports the Advanced Encryption Standard (AES) encryption algorithm, the 3des-cbc algorithm is chosen and not the aes-cfb algorithm, which is because of the first algorithm in the default proposal being selected. In the sample scenario described here, on router 2, if you reverse the order of the algorithm configuration in the proposal so that it is the same order as the one specified on router 1, hmac-sha-256-128 is selected as the authentication method.
- You must be aware of the order of proposals in an IPsec policy at the time of configuration if you want the matching of proposals to happen in a certain order of preference, such as the strongest algorithm to be considered first when a match is made when both policies from the two peers have a proposal.
- The authentication algorithm hmac-sha-256-128 is not supported on the MX104 Universal Routing Platform.

Options

hmac-md5-96—Produces a 128-bit digest.

hmac-sha-256-128—Produces a 256-bit digest.

hmac-sha1-96—Produces a 160-bit digest.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Proposals | 680

authentication-method

Syntax

```
authentication-method (ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
```

Hierarchy Level

```
[edit services (IPsec VPN) ipsec-vpn ike proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
ecdsa-signatures-256 and **ecdsa-signatures-384** options added in Junos OS Release 17.3R1.

Description

Configure an IKE authentication method.

Options

NOTE: In Junos FIPS mode, ECDSA is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.

ecdsa-signatures-256—Elliptic Curve Digital Signature Algorithm (ECDSA) for 256-bit moduli. This can only be used on an MS-MPC or MS-MIC.

ecdsa-signatures-384—ECDSA for 384-bit moduli. This can only be used on an MS-MPC or MS-MIC.

pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange.

rsa-signatures—Public key algorithm (supports encryption and digital signatures).

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

auxiliary-spi

Syntax

```
auxiliary-spi spi-value;
```

Hierarchy Level

```
[edit services (IPsec VPN) ipsec-vpn rule rule-name term term-name then manual direction direction]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure an auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

Options

spi-value—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).

Range: 256 through 16,639

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

backup-remote-gateway

Syntax

```
backup-remote-gateway address;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the backup remote address to which the IPsec traffic is directed when the primary remote gateway is down. Configuring this statement also enables the dead peer detection (DPD) protocol.

Options

address—Backup remote IPv4 or IPv6 address.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

bundle

Syntax

```
bundle (lsq-fpc/pic/port | ... );
```

Hierarchy Level

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number family mlppp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Associate the voice services interface with the logical interface it is joining.

Options

lsq-*fpc*/*pic*/*port*—Name of the voice services interface you are linking.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Voice Services Bundles with MLPPP Encapsulation | 1031

by-destination (IDS MS-DPC)

Syntax

```
by-destination {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
}
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then session-limit**]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Apply limit to sessions based on numbers generated from the configured destination (IP or subnet) or application when using the MS-DPC.

Options
hold-time *seconds*—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum *number*—Maximum number of open sessions per application or IP address.

packets *number*—Maximum peak packets per second per application or IP address.

rate *number*—Maximum number of sessions per second per application or IP address.

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

by-destination (IDS MS-MPC)

Syntax

```
by-destination {
    by-protocol {
        icmp {
            maximum number;
            packets number;
            rate number;
        }
        tcp {
            maximum number;
            packets number;
            rate number;
        }
        udp {
            maximum number;
            packets number;
            rate number;
        }
    }
    maximum number;
    packets number;
    rate number;
}
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then session-limit]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure the IDS rule session limits for an individual destination address or subnet. This protects against network probing attacks and network flooding attacks. This IDS rule can only be assigned to a service set on an MS-MPC.

When a session limit is exceeded for a destination, packets to the destination are dropped until the session limit is no longer exceeded.

To specify limits for destination subnets rather than individual addresses, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level.

Options

maximum *number*—Specify the maximum number of concurrent sessions allowed for an individual destination address or subnet.

packets *number*—Specify the maximum number of packets per second allowed for an individual destination address or subnet.

rate *number*—Specify the maximum number of connections per second allowed for an individual destination address or subnet.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

by-pair (IDS MS-DPC)

Syntax

```
by-pair {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
}
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then session-limit**]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Apply limit to paired stateful firewall and NAT flows (forward and reverse) when using the MS-DPC.

Options
hold-time *seconds*—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum *number*—Maximum number of open sessions per application or IP address.

packets *number*—Maximum peak packets per second per application or IP address.

rate *number*—Maximum number of sessions per second per application or IP address.

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

by-protocol (IDS MS-MPC)

Syntax

```
by-protocol {
    icmp {
        maximum number;
        packets number;
        rate number;
    }
    tcp {
        maximum number;
        packets number;
        rate number;
    }
    udp {
        maximum number;
        packets number;
        rate number;
    }
}
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then session-limit by-destination],
[edit services ids rule *rule-name* term *term-name* then session-limit by-source]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure the IDS rule session limits for an individual destination or source address or subnet for the specified protocol. This protects against network probing attacks and network flooding attacks. This IDS rule can only be assigned to a service set on an MS-MPC.

When a session limit is exceeded for a source or destination for the protocol, packets from the source or to the destination are dropped until the session limit is no longer exceeded.

To specify limits for destination or source subnets rather than individual addresses, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level.

Options

icmp—Apply session limits to ICMP packets.

maximum *number*—Specify the maximum number of concurrent ICMP sessions allowed for an individual destination or source address or subnet.

packets *number*—Specify the maximum number of ICMP packets per second allowed for an individual destination or source address or subnet.

rate *number*—Specify the maximum number of ICMP connections per second allowed for an individual destination or source address or subnet.

tcp—Session limits apply to TCP packets.

maximum *number*—Specify the maximum number of concurrent TCP sessions allowed for an individual destination or source address or subnet.

packets *number*—Specify the maximum number of TCP packets per second allowed for an individual destination or source address or subnet.

rate *number*—Specify the maximum number of TCP connections per second allowed for an individual destination or source address or subnet.

udp—Session limits apply to UDP packets.

maximum *number*—Specify the maximum number of concurrent UDP sessions allowed for an individual destination or source address or subnet.

packets *number*—Specify the maximum number of UDP packets per second allowed for an individual destination or source address or subnet.

rate *number*—Specify the maximum number of UDP connections per second allowed for an individual destination or source address or subnet.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

by-source (IDS MS-DPC)

Syntax

```
by-source {
    hold-time seconds;
    maximum number;
    packets number;
    rate number;
}
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then session-limit (IDS MS-DPC)**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Apply limit to sessions based on numbers generated from the configured source (IP or subnet) or application when using the MS-DPC.

Options

hold-time *seconds*—Length of time for which to stop all new flows once the rate of events exceeds the threshold set by one or more of the **maximum**, **packets**, or **rate** statements.

maximum *number*—Maximum number of open sessions per application or IP address.

packets *number*—Maximum peak packets per second per application or IP address.

rate *number*—Maximum number of sessions per second per application or IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

by-source (IDS MS-MPC)

Syntax

```
by-source {
    by-protocol {
        icmp {
            maximum number;
            packets number;
            rate number;
        }
        tcp {
            maximum number;
            packets number;
            rate number;
        }
        udp {
            maximum number;
            packets number;
            rate number;
        }
    }
    maximum number;
    packets number;
    rate number;
}
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then session-limit]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure the IDS rule session limits for an individual source address or subnet. This protects against network probing attacks and network flooding attacks. When a session limit is exceeded for a source, packets from the source are dropped until the session limit is no longer exceeded. This IDS rule can only be assigned to a service set on an MS-MPC.

When a session limit is exceeded for a source, packets from the source are dropped until the session limit is no longer exceeded.

To specify limits for source subnets rather than individual addresses, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level.

Options

maximum *number*—Specify the maximum number of concurrent sessions allowed for an individual source address or subnet.

packets *number*—Specify the maximum number of packets per second allowed for an individual source address or subnet.

rate *number*—Specify the maximum number of connections per second allowed for an individual source address or subnet.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

bypass-traffic-on-exceeding-flow-limits

Syntax

```
bypass-traffic-on-exceeding-flow-limits;
```

Hierarchy Level

```
[editservices service-set service-set-name service-set-options]
```

Release Information

Statement introduced in Junos OS Release 10.1.
Statement introduced in Junos OS Release 19.3R2 on MX240, MX480 and MX960 routers using the MX-SPC3 services card..

Description

bypass-traffic-on-exceeding-flow-limitsbypass-traffic-on-exceeding-flow-limitsbypass-traffic-on-exceeding-flow-limits

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

bypass-traffic-on-pic-failure

Syntax

```
bypass-traffic-on-pic-failure;
```

Hierarchy Level

```
[edit services service-set service-set-name service-set-options]
```

Release Information
Statement introduced in Junos OS Release 10.1.

Description
When the MultiServices PIC configured for a service set is either administratively taken offline or undergoes a failure, all the traffic entering the configured interface with an IDP service set would be dropped without notification. To avoid this traffic loss, include the **bypass-traffic-on-pic-failure** statement. When this statement is configured, the affected packets are forwarded in the event of a MultiServices PIC failure or offlining, as though interface-style services were not configured.

This issue applies only to Junos Application Aware (previously known as Dynamic Application Awareness) configurations with IDP service sets.

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

cgn-pic

Syntax

```
cgn-pic;
```

Hierarchy Level

```
[edit interfaces interface-name services-options]
```

Release Information
Statement introduced in Junos OS Release 11.2.

Description
Restrict usage of the service PIC to carrier-grade NAT (CGN) or associated services (intrusion detection, stateful firewall, and softwire). All memory is available for CGN or related services and can be used for CGN scaling.

The **cgn-pic** statement is supported only on the MS-DPC, MS-100, MS-400, and MS-500 line cards. The **cgn-pic** statement is *not* supported on MS-MPCs and MS-MICs.

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

RELATED DOCUMENTATION

Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card | 87

child-inactivity-timeout

Syntax

```
child-inactivity-timeout seconds;
```

Hierarchy Level

```
[edit applications application ike-esp-nat]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

For an IKE ALG application, configure the ESP session (IPsec data traffic) idle timeout. If no IPsec data traffic is passed on the ESP session in this time, the session is deleted.

The IKE ALG enables the passing of IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant.

Options

seconds—Number of seconds.

Default: 800 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

ALG Descriptions | **466**

Configuring Application Sets | **501**

Configuring Application Properties | **502**

cisco-interoperability

Syntax

```
cisco-interoperability send-lip-remove-link-for-link-reject;
```

Hierarchy Level

```
[edit interfaces interface-name mlfr-uni-nni-bundle-options]
```

Release Information
Statement introduced in Junos OS Release 7.4.

Description
FRF.16 interoperability settings.

Options
send-lip-remove-link-for-link-reject—Send Link Integrity Protocol remove link when an add-link rejection message is received.

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

RELATED DOCUMENTATION

Configuring SONET APS Interoperability with Cisco Systems FRF.16 | 910

class

Syntax

```
class {
    alg-logs;
    deterministic-nat-configuration-log;
    ids-logs;
    nat-logs;
    packet-logs;
    pcp-logs;
    session-logs <open | close>;
    stateful-firewall-logs ;
    urlf-logs;
}
```

Hierarchy Level

[edit services **service-set** *service-set-name* **syslog host** *hostname*]

Release Information

Statement introduced in Junos OS Release 13.2.
deterministic-nat-configuration-log option introduced in Junos OS Release 17.3R1.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.
urlf-logs option introduced in Junos OS Release 18.3R1.

Description

Set the class of applications to be logged to the system log.

Starting in Junos OS Release 17.4R1, you can configure up to a maximum of four system log servers (combination of local system log hosts and remote system log collectors) for each service set at the **[edit services service-set *service-set-name*]** hierarchy level.

Options

class-name—Enter one of the following values:

- **alg-logs**—Log application-level gateway events.
- **deterministic-nat-configuration-log**—Log deterministic NAT sessions.
- **ids-logs**—Log intrusion detection system events.
- **nat-logs**—Log Network Address Translation events.
- **packet-logs**—Log general packet-related events.
- **pcp-logs**—Log Port Control Protocol events.

- **session-logs**—Log session open and close events.
- **session-logs open**—Log session open events only.
- **session-logs close**—Log session close events.
- **urlf-logs**—Log events for the filtering of DNS requests for blocklisted website domains.

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

RELATED DOCUMENTATION

See Configuring System Logging for Service Sets | 36.

clat-prefix

Syntax

```
clat-prefix clat-prefix;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information
Statement introduced in Junos OS Release 17.1 on MX Series.

Description
Specify the IPv6 prefix that the customer-side translator (CLAT) uses when performing 464XLAT translation to IPv6 (the CLAT is not a Juniper Networks product). The Provider-Side Translater (PLAT) on the MX Series uses the CLAT IPv6 prefix to translate the IPv6 packet back to IPv4.

RELATED DOCUMENTATION

464XLAT Overview | 253
Configuring 464XLAT Provider-Side Translater for IPv4 Connectivity Across IPv6-Only Network | 255

clear-dont-fragment-bit (Interfaces GRE Tunnels)

Syntax

```
clear-dont-fragment-bit;
```

Hierarchy Level

[edit interfaces gr-*fpc/pic/port* **unit** *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces gr-*fpc/pic/port* **unit** *logical-unit-number*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in 10.0R2 for 16x10GE MPC
Statement introduced in 13.2R4 for Multiservices MPC
Statement introduced in Junos OS Release 10.2 for MPC1 and MPC1Q.
Statement introduced in Junos OS Release 10.1 for MPC2 and variants.
Statement introduced in Junos OS Release 11.2R4 for MPC1E and MPC1E Q.
Statement introduced in Junos OS Release 11.2R4 for MPC2E and variants
Statement introduced in Junos OS Release 12.1 for MPC3E and variants
Statement introduced in Junos OS Release 12.2 for MPC2E P
Statement introduced in Junos OS Release 12.3R2 for MPC4E and variants
Statement introduced in Junos OS Release 13.3R2 and later for MPC5E and variants
Statement introduced in Junos OS Release 14.1R4, 14.2R3 and Junos Continuity 15.1 for MPC2E NG and variants
Statement introduced in Junos OS Release 14.1R4, 14.2R3 and Junos Continuity 15.1 for MPC3E NG and variants
Statement introduced in Junos OS Release 15.1F4 with Junos Continuity and 16.1R1 and later for MPC7E and variants
Statement introduced in Junos OS Release 15.1F7 for MPC6E
Statement introduced in Junos OS Release 15.1F7 for MPC8E
Statement introduced in Junos OS Release 15.1F7 for MPC9E
Statement introduced in Junos OS Release 17.3 for MX10003 MPC (Multi-Rate)

Description

Clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the generic routing encapsulation (GRE) tunnel on Adaptive Services (AS) or Multiservices interfaces. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. The statement is supported only on MX Series routers and all M Series routers except the M320 router.

When you configure the **clear-dont-fragment-bit** statement on an interface with the MPLS protocol family enabled, you must specify an MTU value. This MTU value must not be greater than maximum supported value, which is 9192.

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

RELATED DOCUMENTATION

- *Enabling Fragmentation on GRE Tunnels*

clear-dont-fragment-bit (Services IPsec VPN)

Syntax

```
clear-dont-fragment-bit;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Clear the do not fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation.

By default, this statement is disabled (the DF bit value is not cleared on the inner header and outer header by default).

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

clear-dont-fragment-bit (Services NAT Options)

Syntax

```
clear-dont-fragment-bit;
```

Hierarchy Level

[edit services **service-set** *service-set-name* **nat-options stateful-nat64**]

Release Information

Statement introduced with Junos OS Release 12.1.

Description

Clear the DF (don't fragment) bit in a translated IPv4 packet if its packet size is less than 1280 bytes. If the packet is greater than or equal to 1280 bytes, the DF bit is not cleared.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | 21

clear-dont-fragment-bit (Services Service Set)

Syntax

```
clear-dont-fragment-bit;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information
Statement introduced in Junos OS Release 10.0.

Description
Clear the Don't Fragment (DF) bit on all IP version 4 (IPv4) packets entering the IPsec tunnel. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This statement is useful for dynamic endpoint tunnels, for which you cannot configure the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, setting this statement clears the DF bit on packets entering all the static tunnels within this service set. If you want to clear the DF bit on packets entering a specific tunnel, set the **clear-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

By default, this statement is disabled (the DF bit value is not cleared on the inner header and outer header by default).

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

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698
Configuring IPsec Rules | 688

clear-ike-sas-on-pic-restart

Syntax

```
clear-ike-sas-on-pic-restart;
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced in Junos OS Release 8.5.

Description

Clear IKE security associations (SAs) when the corresponding PIC restarts or is taken offline.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Security Associations | 639

clear-ipsec-sas-on-pic-restart

Syntax

```
clear-ipsec-sas-on-pic-restart;
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced in Junos OS Release 9.2.

Description

Clear IPsec security associations (SAs) when the corresponding PIC restarts or is taken offline.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Security Associations | 639

compression

Syntax

```
compression {
   rtp {
      f-max-period number;
      maximum-contexts number <force>;
      port {
         minimum port-number;
         maximum port-number;
      }
      queues [ queue-numbers ];
   }
}
```

Hierarchy Level

```
[edit interfaces interface-nameunit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the compression properties for voice services traffic.

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | 1027

compression-device (Interfaces)

Syntax

```
compression-device interface-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced in Junos OS Release 7.5.

Description

Specify the compression interface for voice services traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Compression Interface with PPP Encapsulation | 1032

copy-dont-fragment-bit (Services IPsec VPN)

Syntax

```
copy-dont-fragment-bit;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information
Statement introduced in Junos OS Release 14.1.

Description
Copy the do not fragment (DF) bit value to only the outer header and not modify the inner header of the IPsec packet. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs. These settings apply for static endpoint tunnels and not for dynamic tunnels, for which you need to include the **copy-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to copy the DF bit value to only the outer header of the packet in a static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

By default, this statement is disabled on MS-MICs and MS-MPCs (the DF bit value is not copied to the outer header by default).

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

copy-dont-fragment-bit (Services Set)

Syntax

```
copy-dont-fragment-bit;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Copy the do not fragment (DF) bit value to only the outer header and not modify the inner header of the IPsec packet in dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **copy-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level to copy the DF bit value to only the outer header of the packet in a static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

By default, this statement is disabled on MS-MICs and MS-MPCs (the DF bit value is not copied to the outer header by default).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

Configuring IPsec Rules | 688

cos-rules (Service Set)

Syntax

```
cos-rules [cos-rule-name];
```

Hierarchy Level

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

Release Information
Statement introduced in Junos OS Release 8.1.

Description
Specify the CoS rules to apply to the service set. You can configure multiple rules.

The service set that the CoS rule is assigned to must include at least one stateful firewall rule or NAT rule, or CoS does not work. Only stateful firewall and NAT rules can be used with CoS rules in a service set.

Options
cos-rule-name—CoS rule name.

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

data (FTP)

Syntax

```
data {
    dscp (alias | bits);
    forwarding-class class-name;
}
```

Hierarchy Level

```
[edit services cos application-profile profile-name ftp]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** value for FTP data.

Default

By default, the system will not alter the DSCP or forwarding class for FTP data traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

video (Application Profile) | **1599**

voice (Application Profile) | **1603**

dead-peer-detection (Services IPsec VPN)

Syntax

```
dead-peer-detection {
    interval seconds;
    threshold number;
}
```

Hierarchy Level

[edit services ipsec-vpn *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 11.4.
IKEv2 support introduced in Junos OS Release 17.2.

Description

Sets dead peer detection options when dead peer detection has been enabled with the **initiate-dead-peer-detection** command. The **dead-peer-detection** options are used for IKEv1 security associations (SAs). Starting in Junos OS Release 17.2R1, the **dead-peer-detection** options are also applicable to IKEv2 SAs. In Junos OS Release 17.1 and earlier, the **dead-peer-detection** options are not applicable to IKEv2 SAs, which use the default values.

Options

- interval—Specify the amount of time that the peer waits for dead-peer-detection (DPD) response from its destination peer before sending next DPD request packet. Range is 1 through 180 seconds. The default value is 10 seconds.
- threshold—Specify the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. Range is 1 through 10. The default value is 3.

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

description (Services IPsec VPN)

Syntax

```
description description;
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name],
[edit services ipsec-vpn ike proposal proposal-name],
[edit services ipsec-vpn ipsec policy policy-name],
[edit services ipsec-vpn ipsec proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the text description for an IKE or IPsec policy or proposal.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- description | 1143
- Configuring IPsec Proposals | 680
- Configuring IPsec Policies | 685

destination-address (Services CoS)

Syntax

```
destination-address (address | any-unicast) <except>;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 8.1.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address for rule matching.

Options

address—Destination IPv4 or IPv6 address or prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring Match Conditions In CoS Rules | 825

destination-address (IDS MS-DPC)

Syntax

```
destination-address (address | any-unicast) <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address for rule matching when using the MS-DPC.

Options

address—Destination IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

destination-address

Syntax

```
destination-address address;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the destination address for rule matching.

Options

address—Destination IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

destination-address (PCP)

Syntax

```
destination-address address <except>;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the destination address that must be matched for the PCP rule. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

address—Destination address or prefix value.

minimum-value—Lower boundary for the address range.

except—(Optional) Prevent the specified address range from matching the PCP rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

destination-address (Services NAT)

Syntax

```
destination-address (address | any-unicast) <except>;
```

Hierarchy Level

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

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 IPv6 and addresses in Junos OS Release 8.5.

Description

Specify the destination address for rule matching.

Options

address—Destination IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Prevent the specified address, prefix, or unicast packets from being translated.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

destination-address (Services Stateful Firewall)

Syntax

```
destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

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 IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address for rule matching.

Options

address—Destination IPv4 or IPv6 address or prefix value. Using a value of 0::0/0 with IPv6 is not allowed for M-Series and MX-Series routers.

any-ipv4—Any IPv4 packet.

any-ipv6—Any IPv6 packet.

any-unicast—Match all unicast packets.

except—(Optional) Exclude the specified address, prefix, IPv4, IPv6, or unicast packets from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

destination-address-range (IDS MS-DPC))

Syntax

```
destination-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address range for rule matching when using the MS-DPC.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exempt the specified address range from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

destination-address-range (PCP)

Syntax

```
destination-address-range high maximum-value low minimum-value <except>;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information
Statement introduced in Junos OS Release 13.2R1.

Description
Specify the destination address range that must be matched for the PCP rule. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options
maximum-value—Upper boundary for the address range.

minimum-value—Lower boundary for the address range.

except—(Optional) Prevent the specified address range from matching the PCP rule.

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

destination-address-range (Services NAT)

Syntax

```
destination-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address range for rule matching.

If the **translation-type** statement in the **then** statement of the nat rule is set to **stateful-nat-64**, the destination address range for rule matching must be within the range specified by the **destination-prefix** statement in the **then** statement.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Prevent the specified address range from being translated.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

destination-address-range (Services Stateful Firewall)

Syntax

```
destination-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination address range for rule matching.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address range from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

destination-pool

Syntax

```
destination-pool nat-pool-name;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the destination address pool for translated traffic.

Options

nat-pool-name—Destination pool name.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

destination-port

Syntax

```
destination-port port-value;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) destination port number.

Options

port-value—Identifier for the port or range of ports. For a complete list of supported application destination port requirements, see "Configuring Source and Destination Ports" on page 509.

Range: 1 through 65,535

NOTE: If you specify a value of 0 as a destination port or beginning of a destination report range, you will receive the following error:

```
'application application-name'
        TCP Destination Port 0 Invalid
    error: configuration check-out failed
```

Required Privilege Level

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

RELATED DOCUMENTATION

ALG Descriptions | 466
Configuring Application Sets | 501
Configuring Application Properties | 502

Examples: Configuring Application Protocols | 524

Verifying the Output of ALG Sessions | 525

Understanding Two-Way Active Measurement Protocol on Routers

destination-port (PCP)

Syntax

```
destination-port high maximum-value low minimum-value;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the destination port range that must be matched for the PCP rule. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

maximum-value—Upper boundary for the port range.

minimum-value—Lower boundary for the port range.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

destination-port range

Syntax

```
destination-port range high maximum-value low minimum-value;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Specify the destination port range for rule matching.

Options

maximum-value—Upper limit of port range for matching.

minimum-value—Lower limit of port range for matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

destination-prefix (IDS)

Syntax

```
destination-prefix prefix-value;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then aggregation]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 17.1 on MS-MPCs.

Description

Specify a prefix length for destination IPv4 address aggregation for the IDS rule. This applies session limits to an aggregation of all attacks to a subnet of the specified length.

For example, if you configure a value of 24 for **destination-prefix**, then attacks to 10.1.1.2 and 10.1.1.3 are counted as attacks to the 10.1.1/24 subnet.

Options

prefix-value—Integer value.

Range: 1 through 32

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Actions in IDS Rules | **586**
- Configuring Protection Against Network Attacks on an MS-MPC | **601**
- Understanding IDS on an MS-MPC | **597**

destination-prefix (Services NAT)

Syntax

```
destination-prefix destination-prefix;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 7.6.
destination-prefix option enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the destination prefix for translated traffic.

Options

destination-prefix—IPv4 or IPv6 destination prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

destination-prefix-ipv6 (IDS)

Syntax

```
destination-prefix-ipv6 prefix;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then aggregation]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 17.1 on MS-MPCs.

Description

Specify a prefix length for destination IPv6 address aggregation for the IDS rule. This applies session limits to an aggregation of all attacks to a subnet of the specified length.

For example, if you configure a value of 64 for **destination-prefix-ipv6**, then attacks to 2001:db8:1234:72a2::2 and 2001:db8:1234:72a2::3 are counted as attacks to the 2001:db8:1234:72a2::/64 subnet.

Options

prefix-value—Integer value.

Range: 1 through 128

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Actions in IDS Rules | **586**
- Configuring Protection Against Network Attacks on an MS-MPC | **601**
- Understanding IDS on an MS-MPC | **597**

destination-prefix-list (PCP)

Syntax

```
destination-prefix-list list-name;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the destination prefix list that must be matched for the PCP rule. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

list-name—Destination prefix list.

except—(Optional) Prevent the specified prefix list from matching the PCP rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

destination-prefix-list (Services CoS)

Syntax

```
destination-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

Routing Policies, Firewall Filters, and Traffic Policers User Guide

destination-prefix-list (Services IDS)

Syntax

```
destination-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Routing Policies, Firewall Filters, and Traffic Policers User Guide

Configuring Match Conditions in IDS Rules | 585

destination-prefix-list (Services NAT)

Syntax

```
destination-prefix-list list-name <except>;
```

Hierarchy Level

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

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.

If the **translation-type** statement in the **then** statement of the nat rule is set to **stateful-nat-64**, the destination prefix list for rule matching must be within the range specified by the **destination-prefix** statement in the **then** statement.

Options

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

Routing Policies, Firewall Filters, and Traffic Policers User Guide

destination-prefix-list (Services Stateful Firewall)

Syntax

```
destination-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

Routing Policies, Firewall Filters, and Traffic Policers User Guide

destined-port

Syntax

```
destined-port port id;
```

Hierarchy Level

```
[edit services nat port-forwarding map-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Specify the destination port number that needs to be translated to another port.

The **destined-port** statement is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, the **destined-port** statement is also supported on the MS-MPC and MS-MIC.

Options

port id—The destination port number from where traffic will be forwarded.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Configuring Port Forwarding Without Destination Address Translation | 291

deterministic-port-block-allocation

Syntax

```
deterministic-port-block-allocation {
    block-size block-size;
    include-boundary-addresses;
}
```

Hierarchy Level

[edit **services** nat **pool** *pool-name* port]

Release Information
Statement introduced in Junos OS Release 12.1.

Description
Configure algorithm-based allocation of blocks of destination ports. By specifying this method, you ensure that an incoming (source) IP address and port always map to the same destination IP address and port block, thus eliminating the need for logging address translations.

Options
block-size—Maximum number of ports that can be allocated to a user.

If **block-size** is configured as zero, the method for computing the block size is as follows:

block-size = int(65412/ceil[(Number of subscribers/Number of IP addresses in the NAT pool)]).

where

64512 is derived from (65535 - 1023) because the regular port assignments start from 1024.

Number of subscribers is derived from the from clause of the applicable NAT rule.

Default: 256

Range: 0 through 32,000

include-boundary-addresses—(Optional) Specifies that the lowest and highest addresses (the network and broadcast addresses) in the source address range of a NAT rule should be translated when the NAT pool is used. If the source address has a prefix of /32, the lowest and highest address are automatically translated.

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

RELATED DOCUMENTATION

Configuring Deterministic NAPT | 202

dh-group

Syntax

```
dh-group (group1 | group2 | group5 |group14 | group15 | group16 | group19 | group20 | group24);
```

Hierarchy Level

```
[edit services ipsec-vpn ike proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
group15, **group16**, and **group24** options added in Junos OS Release 17.4R1.

Description

Configure the IKE Diffie-Hellman prime modulus group to use for performing the new Diffie-Hellman exchange.

Options

group1—768-bit.

group2—1024-bit.

group5—1536-bit.

group14—2048-bit.

group15—3072-bit.

group16—4096-bit.

group19—256-bit random Elliptic Curve Group.

group20—384-bit random Elliptic Curve Group.

group24—2048-bit with 256-bit Prime Order Subgroup.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

dial-options

Syntax

```
dial-options {
    ipsec-interface-id name;
    l2tp-interface-id name;
    (shared | dedicated);
}
```

Hierarchy Level

```
[edit interfaces sp-fpc/pic/port unit logical-unit-number],
[edit interfaces si-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces sp-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces si-fpc/pic/port unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The **[edit ...si-...]** hierarchy levels introduced in Junos OS Release 11.4.

Description

Specify the options for configuring logical interfaces for group and user sessions in L2TP or IPsec dynamic endpoint tunneling.

Options

dedicated—(LNS on M Series routers and MX Series routers only) Specify that a logical interface can host only one session at a time.

ipsec-interface-id *name*—(M Series routers only) Interface identifier for group of dynamic peers. This identifier must be replicated at the **[edit access profile *name* client * ike]** hierarchy level.

l2tp-interface-id *name*—Interface identifier that must be replicated at the **[edit access profile *name*]** hierarchy level.

shared—(LNS on M Series routers only) Specify that a logical interface can host multiple (shared) sessions at a time.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Identifier for Logical Interfaces that Provide L2TP Services | 1046

Configuring Dynamic Endpoints for IPsec Tunnels | 750

Configuring Options for the LNS Inline Services Logical Interface

direction

Syntax

```
direction (inbound | outbound | bidirectional) {
    protocol (ah | bundle | esp);
    spi spi-value;
    auxiliary-spi spi-value;
    authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
    }
    encryption {
        algorithm algorithm;
        key (ascii-text key | hexadecimal key);
    }
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then manual]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the direction in which manual SAs are applied.

Options

bidirectional—Apply the SA in both directions.

inbound—Apply the SA on inbound traffic.

outbound—Apply the SA on outbound traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

disable-natt (Services IPsec VPN)

Syntax

```
disable-natt;
```

Hierarchy Level

```
[edit services ipsec-vpn],
```

Release Information
Statement introduced in Junos OS Release 16.1.

Description
Before Junos OS Release 17.4R1, Network Address Translation-Traversal (NAT-T) is not supported for the Junos VPN Site Secure suite of IPsec features on the MX Series routers. In Junos OS releases before 17.4R1, disable NAT-traversal (NAT-T) when a NAT device is present between two IPsec gateways to cause the Encapsulating Security Payload (ESP) protocol to be used for encapsulation.

In traditional network deployments, IPsec does not work when packets traverse across a device that is configured for network address translation (NAT) or network address port translation (NAPT) for translating packets, IPsec does not work when either one of the device or both the devices that terminate the IPsec tunnel is behind a NAT device. This behavior occurs because NAT checks the port information, which is not present for IPsec-protected traffic.

When NAT-T is configured, IPsec traffic is encapsulated using the UDP header and port information is provided for the NAT devices. By default, Junos OS detects whether either one of the IPsec tunnel is behind a NAT device and automatically switches to using NAT-T for the protected traffic. However, in certain cases, NAT-T support on MX Series routers running a Junos OS Release before 17.4R1 might not work as desired. Also, you might require NAT-traversal to be disabled if you are aware that the network uses IPsec-aware NAT.

To avoid problems with NAT-T on MX series routers, you can disable NAT-T. When you disable NAT-T, the NAT-T functionality is globally switched off. Also, even when a NAT device is present between the two IPsec gateways, only ESP encapsulation is used when you disable NAT-T.

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

RELATED DOCUMENTATION

Disabling NAT-T on MX Series Routers for Handling NAT with IPsec-Protected Packets | 709

distinguished-name

Syntax

distinguished-name container *container-string-values* |wildcard *wildcard-string-values*

Hierarchy Level

[edit services ipsec-vpn **ikepolicy** *policy-name* **local-id**|**remote-id**

Release Information
distinguished-name option added in Junos OS Release 19.1.

Description
Specify one or more distinguished name values.

A distinguished name is a name used with digital certificates to uniquely identify a user. For example a distinguished name can be:

- CN=user
- DC=example
- DC=com

Optionally, you can use the container keyword to specify that the order of the fields in a DN and their values exactly match the configured DN, or use the wildcard keyword to specify that the values of fields in a DN must match but the order of the fields does not matter.

Options
container *container-string-values* —One or more distinguished name container string.

wildcard *wildcard-string-values* —One or more distinguished name wildcard string.

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

RELATED DOCUMENTATION

Configuring IKE Policies | 671

dns-alg-pool

Syntax

```
dns-alg-pool dns-alg-pool;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Specify the Network Address Translation (NAT) pool for destination translation.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

dns-alg-prefix

Syntax

```
dns-alg-prefix dns-alg-prefix;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

Set the Domain Name System (DNS) application-level gateway (ALG) 96-bit prefix for mapping IPv4 addresses to IPv6 addresses.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

dns-filter

Syntax

```
dns-filter {
    database-file filename;
    dns-resp-ttl seconds;
    dns-server [ ip-address ];
    hash-key key-string;
    hash-method hash-method-name;
    statistics-log-timer minutes;
    wildcarding-level level;
}
```

Hierarchy Level

```
[edit services web-filter profile profile-name],
[edit services web-filter profile profile-name dns-filter-template template-name]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series.
Support added for Next Gen Services on MX Series routers MX240, MX480 and MX960 with MX-SPC3 services cards in Junos OS Release 19.3R2.

Description

Configure the settings for filtering DNS requests for disallowed website domains. Filtering can result in either:

- Blocking access to the site by sending the client a DNS response that includes an IP address or domain name of a sinkhole server instead of the disallowed domain.
- Logging the DNS request and allowing access.

Settings at the **[edit services web-filter profile *profile-name* dns-filter-template *template-name*]** hierarchy level override the corresponding settings at the **[edit services web-filter profile *profile-name*]** hierarchy level.

Options

database-file *filename*—Name of the domain filter database file to use when filtering DNS requests.

dns-resp-ttl *seconds*— Number of seconds to live while sending the DNS response after taking the DNS sinkhole action.

Default: 1800

Range: 0 through 86,400

dns-server [*ip-address*]—(Optional) IP addresses (IPv4 or IPv6) for up to three specific DNS servers. DNS filtering examines only DNS requests that are destined for those DNS servers.

hash-key *key-string*—Hash key that you used to create the hashed domain name in the domain filter database file.

hash-method *hash-method-name*—Hash method that you used to create the hashed domain name in the domain filter database file. The only supported hash method is **hmac-sha2-256**.

statistics-log-timer *minutes*—Number of minutes in the interval for logging statistics for DNS requests and for sinkhole actions performed for each customer IP address.

Default: 5

Range: 0 through 60

wildcarding-level *level*—Level of subdomains that are searched for a match. A value of 0 indicates that subdomains are not searched.

For example, if you set the **wildcarding-level** to 4 and the database file includes an entry for **example.com**, the following comparisons are made for a DNS request that arrives with the domain **198.51.100.0.example.com**:

- **198.51.100.0.example.com**: no match
- **51.100.0.example.com**: no match for one level down
- **100.0.example.com**: no match for two levels down
- **0.example.com**: no match for three levels down
- **example.com**: match for four levels down

Range: 0 through 10

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

dns-filter-template

Syntax

```
dns-filter-template template-name {
    client-interfaces [ client-interface-name ];
    client-routing-instance client-routing-instance-name;
    dns-filter {
        database-file filename;
        dns-resp-ttl seconds;
        dns-server [ ip-address ];
        hash-key key-string;
        hash-method hash-method-name;
        statistics-log-timer minutes;
        wildcarding-level level;
    }
    server-interfaces [ server-interface-name ];
    server-routing-instance server-routing-instance-name;
    term term-name {
        from {
            src-ip-prefix [ source-prefix ];
        }
        then {
            accept;
            dns-sinkhole;
        }
    }
}
```

Hierarchy Level

```
[edit services web-filter profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure filtering of DNS requests for disallowed website domains for requests on specific uplink and downlink logical interfaces or routing instances, or for requests from specific source IP address prefixes. The DNS filter template overrides the corresponding settings at the DNS profile level. You can configure up to 32 DNS filter templates in a profile.

Filtering can result in either:

- Blocking access to the site by sending the client a DNS response that includes an IP address or domain name of a sinkhole server instead of the disallowed domain.
- Logging the DNS request and allowing access.

Options

accept—Accept DNS requests for DNS filtering.

client-interfaces [*client-interface-name*]—(Optional) Client-facing (uplink) logical interfaces on which the DNS filter template settings are applied.

client-routing-instance *client-routing-instance-name*—(Optional) Client-facing (uplink) routing instance on which the DNS filter template settings are applied.

dns-filter-template *template-name*—Name of the DNS filter template.

dns-sinkhole—Perform the sinkhole action identified in the domain filter database for disallowed DNS requests.

server-interfaces [*server-interface-name*]—(Optional) Server-facing logical interfaces (downlink) on which the DNS filter template settings are applied.

server-routing-instance *server-routing-instance-name*—(Optional) Server-facing (downlink) routing instance on which the DNS filter template settings are applied.

NOTE: If you configure the client and server interfaces or the client and server routing instances, implicit filters are installed on the interfaces or routing instances to direct DNS traffic to the MS-MPC for DNS filtering. If you configure neither the client and server interfaces nor the routing instances, you must provide a way to direct DNS traffic to the MS-MPC (for example, via routes).

src-ip-prefix [*source-prefix*]—(Optional) Source IP address prefixes of DNS requests you want to filter. You can configure a maximum of 64 prefixes in a term. If you do not specify any source prefixes, then all DNS requests are filtered.

term *term-name*—Name for a term. You can configure a maximum of 64 terms in a template.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

drop-member-traffic (Aggregated Multiservices)

Syntax

```
drop-member-traffic {
   rejoin-timeout rejoin-timeout;
}
```

Hierarchy Level

[edit interfaces *interface-name* load-balancing-options member-failure-options]

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify whether the broadband gateway should drop traffic to a services PIC when it fails.

For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration is valid only when two or more services PICs have failed.

The remaining statement is explained separately. See CLI Explorer.

Default

If this statement is not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

- member-failure-options (Aggregated Multiservices) | 1313
- Understanding Aggregated Multiservices Interfaces | 994
- Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009

ds-lite

Syntax

```
    ds-lite ds-lite-softwire-concentrator {
        auto-update-mtu;
        flow-limit flow-limit | session-limit-per-prefix session-limit-per-prefix;
        mtu-v6 bytes;
        softwire-address softwire-address;
    }
}
```

Hierarchy Level

```
[edit services softwire softwire-concentrator]
[edit services softwires softwire-types]
```

Release Information

Statement introduced in Junos OS Release 10.4.
auto-update-mtu option introduced in Junos OS Release 10.4.
copy-dscp option introduced in Junos OS Release 11.2.
mtu-v6 option introduced in Junos OS Release 10.4.
softwire-address option introduced in Junos OS Release 10.4.
Support for DS-Lite at the **[edit services softwires softwire-types]** added in Junos OS release 20.2R1 for Next Gen Services on MX240, MX480 and MX960 routers.

Description

Configure settings for a DS-Lite concentrator used to process IPv4 packets encapsulated in IPv6.

The **ds-lite** statement is supported on MX Series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 line Multiservices PICs. Starting in Junos OS release 17.4R1, DS-Lite is supported on MX Series routers with MS-MPCs and MS-MICs.

Options

bytes—Maximum transmission unit (MTU), in bytes, for encapsulating IPv4 packets into IPv6. If the final length is greater than the configured value, the IPv6 packet is fragmented. This option is supported on MX Series routers equipped with MS-DPCs. Starting in Junos OS release 18.1R1, this option is also supported on MX Series routers with MS-MPCs or MS-MICs.

ds-lite-softwire-concentrator—Name applied to a DS-Lite softwire concentrator.

auto-update-mtu—This option is not currently supported.

copy-dscp—Copy DSCP information to IPv4 headers during decapsulation.

flow-limit—Maximum number of IPv4 flows per softwire.

Range: 0 through 16384 flows

Range: 0 through 9192 bytes

session-limit-per-prefix—Maximum number of sessions per B4 subnet prefix. This option is supported on MX Series routers equipped with MS-DPCs. Starting in Junos OS Release 18.2R1, this option is also supported on MS-MPCs and MS-MICs.

Range: 0 through 16384 sessions

softwire-address—Address of the DS-Lite softwire concentrator.

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

RELATED DOCUMENTATION

Configuring a DS-Lite Softwire Concentrator | 389

dscp (Services CoS)

Syntax

```
dscp (alias | bits);
```

Hierarchy Level

```
[edit services cos application-profile profile-name (ftp | sip) (data | video | voice)],
[edit services cos rule rule-name term term-name then],
[edit services cos rule rule-name term term-name then reverse]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define the Differentiated Services code point (DSCP) mapping that is applied to the packets. Change the DSCP (or TOS) on the packet to the specified value. Any conformant bit string can be specified, but only the default alias can be used.

Options

alias—Name assigned to a set of CoS markers.

bits—Mapping value in the packet header.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in CoS Rules | **826**.

Configuring CoS Rules on Services PICs

dynamic

Syntax

```
dynamic {
    ike-policy policy-name;
    ipsec-policy policy-name;
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define a dynamic IPsec SA.

Options

ike-policy *policy-name*—Name of the IKE policy. This statement is optional for the non-preshared-key authentication method. For digital signature-based authentication, this statement is optional and the default policy is used if none is supplied.

ipsec-policy *policy-name*—Name of the IPsec policy. This statement is optional and the default policy is used if none is supplied.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

ecmp-alb

Syntax

```
ecmp-alb {
    apply-groups;
    apply-groups-except;
    tolerance;
}
```

Hierarchy Level

```
[edit chassis]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Enable adaptive load balancing for equal-cost multipath (ECMP) next hops.

> **NOTE:** The **ecmp-alb** statement can be enabled only when the **[edit chassis network-services enhanced-ip]** statement is configured.
>
> Starting in Junos OS Release 20.1R1, you can configure adaptive load balancing for ECMP next hops on multiple Packet Forwarding Engines on the same line card for even distribution of the traffic and redundancy.

Options

apply-groups—Specify the groups from which to inherit configuration data.

apply-groups-except—Specify the groups from which configuration data should not be inherited.

tolerance—Specify the adaptive tolerance in percentage.

Default: 20%.

Required Privilege Level

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

ei-mapping-timeout

Syntax

```
mapping-timeout seconds;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

ei-mapping-timeout statement introduced in JUNOS Releases 12.3.

Description

Specify the duration for endpoint independent translations that use the specified NAT pool. This includes endpoint-independent mapping (EIM) and endpoint-independent filtering (EIF).

Options

seconds—Lifetime of endpoint independent mappings in seconds.

Default: 300

Range: 120 through 864,000

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Configuration Overview | 101

eif-flow-limit

Syntax

```
eif-flow-limit number-of-flows
```

Hierarchy Level

```
[editservices nat rule rule-name term term-name then translated secure-nat-mapping]
```

Release Information
Statement introduced in Junos OS Release 12.3

Description
Specify the maximum number of inbound flows allowed on EIF mapping to the configured value. This limit is per EIF mapping and is per given instance of time. For example, if **eif-flow-limit** is configured as n, then only n inbound connections are allowed at a given instance of time, The n+1 and subsequent connections arriving when n connections are alive are dropped . A new inbound connection is allowed only when one of the n connections times out or is closed. This limit is applied for all type of flows.

Starting in Junos OS Release 15.1R3, **eif-flow-limit** is also supported on the MS-MPC and MS-MIC.

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

RELATED DOCUMENTATION

Protecting CGN Devices Against Denial of Service (DOS) Attacks | 409

enable-rejoin (Aggregated Multiservices)

Syntax

```
enable-rejoin;
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options member-failure-options redistribute-all-traffic]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Enable the failed member to rejoin the aggregated Multiservices (AMS) interface after the member comes back online.

For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration allows the failed members to rejoin the pool of active members automatically.

Default

If you do not configure this option, then the failed members do not automatically rejoin the **ams** interface even after coming back online.

Required Privilege Level

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

RELATED DOCUMENTATION

- redistribute-all-traffic (Aggregated Multiservices) | **1393**
- Understanding Aggregated Multiservices Interfaces | **994**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

enable-descriptive-session-syslog

Syntax

```
enable-descriptive-session-syslog;
```

Hierarchy Level

```
edit services service-set service-set-name service-set-options
```

Release Information
Statement introduced in Junos OS Release 20.3 for MX Series routers.

Description
Display descriptive information of session logs.

You can enable syslog to display information related to inside and outside packets, byte count, and the session id for both open and close sessions.

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

RELATED DOCUMENTATION

service-set-options | 1459

encapsulation

Syntax

```
encapsulation type;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the logical link-layer encapsulation type.

Options

atm-mlppp-llc—For ATM2 IQ physical interfaces only, use Multilink Point-to-Point Protocol (MLPPP) over AAL5 LLC encapsulation.

frame-relay-ppp—For Frame Relay circuits, use Frame Relay PPP encapsulation.

multilink-ppp—By default, voice services logical interfaces use MLPPP encapsulation.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Encapsulation for Voice Services | 1029

Junos OS Network Interfaces Library for Routing Devices

encryption

Syntax

```
encryption {
    algorithm algorithm;
    key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level

[edit services ipsec-vpn **rule** *rule-name* **term** *term-name* **then manual** direction *direction*]

Release Information

Statement introduced before Junos OS Release 7.4.
aes-128-cbc, **aes-192-cbc**, and **aes-256-cbc** options added in Junos OS Release 7.6.

Description

Configure an encryption algorithm and key for manual SA.

Options

algorithm—Type of encryption algorithm. The algorithm can be one of the following:

- **des-cbc**—Has a block size of 8 bytes (64 bits); the key size is 48 bits long.
- **3des-cbc**—Has a block size of 8 bytes (64 bits); the key size is 192 bits long.
- **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
- **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
- **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

> **NOTE:** For **3des-cbc**, the first 8 bytes should differ from the second 8 bytes, and the second 8 bytes should be the same as the third 8 bytes.

key—Type of encryption key. The key can be one of the following:

- **ascii-text**—ASCII text key. Following are the key lengths, in ASCII characters, for the different encryption options:
  - **des-cbc** option, 8 ASCII characters
  - **3des-cbc** option, 24 ASCII characters
  - **aes-128-cbc** option, 16 ASCII characters

  - **aes-192-cbc** option, 24 ASCII characters
  - **aes-256-cbc** option, 32 ASCII characters
- **hexadecimal**—Hexadecimal key. Following are the key lengths, in hexadecimal characters, for the different encryption options:
  - **des-cbc** option, 16 hexadecimal characters
  - **3des-cbc** option, 48 hexadecimal characters
  - **aes-128-cbc** option, 32 hexadecimal characters
  - **aes-192-cbc** option, 48 hexadecimal characters
  - **aes-256-cbc** option, 64 hexadecimal characters

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

RELATED DOCUMENTATION

Configuring Security Associations | 639

encryption-algorithm

Syntax

```
encryption-algorithm algorithm;
```

Hierarchy Level

```
[edit services ipsec-vpn ike proposal proposal-name],
[edit services ipsec-vpn ipsec proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
aes-128-cbc, **aes-192-cbc**, and **aes-256-cbc** options added in Junos OS Release 7.6.
aes-128-gcm, **aes-192-gcm**, and **aes-256-gcm** options added in Junos OS Release 17.3R1.

Description

Configure an IKE or IPsec encryption algorithm.

Options

3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long.

aes-128-cbc—Advanced Encryption Standard (AES) 128-bit encryption algorithm.

aes-192-cbc—AES 192-bit encryption algorithm.

aes-256-cbc—AES 256-bit encryption algorithm.

> **NOTE:** In Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.

aes-128-gcm—(IPsec only) Advanced Encryption Standard in Galois/Counter Mode (AES-GCM) 128-bit encryption algorithm with a 16 octet integrity check value (ICV). This can only be used on an MS-MPC or MS-MIC.

aes-192-gcm—(IPsec only) AES-GCM 192-bit encryption algorithm with a 16 octet ICV. This can only be used on an MS-MPC or MS-MIC.

aes-256-gcm—(IPsec only) AES-GCM 256-bit encryption algorithm with a 16 octet ICV. This can only be used on an MS-MPC or MS-MIC.

des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

Configuring IPsec Proposals | 680

establish-tunnels

Syntax

```
establish-tunnels (immediately | on-traffic | responder-only);
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced in Release 8.5 of Junos OS.
responder-only option added in Junos OS Release 18.2R1.

Description

Specify when IKE is activated: immediately after VPN information is configured and configuration changes are committed, or only when data traffic flows. In the second case, IKE needs to be negotiated with the peer gateway. Starting in Junos OS Release 18.2R1, you can also specify that the MX Series router only responds to IKE negotiations.

> **NOTE:** The *immediately* option is required to tear down the st0 interface when dead peer detection (DPD) protocol is configured.

Options

immediately—IKE is activated immediately after VPN configuration and configuration changes are committed.

on-traffic—IKE is activated only when data traffic flows. IKE needs to be negotiated with the peer gateway.

responder-only—Responds to IKE negotiations that are initiated by the peer gateway, but does not initiate IKE negotiations. This option is required when another vendor's peer gateway expects the protocol and port values in the traffic selector from the initiating gateway, which the MX Series does not provide.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Junos VPN Site Secure | 618

f-max-period

Syntax

```
f-max-period number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number compression rtp],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number compression rtp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the maximum number of compressed packets allowed between the transmission of full headers in a compressed Real-time Transport Protocol (RTP) traffic stream.

Options

number—Maximum number of packets.

Default: 256

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | 1027

facility-override

Syntax

facility-override *facility-name*;

Hierarchy Level

[edit interfaces *interface-name* services-options sysloghost *hostname*]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Override default facility for system log reporting.

Options
facility-name—Name of facility that overrides the default assignment.

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

RELATED DOCUMENTATION

Junos OS Services Interfaces Library for Routing Devices

facility-override (Service Sets)

Syntax

```
facility-override facility-name;
```

Hierarchy Level

```
[edit services service-set service-set-name syslog host hostname]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Override the default facility for system log reporting.

Options

facility-name—Name of the facility that overrides the default assignment. Valid entries are:

- **authorization**
- **daemon**
- **ftp**
- **kernel**
- **local0** through **local7**
- **user**

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

facility-override (System Log Reporting)

Syntax

```
facility-override facility-name;
```

Hierarchy Level

```
[edit services l2tp tunnel-group group-name syslog host hostname]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Override the default facility for system log reporting.

Options

facility-name—Name of the facility that overrides the default assignment. Valid entries include:

- **authorization**
- **daemon**
- **ftp**
- **kernel**
- **local0** through **local7**
- **user**

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging of L2TP Tunnel Activity | 1044

family (Aggregated Multiservices)

Syntax

```
family family;
```

Hierarchy Level

```
[edit interfaces interface-name unit interface-unit-number]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure protocol family information for the logical interface.

Options

family—Protocol family. Currently, only one option, **inet** (IP version 4 suite), is supported.

Required Privilege Level

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

RELATED DOCUMENTATION

- unit (Aggregated Multiservices) | **1585**
- Understanding Aggregated Multiservices Interfaces | **994**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

family (Interfaces)

Syntax

```
family inet {
   address address {
      ...
   }
   service {
      input {
         [ service-set service-set-name <service-filterfilter-name> ];
         post-service-filter filter-name;
      }
      output {
         [ service-set service-set-name <service-filter filter-name> ];
      }
   }
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure protocol family information for the logical interface.

Options

family—Protocol family. Valid settings for service interfaces include **inet** (IPv4) and **mpls**.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Network Interfaces Library for Routing Devices for other statements that do not affect services interfaces.

Configuring the Address and Domain for Services Interfaces | 34

Junos OS Network Interfaces Library for Routing Devices

family (Voice Services)

Syntax

```
family (inet | mlppp | ...) {
    address address {
        ...
    }
    bundle interface-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure protocol family information for the logical interface.

Options

family—Protocol family:

- **inet**—IP version 4
- **mlppp**—MLPPP

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

> *Junos OS Network Interfaces Library for Routing Devices* for other statements that do not affect services interfaces.
>
> Configuring Network Interfaces for Voice Services | **1031**
>
> *Junos OS Network Interfaces Library for Routing Devices*

filtering-type

Syntax

```
filtering-type endpoint-independent;
```

Hierarchy Level

[edit**services** nat **rule (Services NAT)** *rule-name* **term (Services NAT)** *term-name* **then (Services NAT) translated**]

Release Information
Statement introduced in JUNOS Release 10.1.

Description
Specify the NAT filtering behavior for sessions initiated from outside to inside.

Options
endpoint-independent—Currently, the only valid setting specifies endpoint-independent filtering behavior.

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | **106**

force-entry (IDS MS-DPC)

Syntax

```
(force-entry | ignore-entry);
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify handling of entries in the IDS events cache when using the MS-DPC:

- **force-entry**—Ensure that the entry has a permanent place in the IDS cache after one event is registered.
- **ignore-entry**—Ensure that all IDS events are ignored.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

forwarding-class (Services PIC Classifiers)

Syntax

```
forwarding-class class-name;
```

Hierarchy Level

```
[edit services cos application-profile profile-name (ftp | sip) (data | video | voice)],
[edit services cos rule rule-name term term-name then],
[edit services cos rule rule-name term term-name then reverse]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Assign the packets to the specified forwarding class.

Options

class-name—Name of the target application.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in CoS Rules | 826.

forwarding-class (Services CoS Fragmentation Properties)

Syntax

```
forwarding-class class-name {
   (fragment-threshold bytes | no-fragmentation);
   multilink-class number;
}
```

Hierarchy Level

```
[edit class-of-service fragmentation-maps]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, define a forwarding class name and associated fragmentation properties within a fragmentation map.

The **fragment-threshold** and **no-fragmentation** statements are mutually exclusive.

Default

If you do not include this statement, the traffic in forwarding class ***class-name*** is fragmented.

Options

class-name—Name of the forwarding class.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces | 839

fragment-limit

Syntax

```
fragment-limit number-of-fragments;
```

Hierarchy Level

```
[edit interfaces interface-name services-options]
[edit security flow]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement added in Junos OS Release 20.3R1 for Next Gen Services on MX240, MX480, and MX960 routers.

Description

Configure the maximum number of fragments permitted in a packet before the packet is dropped.

Options

number-of-fragments—Maximum number of fragments permitted.

Range: 1 to 250 fragments.

Default: 250 fragments.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces | 42

fragment-threshold (Forwarding Class Maps)

Syntax

```
fragment-threshold bytes;
```

Hierarchy Level

```
[edit class-of-service fragmentation-maps forwarding-class class-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, set the fragmentation threshold for an individual forwarding class.

Default

If you do not include this statement, the fragmentation threshold you set at the **[edit interfaces *interface-name* unit *logical-unit-number*]** or **[edit interfaces *interface-name* mlfr-uni-nni-bundle-options]** hierarchy level is the default for all forwarding classes. If you do not set a maximum fragment size anywhere in the configuration, packets are fragmented if they exceed the smallest maximum transmission unit (MTU) of all the links in the bundle.

Options

bytes—Maximum size, in bytes, for multilink packet fragments. Any nonzero value must be a multiple of 64 bytes.

Range: 128 through 16,320 bytes

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces | 839

fragment-threshold (Interfaces LSQ)

Syntax

```
fragment-threshold bytes;
```

Hierarchy Level

```
[edit interfaces lsq-fpc/pic/port unit logical-unit-number],
[edit logical-systems logical-system-name interfaces lsq-fpc/pic/port unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For voice services interfaces, set the fragmentation threshold, in bytes.

Options

bytes—Maximum size, in bytes, for multilink packet fragments. The value must be a multiple of 64 bytes, because zero is also a multiple of 64 bytes.

Range: 128 through 16,320 bytes

Default: 0 bytes (no fragmentation)

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Delay-Sensitive Packet Interleaving | 1028

fragmentation-map

Syntax

```
fragmentation-map map-name;
```

Hierarchy Level

```
[edit class-of-service interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For AS PIC link services IQ (**lsq**) and virtual LSQ redundancy (**rlsq**) interfaces, associate a fragmentation map with a multilink PPP interface or MLFR FRF.16 DLCI.

Default

If you do not include this statement, traffic in all forwarding classes is fragmented.

Options

map-name—Name of the fragmentation map.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Fragmentation by Forwarding Class Overview*
- *Configuring Fragmentation by Forwarding Class*
- *Configuring Fragmentation by Forwarding Class*
- *Example: Configuring Fragmentation by Forwarding Class*
- *Configuring Drop Timeout Interval for Fragmentation by Forwarding Class*
- fragmentation-maps | 1215

fragmentation-maps

Syntax

```
fragmentation-maps {
    map-name {
        forwarding-class class-name {
            drop-timeout milliseconds;
            fragment-threshold bytes;
            multilink-class number;
            no-fragmentation;
        }
    }
}
```

Hierarchy Level

```
[edit class-of-service]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For Multiservices and Services PIC link services IQ (**lsq**) and virtual LSQ redundancy (**rlsq**) interfaces, define fragmentation properties for individual forwarding classes.

Default

If you do not include this statement, traffic in all forwarding classes is fragmented.

Options

map-name—Name of the fragmentation map.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

Fragmentation by Forwarding Class Overview

from (Services CoS)

Syntax

```
from {
    application-sets set-name;
    applications [ application-names ];
    destination-address address;
    destination-prefix-list list-name <except>;
    source-address address;
    source-prefix-list list-name <except>;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Specify input conditions for a CoS term.

Options

For information on match conditions, see the description of firewall filter match conditions in the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

from (IDS MS-DPC)

Syntax

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

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify input conditions for the IDS term when using the MS-DPC.

Options

For information on match conditions, see the description of firewall filter match conditions in the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

from (PCP)

Syntax

```
from {
    application-sets set-name;
    applications [ application-name ];
    destination-address address <except>;
    destination-address-range high maximum-value low minimum-value <except>;
    destination-port high maximum-value low minimum-value;
    destination-prefix-list list-name <except>;
    source-address address <except>;
    source-address-range high maximum-value low minimum-value <except>;
    source-prefix-list list-name <except>;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the match conditions for a PCP rule term. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

from

Syntax

```
from {
    destination-address address;
    ipsec-inside-interface interface-name;
    source-address address;
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify input conditions for the IPsec term.

Options

For information on match conditions, see the description of firewall filter match conditions in the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

from (Services NAT)

Syntax

```
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-port range high maximum-value low minimum-value;
    source-address address (address | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify input conditions for the NAT term.

Options

For information on match conditions, see the description of firewall filter match conditions in the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

from (Services Stateful Firewall)

Syntax

```
from {
    application-sets set-name;
    applications [ application-names ];
    destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
    destination-address-range low minimum-value high maximum-value <except>;
    destination-prefix-list list-name <except>;
    source-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
    source-prefix-list list-name <except>;
}
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify input conditions for a stateful firewall term.

Options

For information on match conditions, see the description of firewall filter match conditions in the *Routing Policies, Firewall Filters, and Traffic Policers User Guide*.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Stateful Firewall Rules | 546

ftp (Services CoS)

Syntax

```
ftp {
    data {
        dscp (alias | bits);
        forwarding-class class-name;
    }
}
```

Hierarchy Level

[edit services cos application-profile *profile-name* ftp]

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** value for FTP.

Default

By default, the system does not alter the DSCP or forwarding class for FTP traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

sip (Application Profile)

gate-timeout

Syntax

```
gate-timeout seconds;
```

Hierarchy Level

```
[edit applications application ike-esp-nat]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

For an IKE ALG application, configure the length of time that can pass after IKE establishes the security association between the IPsec client and server and before the ESP traffic starts in both directions. If the ESP traffic has not started before this timeout value, the ESP gates are deleted and the ESP traffic is blocked.

The IKE ALG enables the passing of IKEv1 and IPsec packets through NAPT-44 and NAT64 rules between IPsec peers that are not NAT-T compliant.

Options

seconds—Number of seconds.

Default: 120 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

ALG Descriptions | 466
Configuring Application Sets | 501
Configuring Application Properties | 502

global-dns-stats-log-timer

Syntax

```
global-dns-stats-log-timer minutes;
```

Hierarchy Level

```
[edit services web-filter profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the interval for logging per-client statistics for filtering of DNS requests for disallowed website domains.

Options

minutes—The number of minutes in the logging interval.

Default: 5

Range: 0 through 60

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

group (Traffic Load Balancer)

Syntax

```
group group-name {
    health-check-interface-subunit health-check-interface-subunit;
    network-monitoring-profile [profile-name1, <profile-name2>];
    real-service-rejoin-options no-auto-rejoin;
    real-services [server-list];
    <routing-instance routing-instance>;
}
```

Hierarchy Level

```
[edit services traffic-load-balance instance instance-name]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure a group of servers as a pool for next-hop session distribution.

Options

group-name—Use the specified string identifier for a group of servers to which sessions are distributed using the server distribution table in conjunction with the session distribution API.

group health-check-interface-subunit *health-check-interface-subunit*—Use the specified subunit of the ms- interface used for health checking.

network-monitoring-profile *profile-name1*—Name of the network monitoring profile used to monitor the health of servers in the group.

network-monitoring-profile *profile-name2*—(Optional) Name of a second network monitoring profile used to monitor the health of servers in the group.

real-services *server-list*—Use the specified list of individual servers to which sessions are distributed using the server distribution table in conjunction with the session distribution API.

real-services-rejoin-options no-auto-rejoin—Disable the default behavior that allows a server to rejoin the group automatically when it comes up.

routing-instance *routing-instance*—(Optional) Use the specified routing instance if the default **inet.0** is not used.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Traffic Load Balancer Overview | **970**

Configuring TLB | **979**

gw-interface

Syntax

```
gw-interface interface-name.logical-unit-number;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options local-gateway address]
```

Release Information

Statement introduced in Junos OS Release 17.2 on MX Series.

Description

Enable the cleanup of IKE triggers and IKE and IPsec SAs when an IPsec tunnel's local gateway IP address goes down or the MS-MIC or MS-MPC being used in the tunnel's service set goes down. If the local gateway IP address for an IPsec tunnel's service set goes down or the MS-MIC or MS-MPC that is being used in the service set goes down, the service set no longer sends IKE triggers. In addition, when the local gateway IP address goes down, the IKE and IPsec SAs are cleared for next-hop service sets, and go to the Not Installed state for interface-style service sets. The SAs that have the Not Installed state are deleted when the local gateway IP address comes back up.

If the local gateway IP address that goes down is for the responder peer, then you need to manually clear the IKE and IPsec SAs on the initiator peer so that the IPsec tunnel comes back up once the local gateway IP address comes back up (see **clear services ipsec-vpn ike security-associations** and **clear services ipsec-vpn ipsec security-associations**).

Options

interface-name—Name of the interface of the IPsec local gateway.

logical-unit-numer—Number of the logical unit of the IPsec local gateway interface. You must include the logical unit number.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

hash-keys (Aggregated Multiservices)

Syntax

```
hash-keys {
    egress-key (destination-ip | source-ip);
    ingress-key (destination-ip | source-ip);
}
```

Hierarchy Level

[edit services service-set *service-set-name* interface-service load-balancing-options]

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure the hash keys used for load balancing in aggregated multiservices (AMS) for service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). The hash keys supported in the ingress and egress direction are the source IP address and destination IP address.

Hash keys are used to define the load-balancing behavior among the various members in the AMS group. For example, if **hash-keys** is configured as **source-ip**, then the hashing would be performed based on the source IP address of the packet. Therefore, all packets with the same source IP address land on the same member. Hash keys must be configured with respect to the traffic direction: ingress or egress. For example, if **hash-keys** is configured as **source-ip** in the ingress direction, then it should be configured as **destination-ip** in the egress direction. This is required to ensure that the packets of the same flow reach the same member of the AMS group.

The configuration of the ingress and egress hash keys is mandatory if you are using AMS for NAT. This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen. Refer to Table 35 on page 1230 for the supported hash keys.

The resource-triggered option enables anchor session PICs to use the load or resource information from the anchor services PICs to select the AMS member will anchor the services for the subscriber for load balancing among AMS members. In addition, for mobile subscriber-aware services (such as HTTP header enrichment), you must configure the **resource-triggered** statement, which means that the load balancing is not done using the ingress and egress keys.

Table 35: Hash Keys Supported for AMS for Service Applications

	Service Set at Ingress Interface		Service Set at Egress Interface	
Hash Keys for NAT				
NAT Type	Ingress hash key	Egress hash key	Ingress hash key	Egress hash key
source static	Destination IP address	Source IP address	Source IP address	Destination IP address
source dynamic	Source IP address	Destination IP address	Destination IP address	Source IP address
Network Address Port Translation (NAPT)	Source IP address	Destination IP address	Destination IP address	Source IP address
destination static	Source IP address	Destination IP address	Destination IP address	Source IP address
Hash Keys for Stateful Firewall				
Stateful Firewall	Destination IP address	Source IP address	Destination IP address	Source IP address
Stateful Firewall	Source IP address	Destination IP address	Source IP address	Destination IP address

NOTE: If NAT is used in the service set (along with stateful firewall and ALG), then the hash keys should be based on the NAT type; otherwise, the hash keys of the stateful firewall should be used.

Options

> **NOTE:** The **egress-keys** option is hidden and is deprecated in Junos OS Release 15.1 and later, and is only maintained for backward compatibility. It might be removed completely in a future software release. Load-balancing or steering of traffic occurs, based on the hash keys in the forward direction. Load-balancing of traffic also occurs, based on the hash keys in the reverse direction except in dynamic NAT scenarios (dynamic NAT, NAT64, and NAPT44). For interface-style services, the ingress hash-key is used for the forward direction and the egress hash-key is used for the reverse direction. These hash-keys are configured within the service-set definition by using the **ingress-key** and **egress-key** statements at the **[edit services service-set *service-set-name* interface-service load-balancing-options]** hierarchy level. For next-hop style services, the ingress hash-key on the inside-domain next-hop is used in the forward direction and the ingress hash-key (not the egress hash-key) on outside-domain next-hop is used for the reverse direction. These hash-keys are configured at the logical AMS interface level by using the **ingress-key** and **egress-key** statements at the **[edit interfaces ams*N* unit *logical-unit-number* load-balancing-options hash-keys]** hierarchy level.

ingress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing in the ingress flow direction.

ingress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing in the ingress flow direction.

egress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction. The configuration is mandatory if you are using AMS for Network Address Translation (NAT). This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen.

egress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction.

Required Privilege Level

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

RELATED DOCUMENTATION

load-balancing-options | **1278**

hash-keys (Interfaces)

Syntax

```
hash-keys {
    egress-key (source-ip | destination-ip);
    ingress-key (source-ip | destination-ip);
    ipv6-source-prefix-length ipv6-source-prefix-length;
}
```

Hierarchy Level

```
[edit interfaces unit unit-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
ipv6-source-prefix-length option introduced in Junos OS Release 18.2R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card. The **ipv6-source-prefix-length** option is not supported for Next Gen Services.

Description

Configure the hash keys used for load balancing in aggregated multiservices (AMS) for next-hop style services. The hash keys supported in the ingress and egress direction are the source IP address and destination IP address.

Hash keys are used to define the load-balancing behavior among the various members in the AMS. For example, if **hash-keys** is configured as **source-ip**, then the hashing is performed based on the source IP address of the packet, so that all packets with the same source IP address land on the same member. When you use **ingress-key** and **egress-key**, you must configure hash keys to take the traffic direction into consideration. For example, if you configure **hash-keys** as **source-ip** in the ingress direction, then you must configure **hash-keys** as **destination-ip** in the egress direction. This is required to ensure that the packets of the same flow reach the same member of the AMS group.

If you are configuring an AMS interface used in a service set for DS-Lite,

The remaining statements are explained separately. See CLI Explorer.

Options

egress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction.

egress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction.

ingress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the ingress flow direction.

ingress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the ingress flow direction.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Load Balancing on AMS Infrastructure | **1004**

header-integrity-check

Syntax

```
header-integrity-check {
    enable-all;
}
```

Hierarchy Level

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

Release Information
Statement introduced in Release 13.2.

Description
Configure Junos OS to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information and to flag such anomalies and errors.

Starting in Junos OS release 17.1R1, the header integrity check on the MS-MPC or MS-MIC drops any packets with header anomalies and includes the following checks:

- ICMP ping of death
- IP unknown protocol
- TCP no flag
- TCP SYN FIN
- TCP FIN no ACK

NOTE: The **header-integrity-check** option that is supported on MS-MICs and MS-MPCs to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information and flag such anomalies and errors has a functionality that is opposite to the functionality caused by passive mode tunneling. If you configure both the **header-integrity-check** statement and the **passive-mode tunneling** statement on MS-MICs and MS-MPCs, and attempt to commit such a configuration, an error is displayed during commit.

The passive mode tunneling functionality (by including the **passive-mode-tunnelin** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level) is a superset of the capability to disable IPsec tunnel endpoint in the traceroute output (by including **no-ipsec-tunnel-in-traceroute** statement at the **[edit services ipsec-vpn]** hierarchy level). Passive mode tunneling also bypasses the active IP checks and tunnel MTU check in addition to not treating an IPsec tunnel as a next-hop as configured by the **no-ipsec-tunnel-in-traceroute** statement.

Required Privilege Level

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

RELATED DOCUMENTATION

service-set-options | **1459**

Configuring Protection Against Network Attacks on an MS-MPC | **601**

hello-interval (L2TP)

Syntax

```
hello-interval seconds;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the keepalive timer for L2TP tunnels.

Options

seconds—Interval, in seconds, after which the server sends a hello message if no messages are received. A value of **0** means that no hello messages are sent.

Range: 0 through 3600

Default: 60 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Timers for L2TP Tunnels | **1043**

Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

hide-avps

Syntax

```
hide-avps;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Hide L2TP attribute-value pairs if the secret shared between the two ends of the tunnel is known.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Default

Attribute-value pairs that can be hidden are exposed, even if the secret information is known.

Required Privilege Level

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

RELATED DOCUMENTATION

Hiding Attribute-Value Pairs for L2TP Tunnels | 1043

high-availability-options (Aggregated Multiservices)

Syntax

```
high-availability-options {
    (many-to-one | one-to-one) {
        preferred-backup preferred-backup;
    }
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the high availability options for the aggregated multiservices (AMS) interface. For service applications, if only the load-balancing feature is being used, then this configuration is optional.

For many-to-one (N:1) high availability support for service applications like Network Address Translation (NAT), the preferred backup services PIC, in hot standby mode, backs up one or more (N) active services PICs.

> **NOTE:** In both cases, if one of the active services PICs goes down, then the backup replaces it as the active PIC. When the failed PIC comes back up, it becomes the new backup. This is called *floating backup*.

One-to-one (1:1) high availability support associates a single backup interface with a single active interface. 1:1 configuration is supported only on the MS-MPC and MX-SPC3. In 1:1 (stateful) configurations, synchronization causes the active and back up PICs to synchronize traffic states and data structures, preventing data loss during a failover event. Stateful synchronization is required for IPsec high availability support. For IPsec connections, AMS supports 1:1 configuration only.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

load-balancing-options | 1278

Understanding Aggregated Multiservices Interfaces | 994

Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009

hint

Syntax

```
hint [ hint-strings ];
```

Hierarchy Level

[edit **services** nat **pool** *nat-pool-name* **pgcp**]

Release Information
Statement introduced in Junos OS Release 9.0.

Description
Configure a hint that enables the border gateway function (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 three 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 *xx* hint *yy*]**.

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

host (L2TP)

Syntax

```
host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
}
```

Hierarchy Level

```
[edit services l2tp tunnel-group group-name syslog]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the hostname for the system logging utility.

Options

hostname—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging of L2TP Tunnel Activity | 1044

host (service-set)

Syntax

```
host hostname {
    class {
        alg-logs;
        deterministic-nat-configuration-log;
        ids-logs;
        nat-logs;
        packet-logs;
        pcp-logurlf-logs;
        session-logs <open | close>;
        stateful-firewall-logs;
        urlf-logs;
    }
    facility-override facility-name;
    interface-service prefix-value;
    log-prefix prefix-value;
    port port-number;
    services severity-level;
    source-address source-address;
}
```

Hierarchy Level

```
[edit services service-set service-set-name syslog]
```

Release Information

Statement introduced before Junos OS Release 7.4.
class option introduced in Junos OS Release 13.2.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.

Description

Specify the hostname for the system logging utility.

Starting in Junos OS Release 17.4R1, you can configure up to a maximum of four system log servers (combination of local system log hosts and remote system log collectors) for each service set at the **[edit services service-set *service-set-name*]** hierarchy level.

NOTE: Starting with Junos OS release 14.1X55, 14.2R5, 15.1R3, and 16.1R1, for multiservices (ms-) interfaces, you cannot configure system logging for PCP and ALGs by including the pcp-logs and alg-logs statements at the **[edit services service-set *service-set-name* syslog host *hostname* class]** hierarchy level. An error message is displayed if you attempt to commit a configuration that contains the pcp-logs and alg-logs options to define system logging for PCP and ALGs for ms- interfaces.

Options

hostname—Name of the system logging utility host machine.

From Junos OS Release 17.4R1, you can configure up to four system log hosts.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

hot-standby

Syntax

```
hot-standby;
```

Hierarchy Level

```
[edit interfaces rlsqnumber redundancy-options],
[edit interfaces rlsqnumber:number redundancy-options]
[edit interfaces rspnumber redundancy-options]
[edit interfaces rmsnumber redundancy-options]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

For one-to-one AS, rsp, or rms redundancy configurations, specify that the failure detection and recovery must take place in less than 5 seconds. For FRF.15 (MLFR) and FRF.16 (MFR) configuration, specify the switch over time of 5 seconds and less for FRF.15 and a maximum of 10 seconds for FRF.16.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912

Configuring AS or Multiservices PIC Redundancy | 29

icmp-code

Syntax

```
icmp-code value;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Internet Control Message Protocol (ICMP) code value.

Options

value—The ICMP code value. For a complete list, see "Configuring the ICMP Code and Type" on page 507.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | 466
- Configuring Application Sets | 501
- Configuring the ICMP Code and Type | 507
- Examples: Configuring Application Protocols | 524
- Verifying the Output of ALG Sessions | 525

icmp-fragment-check (IDS MS-MPC)

Syntax

```
icmp-fragment-check;
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Identify and drop ICMP packets that are IP fragments. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**
Understanding IDS on an MS-MPC | **597**

icmp-large-packet-check (IDS MS-MPC)

Syntax

```
icmp-large-packet-check;
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Identify and drop ICMP packets that are larger than 1024. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**
Understanding IDS on an MS-MPC | **597**

icmp-type

Syntax

```
icmp-type value;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

ICMP packet type value.

Options

value—The ICMP type value, such as **echo** or **echo-reply**. For a complete list, see "Configuring the ICMP Code and Type" on page 507.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring the ICMP Code and Type | **507**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

ids-rules

Syntax

```
ids-rules [rule-name];
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the intrusion detection service (IDS) rules included in this service set. You can configure multiple rules. If the service set is on an MS-MPC, only the first IDS input rule and the first IDS output rule are used.

Options

rule-name—Identifier for the rule to be included.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | **21**

Configuring Protection Against Network Attacks on an MS-MPC | **601**

ids-rule-sets

Syntax

(ids-rule-sets *rule-set-name*);

Hierarchy Level

[edit services service-set *service-set-name*]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the intrusion detection service (IDS) rule set included in this service set. You can configure only one rule set for each service. If the service set is on an MS-MPC, only the first IDS input rule and the first IDS output rule are used.

Options
rule-set-name—Identifier for the set of rules to be included.

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

RELATED DOCUMENTATION

Configuring Service Rules | 21
Configuring Protection Against Network Attacks on an MS-MPC | 601

ignore-entry

See
force-entry

ike

Syntax

```
ike {
    proposal proposal-name {
        authentication-algorithm (sha1 | sha-256 | sha-384);
        authentication-method (ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group2 | group5 |group14 | group15 | group16 | group19 | group20 | group24);
        encryption-algorithm algorithm;
        lifetime-seconds seconds;
    }
    policy policy-name {
        description description;
        local-certificate identifier;
        local-id (ipv4_addr ipv4-address | ipv6-addr ipv6-address | key-id identifier);
        version (1 | 2);
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
        remote-id {
            any-remote-id;
            ipv4_addr [ values ];
            ipv6_addr [ values ];
            key_id [ values ];
        }
    }
}
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure IKE.

The remaining statements are explained separately.

NOTE: In Junos FIPS mode, the **aggressive** option of the **mode** statement is not supported.

NOTE: In Junos FIPS mode, ECDSA options of the **authentication-method** statement are not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | **665**

Configuring IKE Policies | **671**

ike-access-profile

Syntax

```
ike-access-profile profile-name;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Define the access profile for the IPsec traffic on dynamic tunnels.

Options

profile-name—Identifier for access profile, which must match the name configured at the **[edit access profile *name* client * ike]** hierarchy level.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Dynamic Endpoints for IPsec Tunnels | 750

Configuring IPsec Service Sets | 698

inactivity-timeout

Syntax

```
inactivity-timeout seconds;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the inactivity timeout period, in seconds.

Options

seconds—Length of time the application is inactive before it times out.

Default: 14,400 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring the Inactivity Timeout Period | **512**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

initiate-dead-peer-detection

Syntax

```
initiate-dead-peer-detection;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 9.2 for IKEv1.
Support for IKEv2 introduced in Junos OS Release 11.4.

Description

Enable triggering of dead peer detection (DPD) hello messages to the remote peer for the specified tunnel.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Configuring IPsec Rules | **688**
- dead-peer-detection | **1142**
- backup-remote-gateway | **1111**

input (Interfaces)

Syntax

```
input {
    service-set service-set-name <service-filter filter-name>;
    post-service-filter filter-name;
}
```

Hierarchy Level

```
[edit interface interface-name unit logical-unit-number family inet service],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the input service sets and filters to be applied to traffic.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Filters and Services to Interfaces | 25

instance (Traffic Load Balancer)

Syntax

```
instance instance-name {
    client-interface client-interface;
    client-vrf client-vrf;
    group group-name {
        health-check-interface-subunit health-check-interface-subunit;
        network-monitoring-profile profile-name;
        real-service-rejoin-options no-auto-rejoin;
        real-services [ server-list ];
        <routing-instance routing-instance>;
    }
    interface interface-name;
    real-service real-service {
        address server-ip-address;
        admin-down;
    }
    server-inet-bypass-filter server-inet-bypass-filter ;
    server-inet6-bypass-filter server-inet6-bypass-filter ;
    server-interface server-interface;
    server-vrf server-vrf-name;
    virtual-service virtual-service-name {
        address virtual-ip–address;
        group group-name;
        load-balance-method {
            hash {
                hash-key method;
            }
            random;
        }
        mode (layer2-direct-server-return | direct-server-return | translated);
        <routing-instance routing-instance-name>;
        <routing-metric route-metric>;
        server-interface server-interface;
        service service-name {
            protocol (udp | tcp);
            server-listening-port port;
            virtual-port virtual-port;
        }
    }
}
```

Hierarchy Level

[edit services traffic-load-balance]

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure a Traffic Load Balancer instance.

Options

client-interface *client-interface*——For translated mode, client interface where the implicit filter is installed to direct the traffic in the forward direction.

client-vrf *client-vrf*—Use the specified name of the routing instance in which the data traffic in the reverse direction is routed to the clients.

instance *instance-name*—Identifier (text string) for a TLB configuration.

server-inet-bypass-filter *server-inet-bypass-filter*—Name of the firewall filter from which the terms are referenced and added to the server-side implicit filters. This enables the operator to bypass reverse (RIP to VIP) translation of IPv4 traffic.

server-inet6-bypass-filter *server-inet6-bypass-filter*—Name of the firewall filter from which the terms are referenced and added to the server-side implicit filters. This enables the operator to bypass reverse (RIP to VIP) translation of IPv6 traffic.

server-interface *server-interface*—For translated mode, specifies the server interfaces where the server filters are implicitly installed to direct the return traffic to the load balancing next hop.

server-vrf *server-vrf-name*—The routing instance in which the data traffic in the forward direction is routed to the servers

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | **970**

Configuring TLB | **979**

interface

Syntax

```
interface interface-name.unit-number;
```

Hierarchy Level

```
[edit services service-interface-pools pool pool-name]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Add logical service interfaces to the pool of service interfaces.

Options

interface-name.unit-number—Name and logical unit number of the service interface.

- All interfaces in a pool must belong to the same service PIC or DPC.
- All interfaces assigned to the same service must be in the same pool.
- Logical interfaces cannot be in more than one pool.
- All interfaces must have either **family inet** or **family inet6** configured.
- Logical unit 0 cannot be configured in a service interface pool.
- You can configure up to 1000 logical interfaces in a service interface pool.

Required Privilege Level

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

RELATED DOCUMENTATION

Session Border Control Solutions Guide Using BGF and IMSG

interface-service (Services Interfaces)

Syntax

```
interface-service {
    load-balancing-options {
        hash-keys {
            egress-key (destination-ip | source-ip);
            ingress-key (destination-ip | source-ip);
        }
    }
    service-interface name;
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the device name for the interface service Physical Interface Card (PIC).

Options

service-interface *name*—Name of the service device associated with the interface-wide service set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

interfaces (Aggregated Multiservices)

Syntax

```
interfaces interface-name {
    load-balancing-options {
        hash-keys {
            egress-key (source-ip | destination-ip);
            ingress-key (source-ip | destination-ip);
        }
        high-availability-options {
            (many-to-one | one-to-one) {
                preferred-backup preferred-backup;
            }
        }
        member-failure-options {
            drop-member-traffic {
                rejoin-timeout rejoin-timeout;
            }
            redistribute-all-traffic {
                enable-rejoin;
            }
        }
        member-interface interface-name;
    }
    redundancy-options {
        primary mams-a/b/0;
        secondary mams-a/b/0;
    }
    unit interface-unit-number {
        family family;
    }
}
```

Hierarchy Level

```
[edit]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure the aggregated Multiservices (AMS) interface. The AMS interface provides the infrastructure for load balancing and high availability (HA).

Options

interface-name—Name of a valid aggregated multiservices interface (ams)—for example, ams0 or ams1.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Load Balancing on AMS Infrastructure | **1004**
- Understanding Aggregated Multiservices Interfaces | **994**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

interfaces (Voice Services)

Syntax

```
interfaces { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Configure interfaces on the router.

Default
The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

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

RELATED DOCUMENTATION

Junos OS Network Interfaces Library for Routing Devices

interval

Syntax

```
interval seconds;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then dead-peer-detection]
```

Release Information

Statement introduced in Junos OS Release 11.4.
IKEv2 support introduced in Junos OS Release 17.2.

Description

Specify the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet. The **interval** value is used for IKEv1 security associations (SAs). Starting in Junos OS Release 17.2R1, the **interval** value is also applicable to IKEv2 SAs. In Junos OS Release 17.1 and earlier, the **interval** option is not applicable to IKEv2 SAs, which use the default value.

Options

seconds—Number of seconds that the peer waits before sending a DPD request packet.

Range: 1 through 180 seconds

Default: 10 seconds

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

ipsec

Syntax

```
ipsec {
    proposal proposal-name {
        authentication-algorithm (hmac-sha-256);
        description description;
        encryption-algorithm algorithm;
        lifetime-seconds seconds;
        protocol (esp | bundle);
    }
    policy policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2 |group5 |group14 |group15 | group16 | group24);
        }
        proposals [ proposal-names ];
    }
}
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure IPsec.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

ipsec-inside-interface

Syntax

```
ipsec-inside-interface interface-name;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Specify the interface name for next-hop-style service sets. This value is also implicitly generated in dynamic endpoint tunneling.

Options

interface-name—Service interface for internal network.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

Configuring Dynamic Endpoints for IPsec Tunnels | 750

ipsec-vpn-options

Syntax

```
ipsec-vpn-options {
    anti-replay-window-size bits;
    clear-dont-fragment-bit;
    ike-access-profile profile-name;
    local-gateway address;
    no-certificate-chain-in-ike;
    no-anti-replay;
    passive-mode-tunneling;
    trusted-ca [ ca-profile-names ];
    tunnel-mtu bytes;
    udp-encapsulation {
        <udp-dest-port destination-port>;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify IP Security (IPsec) service options.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698
Configuring Service Rules | 21

ipsec-vpn-rules

Syntax

```
(ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
```

Hierarchy Level

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the IPsec rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.

Options
rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

RELATED DOCUMENTATION

Configuring Service Rules | 21

ipv6-multicast-interfaces

Syntax

```
ipv6-multicast-interfaces (all | interface-name) {
    disable;
}
```

Hierarchy Level

```
[edit services nat],
[edit services softwire]
```

Release Information

Statement introduced in Junos OS Release 9.1.

Description

Enable multicast filters on Ethernet interfaces when IPv6 NAT is used for neighbor discovery.

Options

all—Enable filters on all interfaces.

disable—Disable filters on the specified interfaces.

interface-name—Enable filters on a specific interface only.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPv6 Multicast Interfaces | 391

l2tp-access-profile

Syntax

```
l2tp-access-profile profile-name;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the profile used to validate all L2TP connection requests to the local gateway address.

Options

profile-name—Identifier for the L2TP connection profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Access Profiles for L2TP Tunnel Groups | **1041**

Configuring an L2TP Access Profile on the LNS

l2tp-interface-id

Syntax

```
l2tp-interface-id name;
(dedicated | shared);
```

Hierarchy Level

```
[edit interfaces sp-fpc/pic/port unit logical-unit-number interface],
[edit logical-systems logical-system-name interfaces sp-fpc/pic/port unit logical-unit-number interface]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the L2TP options for configuring logical interfaces for group and user sessions.

Options

(**dedicated** | **shared**)—Specifies whether a logical interface can host one (dedicated) or multiple (shared) sessions at one time.

name—Interface identifier that must be replicated at the **[edit access profile *name*]** hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Services Interfaces Library for Routing Devices

land-attack-check

Syntax

```
land-attack-check (ip-only | ip-port );
```

Hierarchy Level

```
[edit services service-set service-set-name nat-options]
```

Release Information

Statement introduced with Junos OS Release 12.3.

Description

Enable land attack checks based on either IP address only or both IP address and IP port number.

> **NOTE:** If you do not configure this statement, there is no land attack check for hairpinning NAT packets.

Options

ip-only—Land attack check is based on IP address only.

ip-port—Land attack check is based on IP address and IP port number.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | 21
max-sessions-per-subscriber | 1309

land-attack-check (IDS MS-MPC)

Syntax

```
land-attack-check (ip-only | ip-port);
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Identify and drop SYN packets that have the same source and destination address or port, which provides protection against land attacks. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Options

ip-only—Identify and drop SYN packets that have the same source and destination address.

ip-port—Identify and drop SYN packets that have the same source and destination address and port.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

learn-sip-register

Syntax

```
learn-sip-register;
```

Hierarchy Level

[edit **applications application** *application-name*]

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Learn potential incoming SIP calls by inspecting the SIP register method.

More information: You can enable the router to accept any incoming SIP calls for the endpoint devices that are behind the NAT firewall. When a device behind the firewall registers with the proxy that is outside the firewall, the AS or Multiservices PIC maintains the registration state. When the **learn-sip-register** statement is enabled, the router can use this information to accept inbound calls. If this statement is not configured, no inbound calls are accepted; only the devices behind the firewall can call devices outside the firewall.

> **NOTE:** You can manually inspect the SIP register by running the **show services stateful-firewall sip-register** command. This command is not supported for the MX240.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring SIP | **514**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

lifetime-seconds

Syntax

```
lifetime-seconds seconds;
```

Hierarchy Level

```
[edit services ipsec-vpn ike proposal proposal-name],
[edit services ipsec-vpn ipsec proposal proposal-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the lifetime of an IKE or IPsec SA. This statement is optional.

Options

seconds—Lifetime

Default: 3600 seconds (IKE); 28,800 seconds (IPsec)

Range: 180 through 86,400

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- Configuring IKE Proposals | **665**
- Configuring IPsec Proposals | **680**
- Configuring Security Associations | **639**

link-layer-overhead

Syntax

```
link-layer-overhead percent;
```

Hierarchy Level

```
[edit interfaces interface-name mlfr-uni-nni-bundle-options],
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, configure the percentage of total bundle bandwidth to be set aside for link-layer overhead. Link-layer overhead accounts for the bit stuffing on serial links. Bit stuffing is used to prevent data from being interpreted as control information. Overhead resulting from link-layer encapsulation and framing is computed automatically.

Options

percent—Percentage of total bundle bandwidth to be set aside for link-layer overhead.

Range: 0 through 50 percent

Default: 0 percent

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Scheduling Queues on Logical LSQ Interfaces | 834

limit-ports-per-address

Syntax

```
limit-ports-per-address number;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

Statement introduced in Junos OS Release 16.1.

Description

Specify the limit for number of ports allocated per host (IP address).

Options

number—Number of ports allocated per host (IP address).

Range: 2 through 65,435

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Pools of Addresses and Ports for Network Address Translation Overview | 103

load-balance

Syntax

```
load-balance {
    per-packet;
    random;
}
```

Hierarchy Level

```
[edit policy-options policy-statement policy-name then]
```

Release Information

Statement introduced in Junos OS Release 14.2.

Description

Specify the type of load balancing of an equal-cost multipath (ECMP) in the forwarding table.

Options

per-packet—Load-balance on a per-packet basis.

random—Load-balance using packet random spray.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Junos OS Routing Protocols and Policies Configuration Guide for Security Devices

load-balancing-options (Aggregated Multiservices)

Syntax

```
load-balancing-options {
    high-availability-options {
        (many-to-one | one-to-one) {
            preferred-backup preferred-backup;
        }
    }
    member-failure-options {
        drop-member-traffic {
            rejoin-timeout rejoin-timeout;
        }
        redistribute-all-traffic {
            enable-rejoin;
        }
    }
    hash-keys {
        egress-key (destination-ip | source-ip);
        ingress-key (destination-ip | source-ip);
    }
    member-interface interface-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the high availability (HA) options for the aggregated multiservices (AMS) interface.

Many-to-one (N:1) high availability mode for service applications like Network Address Translation (NAT) is supported. In the case of N:1 high availability mode, one services PIC is the backup (in hot standby mode) for one or more (N) active services PICs. If one of the active services PICs goes down, then the backup replaces it as the active services PIC. When the failed PIC comes back online, it becomes the new backup. This is called *floating backup mode*. In an N:1 (stateless) configuration, traffic states and data structures are not synchronized between active PICs and the backup PIC.

You can also configure a one-to-one (1:1) high availability mode. In the 1:1 configuration, a single interface is configured as the backup for another single active interface. If the active interface goes down, the backup interface replaces it as the active interface. A 1:1 (stateful) configuration synchronizes traffic states and data structures between the active services PIC and the backup services PIC. This is required for IPsec connections. One-to-one high availability is supported on the MS-MPC but it is not supported for MX-SPC3 in this release.

Load-balancing might not be uniform among member interfaces in certain network deployments. The variance can be because of a misconfiguration, which causes the traffic itself not to be sufficiently randomly distributed, causing the hash keys to be ineffective (for example, the hash key is destination IP but all sessions have only source IP address). The variation can be within the expected range and the load balancing depends on the IP addresses chosen. The hash calculation performs a checksum on several bits of the IP address and not only on the last few lower significant bits of the IP address. In such a scenario, the load-balancing ratio can change, for instance, if the source IP address is changed from 20.0.0.0/24 to 20.0.1.0/24.

The distribution of traffic across member interfaces of an AMS interface is static load-balancing. Flows are load balanced based on a packet hash on parameters such as source IP or destination IP. Load-balancing effectiveness depends on the IP address or protocol diversity. For example, if the hash key is destination IP and all packets have the same destination, then all flows are directed to the same member. This is flow-level load balancing and not per packet. As a result, traffic between a pair of addresses may be 10,000 pps, whereas another pair of addresses may have 1 pps. The load of the former is not distributed among members. High availability is limited to stateless HA. When a backup interface takes over as an active interface, all flows are reestablished (for example. packets may undergo NAT processing differently after failover).

With a stateful firewall, static NAT as basic-nat44 or destination-nat44, and dynamic NAT as nat64, napt-44, dynamic-nat44, and with application layer gateways (ALGs) configured, NAT hairpinning is not supported. Input direction for rule match to be applied is supported only for dynamic NAT types (NAT64, NAT44, and dynamic-NAT44). Service-set policies need to have input or input-output direction only. Flows on all active members are reset when the number of actives changes. The resetting of flows can be avoided at the cost of failed-member's traffic loss using certain options.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces | **994**

Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

load-balancing-options (Service Set)

Syntax

```
load-balancing-options {
    hash-keys {
        egress-key (destination-ip | source-ip);
        ingress-key (destination-ip | source-ip);
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS 11.4.

Description

Configure the load-balancing options for aggregated multiservices (AMS) in service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). AMS for service applications can be used for load balancing with or without high availability (HA). Currently, load balancing is based on the configured hash keys.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces | 994

Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009

local-certificate

Syntax

```
local-certificate identifier;
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name]
```

Release Information

Statement introduced in Junos OS Release 7.5.

Description

Name of the certificate that needs to be sent to the peer during the IKE authentication phase.

Options

identifier—Name of certificate.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

local-gateway (IPSec)

Syntax

```
local-gateway address <gw-interface interface-name.logical-unit-number>;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the local IPv4 or IPv6 address for the IPsec traffic.

NOTE: You cannot use a VRRP *virtual-address* for defining the local-gateway address.

Options

address—Local address.

The remaining statement is explained separately.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Service Rules | 21

local-gateway (L2TP LNS)

Syntax

```
local-gateway {
    address address;
    gateway-name gateway-name;
}
```

Hierarchy Level

[edit services l2tp **tunnel-group** *name*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the IP address or name for the local (LNS) gateway for L2TP tunnel.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Options

address—Local IP address; corresponds to the IP address that is used by LACs to identify the LNS. When the LAC is an MX Series router, this address matches the remote gateway address configured in the LAC tunnel profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Local Gateway Address and PIC | **1042**.

Configuring L2TP Tunnel Groups | **1041**

Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

local-id

Syntax

```
local-id (distinguished-name container container-string-values |wildcard wildcard-string-values ipv4_addr ipv4-address |
    ipv6-addr ipv6-address | key-id identifier fqdn fqdn);
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
ipv6_addr option added in Junos OS Release 7.6.

Description

Specify local identifiers for IKE Phase 1 negotiation. This statement is optional.

Options

ipv4_addr *ipv4-address*—IPv4 address identification value.

ipv6_addr *ipv6-address*—IPv6 address identification value.

key_id *identifier*—Key identification value.

fqdn *fqdn*—Fully-qualified domain name.

distinguished-name container *container-string-values* |wildcard *wildcard-string-values*—One or more distinguished name values.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

log-prefix (L2TP)

Syntax

```
log-prefix prefix-value;
```

Hierarchy Level

```
[edit services l2tp tunnel-group group-name syslog host hostname]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Set the system logging prefix value.

Options

prefix-value—System logging prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging of L2TP Tunnel Activity | 1044

log-prefix (Services)

Syntax

```
log-prefix prefix-value;
```

Hierarchy Level

```
[edit services service-set service-set-name syslog host hostname]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Set the system logging prefix value.

Options

prefix-value—System logging prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

logging (Services)

Syntax

```
logging {
    traceoptions {
        file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 8.0.

Description

Define global services properties.

Options

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Tracing Services PIC Operations | 38

logging (IDS MS-DPC)

Syntax

```
logging {
    syslog;
    threshold rate;
}
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Set logging values for this IDS term when using the MS-DPC.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

lsq-failure-options

Syntax

```
lsq-failure-options {
    no-termination-request;
    trigger-link-failure interface-name;
}
```

Hierarchy Level

```
[edit interfaces lsq-fpc/pic/port]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, define the failure recovery option settings.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Association between LSQ and SONET Interfaces | 909

manual

Syntax

```
manual {
   direction (inbound | outbound | bidirectional) {
      authentication {
         algorithm (hmac-md5-96 | hmac-sha1-96);
         key (ascii-text key | hexadecimal key);
      }
      auxiliary-spi spi-value;
      encryption {
         algorithm algorithm;
         key (ascii-text key | hexadecimal key);
      }
      spi spi-value;
      protocol (ah | esp | bundle);
   }
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define a manual IPsec SA.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

many-to-one (Aggregated Multiservices)

Syntax

```
many-to-one {
    preferred-backup preferred-backup;
}
```

Hierarchy Level

[edit interfaces *interface-name* load-balancing-options high-availability-options]

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the many-to-one (N:1) preferred backup for the aggregated multiservices (AMS) interface.

> **NOTE:** The preferred backup must be one of the member interfaces (mams–) that have already been configured at the [**edit interfaces *interface-name* load-balancing-options**] hierarchy level. Even in the case of mobile control plane redundancy, which is one-to-one (1:1), the initial preferred backup is configured at this hierarchy level.

Options

preferred-backup *preferred-backup*—Use the specified interface as the preferred backup member interface. The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

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

RELATED DOCUMENTATION

high-availability-options (Aggregated Multiservices) | **1238**

Understanding Aggregated Multiservices Interfaces | **994**

map-e

Syntax

```
map-e name {
    disable-auto-route;
    ea-bits-len ea-bits-len;
    ipv4-prefix ipv4-prefix;
    mape-prefix mape-prefix;
    mtu-v6 mtu-v6;
    psid-length psid-length;
    psid-offset psid-offset;
    softwire-address softwire-address;
    v4-reassembly;
    v6-reassembly;
    version-03;
}
```

Hierarchy Level

```
[edit services softwire softwire-concentrator]
[edit services softwires softwire-types
```

Release Information

Statement introduced in Junos OS Release 18.2R1 for MX Series Routers with MPC and MIC interfaces. Support added in Junos OS release 20.2R1 at MAP-E for Next Gen Services on MX240, MX480, and MX960 routers.

Description

Configure Mapping of Address and port – Encapsulation (MAP-E) as an inline service on MX Series routers that use MPC and MIC interfaces. MAP-E is an automatic tunneling mechanism that encapsulates IPv4 packets within an IPv6 address. The IPv4 packets are carried in an IPV4-over-IPV6 tunnel from the MAP-E Customer Edge (CE) devices to the MAP-E Provider Edge (PE) devices (also called as Border Relay (BR) devices) through an IPV6 routing topology, where they are de-tunneled for further processing.

Options

disable-auto-route—Disable auto-routes and enable static routes to facilitate ECMP load balancing.

NOTE: When you enable the **disable-auto-route** option, you must configure static routes.

name—Name of the MAP-E softwire concentrator.

ea-bits-len—Configure rule for Embedded Address (EA) length for the MAP-E domain.

NOTE:

- If **v4-prefix-len** is 0 then **ea-bits-len** must be non-zero, and vice versa.
- It is possible that **ea-bits-len** is equal to 0, but **psid-len** is non-zero.
- If the sum of **v4-prefix-len** and **ea-bits-len** is less than 32, then the **psid-len** must be equal to the difference between 32 and the sum total of **v4-prefix-len** and **ea-bits-len**.

Range: 0 through 48

ipv4-prefix—Configure rule for IPv4 prefix and length of the MAP-E domain.

Range: 0 through 32

mape-prefix—Configure rule for IPV6 prefix and length for the MAP-E domain. The MAP-E IPv4 and IPv6 prefix must be unique per softwire concentrator.

mtu-v6—(Optional) Specify the Maximum transmission unit (MTU) for the MAP-E softwire tunnel.

Default: 9192

Range: 1280 through 9192

psid-length—Configure Port Set ID (PSID) length value for the MAP-E domain.

NOTE:

- If the sum of **v4-prefix-len** and **ea-bits-len** is less than 32, then the **psid-len** must be equal to the difference between 32 and the sum total of **v4-prefix-len** and **ea-bits-len**.

Range: 0 through 16

psid-offset—(Optional) Configure PSID offset value for the MAP-E domain.

Default: 4

Range: 0 through 16

softwire-address—Specify the Border Relay device unicast IPv6 address as the softwire concentrator IPV6 address.

v4-reassembly | v6-reassembly—(Optional) Enable IPv4 and IPv6 reassembly for MAP-E.

version-03—(Optional) Configure version number to distinguish between currently supported version of the Internet draft draft-ietf-softwire-map-03 (expires on July 28, 2013), *Mapping of Address and Port with Encapsulation (MAP)* and the latest available version.

Required Privilege Level

system

mapping-refresh

Syntax

```
mapping-refresh (inbound | outbound | inbound-outbound);
```

Hierarchy Level

[edit **services** nat **rule** *rule-name* **term** *term-name* **then translated secure-nat-mapping**]

Release Information
Statement introduced in Junos OS Release 12.3

Description
Specify how the flow timer should be refreshed based on the mapping refresh configured for all types of fwnat flows.

When configured, **tcp-tickles** sends tickles to both directions irrespective of mapping-refresh direction.

Starting in Junos OS Release 15.1R3, **mapping-refresh** is also supported on the MS-MPC and MS-MIC.

Options
inbound—Refresh the flow timer for inbound flows only.

inbound-outbound—Refresh the flow timer for all flows.

outbound—Refresh the flow timer for outbound flows only.

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

RELATED DOCUMENTATION

Protecting CGN Devices Against Denial of Service (DOS) Attacks | 409

mapping-timeout

Syntax

```
mapping-timeout seconds;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

mapping-timeout statement introduced in JUNOS Release 10.1.

> **NOTE:** This configuration option has been replaced by **app-mapping-timeout**. This option is currently retained only for backward compatibility.

Description

Specify the duration for mappings that use the specified NAT pool.

Options

seconds—Lifetime of mappings in seconds.

Default: 300

Range: 120 through 864,000

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101

mapping-type

Syntax

```
mapping-type endpoint-independent;
```

Hierarchy Level

[edit **services** nat **rule (Services NAT)** *rule-name* **term (Services NAT)** *term-name* **then (Services NAT) translated**]

Release Information
Statement introduced in JUNOS Release 10.1.

Description
Specify the source NAT mapping type.

Options
endpoint-independent—Currently, the only valid setting specifies endpoint-independent mapping behavior.

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | **106**

match-direction (Services CoS)

Syntax

```
match-direction (input | output | input-output);
```

Hierarchy Level

```
[edit services cos rule rule-name]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Specify the direction in which the rule match is applied.

Options

input—Apply the rule match on the input side of the interface.

output—Apply the rule match on the output side of the interface.

input-output—Apply the rule match bidirectionally.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

match-direction (IDS)

Syntax

```
match-direction (input | output | input-output);
```

Hierarchy Level

```
[edit services ids rule rule-name]
```

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.

input-output—Apply the rule match bidirectionally.

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

Configuring Protection Against Network Attacks on an MS-MPC | 601

match-direction

Syntax

```
match-direction (input | output);
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name]
```

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.

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

match-direction (Services NAT)

Syntax

```
match-direction (input | output);
```

Hierarchy Level

```
[edit services nat rule rule-name]
```

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.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

match-direction (PCP)

Syntax

```
match-direction (input | output);
```

Hierarchy Level

```
[edit services pcp rule rule-name]
```

Release Information
Statement introduced in Junos OS Release 13.2R1.

Description
Specify the direction in which the rule match is applied. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options
input—Apply the rule match on input.

output—Apply the rule match on output.

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

match-direction (Services Stateful Firewall)

Syntax

```
match-direction (input | output | input-output);
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name]
```

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 the input side of the interface.

output—Apply the rule match on the output side of the interface.

input-output—Apply the rule match bidirectionally.

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

RELATED DOCUMENTATION

Configuring Stateful Firewall Rules | 546

match-rules-on-reverse-flow

Syntax

```
match-rules-on-reverse-flow;
```

Hierarchy Level

```
[edit services service-set service-set-name cos-options]
```

Release Information

Statement introduced in Junos OS Release 16.1R5 and 17.4R1.

Description

Configure the service set to create a CoS session even if a packet is first received in the reverse direction of the matching direction of the CoS rule. The CoS rule values are then applied as soon as a packet in the correct match direction is received.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring CoS Rules | 823

max-drop-flows

Syntax

```
max-drop-flows {
    ingress ingress-flows;
    egress egress-flows;
}
```

Hierarchy Level

[edit services **service-set** *service-set-name*]

Release Information
Statement introduced in Junos OS Release 12.3

Description
Configure the maximum drop flows allowed per ingress and egress direction. The configuration is per service set. The configured limits indicate the maximum number of drop flows that can be created at a given instance of time in both directions. If max drop flows ingress is 10 and egress is 5 then at a given instance of time maximum of 10 ingress drop flows and 5 egress drop flows can be present. Two counters, one for each direction ingress and egress, are to be added to service set stateful-firewall statistics to track the number of drop flows not created due to the drop flow limits exceeded. These limits applies to all types of drop flows i.e., TCP, UDP, ICMP etc. Ingress drop flows are forward flows for match-direction input rules and reverse flows for match-direction output rules. Similarly egress drop flows are reverse flows for match-direction input and forward flows for match-direction output rules. The limits are applied cumulatively on all the nat rules associated with the service-set.

If you specify the maximum drop flows to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for maximum drop flows.

Options
ingress-flows—Maximum number of drop flows on the ingress interface.

egress-flows—Maximum number of drop flows on the egress interface.

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

RELATED DOCUMENTATION

Configuring Service Set Limitations | 23

max-flows

Syntax

```
max-flows number;
```

Hierarchy Level

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Maximum number of flows allowed for the service set.

Options
number—Maximum number of flows.

> **NOTE:** When an aggregated multiservices (AMS) interface is configured as the service interface for a service set, the **max-flow** value configured for the service set is applied to each of the member interfaces in the AMS interface. That is, if you have configured 1000 as the **max-flow** value for a service set that uses an AMS interface with four active member interfaces, each of the member interfaces can handle 1000 flows each, resulting in an effective **max-flow** value of 4000.

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

RELATED DOCUMENTATION

Configuring Service Set Limitations | 23

max-session-setup-rate (Service Set)

Syntax

```
max-session-setup-rate (number | numberk);
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.1R1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Set the maximum number of session setups allowed per second for the service set. After this setup rate is reached, any additional session setup attempts are dropped. If you do not include the **max-session-setup-rate** statement, the session setup rate is not limited.

Options

max-session-setup-rate *number*—Use the specified maximum number of session setups per second.

Range: 1 through 429,496,729

Default: 0 (The session setup rate is not limited.)

numberk—Maximum number of sessions, expressed in thousands. Starting in Junos OS Release 18.4R1, 1k=1000. Prior to Junos OS Release 18.4R1, 1k=1024.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Set Limitations | 23

max-sessions-per-subscriber

Syntax

```
max-sessions-per-subscriber session-number;
```

Hierarchy Level

```
[edit services service-set service-set-name nat-options]
```

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Set the maximum number of sessions from a single subscriber allowed for NAPT-44. This statement does not apply to other types of NAT. The maximum number of sessions per subscriber is 32,000 sessions.

> **NOTE:** If you do not configure this statement, there is no limit to the number of sessions a subscriber can have.

Options

session-number —Maximum number of sessions a single subscriber can establish for NAPT-44.

Range: 1 through 32000

Default: None

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | 21

land-attack-check | 1271

maximum

Syntax

maximum *number*;

Hierarchy Level

[edit interfaces *interface-name* services-options session-limit]

Release Information

Statement introduced in Junos OS Release 9.6.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the maximum number of sessions allowed simultaneously on services cards. If you specify the maximum number of sessions to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for the maximum number of sessions.

Options

number—Maximum number of sessions.

Range: 1 through 4,294,967,295

Required Privilege Level

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

RELATED DOCUMENTATION

maximum-contexts

Syntax

```
maximum-contexts number <force>;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number compression rtp],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number compression rtp]
```

Release Information

Statement introduced in Junos OS Release 7.5.

Description

Specify the maximum number of RTP contexts to accept during negotiation.

Options

number—Maximum number of contexts.

force—(Optional) Requires the PIC to use the value specified for maximum RTP contexts, regardless of the negotiated value. This option allows the software to interoperate with Junos OS Releases that base the RTP context value on link speed.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | 1027

maximum-send-window

Syntax

```
maximum-send-window packets;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the size of the send window for L2TP tunnels, which limits the remote end's receive window size.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options

packets—Maximum number of packets the send window can hold at one time.

Default: 32

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Window Size for L2TP Tunnels | **1042**

member-failure-options (Aggregated Multiservices)

Syntax

```
member-failure-options {
   drop-member-traffic {
      rejoin-timeout rejoin-timeout;
   }
   redistribute-all-traffic {
      enable-rejoin;
   }
}
```

Hierarchy Level

[edit interfaces *interface-name* load-balancing-options]

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the possible behavior for the aggregated Multiservices (AMS) interface in case of failure of more than one active member.

> **NOTE:** The **drop-member-traffic** configuration and the **redistribute-all-traffic** configuration are mutually exclusive.

Table 36 on page 1314 displays the behavior of the member interface after the failure of the first services PIC. Table 37 on page 1314 displays the behavior of the member interface after the failure of two services PICs.

> **NOTE:** The AMS infrastructure has been designed to handle one failure automatically. However, in the unlikely event that more than one services PIC fails, the AMS infrastructure provides configuration options to minimize the impact on existing traffic flows.

Table 36: Behavior of Member Interface After One Multiservices PIC Fails

High Availability Mode	Member Interface Behavior
Many-to-one (N:1) high availability support for service applications	Automatically handled by the AMS infrastructure

Table 37: Behavior of Member Interface After Two Multiservices PICs Fail

High Availability Mode	Configuration	**rejoin-timeout**	Behavior when member rejoins before **rejoin-timeout** expires	Behavior when member rejoins after **rejoin-timeout** expires
Many-to-one (N:1) high availability support for service applications	**drop-member-traffic**	Configured	The existing traffic for the second failed member will *not* be redistributed to the other members. The first member to rejoin becomes an active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.	The existing traffic for the second failed member will *not* be redistributed to the other members. The first member will rejoin the AMS automatically. However, the other members who are rejoining will be moved to the discard state.
Many-to-one (N:1) high availability support for service applications	**redistribute-all-traffic**	Not applicable	Before rejoin, the traffic is redistributed to existing active members. After a failed member rejoins, the traffic is load-balanced afresh. This may impact existing traffic flows.	

The remaining statements are explained separately. See CLI Explorer.

Default

If **member-failure-options** are not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

load-balancing-options (Aggregated Multiservices) | 1278

Understanding Aggregated Multiservices Interfaces | 994

Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009

member-interface (Aggregated Multiservices)

Syntax

```
member-interface interface-name;
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the member interfaces for the aggregated multiservices (AMS) interface. You can configure multiple interfaces by specifying each interface in a separate statement.

Starting with Junos OS Release 16.2, an AMS interface can have up to 32 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface can have a maximum of 24 member interfaces. If you configure more than 24 member interfaces, you must set the **pic-boot-timeout** value to 240 or 300 seconds at the **[edit interfaces *interface-name* multiservice-options]** hierarchy level for every services PIC interface on the MX Series router.

For high availability service applications like Network Address Translation (NAT) that support many-to-one (N:1) redundancy, you can specify two or more interfaces.

On an MS-MPC, you can configure one-to-one (1:1) redundancy. In a 1:1 (stateful) configuration, a single backup interface provides redundancy for a single active interface. A 1:1 configuration is required for IPsec. 1:1 redundancy is not supported on the MX-SPC3 in this release.

> **NOTE:** The member interfaces that you specify must be members of aggregated multiservices interfaces (mams-).

Options

interface-name—Name of the member interface. The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces for Next Gen Services

Configuring Aggregated Multiservices Interfaces | **1001**

load-balancing-options (Aggregated Multiservices) | **1278**

message-rate-limit

Syntax

```
message-rate-limit messages-per-second
```

Hierarchy Level

```
interfaces interface-name {
    services-options {
        cgn-pic;
        disable-global-timeout-override;
        ignore-errors <alg> <tcp>;
        inactivity-non-tcp-timeout seconds;
        inactivity-tcp-timeout seconds;
        inactivity-timeout seconds;
        open-timeout seconds;
        session-limit {
            maximum number;
            rate new-sessions-per-second;
        }
        session-timeout seconds;
        syslog {
        }
    }
}
```

Release Information

Statement introduced Junos OS Release 11.1.

Description

Maximum system log messages per second allowed from this interface.

> **NOTE:** The message-rate-limit command can be configured only for physical service interfaces (**sp-*x*/*x*/*x***) and not for redundancy services PIC interfaces (**rspx**).

Options

messages-per-second——This option configures the maximum number of system log messages per second that can be formatted and sent from the PIC to either the Routing Engine (local) or to an external server (remote). The default rates are 10,000 for the Routing Engine and 800,000 for an external server.

Range: 0 through 2147483647

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

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

mlfr-uni-nni-bundles-inline

Syntax

```
mlfr-uni-nni-bundles-inline number;
```

Hierarchy Level

```
[edit chassis fpc number pic number]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Specify the number of inline multilink frame relay user-to-network interface (UNI) and network-to-network interface (NNI) bundles.

Options

number—Specify the number of inline multilink frame relay UNI NNI bundles.

Range: 1 through 255

Required Privilege Level

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

RELATED DOCUMENTATION

Inline MLPPP for WAN Interfaces Overview | 924

Example: Configuring Inline MLPPP and Multilink Frame Relay End-to-End (FRF.15) for WAN Interfaces

Example: Configuring Inline Multilink Frame Relay (FRF.16) for WAN Interfaces

mode

Syntax

```
mode (aggressive | main);
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define an IKE policy mode.

Default
main

Options
aggressive—Takes half the number of messages of main mode, has less negotiation power, and does not provide identity protection.

> **NOTE:** In Junos FIPS mode, the **aggressive** option is not supported.

main—Uses six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.

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

RELATED DOCUMENTATION

Configuring IKE Policies | 671

mss (IDS MS-DPC)

Syntax

```
mss value;
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then syn-cookie**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the maximum segment size (MSS) value used in Transmission Control Protocol (TCP) delayed binding when using the MS-DPC.

Options

value—MSS value.

Default: 1500

Range: 128 through 8192

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | **586**

multi-link-layer-2-inline

Syntax

```
multi-link-layer-2-inline;
```

Hierarchy Level

```
[edit chassis fpc number pic number]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Enable inline Layer 2 bundling services.

Required Privilege Level

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

RELATED DOCUMENTATION

Inline MLPPP for WAN Interfaces Overview | **924**

Example: Configuring Inline MLPPP and Multilink Frame Relay End-to-End (FRF.15) for WAN Interfaces

Example: Configuring Inline Multilink Frame Relay (FRF.16) for WAN Interfaces

multilink-class

Syntax

```
multilink-class number;
```

Hierarchy Level

```
[edit class-of-service fragmentation-maps map-name forwarding-class class-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, map a forwarding class into a multiclass MLPPP (MCML).

The **multilink-class** statement and **no-fragmentation** statements are mutually exclusive.

Options

number—The multilink class assigned to this forwarding class.

Range: 0 through 7

Default: None

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces | **839**
- Configuring Multiclass MLPPP on LSQ Interfaces | **927**
- *Configuring Fragmentation by Forwarding Class*
- *Junos OS Services Interfaces Library for Routing Devices*
- multilink-max-classes | **1325**

multilink-max-classes

Syntax

```
multilink-max-classes number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For link services IQ (**lsq**) interfaces only, configure the number of multilink classes to be negotiated when a link joins the bundle.

Options

number—The number of multilink classes to be negotiated when a link joins the bundle.

Range: 1 through 8

Default: None

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Multiclass MLPPP on LSQ Interfaces | 927

multiservice-options

Syntax

```
multiservice-options {
    (syslog | no-syslog);
    (core-dump | no-core-dump);
    (dump-on-flow-control);
    flow-control-options {
        down-on-flow-control;
        dump-on-flow-control;
        reset-on-flow-control;
    }
}
```

Hierarchy Level

[edit interfaces mo-*fpc/pic/port*]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For monitoring services interfaces only, configure multiservice-specific interface properties.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- *Configuring Multiservice Physical Interface Properties*
- *Junos OS Services Interfaces Library for Routing Devices*
- *passive-monitor-mode*

natt-install-interval

Syntax

```
natt-install-interval seconds ;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then dynamic]
```

Release Information

Statement introduced in Junos OS Release 20.2.

Description

Specify the duration of delay in installing IPSec SA in a NAT-T scenario soon after the IPSec SA negotiation is complete. The default value is 0 seconds.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

ipsec-vpn-rules | 1267

nat-keepalive (Services IPsec VPN)

Syntax

```
nat-keepalive seconds;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 17.4 for MX Series routers.

Description

Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.

Options

seconds —Maximum interval in seconds at which NAT keepalive packets can be sent.

Range: 1 through 300 seconds.

Default: 20 seconds.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Junos VPN Site Secure or IPSec VPN

nat-options

Syntax

```
nat-options {
    land-attack-check (ip-only | ip-port);
    max-sessions-per-subscriber session-number;
    stateful-nat64 {
        clear-dont-fragment-bit;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced with Junos OS Release 12.1.
land-attack-check and **max-sessions-per-subscriber** statements added in 13.3.

Description

Specify parameters for NAT operation.

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring Service Rules | 21
- clear-dont-fragment-bit | 1132
- land-attack-check | 1271
- max-sessions-per-subscriber | 1309
- stateful-nat64 | 1499

nat-rule-sets (Service Set)

Syntax

```
nat-rule-sets rule-set-name;
```

Hierarchy Level

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

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the Network Address Translation (NAT) rule set included in the service set. You can configure only one NAT rule set. If you specify a NAT rule set, you cannot specify a NAT rule.

Options
rule-set-name—Name of the NAT rule set.

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

RELATED DOCUMENTATION

Applying Services to Subscriber-Aware Traffic with a Service Set

nat-rules

Syntax

```
(nat-rules rule-name | nat-rule-sets rule-set-name);
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the Network Address Translation (NAT) rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | 21

Applying Services to Subscriber-Aware Traffic with a Service Set

next-hop-service

Syntax

```
next-hop-service {
    inside-service-interface interface-name.unit-number;
    outside-service-interface interface-name.unit-number;
    outside-service-interface-type interface-type;
    service-interface-pool name;
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.
service-interface-pool option added in Junos OS Release 9.3.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify interface names or a service interface pool for the forwarding next-hop service set. You cannot specify both a service interface pool and an inside or outside interface.

Options

inside-service-interface *interface-name.unit-number*—Name and logical unit number of the service interface associated with the service set applied inside the network.

outside-service-interface *interface-name.unit-number*—Name and logical unit number of the service interface associated with the service set applied outside the network.

outside-service-interface-type *interface-type*—Identifies the interface type of the service interface associated with the service set applied outside the network. For inline IP reassembly, set the interface type to local.

service-interface-pool *name*—Name of the pool of logical interfaces configured at the **[edit services service-interface-pools pool *pool-name*]** hierarchy level. You can configure a service interface pool only if the service set has a PGCP rule configured. The service set cannot contain any other type of rule.

> **NOTE:** **service-interface-pool** is not applicable for IP reassembly configuration on L2TP.

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

no-anti-replay

Syntax

```
no-anti-replay;
```

Hierarchy Level

[edit services ipsec-vpn **rule** *rule-name* **term** *term-name* **then**]

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Disable IPsec antireplay service, which occasionally causes interoperability issues for security associations.

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

no-anti-replay (Services Service Set)

Syntax

```
no-anti-replay;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Disable IPsec antireplay service for this service set, which occasionally causes interoperability issues for security associations. This statement is useful for dynamic endpoint tunnels for which you cannot configure the **no-anti-reply** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement disables the antireplay check for all the tunnels within this service set. If antireplay check has to be enabled for a particular tunnel, then set the **anti-replay-window-size** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

> **NOTE:** Setting the **anti-replay-window-size** and **no-anti-replay** statements at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level overrides the settings specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698
Configuring IPsec Rules | 688

no-certificate-chain-in-ike

Syntax

```
no-certificate-chain-in-ike;
```

Hierarchy Level

[edit services **service-set** *name* **ipsec-vpn-options**]

Release Information

Statement introduced in Junos OS Release 18.2R1 on MX Series routers.

Description

To avoid IKE fragmentation, send only the end-entity certificate for certificate-based IKE authentication instead of the full certificate chain.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

no-fragmentation

Syntax

```
no-fragmentation;
```

Hierarchy Level

```
[edit class-of-service fragmentation-maps forwarding-class class-name]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
For link services IQ (**lsq**) interfaces only, set traffic on a particular forwarding class to be interleaved, rather than fragmented. This statement specifies that no extra fragmentation header is prepended to the packets received on this queue and that static-link load balancing is used to ensure in-order packet delivery.

Static-link load balancing is done based on packet payload. For IP version 4 (IPv4) and IP version 6 (IPv6) traffic, the link is chosen based on a hash computed from the source address, destination address, and protocol. If the IP payload is Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) traffic, the hash also includes source port and destination port. For MPLS traffic, the hash includes all MPLS labels and fields in the payload, whether the MPLS payload is IPv4 or IPv6.

Default
If you do not include this statement, the traffic in forwarding class ***class-name*** is fragmented.

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

RELATED DOCUMENTATION

Configuring CoS Fragmentation by Forwarding Class on LSQ Interfaces | 839

no-ipsec-tunnel-in-traceroute

Syntax

```
no-ipsec-tunnel-in-traceroute;
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Disables displaying the IPsec tunnel endpoint in the trace route output. The IPsec tunnel is not treated as a next hop and TTL is not decremented. If the TTL becomes zero, the ICMP time exceeded message will not be generated.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

no-nat-traversal (Services IPsec VPN)

Syntax

```
no-nat-traversal;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 17.4R1 for MX Series routers.

Description

Configure to disable NAT-T at the services-set level (tunnel level). NAT-T is enabled by default therefore you must use the **no-nat-traversal** for disabling the NAT-T.

> **NOTE:** The global disable NAT-T setting at [edit services ipsec-vpn] hierarchy level overrides the default NAT-T setting at [edit service-set] hierarchy level.

Required Privilege Level

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

RELATED DOCUMENTATION

Disabling NAT-T on MX Series Routers for Handling NAT with IPsec-Protected Packets | 709

no-per-unit-scheduler

Syntax

```
no-per-unit-scheduler;
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information
Statement introduced before Junos OS Release 11.4.

Description
To enable traffic control profiles to be applied at FRF.16 bundle (physical) interface level, disable the per-unit scheduler, which is enabled by default. This statement and the **shared-scheduler** statement are mutually exclusive.

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

RELATED DOCUMENTATION

Oversubscribing Interface Bandwidth

no-termination-request

Syntax

```
no-termination-request;
```

Hierarchy Level

```
[edit interfaces interface-name ppp-options],
[edit interfaces lsq-fpc/pic/port lsq-failure-options]
```

Release Information

Statement introduced in Junos OS Release 7.4.
Support at the **[edit interfaces *interface-name* ppp-options]** hierarchy level added in Junos OS Release 8.3.

Description

Inhibit PPP termination-request messages to the remote host if the primary circuit fails.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Association between LSQ and SONET Interfaces | 909

no-translation

Syntax

```
no-translation;
```

Hierarchy Level

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

Release Information
Statement introduced in Junos OS Release 7.6.

Description
Specify that traffic is not to be translated.

The **no-translation** statement is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. The **no-translation** statement is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 15.1R1.

Options
none

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

one-to-one (Aggregated Multiservices)

Syntax

```
one-to-one {
    preferred-backup preferred-backup;
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options high-availability-options]
```

Release Information

Statement introduced in Junos OS Release 15.2.

Description

Configure a single interface to be the preferred one-to-one (1:1) backup for an active aggregated multiservices (AMS) interface. If the active interface fails, the backup interface takes over. A 1:1 (stateful) configuration synchronizes traffic states and data structures between the active and backup PICs. This is required for high availability of IPsec connections. 1:1 configuration is supported only on MS-MPCs but is not currently supported on MX-SPC3s.

> **NOTE:** The preferred backup must be one of the member interfaces (mams-) that have already been configured at the [**edit interfaces *interface-name* load-balancing-options**] hierarchy level.

Options

preferred-backup *preferred-backup*—Use the specified interface as the preferred backup member interface. The member interface format is mams-*a*/*b*/0, where *a* is the Flexible PIC Concentrator (FPC) slot number and *b* is the PIC slot number.

Required Privilege Level

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

RELATED DOCUMENTATION

high-availability-options (Aggregated Multiservices) | **1238**

Understanding Aggregated Multiservices Interfaces | **994**

Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009

output

Syntax

```
output {
   [ service-set service-set-name <service-filter filter-name> ];
}
```

Hierarchy Level

```
[edit interface interface-name unit logical-unit-number family inet service],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the output service sets and filters to be applied to traffic.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Filters and Services to Interfaces | 25

overload-pool

Syntax

```
overload-pool overload-pool-name;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Specify an address pool that can be used if the source pool becomes exhausted.

Options

overload-pool-name—Name of the overload pool.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

overload-prefix

Syntax

```
overload-prefix overload-prefix;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Specify the prefix that can be used if the source pool becomes exhausted.

Options

overload-prefix—Prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

package (Loading on PIC)

Syntax

```
package package-name;
```

Hierarchy Level

```
[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]
```

Release Information

Statement introduced in Junos OS Release 9.1.

Description

Identify a package to be loaded on the PIC. When a package is added or removed, the PIC reboots.

Options

package-name—Name of the package to be loaded on the PIC. There can be up to eight packages loaded on a PIC; however, only one data package is allowed per PIC. An error message is displayed if more than eight packages are specified.

Required Privilege Level

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

passive-mode-tunneling

Syntax

```
passive-mode-tunneling;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Allows tunneling of malformed packets. When this statement is enabled, traffic bypasses the usual active IP checks. The IPsec tunnel is not treated as a next hop and TTL is not decremented. If the packet size exceeds the tunnel MTU value, an ICMP error is not generated. Starting with Junos OS Release 13.3R4 and 14.2R1, passive mode tunneling is supported on MS-MICs and MS-MPCs.

> **NOTE:** The **header-integrity-check** option that is supported on MS-MICs and MS-MPCs to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information and flag such anomalies and errors has a functionality that is opposite to the functionality caused by passive mode tunneling. If you configure both the **header-integrity-check** statement and the **passive-mode tunneling** statement on MS-MICs and MS-MPCs, and attempt to commit such a configuration, an error is displayed during commit.
>
> The passive mode tunneling functionality (by including the **passive-mode-tunnelin** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level) is a superset of the capability to disable IPsec tunnel endpoint in the traceroute output (by including **no-ipsec-tunnel-in-traceroute** statement at the **[edit services ipsec-vpn]** hierarchy level). Passive mode tunneling also bypasses the active IP checks and tunnel MTU check in addition to not treating an IPsec tunnel as a next-hop as configured by the **no-ipsec-tunnel-in-traceroute** statement.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

pba-interim-logging-interval

Syntax

pba-interim-logging-interval *seconds*

Hierarchy Level

[edit interfaces *interface-name* services-options]

Release Information
Statement introduced in Junos OS Release 13.3.

Description
Port block allocation (PBA) generates one syslog entry per set of ports allocated to a subscriber. These logs are UDP based and can be lost in the network,especially for long running flows. Interim logging resends the above logs at a configured interval for all active blocks that have traffic on at least one block. For the MS-MIC and MS-MPC, log messages are generated for sessions which have a port in a block, even if the block has no traffic.

Options
seconds—Interval, in seconds, for re-sending of session logs

Default: 0—This indicates that interim logging is not used.

Range: 1800 to 86,400seconds.

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

RELATED DOCUMENTATION

Configuring NAT Session Logs | 361

pcp-rules

Syntax

```
pcp-rules rule-name;
```

Hierarchy Level

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

Release Information
Statement introduced in Junos OS Release 13.2R1.

Description
Specify the PCP rule to apply to the service set. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC. Starting in Junos OS Release 20.1R1, PCP is also supported for Next Gen Services.

Options
rule-name—The PCP rule to apply to the service set.

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

pcp-server

Syntax

```
pcp-server server-name;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the PCP server that handles the traffic that matches the PCP rule term.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

server-name—Name of the PCP server.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

per-unit-scheduler

Syntax

```
per-unit-scheduler;
```

Hierarchy Level

[edit interfaces *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 13.2 on 16x10GE MPC and MPC3E line cards.
Statement introduced in Junos OS Release 13.2 on PTX Series Packet Transport Routers.
Statement introduced in Junos OS Release 13.3 on MPC4E line cards.
Statement introduced in Junos OS Release 15.1 on MPC6E line cards.

Description

Enable the association of scheduler maps with logical interfaces.

CAUTION: Turning on per-unit scheduling causes the interface to reinitialize, which means all logical interfaces (units) on the interface are deleted and recreated.

When including the **per-unit-scheduler** statement, you must also include the **vlan-tagging** statement or the **flexible-vlan-tagging** statement (to apply scheduling to VLANs) or the **encapsulation frame-relay** statement (to apply scheduling to DLCIs) at the **[edit interfaces *interface-name*]** hierarchy level.

When including the **per-unit-scheduler** statement, you must also include the **guaranteed-rate** statement to ensure a minimum guaranteed rate for the logical interfaces.

NOTE: To enable per-unit scheduling on MX80 and MX104 routers, configure the **per-unit-scheduler** statement at each member physical interface level of a particular aggregated Ethernet interface as well as at that aggregated Ethernet interface level. On other routing platforms, it is enough if you include this statement at the aggregated Ethernet interface level.

NOTE: Per-unit scheduling is not supported on T1 interfaces configured on the Channelized OC12 IQ PIC.

NOTE: On Gigabit Ethernet IQ2 and IQ2-E PICs without the **per-unit-scheduler** statement, the entire PIC supports 4071 VLANs and the user can configure all the VLANs on the same port.

On Gigabit Ethernet IQ2 and IQ2-E PICs with the **per-unit-scheduler** statement, the entire PIC supports 1024 – 2 * number of ports (1024 minus two times the number of ports), because each port is allocated two default schedulers.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- *Applying Scheduler Maps and Shaping Rate to DLCIs and VLANs*
- *Example: Applying Scheduling and Shaping to VLANs*
- *Configuring Virtual LAN Queuing and Shaping on PTX Series Routers*
- *Providing a Guaranteed Minimum Rate*

perfect-forward-secrecy (Services)

Syntax

```
perfect-forward-secrecy {
    keys (group1 | group2 |group5 |group14 |group15 | group16 | group24);
}
```

Hierarchy Level

```
[edit services ipsec-vpn ipsec policy policy-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
group15, **group16**, and **group24** options added in Junos OS Release 17.4R1.

Description

Define Perfect Forward Secrecy (PFS). Creates single-use keys. This statement is optional.

Options

keys—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange. The key can be one of the following:

group1—768-bit.

group2—1024-bit.

group5—1536-bit.

group14—2048-bit.

group15—3072-bit.

group16—4096-bit.

group24—2048-bit with 256-bit Prime Order Subgroup.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Policies | 685

pgcp

Syntax

```
pgcp {
    hint [ hint-strings ];
    ports-per-session ports;
    remotely-controlled;
    transport [ transport-protocols ];
}
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

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.

pgcp-rules

Syntax

```
(pgcp-rules rule-name | pgcp-rules-sets rule-set-name);
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 8.4.

Description

Specify the Packet Gateway Control Protocol (PGCP) rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

pic-boot-timeout

Syntax

```
pic-boot-timeout (240 | 300);
```

Hierarchy Level

```
[edit interfaces interface-name multiservice-options]
```

Release Information

Statement introduced in Junos OS Release 16.2 on MX Series routers.

Description

Set the service PIC boot timeout value to 240 or 300 seconds for every services PIC on the MX Series router if you are configuring more than 24 members in an aggregated multiservices (AMS) interface. We recommend setting the boot timeout value to 240. Starting with Junos OS Release 16.2, an AMS interface can have up to 32 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface can have a maximum of 24 member interfaces.

If you do not set the timeout value to 240 or 300 and you configure an AMS interface with more than 24 members, the default value of 180 causes some of the service PICs to go offline.

Options

240—Service PIC boot timeout is set to 240 seconds.

300—Service PIC boot timeout is set to 300 seconds.

Default: 180

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Aggregated Multiservices Interfaces | 1001

policy (Services IKE)

Syntax

```
policy policy-name {
    description description;
    local-certificate identifier;
    local-id (ipv4_addr ipv4-address | ipv6-addr ipv6-address | key-id identifier);
    version (1 | 2);
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
    remote-id {
        any-remote-id;
        ipv4_addr [ values ];
        ipv6_addr [ values ];
        key_id [ values ];
    }
    respond-bad-spi max-responses
}
```

Hierarchy Level

```
[edit services ipsec-vpn ike]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define an IKE policy.

Options

policy-name—IKE policy name.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

policy (IPsec)

Syntax

```
policy policy-name {
    description description;
    perfect-forward-secrecy {
        keys (group1 | group2 |group5 |group14 |group15 | group16 | group24);
    }
    proposals [ proposal-names ];
}
```

Hierarchy Level

```
[edit services ipsec-vpn ipsec]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define an IPsec policy.

Options

policy-name—IPsec policy name.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Policies | 685

pool

Syntax

```
pool nat-pool-name {
    address ip-prefix</prefix-length>;
    address-allocation round-robin;
    address-range low minimum-value high maximum-value;
    app- mapping-timeout app-mapping-timeout;
    ei-mapping-timeout ei-mapping-timeout;
    limit-ports-per-address number;
    mapping-timeout mapping-timeout;
    pgcp {
        hint [ hint-strings ];
        ports-per-session ports;
        remotely-controlled:
    }
    port {
        automatic (sequential | random-allocation);
        range low minimum-value high maximum-value random-allocation;
        preserve-parity;
        preserve-range;
        secured-port-block-allocation {
            active-block-timeout timeout-seconds;
            block-size block-size;
            max-blocks-per-user max-blocks;
        }
    }
}
```

Hierarchy Level

```
[edit services nat]
```

Release Information

Statement introduced before Junos OS Release 7.4.
pgcp statement added 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.
address-allocation statement added in Junos OS Release 11.2.
sequential statement introduced in Junos OS Release 14.2.

Description

Specify the NAT name and properties.

Options

nat-pool-name—Identifier for the NAT address pool.

The remaining statements are explained separately. See CLI Explorer.

> **NOTE:** If you make any configuration changes to a NAT pool that has secured port block allocation configured, you must delete the existing NAT address pool, wait at least 5 seconds, and then configure a new NAT address pool. We also strongly recommend that you perform this procedure if you make any changes to the NAT pool configuration, even when secured port block allocation is not configured.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Pools of Addresses and Ports for Network Address Translation Overview | 103

pool (Service Interface)

Syntax

```
pool pool-name {
    interface interface-name.unit-number;
}
```

Hierarchy Level

```
[edit services service-interface-pools]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Configure a service interface pool for VPN aggregation for the BGF feature.

Options

pool-name—Name of the service interface pool.

The remaining options are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Interface Pools | 24

port (Services NAT)

Syntax

```
port {
    automatic (sequential | random-allocation);
    range low minimum-value high maximum-value random-allocation;
    preserve-parity;
    preserve-range;
    deterministic-port-block-allocation <block-size block-size> <include-boundary-addresses>;
    secured-port-block-allocation {
        active-block-timeout timeout-seconds;
        block-size block-size;
        max-blocks-per-user max-blocks;
    }
}
```

Hierarchy Level

```
[edit services nat pool nat-pool-name]
```

Release Information

port statement introduced before Junos OS Release 7.4.
random-allocation statement introduced in Junos OS Release 9.3.
secured-port-block-allocation statement introduced in Junos OS Release 11.2.
deterministic-port-block-allocation statement introduced in Junos OS Release 12.1.
sequential statement introduced in Junos OS Release 14.2R1.

Description

Specify the NAT pool port or range. You can configure an automatically assigned port or specify a range with minimum and maximum values.

NOTE: Starting in Junos OS Release 14.2R1, the **sequential** option is introduced to enable you to configure sequential allocation of ports. The **sequential** and **random-allocation** options available with the **port automatic** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level are mutually exclusive. You can include the **sequential** option for sequential allocation and the **random-allocation** option for random delegation of ports. By default, sequential allocation of ports takes place if you include only the **port automatic** statement at the **[edit services nat pool *nat-pool- name*]** hierarchy level.

For releases earlier than Junos OS Release 14.2R1, configure automatic sequential port assignment by using the **auto** option at the **[edit services nat pool *nat-pool-name* port automatic]** hierarchy level.

If you upgrade a router running a Junos OS release earlier than Release 14.2R1 to Release 14.2 and if the router contains the **port automatic** statement defined without the **auto** option included with the configuration, the router validates the auto option present in the configuration for sequential allocation of ports.

Options

automatic—Cause the port assignment type to be automatically performed by the router.

sequential—Allocate ports in a sequential manner. With sequential allocation, the next available address in the NAT pool is selected only when all the ports available from an address are exhausted.

minimum-value—Lower boundary for the port range.

maximum-value—Upper boundary for the port range.

NOTE: Starting with Junos OS Release 15.1R1, the preserve-port and preserve-range functionalities are supported on MX Series routers with MS-MPCs and MS-MICs.

preserve-parity—Allocate ports with same parity as the original port.

preserve-range—Preserve privileged port range after translation.

random-allocation—Allocate ports within a specified range randomly.

Other options are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Source and Destination Addresses Network Address Translation Overview | 101
Configuring Address Pools for Network Address Port Translation (NAPT) Overview | 170

port (Services Voice)

Syntax

```
port {
    minimum port-number;
    maximum port-number;
}
```

Hierarchy Level

[edit interfaces lsq-*fpc*/*pic*/*port* **unit** *logical-unit-number* **compression rtp**],
[edit logical-systems *logical-system-name* interfaces lsq-*fpc*/*pic*/*port* **unit** *logical-unit-number* **compression rtp**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For voice services interfaces only, specify a range of User Datagram Protocol (UDP) destination port numbers in which RTP compression takes place.

Options

minimum *port-number*—Specify the minimum port number.

Range: 0 through 65,535

maximum *port-number*—Specify the maximum port number.

Range: 0 through 65,535

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | 1027

port (System Log Messsages)

Syntax

```
port port-number;
```

Hierarchy Level

```
[edit interfaces interface-name services-options syslog host hostname]
```

Release Information

Statement introduced in Junos OS Release 11.1.

Description

Specify the UDP port for system log messages on the host. The default port is 514.

Options

port-number—Port number for system log messages.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging for Services Interfaces

port-forwarding

Syntax

```
port-forwarding map-name {
    destined-port;
    translated-port;
}
```

Hierarchy Level

```
[edit services nat]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Specify the mapping for port forwarding.

The **port-forwarding** statement is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, the **port-forwarding** statement is also supported on the MS-MPC and MS-MIC.

Options

map-name—Identifier for the port forwarding map.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Configuring Port Forwarding Without Destination Address Translation | 291

port-forwarding-mappings

Syntax

```
port-forwarding-mappings map-name;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Specify the name of the mapping for port forwarding in a Network Address Translation rule.

The **port-forwarding-mappings** statement is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Port forwarding on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS supports only the **dnat-44** and **twice-napt-44** translation types in NAT rules, and supports only IPv4 networks. Starting in Junos OS Release 17.4R1, the **port-forwarding-mappings** statement is also supported on the MS-MPC and MS-MIC.

Options

map-name—Identifier for the port forwarding mapping.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Configuring Port Forwarding Without Destination Address Translation | 291

ports-per-session

Syntax

```
ports-per-session ports;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name pgcp]
```

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), and forward error correction (FEC) for voice and video flows on the Multiservices PIC.

Options

number-of-ports—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.

post-service-filter

Syntax

```
post-service-filter filter-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet service input],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service input]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the filter to be applied to traffic after service processing. The filter is applied only if a service set is configured and selected. You can configure a postservice filter on the input side of the interface only.

The **post-service-filter** statement is not supported when the service interface is on an MS-MIC or MS-MPC.

Options

filter-name—Identifier for the post-service filter.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Filters and Services to Interfaces | 25

ppp-access-profile

Syntax

```
ppp-access-profile profile-name;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the profile used to validate all Point-to-Point Protocol (PPP) session requests through L2TP tunnels established to the local gateway address.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options

profile-name—Identifier for the PPP profile.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Access Profiles for L2TP Tunnel Groups | **1041**

pre-shared-key (Services IKE)

Syntax

```
pre-shared-key (ascii-text key | hexadecimal key);
```

Hierarchy Level

```
[edit services ike policy policy-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define a preshared key for an IKE policy.

Options

key—Value of preshared key. The key can be one of the following:

- **ascii-text**—ASCII text key.
- **hexadecimal**—Hexadecimal key.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

preserve-interface

Syntax

```
preserve-interface;
```

Hierarchy Level

```
[edit interfaces interface-name sonet-options aps]
```

Release Information
Statement introduced in Junos OS Release 7.6.

Description
Provide link PIC replication, providing MLPPP link redundancy at the port level. This feature is supported with SONET APS and the following link PICs:

- Channelized OC3 IQ PIC
- Channelized OC12 IQ PIC
- Channelized STM1 IQ PIC

Link PIC replication provides the ability to add two sets of links, one from the active SONET PIC and the other from the standby SONET PIC, to the same bundle. If the active SONET PIC fails, links from the standby PIC are used without triggering link renegotiation. All the negotiated state is replicated from the active links to the standby links to prevent link renegotiation.

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

RELATED DOCUMENTATION

Configuring Link State Replication for Redundant Link PICs | 915

primary (Adaptive Services Interfaces)

Syntax

```
primary interface-name;
```

Hierarchy Level

```
[edit interfaces (rsp0 | rsp1) redundancy-options]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the primary adaptive services interface.

Options
interface-name—The identifier for the AS or Multiservices PIC interface, which must be of the form **sp-*fpc/pic/port***.

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

RELATED DOCUMENTATION

Configuring AS or Multiservices PIC Redundancy | 29

primary (Link Services IQ PIC Interfaces)

Syntax

```
primary interface-name;
```

Hierarchy Level

```
[edit interfaces rlsqnumber redundancy-options]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Specify the primary Link Services IQ PIC interface.

Options

interface-name—The identifier for the Link Services IQ PIC interface, which must be of the form **lsq-*fpc*/*pic*/*port***.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912

profile (Traffic Load Balancer)

Syntax

```
profile profile-name {
    custom {
        cmd priority {
            default-real-service-status (down | up);
            expect (ascii | binary) receive-string;
            port port;
            real-service-action (down | up);
            send (ascii | binary) send-string;
        }
        protocol (tcp | udp);
    }
    failure-retries number-of-retries;
    http {
        host hostname;
        method (get | option);
        port http-port-number;
        url url;
    }
    icmp;
    probe-interval interval;
    recovery-retries number-of-recovery-retries;
    ssl-hello {
        port port;
        ssl-version;
    }
    tcp {
        port tcp-port-number;
    }
}
```

Hierarchy Level

```
[edit services network-monitoring]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure a monitoring profile that can be used for health-checking a group of TLB servers.

Options

custom—Use custom probes for server health checking.

cmd *priority*—Use the specified command priority to send for a custom probe.

Values: 1 or 2

default-real-service-status (down | up)—Assign a server status for when the probe times out. The **up** value is used when the server or the intermediate network nodes are only expected to send a negative response to a probe.

Default: down

expect (ascii | binary) *receive-string* —Use the specified ascii or binary string as an expected probe response.

Range: 1 through 512 characters

port *port*—Use the specified port for custom probes.

protocol (tcp | udp)—Use the selected protocol for custom probes.

real-service-action (down | up)—Assign a server status for when the expected response to the probe is received.

Default: down

send (ascii | binary) *send-string* —Send the specified ascii or binary string as a probe.

Range: 1 through 512 characters

failure-retries *number-of-retries*—Use the specified number of probes that are sent after which the real server is tagged as down.

Default: 5

http—Use HTTP probes for server health checking.

host *hostname*—Use the specified hostname for HTTP probes for server health checks.

method (get | option)—Use the get or option HTTP method for server health checks.

port *http-port-number*—Use the specified port number for HTTP probes.

url *url*—Use the specified URL for HTTP probes. Maximum length is 128 bytes.

icmp—Use ICMP probes for server health checking.

probe-interval *interval*—Use the specified interval of time, in seconds, at which health check probes are sent.

Default: 5

profile-name—Identifier for the network monitoring profile.

recovery-retries ***number-of-recovery-retries***—Use the specified number of successful probe attempts after which the server is declared up.

Default: 5

ssl-hello—Use a **Client Hello** for server health checks

port ***port***—Use the specified port number for **Client Hello** server health checks.

ssl-version—SSL version.

Default: 3

tcp—Use TCP probes for server health checks.

port ***tcp-port-number***—Use the specified port number for TCP probes.

Required Privilege Level

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | **970**

Configuring TLB | **979**

profile (Web Filter)

Syntax

```
profile profile-name {
dns-filter {
    database-file filename;
    dns-resp-ttl seconds;
    dns-server [ ip-address ];
    hash-key key-string;
    hash-method hash-method-name;
    statistics-log-timer minutes;
    wildcarding-level level;
}
dns-filter-template template-name {
    client-interfaces [ client-interface-name ];
    client-routing-instance client-routing-instance-name;
    dns-filter {
        database-file filename;
        dns-resp-ttl seconds;
        dns-server [ ip-address ];
        hash-key key-string;
        hash-method hash-method-name;
        statistics-log-timer minutes;
        wildcarding-level level;
    }
    server-interfaces [ server-interface-name ];
    server-routing-instance server-routing-instance-name;
    term term-name {
        from {
            src-ip-prefix [ source-prefix ];
        }
        then {
            accept;
            dns-sinkhole;
        }
    }
}
global-dns-stats-log-timer minutes;
url-filter-database filename;
(url-filter-template | template) template-name {
    client-interfaces [ client-interface-name1 client-interface-name2 ];
    disable-url-filtering;
    dns-resolution-interval minutes;
    dns-resolution-rate seconds;
```

```
    dns-retries number;
    dns-routing-instance dns-routing-instance-name;
    dns-server [ ip-address1 ip-address2 ip-address3 ];
    dns-source-interface loopback-interface-name;
    dns-routing-instance dns-routing-instance-name;
    routing-instance routing-instance-name;
    server-interfaces [ server-interface-name1 server-interface-name2 ];
    term term-name {
        from {
            src-ip-prefix [prefix1 prefix2];
            dest-port [port1 port2];
        }
        then {
            accept;
            custom-page custom-page;
            http-status-code http-status-code;
            redirect-url redirect-url;
            tcp-reset;
        }
    }
    url-filter-database filename
}
```

Hierarchy Level (starting in Junos OS Release 18.3R1

```
[edit services web-filter]
```

Hierarchy Level (before Junos OS Release 18.3R1)

```
[edit services url-filter]
```

Release Information

Statement introduced in Junos OS Release 17.2.

dns-filter, **dns-filter-templates**, **global-dns-stats-log-timer**, and **url-filter-template** options introduced in Junos OS Release 18.3R1.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Define URL filter profile or DNS filter profile.

A URL filter profile is for filtering access to disallowed URLs. A URL filter profile includes a general database setting and templates. The template settings apply to specific interfaces or to access from specific source IP address prefixes, and override the database setting at the profile level.

A DNS filter profile is used to filter DNS requests for disallowed website domains. A DNS filter profile includes general DNS filtering settings and up to 32 templates. The template settings apply to DNS requests on specific interfaces or to DNS requests from specific source IP address prefixes, and override the corresponding settings at the profile level. You can configure up to eight DNS filter profiles.

> **NOTE:** For URL filtering, use the **url-filter-template** option starting in Junos OS Release 18.3R1 and use the **template** option in Junos OS Releases before 18.3R1.

Options

profile-name—Name of the filter profile.

url-filter-database *filename*—Specify the filename of the URL filter database. This option is mandatory.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

Configuring URL Filtering | 55

proposal (Services IKE)

Syntax

```
proposal proposal-name {
    authentication-algorithm (md5 | sha1 | sha-256);
    authentication-method (ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2 | group5 |group14 | group15 | group16 | group19 | group20 | group24);
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
}
```

Hierarchy Level

```
[edit services ipsec-vpn ike]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define an IKE proposal for a dynamic SA.

> **NOTE:** In Junos FIPS mode, ECDSA options of the **authentication-method** statement are not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.

Options

proposal-name—IKE proposal name.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665

proposal (Services IPsec VPN)

Syntax

```
proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm algorithm;
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
}
```

Hierarchy Level

```
[edit services ipsec-vpn ipsec]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define an IPsec proposal for a dynamic SA.

Options

proposal-name—IPsec proposal name.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Proposals | 680

proposals

Syntax

```
proposals [ proposal-names ];
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name],
[edit services ipsec-vpn ipsec policy policy-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define a list of proposals to include in the IKE or IPsec policy.

Options

proposal-names—List of IKE or IPsec proposal names.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Proposals | 665
Configuring IPsec Proposals | 680

protocol (Applications)

Syntax

```
protocol type;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Networking protocol type or number.

Options

type—Networking protocol type. The following text values are supported:

- **ah**
- **egp**
- **esp**
- **gre**
- **icmp**
- **icmp6**
- **igmp**
- **ipip**
- **ospf**
- **pim**
- **rsvp**
- **tcp**
- **udp**

NOTE: IP version 6 (IPv6) is not supported as a network protocol in application definitions.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Sets | **501**
- Configuring Application Properties | **502**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

protocol (IPsec)

Syntax

```
protocol (ah | esp | bundle);
```

Hierarchy Level

```
[edit services ipsec-vpn ipsec proposal proposal-name],
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define an IPsec protocol for a dynamic or manual SA.

Options

ah—(Not supported on MS-MPCs and MS-MICs on MX Series routers) Use the Authentication Header protocol.

esp—Use the Encapsulating Security Payload protocol.

bundle—(Not supported on MS-MPCs and MS-MICs on MX Series routers) Use the AH and ESP protocol.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

ptsp-rules

Syntax

```
(ptsp-rules rule-name | ptsp-rules-sets rule-set-name);
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 10.2.

Description

Specify the PTSP rules or rule set included in this service set. You can configure multiple rules but only one rule set for each service.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

queues

Syntax

```
queues [ queue-numbers ];
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number compression rtp],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number compression rtp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For voice services interfaces only, assign queue numbers on which RTP compression takes place.

Options

queues *queue-numbers*—Assign one or more of the following queues: **q0**, **q1**, **q2**, and **q3**.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | 1027

real-service (Traffic Load Balancer)

Syntax

```
real-service real-service-name {
    address server-ip-address;
    admin-down;
}
```

Hierarchy Level

```
[edit services traffic-load-balance instance instance-name]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure a traffic load balancer server.

Options

admin-down—Set a server's status to Down.

real-service-name—Identifier for a server to which sessions can be distributed using the server distribution table in conjunction with the session distribution API.

server-ip-address—IP address for the server.

Required Privilege Level

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | 970

Configuring TLB | 979

reassembly-timeout

Syntax

```
reassembly-timeout seconds;
```

Hierarchy Level

```
[edit interfaces interface-name services-options]
[edit security flow]
```

Release Information

Statement introduced in Junos OS Release 12.1.
Statement added in Junos OS Release 20.3R1 for Next Gen Services on MX240, MX480, and MX960 routers.

Description

The maximum acceptable time, in seconds, from the receipt of the first and latest fragments in a packet. When the number is exceeded, the packet is dropped.

Options

seconds—Maximum seconds allowed.

Range: 1 to 60 seconds.

Default: 4 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Fragmentation Control for MS-DPC and MS-PIC Service Interfaces | 42

receive-window

Syntax

```
receive-window packets;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the size of the receive window for L2TP tunnels, which limits the number of packets the server processes concurrently.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options

packets—Maximum number of packets the receive window can hold at one time.

Default: 16

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Window Size for L2TP Tunnels | 1042

redistribute-all-traffic (Aggregated Multiservices)

Syntax

```
redistribute-all-traffic {
    enable-rejoin;
}
```

Hierarchy Level

[edit interfaces *interface-name* load-balancing-options member-failure-options]

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Enable the option to redistribute traffic of a failed active member to the other active members.

For many-to-one (N:1) high availability support for Network Address Translation (NAT), the traffic for the failed member is automatically redistributed to the other active members.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Aggregated Multiservices Interfaces | 994
- Example: Configuring an Aggregated Multiservices Interface (AMS) | 1009
- member-failure-options (Aggregated Multiservices) | 1313

redundancy-event (Services Redundancy Daemon)

Syntax

```
redundancy-event event-name {
    monitor {
        <link-down interface-name;>
        <peer {
            (mastership-acquire | mastership-release);
        }>
        <process routing abort;>
        <process routing restart;>
    }
]
```

Hierarchy Level

```
[edit services event-options]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure events monitored to trigger change of mastership and routing using inter-chassis redundancy.

Options

event-name—Alphanumeric name for a monitored event.

link-down *interface-name*—Name of an interface, link, or link aggregation, to monitor.

peer mastership-acquire—(Optional) Monitor mastership acquisition peer events.

peer mastership-release—(Optional) Monitor mastership release peer events.

process routing abort—(Optional, and only applies to Next Gen Services) Monitor process routing daemon (rpd) abort requests.

process routing restart—(Optional) Monitor process routing daemon (rpd) restart requests.

Required Privilege Level

maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Inter-Chassis Services Redundancy for Next Gen Services

Configuring the Service Redundancy Daemon | 878

redundancy-options (Adaptive Services Interfaces)

Syntax

```
redundancy-options {
    primary sp-fpc/pic/port;
    secondary sp-fpc/pic/port;
    hot-standby
}
```

Hierarchy Level

```
[edit interfaces rspnumber]
[edit interfaces rmsnumber]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the primary and secondary (backup) adaptive services interfaces.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring AS or Multiservices PIC Redundancy | 29

redundancy-options (Aggregated Multiservices)

Syntax

```
redundancy-options {
    primary mams-a/b/0;
    secondary mams-a/b/0;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 17.2 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure warm standby for an aggregated multiservices (AMS) interface. Specify a primary and a secondary (backup) member services interface for the AMS interface. The primary interface is the service interface that you want to back up, and it is the active interface unless it fails. The secondary interface is the backup interface, and does not handle any traffic unless the primary interface fails. You can use the same services interface as the backup in multiple warm standby AMS interfaces.

You cannot use both the **redundancy-options** and the **load-balancing-options** statements in the same AMS interface.

Options

primary mams-*a*/*b*/0—Name of the primary services interface, where *a* is the FPC slot number and *b* is the PIC slot number.

secondary mams-*a*/*b*/0—Name of the secondary (backup) services interface, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Warm Standby for Services Interfaces | 1008

redundancy-options (Link Services IQ PIC Interfaces)

Syntax

```
redundancy-options {
    (hot-standby | warm-standby);
    primary lsq-fpc/pic/port;
    secondary lsq-fpc/pic/port;
}
```

Hierarchy Level

```
[edit interfaces rlsqnumber]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Specify the primary and secondary (backup) Link Services IQ PIC interfaces.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912

redundancy-options (Stateful Synchronization)

Syntax

```
redundancy-options {
    redundancy-local {
        data-address address;
    }
    redundancy-peer {
        ipaddress address;
    }
    replication-threshold seconds;
    routing-instance instance-name;
    apply-groups (apply-groups-except |redundancy-local | redundancy-peer)
    replication-options (apply-groups | apply-groups-except | mtu | replication-threshold | replication-threshold
        routing-instance )
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 13.3.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card (interfaces of type **vms-x/y/z**).

Description

Specify the primary and secondary (backup) adaptive services PIC interfaces.

Options

data-address *address*—Internal IP address of the local redundant PIC.

ipaddress *address*—Internal IP address of the remote redundant PIC.

instance-name—Name of the routing instance to apply to the HA synchronization traffic between the high availability pair.

seconds—Length of time that the flow remains active for replication.

Default: 180 seconds

apply-groups *apply-groups-except*—Specify the groups from which NOT to inherit the configuration.

apply-groups *redundancy-local*—Specify information for the local peer.

apply-groups *redundancy-peer*—Specify information for peer.

replication-options *apply-groups*—Specify groups from which to inherit the configuration.

replication-options *apply-groups-except*—Specify the groups from which NOT to inherit the configuration.

replication-options *mtu*—Specify the maximal packet size for the replicated data.

Range: 1500 through 8000 bytes

replication-options *replication-threshold*—Specify the duration for which flow should remain active for replication.

Range: 60 through 3600 seconds

replication-options *replication-threshold routing-instance*—Specify routing-instance for the HA traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) (Release 16.1 and later) | **860**

Inter-Chassis High Availability for MS-MIC and MS-MPC (Release 15.1 and earlier) | **888**

redundancy-policy (Interchassis Services Redundancy)

Syntax

```
redundancy-policy policy-name {
   redundancy-events [event-list] {
      then {
         acquire-mastership;
         <add-static-route destination {
            (next-hop next-hop | receive);
            routing-instance routing-instance
         }>
         <broadcast-warning> ;
         <delete-static-route destination  {
            routing-instance routing-instance;
         }>
         <(release-mastership | release-mastership-force);>
      }
   }
}
```

Hierarchy Level

```
[edit policy-options]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the actions to be taken for redundancy events. These include acquiring or releasing mastership and adding or deleting static routes.

Options

acquire-mastership—Switch from standby to master role.

add-static-route *destination*—(Optional) Use the specified destination IP address and prefix for an added signal route.

broadcast-warning—(Optional) Switch status from Standby to Standby (Warned).

delete-static-route *destination*—(Optional) Use the specified destination IP address and prefix for a deleted signal route.

event-list—List of names of one or more monitored events that trigger the actions specified in this policy.

next-hop—Interface name for the next hop for an added signal route.

policy-name—Name of the redundancy policy.

receive—Use the added signal route as a receive route.

release-mastership—(Optional) Switch from master to standby role.

release-mastership-force—(Optional) Force switch from master to standby role.

routing-instance *routing-instance*—(Optional) Name of the vrf used for the added signal route.

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

RELATED DOCUMENTATION

Configuring Inter-Chassis Services Redundancy for Next Gen Services

Configuring the Service Redundancy Daemon | **878**

redundancy-set

Syntax

```
redundancy-set redundancy-set {
    healthcheck-timer-interval healthcheck-timer-interval;
    hold-time hold-time;
    keepalive keepalive;
    redundancy-group redundancy-group;
    redundancy-policy [redundancy-policy-list]
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the characteristics of a redundancy set.

Options

healthcheck-timer-interval *healthcheck-timer-interval*—Frequency of health check probes in seconds.

Range: 0 through 3600 seconds

hold-time—Maximum wait time for a health check response. When this time expires, the peer is considered down.

Range: 0 through 3600 seconds

keepalive—Frequency of srd hello messages in seconds.

Range: 1 through 60 seconds

redundancy-group—Redundancy group identifier. This must match a redundancy group ID in the ICCP configuration.

Range: 1 through 100

redundancy-policy-list—Names of one or more redundancy policies applied to the redundancy set.

redundancy-set—Redundancy set identifier.

Range: 1 through 100

Required Privilege Level

maintenance—To view this statement in the configuration.

maintenance-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Inter-Chassis Services Redundancy for Next Gen Services

Configuring the Service Redundancy Daemon | **878**

redundancy-set-id (Service Set)

Syntax

```
redundancy-set-id redundancy-set;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the identifier of the redundancy set to use in the stateful synchronization of services for a service set.

Options

redundancy-set—Identifier for the redundancy set. The identifier can be a number from 1-100.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Inter-Chassis Services Redundancy for Next Gen Services

Configuring the Service Redundancy Daemon | 878

reflexive | revert | reverse

Syntax

```
reflexive; | revert; | reverse {
    application-profile profile-name;
    dscp (alias | bits);
    forwarding-class class-name;
    syslog;
}
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 8.1.
revert option introduced in Junos OS Release 16.1R5 and 17.4R1.

Description

reflexive—Applies the CoS rule actions to flows in the reverse direction as well as to flows in the matching direction.

revert—Stores the DSCP and forwarding class of a packet that is received in the match direction of the rule and then applies that DSCP and forwarding class to packets that are received in the reverse direction of the same session.

reverse—Allows you to define CoS behavior for flows in the reverse direction.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring CoS Rules | 823

rejoin-timeout (Aggregated Multiservices)

Syntax

```
rejoin-timeout rejoin-timeout;
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options member-failure-options drop-member-traffic]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the time by when failed members (members in the **DISCARD** state) should rejoin the aggregated Multiservices (AMS) interface automatically. All members that do not rejoin by the configured time are moved to the **INACTIVE** state and the traffic meant for each of the members is dropped.

If multiple members fail around the same time, then they are held in the **DISCARD** state using a single timer. When the timer expires, all the failed members move to **INACTIVE** state at the same time.

Default

If you do not configure a value, the default value of 120 seconds is used.

Options

rejoin-timeout—Time, in seconds, by which a failed member must rejoin.

Default: 120 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Aggregated Multiservices Interfaces | **994**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**
- drop-member-traffic (Aggregated Multiservices) | **1183**

remote-gateway

Syntax

```
remote-gateway address;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the remote address to which the IPsec traffic is directed.

Options

address—Remote IPv4 or IPv6 address.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

remote-id

Syntax

```
remote-id {
    any-remote-id;
    ipv4_addr [ values ];
    ipv6_addr [ values ];
    key_id [ values ];
    fqdn fqdn
    distinguished-name container container-string-values |wildcard wildcard-string-values
}
```

Hierarchy Level

```
[edit services ipsec-vpn ikepolicy policy-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
ipv6_addr option added in Junos OS Release 7.6.
any-remote-id option added in Junos OS Release 8.2.
distinguished-name container*container-string-values* |wildcard *wildcard-string-values* option added in Junos OS Release 19.1.

Description

Define the remote identification values to which the IKE policy applies.

Options

any-remote-id—Allow any remote address to connect. This option is supported only in dynamic configurations and cannot be configured with specific values.

ipv4_addr [*values*]—Define one or more IPv4 address identification values.

ipv6_addr [*values*]—Define one or more IPv6 address identification values.

key_id [*values*]—Define one or more key identification values.

fqdn *fqdn*—Fully-qualified domain name.

distinguished-name container*container-string-values* |wildcard *wildcard-string-values*—One or more distinguished name values.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

remotely-controlled

Syntax

```
remotely-controlled;
```

Hierarchy Level

```
[edit services nat pool nat-pool-name 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.

respond-bad-spi (Services IKE Policy)

Syntax

```
respond-bad-spi max-responses;
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy]
```

Release Information

Statement introduced in Junos OS Release 12.3.

Description

Enable response to invalid IPsec Security Parameter Index (SPI) values. If the security associations (SAs) between two peers of an IPsec VPN become unsynchronized, the device resets the state of a peer so that the two peers are synchronized.

Options

max-responses—Number of times to respond to invalid SPI values per gateway.

Range: 1 through 30

Default: 5

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

retransmit-interval (Services)

Syntax

```
retransmit-interval seconds;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the maximum retransmit interval for L2TP tunnels.

> **NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

Options

seconds—Interval, in seconds, after which the server retransmits data if no acknowledgment is received.

Default: 30 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Timers for L2TP Tunnels | 1043

rpc-program-number

Syntax

```
rpc-program-number number;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Remote procedure call (RPC) or Distributed Computing Environment (DCE) value.

Options

number—RPC or DCE program value.

Range: 100,000 through 400,000

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | 466
- Configuring an RPC Program Number | 523
- Examples: Configuring Application Protocols | 524
- Verifying the Output of ALG Sessions | 525

routing-engine-services

Syntax

```
routing-engine-services;
```

Hierarchy Level

[edit services **service-set** *service-set* **service-set-options**]

Release Information

Statement introduced in Junos OS Release 15.1.
Support for Next Gen Services introduced in Junos OS Release 19.3R2.

Description

When configuring a Routing Engine-based captive portal service, specify the service set options to apply to a service set. The services interfaces on the Routing Engine are identified with an si- prefix (for example, si-1/1/0). The si- interface contains all redirect and rewrite traffic and services for the Routing Engine.

Required Privilege Level

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

RELATED DOCUMENTATION

- *HTTP Redirect Service Overview*
- *Configuring MS-MPC-Based or MX-SPC3-Based Static HTTP Redirect Services*
- *Configuring MS-MPC-Based or MX-SPC3-Based Converged HTTP Redirect Services*
- *Configuring Routing Engine-Based, Static HTTP Redirect Services*
- *Configuring Routing Engine-Based, Converged HTTP Redirect Services*

rtp

Syntax

```
rtp {
   f-max-period number;
   maximum-contexts number <force>;
   port {
      minimum port-number;
      maximum port-number;
   }
   queues [ queue-numbers ];
}
```

Hierarchy Level

[edit interfaces *interface-name* **unit** *logical-unit-number* **compression**],
[edit logical-systems *logical-system-name* interfaces *interface-name* **unit** *logical-unit-number* **compression**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the RTP properties for voice services traffic.

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Compression of Voice Traffic | **1027**

rule (Services CoS)

Syntax

```
rule rule-name {
   match-direction (input | output | input-output);
   term term-name {
      from {
         application-sets set-name;
         applications [ application-names ];
         destination-address address;
         destination-prefix-list list-name <except>;
         source-address address;
         source-prefix-list list-name <except>;
      }
      then {
         application-profile profile-name;
         dscp (alias | bits);
         forwarding-class class-name;
         syslog;
         reflexive; | revert; | reverse {
            application-profile profile-name;
            dscp (alias | bits);
            forwarding-class class-name;
            syslog;
         }
      }
   }
}
```

Hierarchy Level

```
[edit services cos],
[edit services cos rule-set rule-set-name]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Specify the rule the router uses when applying this service.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

Configuring CoS Rules on Services PICs

rule (IDS MS-DPC)

Syntax

```
rule rule-name {
  match-direction (input | output | 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>;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
    }
    then {
      aggregation (IDS) {
        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
      }
      (force-entry | ignore-entry);
      logging {
        syslog;
        threshold rate;
      }
      session-limit {
        by-destination (IDS MS-DPC) {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-pair (IDS MS-DPC) {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
        by-source (IDS MS-DPC) {
          hold-time seconds;
          maximum number;
          packets number;
          rate number;
        }
      }
```

```
        syn-cookie {
            mss value;
            threshold rate;
        }
    }
  }
}
```

Hierarchy Level

```
[edit services ids],
[edit services ids 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 on the MS-DPC.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IDS Rules on an MS-DPC | 583

rule (IDS MS-MPC)

Syntax

```
rule {
    match-direction (input | output | input-output);
    term {
        then {
            aggregation (IDS) {
                destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
                source-prefix prefix-value | source-prefix-ipv6 prefix-value;
            }
            allow-ip-options {
                any;
                loose-source-route;
                route-record;
                route-alert;
                security;
                stream-id;
                strict-source-route;
                timestamp;
            }
            allow-ipv6-extension-header {
                any;
                ah;
                dstopts;
                esp;
                fragment;
                hop-by-hop;
                mobility;
                routing;
            }
            icmp-fragment-check;
            icmp-large-packet-check;
            land-attack-check (ip-only | ip-port);
            session-limit {
                by-destination {
                    by-protocol {
                        icmp {
                            maximum number;
                            packets number;
                            rate number;
                        }
                        tcp {
                            maximum number;
```

```
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
    by-source {
        by-protocol {
            icmp {
                maximum number;
                packets number;
                rate number;
            }
            tcp {
                maximum number;
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
  }
  tcp-syn-defense;
  tcp-syn-fragment-check;
  tcp-winnuke-check;
 }
 }
}
```

Hierarchy Level

[edit services ids]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure network attack protection for a service set on an MS-MPC.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

rule

Syntax

```
rule rule-name {
    match-direction (input | output);
    term term-name {
        from {
            destination-address address;
            ipsec-inside-interface interface-name;
            source-address address;
        }
        then {
            anti-replay-window-size bits;
            backup-remote-gateway address;
            clear-dont-fragment-bit;
            dynamic {
                ike-policy policy-name;
                ipsec-policy policy-name;
            }
            initiate-dead-peer-detection;
            manual {
                direction (inbound | outbound | bidirectional) {
                    authentication {
                        algorithm (hmac-md5-96 | hmac-sha1-96);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi spi-value;
                    encryption {
                        algorithm algorithm;
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | bundle | esp);
                    spi spi-value;
                }
            }
            no-anti-replay;
            remote-gateway address;
            syslog;
            tunnel-mtu bytes;
        }
    }
}
```

Hierarchy Level

[edit services ipsec-vpn],
[edit services ipsec-vpn **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.

Options
rule-name—Identifier for the collection of terms that comprise this rule.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring IPsec Rules | **688**
Configuring IPsec Rule Sets | **697**
Configuring Security Associations | **639**

rule (PCP)

Syntax

```
rule rule-name {
   match-direction (input | output);
   term term-name {
      from {
         application-sets set-name;
         applications [ application-name ];
         destination-address address <except>;
         destination-address-range high maximum-value low minimum-value <except>;
         destination-port high maximum-value low minimum-value;
         destination-prefix-list list-name <except>;
         source-address address <except>;
         source-address-range high maximum-value low minimum-value <except>;
         source-prefix-list list-name <except>;
      }
      then {
         pcp-server server-name;
      }
   }
   }
}
```

Hierarchy Level

```
[edit services pcp]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Configure a rule to assign the port control protocol (PCP) server that handles selected traffic. PCP enables hosts to operate servers for a long time (as in the case of a webcam) or a short time (for example, while playing a game or on a phone call) when behind a NAT device, including when behind a carrier-grade NAT operated by their ISP. PCP enables applications to create mappings from an external IP address and port to an internal IP address and port.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

rule-name—Rule name

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

rule (Services NAT)

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-port range high maximum-value low minimum-value;
      source-address (address | any-unicast) <except>;
      source-address-range low minimum-value high maximum-value <except>;
    }
    then {
      no-translation;
      port-forwarding-mappings map-name;
      translated {
        address-pooling paired;
        clat-prefix clat-prefix;
        destination-pool nat-pool-name;
        destination-prefix 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-nat-pt | basic-nat44 | basic-nat66 | deterministic-napt44 | deterministic-napt64
          |dnat-44 | dynamic-nat44 | napt-44 | napt-66 | napt-pt | stateful-nat464 | stateful-nat64 |
          twice-basic-nat-44 | twice-dynamic-nat-44 | twice-napt-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: You are limited to a maximum of 200 terms for a NAT rule that is applied to an inline services (type si) interface. If you specify more than 200 terms, you will receive following error when you commit the configuration:

```
[edit]
  'service-set service-set-name'
    NAT rule rule-name  with more than 200 terms is disallowed for
si-n/n/n.n
error: configuration check-out failed
```

Options
rule-name—Identifier for the collection of terms that make up this rule.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

rule (Services Stateful Firewall)

Syntax

```
rule rule-name {
   match-direction (input | output | input-output);
   term term-name {
      from {
         application-sets set-name;
         applications [ application-names ];
         destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
         destination-address-range low minimum-value high maximum-value <except>;
         destination-prefix-list list-name <except>;
         source-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
         source-address-range low minimum-value high maximum-value <except>;
         source-prefix-list list-name <except>;
      }
      then {
         (accept <skip-ids>| discard | reject);
         syslog;
      }
   }
}
```

Hierarchy Level

```
[edit services stateful-firewall],
[edit services stateful-firewall 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.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Stateful Firewall Rules | 546

rule (Softwire)

Syntax

```
rule rule-name {
    match-direction (input | output);
    term term-name {
        then {
            (ds-lite ds-lite-softwire-concentrator | map-e name | v6rd v6rd-softwire-concentrator);
        }
    }
}
```

Hierarchy Level

```
[edit services softwire],
[edit services softwire rule-set rule-set-name]
```

Release Information

Statement introduced in Junos OS Release 10.4.
map-e *name* option introduced in Junos OS Release 18.2R1 for MX Series Routers with MPC and MIC interfaces.

Description

Configure a rule to apply a softwire concentrator for a flow.

Softwire rules are supported on the MS-DPC, MS-100, MS-400, and MS-500 line cards. Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.

Options

rule-name—Identifier for the collection of terms that constitute this rule.

input—Apply the rule match on the input side of the interface.

output—Apply the rule match on the output side of the interface.

ds-lite-softwire-concentrator—Specify the DS-Lite softwire concentrator to use.

map-e *name*—Specify the Mapping of Address and Port with Encapsulation (MAP-E) softwire concentrator to use.

v6rd-softwire-concentrator—Specify the 6rd softwire concentrator to use.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Softwire Rules | 381

rule-set (Services CoS)

Syntax

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

Hierarchy Level

```
[edit services cos]
```

Release Information
Statement introduced in Junos OS Release 8.1.

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

Options
rule-set-name—Identifier for the collection of rules that constitute this rule set.

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

RELATED DOCUMENTATION

Configuring CoS Rule Sets on Services PICs

rule-set (Services IDS)

Syntax

```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

Hierarchy Level

```
[edit services ids]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

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

Options

rule-set-name—Identifier for the collection of rules that constitute this rule set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IDS Rule Sets on an MS-DPC | 592

rule-set

Syntax

```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

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

Options

rule-set-name—Identifier for the collection of rules that constitute this rule set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rule Sets | 697
Configuring IPsec Rules | 688

rule-set (Services NAT)

Syntax

```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

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

rule-set-name—Identifier for the collection of rules that constitute this rule set.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

rule-set (Services Stateful Firewall)

Syntax

```
rule-set rule-set-name {
    [ rule rule-names ];
}
```

Hierarchy Level

```
[edit services stateful-firewall]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

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

Options

rule-set-name—Identifier for the collection of rules that constitute this rule set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Stateful Firewall Rule Sets | 552

rule-set (Softwire)

Syntax

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

Hierarchy Level

```
[edit services softwire]
```

Release Information

Statement introduced in Junos OS Release 10.4.

Description

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

Options

rule-set-name—Identifier for the collection of rules that constitute this rule set.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Softwire Rules | 381

secondary (Adaptive Services Interfaces)

Syntax

```
secondary interface-name;
```

Hierarchy Level

```
[edit interfaces (rsp0 | rsp1) redundancy-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the secondary (backup) adaptive services interface.

Options

interface-name—The identifier for the adaptive services interface, which must be of the form **sp-*fpc*/*pic*/*port***.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring AS or Multiservices PIC Redundancy | 29

secondary (Link Services IQ PIC Interfaces)

Syntax

```
secondary interface-name;
```

Hierarchy Level

```
[edit interfaces rlsqnumber redundancy-options]
```

Release Information

Statement introduced in Junos OS Release 7.6.

Description

Specify the secondary (backup) Link Services IQ PIC interface.

Options

interface-name—The identifier for the Link Services IQ PIC interface, which must be of the form **lsq-*fpc*/*pic*/*port***.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912

secure-nat-mapping

Syntax

```
secure-nat-mapping {
    mapping-refresh (inbound | outbound | inbound-outbound);
    eif-flow-limit number-of-flows'
}
```

Hierarchy Level

[edit services nat rule *rule-name* term *term-name* then translated]

Release Information

Statement introduced in Junos OS Release 12.3 on MS-DPCs.
Statement introduced in Junos OS Release 15.1R3 on MS-MPCs and MS-MICs.

Description

Specify configuration options that help prevent or minimize the effect of attempted denial of service (DOS) attacks for NAT operations.

Options

The remaining statements are explained separately. See CLI Explorer.

—

Required Privilege Level

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

RELATED DOCUMENTATION

Protecting CGN Devices Against Denial of Service (DOS) Attacks | 409

secured-port-block-allocation

Syntax

```
secured-port-block-allocation {
    active-block-timeout timeout-seconds;
    block-size block-size;
    max-blocks-per-address max-blocks;
}
```

Hierarchy Level

[edit **services** nat **pool** *pool-name* port]

Release Information

Statement introduced in Junos OS Release 11.2.

Description

When you use block allocation, one or more blocks of ports in a NAT pool address range are available for assignment to a subscriber.

Port block allocation is supported on MX series routers with MS-DPCs and on M Series routers with MS-100, MS-400, and MS-500 MultiServices PICS. Port block allocation is supported on MX series routers with MS-MPCs and MS-MICs starting in Junos OS release 14.2R2.

> **NOTE:** If you define the session lifetime globally for a Multiservices (**ms-**) interface (by using the **session-timeout seconds** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level), the session is terminated even if traffic continues to flow beyond that time period. When continuous traffic transmission occurs, the session is reset immediately after the timeout period. When you configure the same value for the session timeout and the active port block allocation timeout, the system might not determine that the active port block timeout period has elapsed. As a result, when the active port block timeout elapses, the system might use the same block for the initial port allocation that was used previously. However, for the subsequent allocation of a port block, the system identifies the active block timeout value correctly and allocates a port from a new block. This behavior is expected when the session timeout and port block timeout values are identical. To avoid this problem, we recommend that you configure different values for session timeout and port block timeout so that the **JSERVICES_NAT_PORT_BLOCK_ALLOC** system logging message is generated at correct intervals of the active port block timeout value.

NOTE: If you make any configuration changes to a NAT pool that has secured port block allocation configured, you must delete the existing NAT address pool, wait at least 5 seconds, and then configure a new NAT address pool. We also strongly recommend that you perform this procedure if you make any changes to the NAT pool configuration, even when secured port block allocation is not configured.

Options

active-block-timeout *timeout-seconds*—Interval, in seconds, during which a block is active. After the timeout elapses, a new block is allocated, even if ports are available in the active block.

Range: 0 through 86400. When you specify 0, the active block transitions to inactive only when it runs out of ports and a new block is allocated. Any inactive block without any ports in use will be freed to the NAT pool, unless it is active block.

Default: 120

block-size *block-size*—Number of ports included in a block.

Range: For the Multiservices DPC only, 1 through 32,000

Range: For the Multiservices MPC and Multiservices MIC only, 1 through the total number of configured ports. For example, for a port range of 1024 through 61,024, the block-size range is 1 through 60,000.

Default: 128

max-blocks-per-address *max-blocks*—Maximum number of blocks that can be allocated to a user address.

Range: 1 to 512

timeout-seconds—Interval, in seconds, during which a block is active. After timeout, a new block is allocated, even if ports are available in the active block.

Default: 120

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Address Pools for Network Address Port Translation (NAPT) Overview | **170**

security-intelligence

Syntax

```
    authentication {
        auth-token auth-token;
    tls-profile tls-profile;
    traceoptions {
        no-remote-trace;
        file [ filename <files number> <size  bytes> <match expression> <world-readable | no-world-readable>];
        flag [all | feed | ipc];
        level [all| error | info | notice | verbose | warning];
    no-remote-trace;
url url;
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers with Juniper Sky Advanced Threat Prevention (ATP).
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480, and MX960. This support runs inline on the MPC card.

Description

You can configure security intelligence profiles and policies to work with security intelligence feeds, such as infected hosts and C&C. You then configure a firewall policy to include the security intelligence policy, for example, block outgoing requests to a C&C host.

Options

authentication—Configure authentication, such as an auth token or TLS profile, to commute with the feed server. This operation is performed by the ops script used to enroll your devices and is typically not required afterwards. If you have problems establishing a connection with the Juniper Sky ATP cloud server, we recommend that you rerun the ops script instead of manually entering all the CLI commands.

traceoptions—Set security intelligence trace options.

- file—Name of the file to receive the output of the tracing operation.
  - **files *number*** —Maximum number of trace files

    Range: 2 through 1000
  - match— Regular expression for lines to be logged

  - no-world-readable—Prevent any user from reading the log file
  - size—Maximum size of each trace file

    Range: 10240 through 1073741824
  - world-readable—Allow any user to read the log file
- flag—Tracing operation to perform
  - all—All interface tracing operation
  - feed—Trace feed operation
  - ipc—Trace interface interprocess communication (IPC) module messages
- level—Level of debugging output
- no-remote-trace—Disable the remote trace

url *url-address*—Configure the URL of the feed server. This operation is performed by the ops script used to enroll your devices and is typically not required afterwards. If you have problems establishing a connection with the Juniper Sky ATP cloud server, we recommend that you rerun the ops script instead of manually entering all the CLI commands.

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

security-intelligence-policy

Syntax

```
security-intelligence-policy {
    threat-level threat-level;
    threat-action {
        drop
        drop-and-log
        drop-and-sample
        drop-log-and-sample
        log
        log-and-sample
        sample
    }
}
```

Hierarchy Level

```
[edit services web-filter profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 19.3R1 on MX Series routers with Juniper Sky Advanced Threat Prevention (Juniper Sky ATP) .

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480, and MX960 with the MX-SPC3 services card

Description

Define the threat level and action for the Web filter profile. The packets are redirected at the Packet Forwarding Engine based on the configured threat-level action associated with the threat-level of the destination IP address.

Options

threat-level—Define the Web filtering threat level. The value ranges from 1 through 10

threat-action—Define the way the Packet Forwarding Engine processes packets in response to a threat. Only one action can be configured for each threat level that is defined. The default threat-action is **accept**.

- **drop**—Drop the packets and do not generate a log message.
- **drop-and-log**—Drop the packets and generate a log message.
- **drop-and-sample**—Drop and sample the packets.

- **drop-log-and-sample**—Drop, sample, and allow the packets, and generate a log message.
- **log**—Allow the packets and generate a log message.
- **log-and-sample**—Allow, sample the packets, and generate a log message.
- **sample**—Sample the packets.

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

RELATED DOCUMENTATION

web-filter | **1605**

server (pcp)

Syntax

```
server server-name {
    ipv4-address ipv4-address;
    ipv6-address ipv6-address;
    long-lifetime-error long-lifetime-error;
    mapping-lifetime-max mapping-lifetime-max;
    mapping-lifetime-min mapping-lifetime-min;
    max-mappings-per-client max-mappings-per-client;
    nat-options {
        pool pool-name ;
    }
    pcp-options {
        prefer-failure;
        third-party;
    }
    short-lifetime-error short-lifetime-error;
    softwire-concentrator softwire-concentrator-name;
}
```

Hierarchy Level

```
[edit services pcp]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Configure PCP server options. PCP enables hosts to operate servers for a long time (as in the case of a webcam) or a short time (for example, while playing a game or on a phone call) when behind a NAT device, including when behind a carrier-grade NAT operated by their ISP. PCP enables applications to create mappings from an external IP address and port to an internal IP address and port.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC. Starting in Junos OS Release 20.1R1, PCP is also supported for Next Gen Services.

Options

ipv4-address—IPv4 address of the PCP server.

ipv6-address—IPv6 address of the PCP server.

long-lifetime-error —Time limit for generating long lifetime errors.

Default: 1800 seconds

Range: 900 through 18,000 seconds

mapping-lifetime-max—Maximum lifetime, in seconds, for PCP mapping. If the PCP client requests a lifetime less than the maximum configured, the server will assign the maximum lifetime and respond accordingly.

Default: 86,400 seconds

Range: 3600 through 4294667 seconds

mapping-lifetime-min—Minimum lifetime, in seconds, for PCP mapping. If a PCP client requests a lifetime less than the minimum configured, the server will assign a minimum lifetime and respond accordingly.

Default: 300 seconds

Range: 120 through 3600 seconds

max-mappings-per-client—Maximum number of PCP mappings that the PCP client can request.

Default: 32

Range: 1 through 32

pool-name—Name of the NAT pool to use for PCP mapping. You can identify multiple pools. If you do not specify a NAT pool for mapping, the Junos OS performs a partial rule match based on the source IP, source port, and protocol, and the Junos OS uses the NAT pool configured for the first matching rule to allocate mappings for PCP.

prefer-failure—Generate an error message when the PCP client requests a specific IP address or port that is not available, rather than assigning another available address from the NAT pool.

short-lifetime-error—Time limit for generating short lifetime errors.

Default: 30 seconds

Range: 15 through 300 seconds

softwire-concentrator-name—Softwire concentrator name whose softwire-address is used in creating PCP mappings. The PCP server address must be the same as the softwire-concentrator address.

third-party—Enable third-party requests by the PCP client.

The other statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

service

Syntax

```
service {
   input {
      [ service-set service-set-name <service-filter filter-name> ];
      post-service-filter filter-name;
   }
   output {
      [ service-set service-set-name <service-filter filter-name> ];
   }
}
```

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family inet],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the service sets and filters to be applied to an interface.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Filters and Services to Interfaces | 25

service-domain

Syntax

```
service-domain (inside | outside);
```

Hierarchy Level

[edit interfaces *interface-name* **unit** *logical-unit-number* **family** inet],
[edit logical-systems *logical-system-name* interfaces *interface-name* **unit** *logical-unit-number* **family** inet]

Release Information

Statement introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the service interface domain. If you specify this interface using the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level, the interface domain must match that specified with the **inside-service-interface** and **outside-service-interface** statements.

Options

inside—Interface used within the network.

outside—Interface used outside the network.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Address and Domain for Services Interfaces | 34

service-filter (Interfaces)

Syntax

```
service-filter filter-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet service (input | output) service-set service-set-name],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service (input |
    output) service-set service-set-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the filter to be applied to traffic before it is accepted for service processing. Configuration of a service filter is optional; if you include the **service-set** statement without a **service-filter** definition, Junos OS assumes the match condition is true and selects the service set for processing automatically.

Options

filter-name—Identifies the filter to be applied in service processing. You can include special characters, such as a forward slash (/), colon (:), or a period (.).

Required Privilege Level

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

RELATED DOCUMENTATION

Applying Filters and Services to Interfaces | 25

Junos OS Services Interfaces Library for Routing Devices

service-interface (Services Interfaces)

Syntax

```
service-interface interface-name;
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the name for the services interface associated with an interface-wide service set.

Options

interface-name—Identifier of the service interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

Applying Services to Subscriber-Aware Traffic with a Service Set

service-interface (L2TP Processing)

Syntax

service-interface *interface-name*;

Hierarchy Level

[edit services l2tp **tunnel-group** *name*]

Release Information

Statement introduced before Junos OS Release 7.4.
si-*fpc*/*pic*/*port* option added in Junos OS Release 11.4.
Option **asi*fpc* added in Junos OS Release 16.2.**

Description

Specify the service interface responsible for handling L2TP processing.

> **NOTE:** On MX Series routers, the service interface configuration is required for static LNS sessions. Either the service interface configuration or the service device pool configuration can be used for dynamic LNS sessions.

Options

interface-name—Name of the service interface. The ae, si, and sp interface types are supported as follows:

- **asi*x***—(MPCs on MX Series routers) Aggregated inline services interface.
- **sp-*fpc*/*pic*/*port***—On AS or Multiservices PICs on M7i, M10i, and M120 routers.
- **si-*fpc*/*pic*/*port***—On MPCs on MX Series routers.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Local Gateway Address and PIC | **1042**

Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

service-interface-pools

Syntax

```
service-interface-pools {
    pool pool-name {
        interface interface-name.unit-number;
    }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Configure service interface pools used for VPN aggregation.

Options

The options are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Interface Pools | 24

service-set (Interfaces)

Syntax

```
service-set service-set-name;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet service (input | output)],
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet service (input
    | output)]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Define one or more service sets to be applied to an interface. If you define multiple service sets, the router software evaluates the filters in the order in which they appear in the configuration.

Options

service-set-name—Name of the service set.

Required Privilege Level

System—To view this statement in the configuration.
System-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Guidelines for Configuring Service Filters

service-set (Services)

Syntax

```
service-set service-set-name {
    allow-multicast;
    captive-portal-content-delivery-profile;
    cos-options {
        match-rules-on-reverse-flow;
    }
    cos-rules [cos-rule-name];
    extension-service service-name {
        provider-specific-rules-configuration;
    }
    (ids-rules rule-name | ids-rule-sets rule-set-name);
    interface-service {
        load-balancing-options {
            hash-keys {
                egress-key (destination-ip | source-ip);
                ingress-key (destination-ip | source-ip);
            }
        }
        service-interface interface-name;
    }
    ipsec-vpn-options {
        anti-replay-window-size bits;
        clear-dont-fragment-bit;
        ike-access-profile profile-name;
        local-gateway address;
        no-anti-replay;
        no-certificate-chain-in-ike;
        passive-mode-tunneling;
        trusted-ca [ ca-profile-names ];
        tunnel-mtu bytes;
        udp-encapsulation {
            <udp-dest-port destination-port>;
        }
    }
    ip-reassembly-rules rule-name};
    (ipsec-vpn-rules rule-name | ipsec-vpn-rule-sets rule-set-name);
    max-flows number;
    max-drop-flows {
        ingress ingress-flows;
        egress egress-flows;
    }
```

```
max-session-setup-rate max-setup-rate;
nat-options {
   land-attack-check (ip-only | ip-port);
   max-sessions-per-subscriber session-number;
   stateful-nat64{
      clear-dont-fragment-bit;
   }
}
(nat-rules rule-name | nat-rule-sets rule-set-name);
next-hop-service {
   inside-service-interface interface-name.unit-number;
   outside-service-interface interface-name.unit-number;
   outside-service-interface-type local;
   service-interface-pool name;
}
pcp-rules rule-name;
(pgcp-rules rule-name | pgcp-rule-sets rule-set-name);
(ptsp-rules rule-name | ptsp-rule-sets rule-set-name);
service-set-options {
   bypass-traffic-on-exceeding-flow-limits;
   bypass-traffic-on-pic-failure;
   disable-session-open-syslog
   enable-asymmetric-traffic-processing;
   header-integrity-check
   routing-engine-services;
   support-uni-directional-traffic;
}
snmp-trap-thresholds{
   flows high high-threshold | low low-threshold;
   nat-address-port high-threshold | low low-threshold;
   }
}
softwire-options {
   dslite-ipv6-prefix-length dslite-ipv6-prefix-length;
}
(softwire-rules rule-name | softwire-rule-sets rule-set-name);
(stateful-firewall-rules rule-name | stateful-firewall-rule-sets rule-set-name);
```

```
    syslog {
        host hostname {
            class {
                alg-logs;
                deterministic-nat-configuration-log;
                ids-logs;
                nat-logs;
                packet-logs;
                pcp-logs;
                session-logs <open | close>;
                stateful-firewall-logs ;
            }
            services severity-level;
            facility-override facility-name;
            interface-service prefix-value;
            port port-number;
            services severity-level;
        }
    }
    (web-filter-profile | url-filter-profile) profile-name;
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced before Junos OS Release 7.4.
pcp-rules option added in Junos OS Release 13.2R1.
pgcp-rules and **pgcp-rule-sets** options added in Junos OS Release 8.4.
server-set-options option added in Junos OS Release 10.1.
ptsp-rules and **ptsp-rule-sets** options added in Junos OS Release 10.2.
softwire-rules and **clear-rule-sets** options added in Junos OS Release 10.4.
softwire-options option added in Junos OS Release 14.1.
url-filter-profile option added in Junos OS Release 17.2R1.
match-rules-on-reverse-flow option added in Junos OS Release 16.1R5 and 17.4R1
web-filter-profile option added in Junos OS Release 18.3R1.
Support added in Junos 20.2R1 for Next Gen Services NAT PT feature.

Description

Define the service set.

> **NOTE:** Use the **web-filter-profile** option starting in Junos OS Release 18.3R1 and use the **url-filter-profile** option in Junos OS Releases before 18.3R1.

Options

service-set-name—Name of the service set. You can include special characters, such as a forward slash (/), colon (:), or a period (.).

Range: Up to 64 alphanumeric characters.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Understanding Service Sets | 6

service-set-options

Syntax

```
service-set-options {
    bypass-traffic-on-exceeding-flow-limits;
    bypass-traffic-on-pic-failure;
    enable-asymmetric-traffic-processing;
    enable-descriptive-session-syslog
    header-integrity-check;
    routing-engine-services;
    support-uni-directional-traffic;
    tcp-fast-open {
        disabled;
        drop;
    }
    tcp-non-syn {
        drop-flow;
        drop-flow-send-rst;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 10.1.
enable-asymmetric-traffic-processing and **support-uni-directional-traffic** options added in Junos OS Release 11.2.
routing-engine-services option added in Junos OS Release 15.1.
enable-change-on-ams-redistribution option added in Junos OS Release 15.1.
tcp-fast-open option added in Junos OS Release 17.2.

Description

Specify the service set options to apply to a service set.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

Configuring APPID Support for Unidirectional Traffic

services (NAT)

Syntax

```
services nat { ... }
```

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 Level

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

session-limit (IDS MS-DPC)

Syntax

```
session-limit {
    by-destination (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
    by-pair (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
    by-source (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
    }
}
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable flow limitation by configuring thresholds on source, destination, or stateful firewall and network address translation (NAT) paired traffic flows when using the MS-DPC.

Options

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

session-limit (IDS MS-MPC)

Syntax

```
session-limit {
    by-destination {
        by-protocol {
            icmp {
                maximum number;
                packets number;
                rate number;
            }
            tcp {
                maximum number;
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
    by-source {
        by-protocol {
            icmp {
                maximum number;
                packets number;
                rate number;
            }
            tcp {
                maximum number;
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
```

```
        maximum number;
        packets number;
        rate number;
    }
}
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information
Statement introduced in Junos OS Release 17.1 on MX Series.

Description
Configure the IDS rule session limits for an individual destination or source address or subnet. This protects against network probing attacks and network flooding attacks. This IDS rule can only be assigned to a service set on an MS-MPC.

You can specify limits for specific protocols (ICMP, TCP, and UDP), or specify limits independent of a protocol.

When a session limit is exceeded for a source or destination, packets from the source or to the destination are dropped until the session limit is no longer exceeded.

To specify limits for destination or source subnets rather than individual addresses, include the **aggregation** statement at the **[edit services ids rule *rule-name* term *term-name* then]** hierarchy level.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

session-offload

Syntax

```
session-offload;
```

Hierarchy Level

```
[edit chassis fpc slot-number pic number adaptive-services service-package extension-provider]
```

Release Information

Statement introduced on MX Series 5G Universal Routing Platforms with MS-DPCs in Junos OS Release 9.6.

Description

Enable session offloading on a per-PIC basis for a Multiservices PIC.

Default

Session offloading is disabled.

Required Privilege Level

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

RELATED DOCUMENTATION

Enabling Session Offloading for Multiservices DPCs | 32

set-dont-fragment-bit (Services Set)

Syntax

```
set-dont-fragment-bit;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 14.1.

Description

Configure the do not fragment (DF) bit in only the outer header of the IPsec packet and leave the inner header unmodified for dynamic endpoint tunnels. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. These settings apply for dynamic endpoint tunnels and not for static tunnels, for which you need to include the **set-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level to set the DF bit in the outer header of the IPv4 packets that enter the static IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

By default, this statement is disabled on MS-MICs and MS-MPCs (the DF bit value is not configured in the outer header by default).

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698
Configuring IPsec Rules | 688

set-dont-fragment-bit (Services IPsec VPN)

Syntax

```
set-dont-fragment-bit;
```

Hierarchy Level

[edit services ipsec-vpn **rule** *rule-name* **term** *term-name* **then**]

Release Information
Statement introduced in Junos OS Release 14.1.

Description
Configure the do not fragment (DF) bit in only the outer header of the IPsec packet and leave the inner header unmodified. If the encapsulated packet size exceeds the tunnel maximum transmission unit (MTU), the packet is fragmented before encapsulation. These settings apply for static endpoint tunnels and not for dynamic tunnels, for which you need to include the **set-dont-fragment-bit** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level to set the DF bit in the outer header of the IPv4 packets that enter the dynamic IPsec tunnel. This functionality is supported on MX Series routers with MS-MICs and MS-MPCs.

By default, this statement is disabled on MS-MICs and MS-MPCs (the DF bit value is not configured in the outer header by default).

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

sip-call-hold-timeout

Syntax

```
sip-call-hold-timeout seconds;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

Timeout period for SIP calls placed on hold, in seconds.

Options

seconds—Length of time the application holds a SIP call open before it times out.

Default: 7200 seconds

Range: 0 through 36,000 seconds (10 hours)

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring SIP | **514**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

sip

Syntax

```
sip {
    video {
        dscp (alias | bits);
        forwarding-class class-name;
    }
    voice {
        dscp (alias | bits);
        forwarding-class class-name;
    }
}
```

Hierarchy Level

```
[edit services cos application-profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** value for SIP traffic.

Default

By default, the system will not alter the DSCP or forwarding class for SIP traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

snmp-command

Syntax

```
snmp-command command;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

SNMP command format.

Options

command—Supported commands are SNMP **get**, **get-next**, **set**, and **trap**.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring an SNMP Command for Packet Matching | **523**
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

snmp-trap-thresholds

Syntax

```
snmp-trap-thresholds {
    flows high high-threshold | low low-threshold;
    nat-address-port high high-threshold | low low-threshold;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 13.1.

Description

Configures SNMP flow thresholds for all flows for a service set or flows for all NAT pools configured for a service set..

Options

The remaining options are described separately.

flows high *high-threshold*—Configure the upper limit for all flows on the service set. The limit is expressed as a percentage of **max-flows** configured for the service set. When the number of active flows exceeds this limit, an SNMP trap is set.

Default: 90 percent of **max-flows**

flows low *low-threshold*—Configure the lower limit for all flows on the service set . The limit is expressed as a percentage of **max-flows** configured for the service set. When the number of active flows falls below this limit, an SNMP trap is set.

Default: 70 percent of **max-flows**

nat-address-port high *high-threshold*—Configure the upper limit for flows for all NAT pools on the service set. The limit is expressed as a percentage of **max-flows** configured for the service set. When the number of active flows exceeds this limit, an SNMP trap is set.

Default: 90 percent of **max-flows**

nat-address-port low *low-threshold*—Configure the lower limit for flows. The limit is expressed as a percentage of **max-flows** configured for the service set. When the number of active flows falls below this limit, an SNMP trap is set.

Default: 80 percent of **max-flows**

NOTE: SNMP traps that are generated when you modify the threshold value for flows of NAT address pools in a service set (by using the **snmp-trap-thresholds nat-address-port (high *high-threshold* | low *low-threshold*)** statement) are not effective in the PIC. Only the initial threshold value that is set is effective on the PIC and subsequent changes to the threshold value are not reflected on the PIC. As a workaround, for the configuration changes under the **[edit services nat pool *nat-pool-name*]** hierarchy level, you must deactivate and activate the relevant service-set to enable the updated configuration to become effective. Otherwise, you must reboot the PIC for the updated threshold value of to take effect.

NOTE: Until Junos OS Release 14.1, when the NAT pool utilization exceeded the high threshold value configured, an SNMP trap was sent. However, a similar SNMP trap was not triggered when the NAT pool utilization fell below the configured lower limit or threshold. Because NMS systems are being used to monitor and set alarm for threshold values, the absence of an SNMP trap when the low threshold value was reached caused NMS to retain an active alarm in the alarms list. As a result, starting with Release 14.2R1, an SNMP trap is generated when the NAT pool utilization reaches the lower threshold, thereby causing the alarm in NMS to be reset.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Set Limitations | 23

softwire-concentrator

Syntax

```
softwire-concentrator {
    ds-lite ds-lite-softwire-concentrator {
        auto-update-mtu;
        flow-limit flow-limit | session-limit-per-prefix session-limit-per-prefix;
        mtu-v6 bytes;
        softwire-address address;
    }
    map-e
    v6rd v6rd-softwire-concentator {
        ipv4-prefix ipv4-prefix;
        v6rd-prefix ipv6-prefix;
        mtu-v4 mtu-v4;
    }
}
```

Hierarchy Level

```
[edit services softwire]
```

Release Information

Statement introduced in Junos OS Release 10.4.
map-e option introduced in Junos OS Release 18.2R1 for MX Series Routers with MPC and MIC interfaces.

Description

Configure settings for a softwire concentrator.

Softwires are supported on the MS-DPC, MS-100, MS-400, and MS-500 line cards. Starting in Junos OS release 17.4R1, softwires for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a DS-Lite Softwire Concentrator | 389

Configuring a 6rd Softwire Concentrator | 414

softwire-options

Syntax

```
softwire-options {
    dslite-ipv6-prefix-length dslite-ipv6-prefix-length ;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 14.1.
Support added in Junos OS 20.2R1 for Next Gen Services on MX240, MX480, and MX960 routers.

Description

Specify the IPv6 prefix length associated with a subscriber's basic broadband bridging device that is subject to a limited number of sessions.

This feature is supported on MX Series routers equipped with MS-DPCs. Starting in Junos OS Release 18.2R1, this option is also supported on MS-MPCs and MS-MICs.

Options

dslite-ipv6-prefix-length—Subnet prefix representing the size of the subnet subject to session limitation.

Values: 56, 64, 96, 128

Default: 0—no limitation.

Required Privilege Level

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

RELATED DOCUMENTATION

DS-Lite Per Subnet Limitation Overview | 410

softwire-rules

Syntax

(softwire-rule *rule-name* | softwire-rule-sets *rule-set-name*);

Hierarchy Level

[edit services **service-set** *service-set-name*]

Release Information
Statement introduced in Junos OS Release 10.4.

Description
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.

Softwire rules are supported on the MS-DPC, MS-100, MS-400, and MS-500 line cards. Starting in Junos OS release 17.4R1, softwire rules for DS-Lite are supported on MX Series routers with MS-MPCs and MS-MICs.

Options
rule-name—Identifier for the collection of terms that constitute this rule.

rule-set-name—Identifier for the set of rules to be included.

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

RELATED DOCUMENTATION

Configuring Service Rules | 21

source-address (PCP)

Syntax

```
source-addressaddress <except>;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information
Statement introduced in Junos OS Release 13.2R1.

Description
Specify the source address that must be matched for the PCP rule. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options
address—Destination address or prefix value.

except—(Optional) Prevent the specified address or prefix from matching the PCP rule.

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

source-address (Service Sets)

Syntax

```
source-address source-address
```

Hierarchy Level

```
[edit services service-set service-set-name syslog host hostname]
```

Release Information

Statement introduced in Junos OS Release 13.1.

Description

Specify a source address to record in system log messages that are directed to a remote machine specified in the ***hostname*** statement.

> **NOTE:** The supported interfaces are ms, rms, and mams interfaces. If you do not specify the interface parameter, the command loops on all supported interfaces.

Options

source-address—A valid IP address, which is recorded as the message source in messages sent to the remote machines specified in the **host *hostname*** statement

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring System Logging for Service Sets | 36
- host | 1241
- service-set | 1455

source-address (Services CoS)

Syntax

```
source-address address;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 8.1.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Source address for rule matching.

Options

address—Source IPv4 or IPv6 address or prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring Match Conditions In CoS Rules | 825

source-address (IDS MS-DPC)

Syntax

```
source-address (address | any-unicast) <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.
address option enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the source address for rule matching when using the MS-DPC.

Options

address—Source IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Exempt the specified address, prefix, or unicast packets from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

source-address

Syntax

```
source-address address;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name from]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the source address for rule matching.

Options

address—Source IP address.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

source-address (Services NAT)

Syntax

```
source-address (address | any-unicast) <except>;
```

Hierarchy Level

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

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 IPv6 addresses in Junos OS Release 8.5.

Description

Specify the source address for rule matching.

Options

address—Source IPv4 or IPv6 address or prefix value.

any-unicast—Any unicast packet.

except—(Optional) Prevent the specified address or unicast packets from being translated.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

source-address (Services Stateful Firewall)

Syntax

```
source-address (address | any-ipv4 | any-ipv6 | any-unicast ) <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

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 IPv6 addresses in Junos OS Release 8.5.

Description

Source address for rule matching.

Options

address—Source IPv4 or IPv6 address or prefix value.

any-ipv4—Any IPv4 packet.

any-ipv6—Any IPv6 packet.

any-unicast—Any unicast packet.

except—(Optional) Exclude the specified address, prefix, IPv4, IPv6, or unicast packets from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

source-address-range (IDS MS-DPC)

Syntax

```
source-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Specify the source address range for rule matching when using the MS-DPC.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exempt the specified address range from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

source-address-range (PCP)

Syntax

```
source-address-range high maximum-value low minimum-value <except>;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the source address range that must be matched for the PCP rule. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

maximum-value—Upper boundary for the address range.

minimum-value—Lower boundary for the address range.

except—(Optional) Prevent the specified address range from matching the PCP rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

source-address-range (Services NAT)

Syntax

```
source-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the source address range for rule matching.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Prevent the specified address range from being translated.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

source-address-range (Services Stateful Firewall)

Syntax

```
source-address-range low minimum-value high maximum-value <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 7.6.
minimum-value and ***maximum-value*** options enhanced to support IPv4 and IPv6 addresses in Junos OS Release 8.5.

Description

Source address range for rule matching.

Options

minimum-value—Lower boundary for the IPv4 or IPv6 address range.

maximum-value—Upper boundary for the IPv4 or IPv6 address range.

except—(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

source-pool

Syntax

```
source-pool nat-pool-name;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the source address pool for translated traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

source-port

Syntax

```
source-port port-number;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Source port identifier.

Options

port-value—Identifier for the port. For a complete list, see "Configuring Source and Destination Ports" on page 509.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring Application Properties | **502**
- Configuring Source and Destination Ports | **509**
- Verifying the Output of ALG Sessions | **525**

source-prefix (IDS)

Syntax

```
source-prefix prefix-value;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then aggregation]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 17.1 on MS-MPCs.

Description

Specify the prefix length for source IPv4 address aggregation for the IDS rule. This applies session limits to an aggregation of all attacks from within a subnet of the specified length.

For example, if you configure a value of 24 for **source-prefix**, then attacks from 10.1.1.2 and 10.1.1.3 are counted as attacks from the 10.1.1/24 subnet. However, if a single host on a subnet generates a large number of network probing or flooding attacks, the flows for the entire subnet might be stopped.

Options

prefix-value—Integer value.

Range: 1 through 32

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring IDS Rules on an MS-DPC | **583**
- Configuring Protection Against Network Attacks on an MS-MPC | **601**
- Understanding IDS on an MS-MPC | **597**

source-prefix (Services NAT)

Syntax

```
source-prefix source-prefix;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced in Junos OS Release 7.6.
source-prefix option enhanced to support IPv6 addresses in Junos OS Release 8.5.

Description

Specify the source prefix for translated traffic.

Options

source-prefix—IPv4 or IPv6 source prefix value.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

source-prefix-ipv6 (IDS)

Syntax

```
source-prefix-ipv6 prefix-value;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then aggregation]
```

Release Information

Statement introduced in Junos OS Release 8.5.
Statement introduced in Junos OS Release 17.1 on MS-MPCs.

Description

Specify the prefix length for source IPv6 address aggregation for the IDS rule. This applies session limits to an aggregation of all attacks from within a subnet of the specified length.

For example, if you configure a value of 64 for **source-prefix-ipv6**, then attacks from 2001:db8:1234:72a2::2 and 2001:db8:1234:72a2::3 are counted as attacks from the 2001:db8:1234:72a2::/64 subnet. However, if a single host on a subnet generates a large number of network probing or flooding attacks, the flows for the entire subnet might be stopped.

Options

prefix-value—Integer value.

Range: 1 through 128

Required Privilege Level

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

RELATED DOCUMENTATION

- Configuring IDS Rules on an MS-DPC | **583**
- Configuring Protection Against Network Attacks on an MS-MPC | **601**
- Understanding IDS on an MS-MPC | **597**

source-prefix-list (PCP)

Syntax

```
source-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services pcp rule rule-name term term-name from]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the source prefix list that must be matched for the PCP rule. You configure the prefix list by including the **prefix-list** statement at the **[edit policy-options]** hierarchy level. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

Options

list-name—Source prefix list.

except—(Optional) Prevent the specified prefix list from matching the PCP rule.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

source-prefix-list (Services CoS)

Syntax

```
source-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules | 823

Routing Policies, Firewall Filters, and Traffic Policers User Guide

source-prefix-list (Services IDS)

Syntax

```
source-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in IDS Rules | 585

Routing Policies, Firewall Filters, and Traffic Policers User Guide

source-prefix-list (Services NAT)

Syntax

```
source-prefix-list list-name <except>;
```

Hierarchy Level

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

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

Routing Policies, Firewall Filters, and Traffic Policers User Guide

source-prefix-list (Services Stateful Firewall)

Syntax

```
source-prefix-list list-name <except>;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name from]
```

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

list-name—Destination prefix list.

except—(Optional) Exclude the specified prefix list from rule matching.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Match Conditions in Stateful Firewall Rules | 549

Routing Policies, Firewall Filters, and Traffic Policers User Guide

spi

Syntax

```
spi spi-value;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then manual direction direction]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the SPI for an SA.

Options

spi-value—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).

Range: 256 through 16,639

> **NOTE:** Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Security Associations | 639

stateful-firewall-rules

Syntax

```
(stateful-firewall-rules rule-names | stateful-firewall-rule-sets rule-set-name);
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the stateful firewall rules or rule set included in this service set. You can configure multiple rules, but only one rule set for each service.

Options

rule-name—Identifier for the collection of terms that make up this rule.

rule-set-name—Identifier for the set of rules to be included.

Required Privilege Level

System—To view this statement in the configuration.
System-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Service Rules | 21

stateful-nat64

Syntax

```
stateful-nat64 {
    clear-dont-fragment-bit;
}
```

Hierarchy Level

```
[edit services service-set service-set-name nat-options]
```

Release Information

Statement introduced with Junos OS Release 12.1.

Description

Set parameters for stateful NAT64 operation.

> **NOTE:** These parameters do not change the operation of other types of NAT.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Rules | 21
clear-dont-fragment-bit | 1132

syslog (Services CoS)

Syntax

```
syslog;
```

Hierarchy Level

```
[edit services cos rule rule-name term term-name then],
[edit services cos rule rule-name term term-name then reverse]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Enable system logging. The system log information from the Multiservices and Services PICs is passed to the kernel for logging in the **/var/log** directory. This setting overrides any **syslog** statement setting included in the service set or interface default configuration.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring Actions in CoS Rules | 826

syslog (IDS MS-DPC)

Syntax

```
syslog;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then logging]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable system logging when using the MS-DPC. The system log information from the MS-DPC is passed to the kernel for logging in the **/var/log** directory.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

syslog

Syntax

```
syslog;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable system logging. The system log information for the Adaptive Services or Multiservices Physical Interface Card (PIC) is passed to the kernel for logging in the **/var/log** directory.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

syslog (Interfaces)

Syntax

```
syslog {
    host hostname {
        facility-override facility-name;
        log-prefix prefix-number;
        services priority-level;
    }
}
```

Hierarchy Level

```
[edit interfaces interface-name services-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

For adaptive services interfaces, configure generation of system log messages for the service set. System log information is passed to the kernel for logging in the **/var/log** directory. Any values configured in the service set definition override these values.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Services Interfaces Library for Routing Devices

syslog (Services L2TP)

Syntax

```
syslog {
    host hostname {
        services severity-level;
        facility-override facility-name;
        log-prefix prefix-value;
    }
}
```

Hierarchy Level

```
[edit services l2tp tunnel-group group-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure the generation of system log messages for L2TP services. System log information is passed to the kernel for logging in the **/var/log/l2tpd** directory.

> **NOTE:** This statement is not supported for L2TP LNS on MX Series routers.

Options

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging of L2TP Tunnel Activity | 1044

syslog (Services NAT)

Syntax

```
syslog;
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then]
```

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.

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

syslog (Services Service Set)

Syntax

```
syslog {
    host hostname {
        class {
            alg-logs;
            deterministic-nat-configuration-log;
            ids-logs;
            nat-logs;
            packet-logs;
            pcp-logs;
            session-logs <open | close>;
            stateful-firewall-logs;
            urlf-logs;
        }
        facility-override facility-name;
        interface-service prefix-value;
        log-prefix prefix-value;
        port port-number;
        services severity-level;
        source-address source-address;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure generation of system log messages for the service set. The system log information is passed to the kernel for logging in the **/var/log** directory. These settings override the values defined at the **[edit interfaces *interface-name* services-options]** hierarchy level; for more information on configuring those values, see *Configuring System Logging for Services Interfaces*.

NOTE: Starting with Junos OS release 14.1X55, 14.2R5, 15.1R3, and 16.1R1, for multiservices (ms-) interfaces, you cannot configure system logging for PCP and ALGs by including the pcp-logs and alg-logs statements at the [edit services service-set service-set-name syslog host hostname class] hierarchy level. An error message is displayed if you attempt to commit a configuration that contains the pcp-logs and alg-logs options to define system logging for PCP and ALGs for ms- interfaces.

Options

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring System Logging for Service Sets | 36

syslog (Services Stateful Firewall)

Syntax

```
syslog;
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name then]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable system logging. The system log information from the Adaptive Services or Multiservices PIC is passed to the kernel for logging in the **/var/log** directory. This setting overrides any **syslog** statement setting included in the service set or interface default configuration.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in Stateful Firewall Rules | 550

syn-cookie (IDS MS-DPC)

Syntax

```
syn-cookie {
    mss value;
    threshold rate;
}
```

Hierarchy Level

[edit services ids **rule** *rule-name* **term** *term-name* **then**]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable SYN-cookie defenses against SYN attacks when using the MS-DPC. By default, SYN-cookie techniques are not applied.

When SYN cookie is enabled on Junos OS and becomes the TCP-negotiating proxy for the destination server, it replies to each incoming SYN segment with a SYN/ACK containing an encrypted cookie as its initial sequence number (ISN). The cookie is an MD5 hash of the original source address and port number, destination address and port number, and ISN from the original SYN packet. After sending the cookie, Junos OS drops the original SYN packet and deletes the calculated cookie from memory. If there is no response to the packet containing the cookie, the attack is noted as an active SYN attack and is effectively stopped.

If the initiating host responds with a TCP packet containing the cookie +1 in the TCP ACK field, Junos OS extracts the cookie, subtracts 1 from the value, and recomputes the cookie to validate that it is a legitimate ACK. If it is legitimate, Junos OS starts the TCP proxy process by setting up a session and sending a SYN to the server containing the source information from the original SYN. When Junos OS receives a SYN/ACK from the server, it sends ACKs to the server and to the initiation host. At this point the connection is established and the host and server are able to communicate directly.

Options

The remaining statements are described separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

tcp-fast-open

Syntax

```
tcp-fast-open {
    disabled;
    drop;
}
```

Hierarchy Level

```
[edit services service-set service-set-name service-set-options]
```

Release Information

Statement introduced in Junos OS Release 17.2.

Description

Specify how TCP Fast Open (TFO) enabled packets are to be handled.

Default

By default, all TFO packets are forwarded by the service PIC.

Options

disabled—Any TCP packet with the TFO option present has the TFO option stripped from the TCP header of the packet, and the rest of the packet is forwarded as is. The benefit of stripping the header over dropping the packet is that the client does not have to wait for the retransmission timer to go off and then retransmit the SYN packet without the TFO option.

drop—Any TCP packet with the TFO option present is dropped.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Exchanging Data More Efficiently Using TCP Fast Open | 60

tcp-mss (Services)

Syntax

```
tcp-mss number;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.5.

Description

Specify the TCP Maximum Segment Size (MSS) allowed for the service set.

Options

number—MSS value.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Set Limitations | 23

tcp-non-syn

Syntax

```
tcp-non-syn {
    drop-flow;
    drop-flow-send-rst;
}
```

Hierarchy Level

[edit services service-set *service-set-name* service-set-options]

Release Information

Statement introduced in Junos OS Release 16.1R2.

Description

Specify how the first non-SYN TCP packet is processed on services PICs. When a services PIC receives the first non-SYN TCP packet for processing, the packet is dropped.

Options

drop-flow—When a services PIC receives the first non-SYN TCP packet for processing, the packet is dropped.

A drop flow created on the services PIC ensures that subsequent non-SYN TCP packets with the same 5-tuple information (source and destination addresses, protocol, and source and destination ports) are dropped. If this statement is not configured, a session is created when a packet hits the services set and matches the stateful firewall rule even if the packet is a non-SYN packet.

drop-flow-send-rst—When a services PIC receives the first non-SYN TCP packet for processing, the packet is dropped and a reset packet is sent to originator to ensure that no further packets are generated.

A drop flow created on the services PIC ensures that subsequent non-SYN TCP packets with the same 5-tuple information (source and destination addresses, protocol, and source and destination ports) are dropped. If this statement is not configured, a session is created when a packet hits the services set and matches the stateful firewall rule even if the packet is a non-SYN packet.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces | 9

tcp-syn-defense (IDS MS-MPC)

Syntax

```
tcp-syn-defense;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Close unestablished TCP connections and send a TCP RST to the end host to clear the TCP states on it when the **open-timeout** value at the **[edit interfaces *interface-name* service-options]** hierarchy level expires. This provides protection against TCP SYN flooding attacks. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | 601
Understanding IDS on an MS-MPC | 597

tcp-syn-fragment-check (IDS MS-MPC)

Syntax

```
tcp-syn-fragment-check;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Identify and drop TCP SYN packets that are IP fragments. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**
Understanding IDS on an MS-MPC | **597**

tcp-winnuke-check (IDS MS-MPC)

Syntax

```
tcp-winnuke-check;
```

Hierarchy Level

[edit services ids rule *rule-name* term *term-name* then]

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Identify and drop TCP segments that are destined for port 139 and have the urgent (URG) flag set, which provides protection against WinNuke attacks. This statement can only be used in IDS rules assigned to a service set on an MS-MPC.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

template

Syntax

```
template template-name {
    client-interfaces [ client-interface-name1 client-interface-name2 ];
    disable-url-filtering;
    dns-resolution-interval minutes;
    dns-resolution-rate seconds;
    dns-retries number;
    dns-routing-instance dns-routing-instance-name;
    dns-server [ ip-address1 ip-address2 ip-address3 ];
    dns-source-interface loopback-interface-name;
    routing-instance routing-instance-name;
    server-interfaces [ server-interface-name1 server-interface-name2 ];
    term term-name {
        from {
            src-ip-prefix [prefix1 prefix2];
            dest-port [port1 port2];
        }
        then {
            accept;
            custom-page custom-page;
            http-status-code http-status-code;
            redirect-url redirect-url;
            tcp-reset;
        }
    }
    url-filter-database filename
}
```

Hierarchy Level

```
[edit services url-filter profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 17.2.
disable-url-filtering option introduced in Junos OS Release 17.2R2 and 17.4R1.

Description

Configure a URL filter template.

NOTE: Starting in Junos OS Release 18.3R1, the **template** statement is deprecated and has been replaced by the **url-filter-template** statement. The **template** statement is supported for backward compatibility.

Options

template-name—Name of the template.

client-interfaces [***client-interface-name1 client-interface-name2*** **]**—The list of client-facing logical interfaces (uplink) on which the URL filtering is configured. This option is mandatory.

disable-url-filtering—Disables the filtering of HTTP traffic that contains an embedded IP address (for example, http:/10.1.1.1) belonging to a blocklisted domain name in the URL filter database.

dns-resolution-interval ***minutes***—DNS resolution time interval in minutes.

Default: 1440

Range: 60 through 1440 minutes.

dns-resolution-rate ***seconds***—Number of DNS queries per second sent out from the system before initiating further DNS queries.

Default: 50

Range: 50 through 100.

dns-retries ***number***—Number of retries for a DNS query in case query fails or times out.

Default: 3

Range: 1 through 5.

dns-routing-instance ***dns-routing-instance-name***—The VRF on which the DNS server is reachable. This option is mandatory. You can use the default routing instance inet.0 or a defined routing instance.

dns-server [***ip-address1 ip-address2 ip-address3*** **]**—One or more IP (IPv4 or IPv6) addresses of DNS servers to which the DNS queries are sent out. This option is mandatory.

dns-source-interface ***loopback-interface-name***—The loopback interface for which source IP address is picked for sending DNS queries. This option is mandatory.

routing-instance ***routing-instance-name***—The VRF on which URL filtering feature is configured. This option is mandatory. You can use the default routing instance inet.0 or a defined routing instance.

server-interfaces [***server-interface-name1 server-interface-name2*** **]**—Server-facing interfaces to which traffic is destined. This option is mandatory.

The list of server-facing logical interfaces (downlink) on which the URL filtering is configured. This option is mandatory.

url-filter-database ***filename***—The filename of the URL filter database. The file should be placed in the **/var/db/url-filterd** directory, but indicate just the filename here and not the full path.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring URL Filtering | 55

term (Services CoS)

Syntax

```
term term-name {
  from {
    application-sets set-name;
    applications [ application-names ];
    destination-address address;
    destination-prefix-list list-name <except>;
    source-address address;
    source-prefix-list list-name <except>;
  }
  then {
    application-profile profile-name;
    dscp (alias | bits);
    forwarding-class class-name;
    syslog;
    reflexive; | revert; | reverse {
      application-profile profile-name;
      dscp (alias | bits);
      forwarding-class class-name;
      syslog;
    }
  }
}
```

Hierarchy Level

```
[edit services cos rule rule-name]
```

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define the CoS term properties.

Options

term-name—Identifier for the term.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring CoS Rules | 823.

Configuring CoS Rules on Services PICs

term (IDS MS-DPC)

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>;
    source-address (address | any-unicast) <except>;
    source-address-range low minimum-value high maximum-value <except>;
  }
  then {
    aggregation (IDS) {
      destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
      source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    (force-entry | ignore-entry);
    logging {
      syslog;
      threshold rate;
    }
    session-limit {
      by-destination (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
      by-pair (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
      by-source (IDS MS-DPC) {
        hold-time seconds;
        maximum number;
        packets number;
        rate number;
      }
    }
    syn-cookie {
      mss value;
```

```
        threshold rate;
      }
    }
}
```

Hierarchy Level

```
[edit services ids rule rule-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the IDS term properties when using the MS-DPC.

Options

term-name—Identifier for the term.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IDS Rules on an MS-DPC | 583

term

Syntax

```
term term-name {
    from {
        destination-address address;
        ipsec-inside-interface interface-name;
        source-address address;
    }
    then {
        anti-replay-window-size bits;
        backup-remote-gateway address;
        clear-dont-fragment-bit;
        dynamic {
            ike-policy policy-name;
            ipsec-policy policy-name;
        }
        initiate-dead-peer-detection;
        manual {
            direction (inbound | outbound | bidirectional) {
                authentication {
                    algorithm (hmac-sha-256);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi spi-value;
                encryption {
                    algorithm algorithm;
                    key (ascii-text key | hexadecimal key);
                }
                protocol (bundle | esp);
                spi spi-value;
            }
        }
        no-anti-replay;
        remote-gateway address;
        syslog;
        tunnel-mtu bytes;
    }
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the IPsec term properties.

Options

term-name—Identifier for the term.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

term (IDS MS-MPC)

Syntax

```
term {
  then {
    aggregation (IDS) {
      destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
      source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    allow-ip-options {
      any;
      loose-source-route;
      route-record;
      route-alert;
      security;
      stream-id;
      strict-source-route;
      timestamp;
    }
    allow-ipv6-extension-header {
      any;
      ah;
      dstopts;
      esp;
      fragment;
      hop-by-hop;
      mobility;
      routing;
    }
    icmp-fragment-check;
    icmp-large-packet-check;
    land-attack-check (ip-only | ip-port);
    session-limit {
      by-destination {
        by-protocol {
          icmp {
            maximum number;
            packets number;
            rate number;
          }
          tcp {
            maximum number;
            packets number;
            rate number;
```

```
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
    by-source {
        by-protocol {
            icmp {
                maximum number;
                packets number;
                rate number;
            }
            tcp {
                maximum number;
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
  }
  tcp-syn-defense;
  tcp-syn-fragment-check;
  tcp-winnuke-check;
 }
}
```

Hierarchy Level

```
[edit services ids rule rule-name]
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure the network attack prevention actions for an IDS rule for a service set on an MS-MPC.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

term (PCP)

Syntax

```
term term-name {
   from {
      application-sets set-name;
      applications [ application-name ];
      destination-address address <except>;
      destination-address-range high maximum-value low minimum-value <except>;
      destination-port high maximum-value low minimum-value;
      destination-prefix-list list-name <except>;
      source-address address <except>;
      source-address-range high maximum-value low minimum-value <except>;
      source-prefix-list list-name <except>;
   }
   then {
      pcp-server server-name;
   }
}
```

Hierarchy Level

```
[edit services pcp rule rule-name]
```

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Define the PCP rule term properties. A PCP rule assigns the PCP server that handles selected traffic.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

The remaining statements are explained separately.

Options

term-name—Identifier for the term.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

term (Services NAT)

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-port range high maximum-value low minimum-value;
        source-address (address | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
    }
    then {
        no-translation;
        port-forwarding-mappings map-name;
        translated {
            address-pooling paired;
            clat-prefix clat-prefix;
            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;
            source-pool nat-pool-name;
            source-prefix source-prefix;
            translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | dnat-44 | deterministic-napt44 |
                deterministic-napt64 |dynamic-nat44 | napt-44 | napt-66 | napt-pt | stateful-nat464 | stateful-nat64 |
                twice-basic-nat-44 | twice-dynamic-nat-44 | twice-napt-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.

Options

term-name—Identifier for the term.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

term (Services Stateful Firewall)

Syntax

```
term term-name {
    from {
        application-sets set-name;
        applications [ application-names ];
        destination-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
        destination-address-range low minimum-value high maximum-value <except>;
        destination-prefix-list list-name <except>;
        source-address (address | any-ipv4 | any-ipv6 | any-unicast) <except>;
        source-address-range low minimum-value high maximum-value <except>;
        source-prefix-list list-name <except>;
    }
    then {
        (accept | discard | reject);
        syslog;
    }
}
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the stateful firewall term properties.

Options

term-name—Identifier for the term.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Stateful Firewall Rules | 546

term (URL Filter)

Syntax

```
term term-name {
    from {
        src-ip-prefix [prefix1 prefix2];
        dest-port [port1 port2];
    }
    then {
        accept;
        custom-page custom-page;
        http-status-code http-status-code;
        redirect-url redirect-url;
        tcp-reset;
    }
}
```

Hierarchy Level (starting in Junos OS Release 18.3R1)

```
[edit services web-filter profile profile-name url-filter-template template-name]
```

Hierarchy Level (before Junos OS Release 18.3R1)

```
[edit services url-filter profile profile-name template template-name]
```

Release Information

Statement introduced in Junos OS Release 17.2.

Description

Define a URL filtering term. A term is a set of match criteria with actions to be taken if the match criteria is met. You must configure **term** to configure URL filtering.

Options

term-name—Name of the term.

from—Define match criteria.

> The **from** statement is optional. If you omit the **from** statement, all source IP prefixes and all destination ports are considered to match. All such combinations then take the configured actions of the term.
>
> Only one term in a template can have an optional **from** statement. If you omit more than one **from** statement per template, you will get the following error message on commit:

```
URLFD_CONFIG_FAILURE: Configuration not valid:
Cannot have two wild card terms in template template1
error: configuration check-out failed
```

Similarly, no two templates within a profile can have a term without a **from** statement.

dest-ports—Destination port list specification.

Range: 1 through 65535

src-ip-prefix—Source IP prefix list specification.

then—Specify one of the following actions to be taken if the **from** condition is matched:

accept—Accept the traffic and allow it to flow as normal.

custom-page *custom-page*—Custom-page string.

http-status-code *http-status-code*—HTTP status code value.

Range: 400 through 599

redirect-url *redirect-url*—URL to redirect traffic to.

tcp-reset—Reset TCP.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

then (Services CoS)

Syntax

```
then {
    application-profileprofile-name;
    dscp (alias | bits);
    forwarding-class class-name;
    syslog;
    reflexive; | revert; | reverse {
        application-profile profile-name;
        dscp (alias | bits);
        forwarding-class class-name;
        syslog;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 8.1.

Description

Define the CoS term actions.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

Configuring Actions in CoS Rules | 826

then (IDS MS-DPC)

Syntax

```
then {
    aggregation (IDS) {
        destination-prefix prefix-number | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-number | source-prefix-ipv6 prefix-value;
    }
    (force-entry | ignore-entry);
    logging {
        syslog;
        threshold rate;
    }
    session-limit {
        by-destination (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-pair (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
        by-source (IDS MS-DPC) {
            hold-time seconds;
            maximum number;
            packets number;
            rate number;
        }
    }
    syn-cookie {
        mss value;
        threshold rate;
    }
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the IDS term actions when using the MS-DPC.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IDS Rules on an MS-DPC | 583

then (IDS MS-MPC)

Syntax

```
then {
    aggregation (IDS) {
        destination-prefix prefix-value | destination-prefix-ipv6 prefix-value;
        source-prefix prefix-value | source-prefix-ipv6 prefix-value;
    }
    allow-ip-options {
        any;
        loose-source-route;
        route-record;
        route-alert;
        security;
        stream-id;
        strict-source-route;
        timestamp;
    }
    allow-ipv6-extension-header {
        any;
        ah;
        dstopts;
        esp;
        fragment;
        hop-by-hop;
        mobility;
        routing;
    }
    icmp-fragment-check;
    icmp-large-packet-check;
    land-attack-check (ip-only | ip-port);
    session-limit {
        by-destination {
            by-protocol {
                icmp {
                    maximum number;
                    packets number;
                    rate number;
                }
                tcp {
                    maximum number;
                    packets number;
                    rate number;
                }
```

```
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
    by-source {
        by-protocol {
            icmp {
                maximum number;
                packets number;
                rate number;
            }
            tcp {
                maximum number;
                packets number;
                rate number;
            }
            udp {
                maximum number;
                packets number;
                rate number;
            }
        }
        maximum number;
        packets number;
        rate number;
    }
  }
  tcp-syn-defense;
  tcp-syn-fragment-check;
  tcp-winnuke-check;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Configure the network attack prevention actions for an IDS rule for a service set on an MS-MPC.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

Understanding IDS on an MS-MPC | **597**

then

Syntax

```
then {
    anti-replay-window-size bits;
    backup-remote-gateway address;
    clear-dont-fragment-bit;
    dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
    }
    initiate-dead-peer-detection;
    manual {
        direction (inbound | outbound | bidirectional) {
            authentication {
                algorithm (hmac-sha-256);
                key (ascii-text key | hexadecimal key);
            }
            auxiliary-spi spi-value;
            encryption {
                algorithm algorithm;
                key (ascii-text key | hexadecimal key);
            }
            protocol (bundle | esp);
            spi spi-value;
        }
    }
    no-anti-replay;
    remote-gateway address;
    syslog;
    tunnel-mtu bytes;
}
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define the IPsec term actions.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

then (Services NAT)

Syntax

```
then {
    no-translation;
    port-forwarding-mappings map-name;
    translated {
        address-pooling paired;
        clat-prefix clat-prefix;
        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;
        source-pool nat-pool-name;
        source-prefix source-prefix;
        translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | deterministic-napt44 | deterministic-napt64 | dnat-44
            | dynamic-nat44 | napt-44 | napt-66 | napt-pt | stateful-nat464 | stateful-nat64 | twice-basic-nat-44 |
            twice-dynamic-nat-44 | twice-napt-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.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

then (PCP)

Syntax

```
then {
    pcp-server server-name;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 13.2R1.

Description

Specify the PCP server to handle the traffic that matches the PCP rule term.

PCP is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, PCP is also supported on the MS-MPC and MS-MIC.

The remaining statements are explained separately.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Control Protocol | 261

then (Services Stateful Firewall)

Syntax

```
then {
   (accept <skip-ids>| discard | reject);
   syslog;
}
```

Hierarchy Level

```
[edit services stateful-firewall rule rule-name term term-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.
skip-ids option added in Junos OS Release 17.1 on MS-MPC and MS-MIC on MX Series.

Description

Define the stateful firewall term actions. You can configure the router to accept, discard, or reject the targeted traffic. The other actions are optional.

Options

accept—Accept the traffic and send it on to its destination.

accept skip-ids—The packet is accepted and sent on to its destination, but IDS rule processing configured on an MS-MPC or MS-MIC is skipped.

discard—Do not accept traffic or process it further.

reject—Do not accept the traffic and return a rejection message. Rejected traffic can be logged or sampled.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in Stateful Firewall Rules | 550

Routing Policies, Firewall Filters, and Traffic Policers User Guide

Configuring Protection Against Network Attacks on an MS-MPC | 601

threshold (Services IPsec)

Syntax

```
threshold number;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then dead-peer-detection]
```

Release Information

Statement introduced in Junos OS Release 11.4.
IKEv2 support introduced in Junos OS Release 17.2.

Description

Specify the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. The **threshold** value is used for IKEv1 security associations (SAs). Starting in Junos OS Release 17.2R1, the **threshold** value is also applicable to IKEv2 SAs. In Junos OS Release 17.1 and earlier, the **threshold** option is not applicable to IKEv2 SAs, which use the default value.

Options

number—Maximum number of unsuccessful DPD requests to be sent.

Range: 1 through 10

Default: 3

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Rules | 688

threshold (Services Logging and SYN-Cookie Defenses)

Syntax

```
threshold rate;
```

Hierarchy Level

```
[edit services ids rule rule-name term term-name then logging],
[edit services ids rule rule-name term term-name then syn-cookie]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the threshold for logging or applying SYN-cookie defenses when using the MS-DPC.

Options

rate—Logging threshold number of events per second.

rate—SYN-cookie defense number of SYN attacks per second.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Actions in IDS Rules | 586

traceoptions (Health Check Monitoring)

Syntax

```
traceoptions {
    file file-name ;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    monitor monitor-object-name {
        group-name group-name;
        real-services-name real-service-name;
    }
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services network-monitoring]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.

Description

Specify tracing options for the traffic load balancer health check monitoring function.

Options

file *file-name*—Use the specified name of the file to receive the output of the tracing operation.

flag *flag*—Specify which operations you want to trace. To specify more than one operation, include multiple flag statements. Table 38 on page 1550 species the various values you can set this option to.

Table 38: Trace Flags

Flag	Support on MS-MPC and SPC3 Cards	Description
all	MS-MPC and SPC3	Trace all operations.
all-real-services	SPC3	Trace all real services.
config	MS-MPC	Trace traffic load balancer configuration events.
connect	MS-MPC	Trace traffic load balancer ipc events.
database	MS-MPC and SPC3	Trace database events.
file-descriptor-queue	MS-MPC	Trace file descriptor queue events.
inter-thread	MS-MPC	Trace inter-thread communication events.
filter	MS-MPC	Trace traffic load balancer filter programming events.
health	MS-MPC	Trace traffic load balancer health events.
messages	MS-MPC and SPC3	Trace normal events.
normal	MS-MPC	Trace normal events.
operational-commands	MS-MPC	Trace traffic load balancer show events.
parse	MS-MPC	Trace traffic load balancer parse events.
probe	MS-MPC and SPC3	Trace probe events.
probe-infra	MS-MPC and SPC3	Trace probe infra events.
route	MS-MPC	Trace traffic load balancer route events.
snmp	MS-MPC	Trace traffic load balancer SNMP events.
statistics	MS-MPC	Trace traffic load balancer statistics events.
system	MS-MPC	Trace traffic load balancer system events.

group-name *group-name*—Specify which server group is to be traced.

level—Use the specified level of tracing. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

monitor *monitor-object-name*—Name of a monitoring object that contains server group or real service.

no-remote-trace—Disable remote tracing.

real-services-name *real-service-name*—Specify which real service is to be traced.

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

RELATED DOCUMENTATION

Configuring TLB | **979**

traceoptions (Security PKI)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag;
}
```

Hierarchy Level

```
[edit security pki]
```

Description

Configure security public key infrastructure (PKI) trace options. To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the **/var/log/pkid** file.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. To include the **file** statement, you must specify a filename.

files *number*—(Optional) Maximum number of trace files. When a trace file (for example, **pkid**) reaches its maximum size, it is renamed **pkid.0**, then **pkid.1**, and so on, until the maximum number of trace files is reached. When the maximum number is reached, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 2 files

flag—Trace operation to perform. To specify more than one trace operation, include multiple flag statements:

all—Trace with all flags enabled.

certificate-verification—Trace PKI certificate verification events.

online-crl-check—Trace PKI online certificate revocation list (CRL) events.

enrollment—PKI certificate enrollment tracing.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

size *maximum-file-size*—(Optional) Maximum size of each trace file, in kilobytes (KB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files *number*** option.

Default: 1024 KB

world-readable | no-world-readable—(Optional) By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

Required Privilege Level

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Tracing Junos VPN Site Secure Operations | 710

traceoptions (Services IPsec VPN)

Syntax

```
traceoptions {
    file <filename> <files number> <match regular-expression> <size bytes> <world-readable | no-world-readable>;
    flag flag;
    level level;
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services ipsec-vpn]
```

Release Information

Statement introduced in Junos OS Release 7.5.
level option added in Junos OS Release 10.0.

Description

Configure IPsec tracing operations. By default, messages are written to **/var/log/kmd**.

Options

files *number*—Maximum number of trace data files.

Range: 2 through 1000

flag *flag*—Tracing operation to perform:

- **all**—Trace everything.
- **certificates**—Trace certificates that apply to the IPsec service set.
- **database**—Trace security associations database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **snmp**—Trace SNMP operations.
- **timer**—Trace internal timer events.

level *level*—Key management process (kmd) tracing level. The following values are supported:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**–Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

size *bytes*—Maximum trace file size.

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

traceoptions (Services L2TP)

Syntax

```
traceoptions {
    debug-level level;
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-readable |
        no-world-readable>;
    filter {
        protocol name;
        user user@domain;
        user-name username;
    }
    flag flag;
    interfaces interface-name {
        debug-level level;
        flag flag;
    }
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services l2tp]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Define tracing operations for L2TP processes.

Options

debug-level *level*—Trace level for PPP, L2TP, RADIUS, and UDP; this option does not apply to L2TP on MX Series routers:

- **detail**—Trace detailed debug information.
- **error**—Trace error information.
- **packet-dump**—Trace packet decoding information.

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

filter—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifiers simplifies troubleshooting in a scaled environment.

- **protocol** *name*—One of the following protocols; this option does not apply to L2TP on MX Series routers:
  - **l2tp**
  - **ppp**
  - **radius**
  - **udp**
- **user** *user@domain*—Username of a subscriber; this option does not apply to L2TP on M Series routers. Optionally use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term or both terms.
- **user-name** *username*—Username of a subscriber; this option does not apply to L2TP on MX Series routers.

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **configuration**—Trace configuration events.
- **events**—Trace interface events.
- **general**—Trace general events.
- **gres**—Trace GRES events.
- **init**—Trace daemon initialization.
- **ipc-rx**—Trace IPC receive events.
- **ipc-tx**—Trace IPC transmit events.
- **memory**—Trace memory management code.
- **message**—Trace message processing code.
- **packet-error**—Trace packet error events.
- **parse**—Trace parsing events.
- **protocol**—Trace L2TP events.
- **receive-packets**—Trace received L2TP packets.
- **routing-process**—Trace routing process interactions.
- **routing-socket**—Trace routing socket events.
- **session-db**—Trace session database interactions.
- **states**—Trace state machine events.
- **timer**—Trace timer events.
- **transmit-packets**—Trace transmitted L2TP packets.
- **tunnel**—Trace tunnel events.

interfaces *interface-name*—Apply L2TP traceoptions to a specific services interface. This option does not apply to L2TP on MX Series routers.

- **debug-level *level***—Trace level for the interface; this option does not apply to L2TP on MX Series routers:
  - **detail**—Trace detailed debug information.
  - **error**—Trace error information.
  - **extensive**—Trace all PIC debug information.
- **flag *flag***—Tracing operation to perform for the interface. This option does not apply to L2TP on MX Series routers. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:
  - **all**—Trace everything.
  - **ipc**—Trace L2TP Inter-Process Communication (IPC) messages between the PIC and the Routing Engine.
  - **packet-dump**—Dump each packet content based on debug level.
  - **protocol**—Trace L2TP, PPP, and multilink handling.
  - **system**—Trace packet processing on the PIC.

level—Specify level of tracing to perform. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***size*k** to specify KB, ***size*m** to specify MB, or ***size*g** to specify GB

Range: 10240 through 1073741824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Tracing L2TP Operations | **1053**

Tracing L2TP Events for Troubleshooting

traceoptions (Services Logging)

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression> <size size> <world-readable | no-world-readable>;
    flag flag;
    no-remote-trace;
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.
file option added in Release 8.0.

Description

Configure Adaptive Services or Multiservices PIC tracing operations. The messages are output to **/var/log/serviced**.

Options

file *filename*—Name of the file to receive the output of the tracing operation. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files. When a trace file named ***trace-file*** reaches its maximum size, it is renamed ***trace-file*.0**, then ***trace-file*.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 3 files

flag *flag*—Tracing operation to perform:

- **all**—Trace everything.
- **command-queued**—Trace command enqueue events.
- **config**—Trace configuration events.
- **handshake**—Trace handshake events.
- **init**—Trace initialization events.

- **interfaces**—Trace interface events.
- **mib**—Trace GGSN SNMP MIB events.
- **removed-client**—Trace client cleanup events.
- **show**—Trace CLI command servicing.

match *regex*—(Optional) Match output to a defined regular expression (regex).

Default: If you do not include this option, the trace operation output includes all lines relevant to the logged events.

no-world-readable—(Optional) Prevent any user from reading the log file.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named ***trace-file*** reaches this size, it is renamed ***trace-file*.0**. When the ***trace-file*** again reaches its maximum size, ***trace-file*.0** is renamed ***trace-file*.1** and ***trace-file*** is renamed ***trace-file*.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: ***x*k** to specify KB, ***x*m** to specify MB, or ***x*g** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Allow any user to read the log file.

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

RELATED DOCUMENTATION

Tracing Services PIC Operations | 38

traceoptions (Traffic Load Balancer)

Syntax

```
traceoptions {
    file file-name <files number> <no-word-readable | world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    monitor monitor-object-name {
        instance-name instance-name;
        virtual-svc-name virtual-service-name;
    }
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services traffic-load-balance]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
instance-name and **virtual-service-name** options added in Junos OS Release 16.1R6 and 18.2R1 on MX Series.
Support for Next Gen Services MX-SPC3 services card add in Junos OS Release 19.3R2.

Description

Configure tracing options for the traffic load balancer.

Options

file *file-name*—Name of the file to receive the output of the tracing operation.

files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Range: 2 through 1000 files

Default: 3 files

flag *flag*— Specify which operations you want to trace from Table 39 on page 1564. To specify more than one operation, include multiple flag statements.

Table 39: Trace Flags

Flag	Support on MS-MPC and MX-SPC3 Cards	Description
all	MS-MPC and MX-SPC3	Trace all operations.
all-real-services	MS-MPC and MX-SPC3	Trace all real services.
database	MS-MPC and MX-SPC3	Trace database events.
file-descriptor-queue	MS-MPC and MX-SPC3	Trace file descriptor queue events.
inter-thread	MS-MPC and MX-SPC3	Trace inter-thread communication events.
messages	MS-MPC and MX-SPC3	Trace normal events.
probe	MS-MPC and MX-SPC3	Trace probe events.
probe-infra	MS-MPC and MX-SPC3	Trace probe infra events.

instance-name *instance-name*—(Optional) Name of the TLB instance to monitor.

level—Use the specified level of tracing. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

These trace levels are available for both the MS-MPC and MX-SPC3 services cards unless otherwise specified.

monitor *monitor-object-name*—Name of a monitoring object that contains an instance name or virtual service name.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

For Next Gen Services on the MX-SPC3 services card, set the *monitor-object-name* to either:

group-name—Name of the group.

real-services-name—Name of the real service

size *size*—(Optional) Use the maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.

Range: 10,240 through 1,073,741,824 bytes.

Default: 128 KB

virtual-svc-name *virtual-service-name*—(Optional) Name of the virtual service to monitor.

word-readable—(Optional) Enable unrestricted file access.

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | **970**

Configuring TLB | **979**

traceoptions (Services Redundancy Daemon)

Syntax

```
traceoptions {
    file file-name <files number> <no-word-readable | world-readable> <size size>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services redundancy-set]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.

Description

Specify the level of redundancy system events to be traced.

Options

file *file-name*—Name of the file to receive the output of the tracing operation.

files *number*—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Range: 2 through 1000 files

Default: 3 files

flag *flag*—Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.

- **all**—Trace everything.
- **config**—Trace services redundancy configuration events.
- **connect**—Trace services redundancy ipc events.
- **error**—Trace services redundancy errors.
- **database**—Trace services database events.
- **normal**—Trace normal events.
- **opcmd**—Trace services redundancy opcmd events.
- **parse**—Trace services redundancy parse events.

- **route**—Trace services redundancy route events.
- **snmp**—Trace services redundancy snmp events.
- **state**—Trace services redundancy set state-machine.
- **switchover**—Trace switchover events.
- **system**—Trace services redundancy system events.

level—Use the specified level of tracing. You can specify any of the following levels:

- **all**—Match all levels.
- **critical**—Match critical conditions.
- **error**—Match error conditions.
- **info**—Match informational messages
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Use the maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.

Range: 10,240 through 1,073,741,824 bytes.

Default: 128 KB

word-readable—(Optional) Enable unrestricted file access.

Required Privilege Level

maintenance—To view this statement in the configuration.
maintenance-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring the Service Redundancy Daemon | 878

traffic-load-balance (Traffic Load Balancer)

Syntax

```
traffic-load-balance {
   instance instance-name {
      client-interface client-interface;
      client-vrf client-vrf;
      group group-name {
         health-check-interface-subunit health-check-interface-subunit;
         network-monitoring-profile [profile-name1, <profile-name2>];
         real-service-rejoin-options no-auto-rejoin;
         real-services [server-list];
         <routing-instance routing-instance>;
      }
      interface interface-name;
      real-service real-service {
         address server-ip-address;
         admin-down;
      }
      server-inet-bypass-filter server-inet-bypass-filter ;
      server-inet6-bypass-filter server-inet6-bypass-filter ;
      server-interface server-interface;
      server-vrf server-vrf;
      traceoptions {
         file file-name <files number> <no-word-readable | world-readable> <size size>;
         flag flag;
         level (all | critical | error | info | notice | verbose | warning);
         monitor {
            instance-name instance-name;
            virtual-svc-name virtual-service-name;
         }
         no-remote-trace;
      }
      virtual-service virtual-service-name {
         address virtual-ip–address;
         group group-name;
         load-balance-method {
            hash {
               hash-key method;
            }
            random;
         }
         mode ( layer2-direct-server-return | direct-server-return | translated );
         <routing-instance routing-instance-name>;
```

```
        <routing-metric route-metric>;
        server-interface server-interface;
        service service-name {
            protocol (udp | tcp);
            server-listening-port port;
            virtual-port virtual-port;
        }
    }
  }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure traffic load balancer options.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | 970

Configuring TLB | 979

translated

Syntax

```
translated {
    address-pooling paired;
    clat-prefix clat-prefix;
    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-name;
    overload-prefix;
    source-pool nat-pool-name;
    translation-type (basic-nat-pt | basic-nat44 | basic-nat66 |deterministic-napt44 | deterministic-napt64 | dnat-44
        | dynamic-nat44 | napt-44 | napt-66 | napt-pt | stateful-nat464 | stateful-nat64 | twice-basic-nat-44 |
        twice-dynamic-nat-44 | twice-napt-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.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

transport

Syntax

```
transport [ transport-protocols ];
```

Hierarchy Level

```
[edit services nat pool nat-pool-name 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

[*transport-protocol*]—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.

trigger-link-failure

Syntax

```
trigger-link-failure interface-name;
```

Hierarchy Level

```
[edit interfaces lsq-fpc/pic/port lsq-failure-options]
```

Release Information

Statement introduced in Junos OS Release 7.4.

Description

List of SONET interfaces connected to the LSQ interface that can implement Automatic Protection Switching (APS) if the Link Services IQ PIC fails.

Options

interface-name—Name of SONET interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Association between LSQ and SONET Interfaces | 909

translated-port

Syntax

```
translated-port port id;
```

Hierarchy Level

```
[edit services nat port-forwarding map-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Specify the port to which all traffic will be translated.

The **translated-port** statement is supported on the MS-DPC, MS-100, MS-400, and MS-500 MultiServices PICS. Starting in Junos OS Release 17.4R1, the **translated-port** statement is also supported on the MS-MPC and MS-MIC.

Options

port id—The port number to which traffic will be translated.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Port Forwarding for Static Destination Address Translation | 287

Configuring Port Forwarding Without Destination Address Translation | 291

translation-type

Syntax

```
translation-type (basic-nat-pt | basic-nat44 | basic-nat66 | nat-44 | deterministic-napt44 | deterministic-napt64 |
    dnat-44 | dynamic-nat44 | napt-44 | napt-66 | napt-pt | nptv6 | stateful-nat464 | stateful-nat64 | twice-basic-nat-44
    | twice-dynamic-nat-44 | twice-napt-44)
```

Hierarchy Level

```
[edit services nat rule rule-name term term-name then translated]
```

Release Information

Statement introduced before Junos OS Release 7.4.
The following options introduced in Junos OS Release 11.2, replacing all previous options.

- **basic-nat44**
- **basic-nat66**
- **basic-nat-pt**
- **dnat-44**
- **dynamic-nat44**
- **napt-44**
- **napt-66**
- **napt-pt**
- **stateful-nat64**

deterministic-napt44 option introduced in Junos OS Release 12.1.
deterministic-napt64 option introduced in Junos OS Release 17.4R1.
nptv6 option introduced in Junos OS Release 15.1
stateful-nat464 option introduced in Junos OS Release 17.1R1.
twice-basic-nat-44 option introduced in Junos OS Release 11.4.
twice-dynamic-nat-44 option introduced in Junos OS Release 11.4.
twice-napt-44 option introduced in Junos OS Release 11.4.

Description

Specify the NAT translation types. To identify the interface cards and Junos OS releases that support each translations type, see "Carrier-Grade NAT Feature Comparison for Junos Address Aware by Type of Interface Card" on page 87.

Options

basic-nat44—Translate the source address statically (IPv4 to IPv4).

basic-nat66—Translate the source address statically (IPv6 to IPv6).

basic-nat-pt—Translate the addresses of IPv6 hosts as they originate sessions to the IPv4 hosts in the external domain. The **basic-nat-pt** option is always implemented with DNS ALG.

deterministic-napt44—Translate as deterministic NAPT44.

deterministic-napt64—Translate as deterministic NAPT64.

dnat-44—Translate the destination address statically (IPv4 to IPv4).

dynamic-nat44—Translate only the source address by dynamically choosing the NAT address from the source address pool.

napt-44—Translate the transport identifier of the IPv4 private network to a single IPv4 external address.

napt-66—Translate the transport identifier of the IPv6 private network to a single IPv6 external address.

napt-pt—Bind addresses in an IPv6 network with addresses in an IPv4 network and vice versa to provide transparent routing for the datagrams traversing between the address realms.

nptv6—Translate the source address prefix in a stateless manner (IPv6 to IPv6).

stateful-nat464—Implement 464XLAT Provider-Side Translater (PLAT) address translation for source IP addresses and IPv6 prefix removal translation for destination IPv4 addresses.

stateful-nat64—Implement dynamic address and port translation for source IP addresses (IPv6-to-IPv4) and prefix removal translation for the destination IP addresses (IPv6-to-IPv4).

twice-basic-nat-44—Translate the source and destination addresses statically (IPv4 to IPv4).

> **NOTE:** Starting with Junos OS Release 15.1R1, the twice NAT functionality (**twice-basic-nat-44**, **twice-dynamic-nat-44**, and **twice-dynamic-napt-44** options) is supported on MX Series routers with MS-MPCs and MS-MICs.

twice-dynamic-nat-44—Translate the source address by dynamically choosing the NAT address from the source address pool. Translate the destination address statically.

twice-dynamic-napt-44—Translate the transport identifier of the IPv4 private network to a single IPv4 external address. Translate the destination address statically.

Required Privilege Level

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

RELATED DOCUMENTATION

Network Address Translation Rules Overview | 106

trusted-ca

Syntax

```
trusted-ca ca-profile-name;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 7.5.

Description

Identify one or more trusted IPsec certification authorities.

Options

ca-profile-name—Name of certification authority profile, which is configured at the **[edit security pki]** hierarchy level.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

ttl-threshold

Syntax

```
ttl-threshold number;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the traceroute time-to-live (TTL) threshold value. This value sets the acceptable level of network penetration for trace routing.

Options

number—TTL threshold value.

Required Privilege Level

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

RELATED DOCUMENTATION

- ALG Descriptions | **466**
- Configuring the TTL Threshold | **523**.
- Examples: Configuring Application Protocols | **524**
- Verifying the Output of ALG Sessions | **525**

tunnel-group

Syntax

```
tunnel-group group-name {
    aaa-access-profile profile-name;
    dynamic-profile profile-name;
    hello-interval seconds;
    hide-avps;
    l2tp-access-profile profile-name;
    local-gateway address {
        address address;
        gateway-name gateway-name;
    }
    maximum-send-window packets;
    maximum-sessions number;
    ppp-access-profile profile-name;
    receive-window packets;
    retransmit-interval seconds;
    service-device-pool pool-name;
    service-interface interface-name;
    service-profile profile-name(parameter)&profile-name;
    syslog {
        host hostname {
            services severity-level;
            facility-override facility-name;
            log-prefix prefix-value;
        }
    }
    tos-reflect;
    tunnel-switch-profile profile-name;
    tunnel-timeout seconds;
}
```

Hierarchy Level

```
[edit services l2tp]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Support for MX Series routers introduced in Junos OS Release 11.4.

Description

Specify the L2TP tunnel properties.

NOTE: Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

Options

group-name—Identifier for the tunnel group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring L2TP Tunnel Groups | **1041**

Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

tunnel-mtu (Services IPsec VPN)

Syntax

```
tunnel-mtu bytes;
```

Hierarchy Level

```
[edit services ipsec-vpn rule rule-name term term-name then]
```

Release Information

Statement introduced in Junos OS Release 7.5.

Description

Maximum transmission unit (MTU) size for IPsec tunnels. This defines the maximum size of an IP packet, including the IPsec overhead.

Options

bytes—MTU size.

Default: 1500 bytes

Range: 256 through 9192 bytes

> **NOTE:** Clear the **IPsec SA** in **tunnel-mtu** to accomodate Jumbo frames larger than 1500 bytes.

Required Privilege Level

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

tunnel-mtu (Services Service Set)

Syntax

```
tunnel-mtu bytes;
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 10.0.

Description

Maximum transmission unit (MTU) size for IPsec tunnels. This statement is useful for dynamic endpoint tunnels for which you cannot configure the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

For static IPsec tunnels, this statement sets the tunnel MTU value for all the tunnels within this service set. If you need a specific value for a particular tunnel, then set the **tunnel-mtu** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level.

> **NOTE:** The **tunnel-mtu** setting at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level overrides the value specified at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

Options

bytes—MTU size.

Default: 1500 bytes

Range: 256 through 9192 bytes

Required Privilege Level

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

RELATED DOCUMENTATION

- *mtu*

Configuring IPsec Service Sets | 698

Configuring IPsec Rules | 688

tunnel-timeout

Syntax

```
tunnel-timeout seconds;
```

Hierarchy Level

```
[edit services l2tp tunnel-group name]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the maximum downtime for an L2TP tunnel, after which the tunnel is terminated because the connection is presumed to have been lost.

Options

seconds—Interval after which the tunnel is terminated if no data can be sent.

Default: 120 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Timers for L2TP Tunnels | 1043

Configuring an L2TP Tunnel Group for LNS Sessions with Inline Services Interfaces

udp-encapsulation

Syntax

```
udp-encapsulation {
    <udp-dest-port destination-port>;
}
```

Hierarchy Level

```
[edit services service-set service-set-name ipsec-vpn-options]
```

Release Information

Statement introduced in Junos OS Release 16.1 on the MX Series.

Description

Enable multiple path forwarding of IPsec traffic by adding a UDP header to the IPsec encapsulation of packets. Doing this increases the throughput of IPsec traffic. If you do not enable UDP encapsulation, all the IPsec traffic follows a single forward path rather than using multiple available paths.

Options

udp-dest-port *destination-port*—(Optional) Use the specified UDP destination port for the UDP header that is appended to the ESP encapsulation.

Range: 1025 through 65536. Do not use 4500.

Default: If you do not include the **udp-dest-port** statement, the default UDP destination port is 4565.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring IPsec Service Sets | 698

IPsec Multipath Forwarding with UDP Encapsulation | 627

unit (Aggregated Multiservices)

Syntax

```
unit interface-unit-number {
   family family;
}
```

Hierarchy Level

```
[edit interfaces interface-name]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure the logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

The remaining statements are explained separately. See CLI Explorer.

Options

interface-unit-number—Number of the logical unit.

> **NOTE:** Unit 0 is reserved and cannot be configured under the aggregated Multiservices interface (**ams**).

Range: 1 through 16,384

Required Privilege Level

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

RELATED DOCUMENTATION

- Understanding Aggregated Multiservices Interfaces | **994**
- Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**
- interfaces | **1260**

unit (Interfaces)

Syntax

```
unit logical-unit-number {
    family inet {
        address address {
        }
        service {
            input {
                [ service-set service-set-name <service-filter filter-name> ];
                post-service-filter filter-name;
            }
            output {
                [ service-set service-set-name <service-filter filter-name> ];
            }
        }
        service-domain (inside | outside);
    }
}
```

Hierarchy Level

```
[edit interfaces interface-name ]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options

logical-unit-number—Number of the logical unit.

Range: 0 through 16,384

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Network Interfaces Library for Routing Devices for other statements that do not affect services interfaces.

unit (Voice Services)

Syntax

```
unit logical-unit-number {
    compression {
        rtp {
            f-max-period number;
            maximum-contexts number <force>;
            port {
                minimum port-number;
                maximum port-number;
            }
            queues [ queue-numbers ];
        }
    }
    compression-device interface-name;
    encapsulation type;
    family family {
        address address {
            ...
        }
        bundle (lsq-fpc/pic/port | ...);
    }
}
```

Hierarchy Level

```
[edit interfaces interface-name ]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options

logical-unit-number—Number of the logical unit.

Range: 0 through 16,384

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Junos OS Network Interfaces Library for Routing Devices for other statements that do not affect services interfaces.

Configuring Services Interfaces for Voice Services | **1026**

url-filter

Syntax

```
url-filter {
   profile  profile-name {
      template template-name {
         client-interfaces [ client-interface-name1 client-interface-name2 ];
         disable-url-filtering;
         dns-resolution-interval minutes;
         dns-resolution-rate seconds;
         dns-retries number;
         dns-routing-instance dns-routing-instance-name;
         dns-server [ ip-address1 ip-address2 ip-address3 ];
         dns-source-interface loopback-interface-name;
         routing-instance routing-instance-name;
         server-interfaces [ server-interface-name1 server-interface-name2 ];
         term term-name {
            from {
               src-ip-prefix [prefix1 prefix2];
               dest-port [port1 port2];
            }
            then {
               accept;
               custom-page custom-page;
               http-status-code http-status-code;
               redirect-url redirect-url;
               tcp-reset;
            }
         }
         url-filter-database filename
      }
      url-filter-database filename;
   }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 17.2.

Description

Configure URL filtering service.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **url-filter** statement is deprecated and has been replaced by the **web-filter** statement. The **url-filter** statement is supported for backward compatibility.

Options

url-filter-database *filename*—Specify the filename of the URL filter database. This option is mandatory.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring URL Filtering | 55
URL Filtering Overview | 52

url-filter-profile

Syntax

```
url-filter-profile profile-name;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.2.

Description

Specify the URL filter profile that the service set uses. The URL filter profile specifies how to filter access to disallowed URLs, and is configured at the **[edit services url-filter]** hierarchy level.

NOTE: You must also configure the **next-hop-service** statement with this statement.

NOTE: Starting in Junos OS Release 18.3R1, the **url-filter-profile** statement is deprecated and has been replaced by the **web-filter-profile** statement. The **url-filter-profile** statement is supported for backward compatibility.

Options

profile-name—Name of the URL filter profile.

Required Privilege Level

system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring URL Filtering | 55
URL Filtering Overview | 52
url-filter | 1590

url-filter-template

Syntax

```
url-filter-template template-name {
    client-interfaces [ client-interface-name1 client-interface-name2 ];
    disable-url-filtering;
    dns-resolution-interval minutes;
    dns-resolution-rate seconds;
    dns-retries number;
    dns-routing-instance dns-routing-instance-name;
    dns-server [ ip-address1 ip-address2 ip-address3 ];
    dns-source-interface loopback-interface-name;
    routing-instance routing-instance-name;
    security-intelligence-policy
    server-interfaces [ server-interface-name1 server-interface-name2 ];
    term term-name {
        from {
            src-ip-prefix [prefix1 prefix2];
            dest-port [port1 port2];
        }
        then {
            accept;
            custom-page custom-page;
            http-status-code http-status-code;
            redirect-url redirect-url;
            tcp-reset;
        }
    }
    url-filter-database filename
}
```

Hierarchy Level

```
[edit services web-filter profile profile-name]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series.
Statement introduced in Junos OS Release 20.1R1 for Next Gen Services on MX240, MX480, and MX960 routers.

Description

Configure a URL filter template.

Options

template-name—Name of the URL filter template.

client-interfaces [***client-interface-name1 client-interface-name2*** **]**—The list of client-facing logical interfaces (uplink) on which the URL filtering is configured. This option is mandatory.

disable-url-filtering—Disables the filtering of HTTP traffic that contains an embedded IP address (for example, http:/10.1.1.1) belonging to a disallowed domain name in the URL filter database.

dns-resolution-interval ***minutes***—DNS resolution time interval in minutes.

Default: 1440

Range: 60 through 1440 minutes.

dns-resolution-rate ***seconds***—Number of DNS queries per second sent out from the system before initiating further DNS queries.

Default: 50

Range: 50 through 100.

dns-retries ***number***—Number of retries for a DNS query in case query fails or times out.

Default: 3

Range: 1 through 5.

dns-routing-instance ***dns-routing-instance-name***—The VRF on which the DNS server is reachable. This option is mandatory. You can use the default routing instance inet.0 or a defined routing instance.

dns-server [***ip-address1 ip-address2 ip-address3*** **]**—One or more IP (IPv4 or IPv6) addresses of DNS servers to which the DNS queries are sent out. This option is mandatory.

dns-source-interface ***loopback-interface-name***—The loopback interface for which source IP address is picked for sending DNS queries. This option is mandatory.

routing-instance ***routing-instance-name***—The VRF on which URL filtering feature is configured. This option is mandatory. You can use the default routing instance inet.0 or a defined routing instance.

server-interfaces [***server-interface-name1 server-interface-name2*** **]**—Server-facing interfaces to which traffic is destined. This option is mandatory.

The list of server-facing logical interfaces (downlink) on which the URL filtering is configured. This option is mandatory.

url-filter-database ***filename***—The filename of the URL filter database. The file should be placed in the **/var/db/url-filterd** directory, but indicate just the filename here and not the full path.

The remaining statements are explained separately.

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

RELATED DOCUMENTATION

- Configuring URL Filtering | 55

uuid

Syntax

```
uuid hex-value;
```

Hierarchy Level

```
[edit applications application application-name]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Specify the Universal Unique Identifier (UUID) for DCE RPC objects.

Options
hex-value—Hexadecimal value.

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

RELATED DOCUMENTATION

- ALG Descriptions | 466
- Configuring a Universal Unique Identifier | 524
- Examples: Configuring Application Protocols | 524
- Verifying the Output of ALG Sessions | 525

v6rd

Syntax

```
v6rd v6rd-softwire-concentator {
    ipv4-prefix ipv4-prefix;
    v6rd-prefix ipv6-prefix;
    mtu-v4 mtu-v4;
    softwire-address ipv4-address;
}
```

Hierarchy Level

```
[edit services softwire softwire-concentrator]
[edit services softwires softwire-types
```

Release Information

Statement introduced in Junos OS Release 10.4.
Support added in Junos OS release 20.2R1 for the v6rd concentrator at the **[edit services softwires softwire-types** edit hierarchy for Next Gen Services on MX240, MX480, and MX860 routers.

Description

Configure settings for a 6rd concentrator used to process IPv6 packets encapsulated in IPv4 packets.

The **v6rd** statement is supported only on the MS-DPC, MS-100, MS-400, and MS-500 line cards. The **v6rd** statement is *not* supported on MS-MPCs and MS-MICs.

Options

ipv4-prefix—IPv4 prefix of the customer edge (CE) network

ipv6-prefix—IPv6 prefix of the 6rd domain.

mtu-v4— 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.

address—IPv4 address of a softwire concentrator. This is an IPv4 address independent of any interface and on a different prefix.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring a 6rd Softwire Concentrator | 414

version (IKE)

Syntax

```
version ( 1 | 2);
```

Hierarchy Level

```
[edit services ipsec-vpn ike policy policy-name],
```

Release Information

Statement introduced in Junos OS Release 11.4.

Description

Configure the Internet Key Exchange (IKE) version that is used to negotiate dynamic SAs for IPSec.

Options

1—Uses IKEv1.

2—Uses IKEv2.

> **NOTE:** By default, Junos OS uses IKE policy version 1.0. Version 2.0 is supported only in Junos OS Release 11.4 and later. If no version is explicitly configured, Junos OS sets the version to version 1.0.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

RELATED DOCUMENTATION

Configuring IKE Policies | 671

video

Syntax

```
video {
    dscp (Services CoS) (alias | bits);
    forwarding-class (Services PIC Classifiers) class-name;
}
```

Hierarchy Level

```
[edit services (CoS) cos application-profile profile-name sip]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** values for SIP video traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Application Profiles for Use as CoS Rule Actions | 827

video (Application Profile)

Syntax

```
video {
    dscp (alias | bits);
    forwarding-class class-name;
}
```

Hierarchy Level

```
[edit services cos application-profileprofile-name sip]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** values for SIP video traffic.

Default

By default, the system will not alter the DSCP or forwarding class for SIP video traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

voice (Application Profile) | 1603

virtual-service (Traffic Load Balancer)

Syntax

```
virtual-service virtual-service-name {
    address virtual-ip–address;
    group group-name;
    load-balance-method {
        hash {
            hash-key method;
        }
        random;
    }
    mode ( layer2-direct-server-return | direct-server-return | translated );
    <routing-instance routing-instance-name>;
    <routing-metric route-metric>;
    server-interface server-interface;
    service service-name {
        protocol (udp | tcp);
        server-listening-port port;
        virtual-port virtual-port;
    }
}
```

Hierarchy Level

```
[edit services traffic-load-balance instance instance-name]
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure a TLB virtual service.

Options

address *virtual-ip-address*—Address of the virtual service.

group *group-name*—Server group for the virtual service.

load-balance method hash hash-key *method*—Use a combination of these hash-key methods for the session distribution API:

dest-ip—Hash on destination IP address.

proto—Hash on protocol.

source-ip—Hash on source IP address.

load-balance-method random—Use randomizing algorithm for session distribution.

mode (layer2-direct-server-return | direct-server-return | translated)—Traffic load balancer mode of operation:

direct-server-return—Transparent mode Layer 3 direct server return.

layer2-direct-server-return—Transparent mode Layer 2 direct server return. Load balancing works by changing the Layer 2 MAC of packets; Layer 3 and higher level headers are not modified.

translated—The Packet Forwarding Engine performs stateless load balancing.

route-metric—(Optional) Route metric

Range: 1 through 255

routing-instance-name—(Optional) Routing instance for the virtual service. Default is **inet.0**.

server-interface *server-interface*—(Optional) The server-interface specified under the virtual-service, will be used instead of the values provided under the instance level.

service *service-name*—Translated mode details. Packets destined to this virtual ip-address + virtual-port + protocol will be load balanced to the appropriate server. The destination IP address and port are replaced by the real services IP address and the server-listening-port (configured here).

protocol (udp | tcp)—Protocol.

server-listening-port *port*—Port number.

virtual-port *virtual-port*—Virtual port number.

virtual-ip-address—Local address for the virtual service.

virtual-service-name—Identifier for the virtual service.

Required Privilege Level

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

RELATED DOCUMENTATION

Traffic Load Balancer Overview | 970

Configuring TLB | 979

voice

Syntax

```
voice {
    dscp (Services CoS) (alias | bits);
    forwarding-class (Services PIC Classifiers) class-name;
}
```

Hierarchy Level

[edit services (CoS) cos **application-profile** *profile-name* sip]

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** values for SIP voice traffic.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Application Profiles for Use as CoS Rule Actions | 827

voice (Application Profile)

Syntax

```
voice {
    dscp (alias | bits);
    forwarding-class class-name;
}
```

Hierarchy Level

```
[edit services cos application-profileprofile-name sip]
```

Release Information

Statement introduced in Junos OS Release 9.3.

Description

Set the appropriate **dscp** and **forwarding-class** values for SIP voice traffic.

Default

By default, the system will not alter the DSCP or forwarding class for SIP voice traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring CoS Rules on Services PICs

video (Application Profile) | **1599**

warm-standby

Syntax

```
warm-standby;
```

Hierarchy Level

```
[edit interfaces rlsq<number> redundancy-options]
```

Release Information

Statement introduced in Junos OS Release 8.0.

Description

For AS or Multiservices PIC redundancy configurations, specify that the failure detection and recovery involves one backup PIC supporting multiple working PICs. Recovery time is not guaranteed.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring LSQ Interface Redundancy in a Single Router Using Virtual Interfaces | 912

web-filter

Syntax

```
web-filter {
    profile (Web Filter) profile-name {
        dns-filter {
            database-file filename;
            dns-resp-ttl seconds;
            dns-server [ ip-address ];
            hash-key key-string;
            hash-method hash-method-name;
            statistics-log-timer minutes;
            wildcarding-level level;
        }
        dns-filter-template template-name {
            client-interfaces [ client-interface-name ];
            client-routing-instance client-routing-instance-name;
            dns-filter {
                database-file filename;
                dns-resp-ttl seconds;
                dns-server [ ip-address ];
                hash-key key-string;
                hash-method hash-method-name;
                statistics-log-timer minutes;
                wildcarding-level level;
            }
            server-interfaces [ server-interface-name ];
            server-routing-instance server-routing-instance-name;
            term term-name {
                from {
                    src-ip-prefix [ source-prefix ];
                }
                then {
                    accept;
                    dns-sinkhole;
                }
            }
        }
        global-dns-stats-log-timer minutes;
        url-filter-database filename;
        url-filter-template template-name {
            client-interfaces [ client-interface-name1 client-interface-name2 ];
            disable-url-filtering;
            dns-resolution-interval minutes;
```

```
        dns-resolution-rate seconds;
        dns-retries number;
        dns-routing-instance dns-routing-instance-name;
        dns-server [ ip-address1 ip-address2 ip-address3 ];
        dns-source-interface loopback-interface-name;
        dns-routing-instance dns-routing-instance-name;
        routing-instance routing-instance-name;
        server-interfaces [ server-interface-name1 server-interface-name2 ];
        term term-name {
          from {
            src-ip-prefix [prefix1 prefix2];
            dest-port [port1 port2];
          }
          then {
            accept;
            custom-page custom-page;
            http-status-code http-status-code;
            redirect-url redirect-url;
            tcp-reset;
          }
        }
        url-filter-database filename
      }
    }
}
```

Hierarchy Level

```
[edit services]
```

Release Information

Statement introduced in Junos OS Release 18.3R1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure filtering of DNS requests for disallowed website domains. Filtering can result in either:

- Blocking access to the site by sending the client a DNS response that includes an IP address or domain name of a sinkhole server instead of the disallowed domain.
- Logging the DNS request and allowing access.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

web-filter-profile

Syntax

```
web-filter-profile profile-name;
```

Hierarchy Level

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

Release Information
Statement introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description
Specify the DNS filter profile or the URL filter profile that the service set uses. The filter profile is configured at the **[edit services web-filter]** hierarchy level, and specifies how to filter DNS requests for disallowed website domains or how to filter access to disallowed URLs.

Options
profile-name—Name of the DNS filter profile.

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

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

CHAPTER 51

Operational Commands

IN THIS CHAPTER

clear services cos statistics

Syntax

```
clear services cos statistics
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 8.1.

Description

Clear statistics for class-of-service (CoS) code point bit patterns and forwarding classes as configured in CoS services for the AS PIC.

Options

none—Clear all services CoS statistics.

interface *interface-name*—(Optional) Clear statistics for the specified interface only.

service-set *service-set-name*—(Optional) Clear statistics for the specified service set only.

Required Privilege Level

view

List of Sample Output

clear services cos statistics on page 1613

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services cos statistics

```
user@host> clear services cos statistics
```

clear services crtp statistics

Syntax

```
clear services crtp statistics
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear Compressed Real-Time Transport Protocol (CRTP) flow statistics.

Options

none—Clear CRTP flow statistics on all interfaces.

interface *interface-name*—(Optional) Clear CRTP flow statistics for the specified interface. On M Series and T Series routers, a link services IQ (**lsq-*fpc/pic/port***) or redundant link services IQ (**rlsq-*fpc/pic/port***) interface.

Required Privilege Level

view

List of Sample Output

clear services crtp statistics on page 1614

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services crtp statistics

```
user@host> clear services crtp statistics
```

clear services ids

Syntax

```
clear services ids
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear intrusion detection service (IDS) events.

Options

none—Clear all IDS events for all adaptive services interfaces for all service sets, and clear and reset IDS.

interface *interface-name*—(Optional) On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number*.**

service-set *service-set-name*—(Optional) Clear all IDS events for a particular service set.

Required Privilege Level

view

List of Sample Output

clear services ids on page 1615

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ids

```
user@host> clear services ids
```

clear services ids destination-table

Syntax

```
clear services ids destination-table
<destination-prefix destination-prefix-name>
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear the intrusion detection service (IDS) events for a particular address that might be under attack.

Options

none—Clear the attack destination address table.

destination-prefix *destination-prefix-name*—(Optional) Clear the attack destination table for a particular destination prefix.

interface *interface-name*—(Optional) Clear the attack destination table for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

service-set *service-set-name*—(Optional) Clear the attack destination table for a particular service set.

Required Privilege Level

view

List of Sample Output

clear services ids destination-table on page 1616

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ids destination-table

```
user@host> clear services ids destination-table
```

clear services ids pair-table

Syntax

```
clear services ids pair-table
<destination-prefix destination-prefix-name>
<interface interface-name>
<service-set service-set-name>
<source-prefix source-prefix-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear the intrusion detection service (IDS) attack source and destination address pair table.

Options

none—Clear the attack source and destination address pair table.

destination-prefix *destination-prefix-name*—(Optional) Clear the attack source and destination address pair table for a particular destination prefix.

interface *interface-name*—(Optional) Clear the attack destination table for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

service-set *service-set-name*—Optional) Clear the attack source and destination address pair table for a particular service set.

source-prefix *source-prefix-name*—(Optional) Clear the attack source and destination address pair table for a particular source prefix.

Required Privilege Level

view

List of Sample Output

clear services ids pair-table on page 1618

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ids pair-table

```
user@host> clear services ids pair-table
```

clear services ids source-table

Syntax

```
clear services ids source-table
<interface interface-name>
<service-set service-set-name>
<source-prefix source-prefix-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear all intrusion detection service (IDS) events for addresses that are suspected attackers.

Options

none—Clear the attack source address table.

interface *interface-name*—(Optional) On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

service-set *service-set-name*—(Optional) Clear the attack source address table for a particular service set.

source-prefix source-prefix-name—(Optional) Clear the attack source address table for a particular source prefix.

Required Privilege Level

view

List of Sample Output

clear services ids source-table on page 1619

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ids source-table

```
user@host> clear services ids source-table
```

clear services inline nat pool

Syntax

```
clear services inline nat pool pool-name
```

Release Information
Command introduced in Junos OS Release 11.4.

Description
Clear global inline NAT statistics.

Options
pool-name—Name of the NAT pool for which statistic are cleared.

Required Privilege Level
clear

List of Sample Output
clear services inline nat pool on page 1620

Output Fields
When you enter this command, the NAT pool statistics are cleared. There is no specific output.

Sample Output

clear services inline nat pool

```
user@host> clear services inline nat pool p1
```

clear services inline nat statistics

Syntax

```
clear services inline nat statistics
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 11.4.

Description

Clear global inline NAT statistics.

Options

interface *interface-name*—(Optional) Clear inline NAT statistics for the specified interface only.

Required Privilege Level

clear

List of Sample Output

clear services inline nat statistics on page 1621

Output Fields

When you enter this command, the global inline NAT statistics are cleared. There is no specific output.

Sample Output

clear services inline nat statistics

```
user@host> clear services inline nat statistics
```

clear services inline softwire statistics

Syntax

```
clear services inline softwire statistics
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 13.3R3.

Description

Clear global inline softwire statistics.

> **NOTE:** The following two limitations apply to the clearing of data plane statistics using the **clear services inline softwire statistics** command:
>
> - When traffic is continuously flowing and the counters are being updated in the data plane, none of the statistical values except the counter for 6rd decapsulation errors is reset.
> - When you delete the softwire concentrator or the service set associated with an inline services (**si-**) interface, the counter for 6rd decapsulation errors might display all the previously accumulated values.

Options

interface *interface-name*—(Optional) Clear inline softwire statistics for the specified interface only.

Required Privilege Level

clear

List of Sample Output

clear services inline softwire statistics on page 1622

Output Fields

When you enter this command, the global inline softwire statistics are cleared. There is no specific output.

Sample Output

clear services inline softwire statistics

```
user@host> clear services inline softwire statistics
```

clear services ipsec-vpn certificates

Syntax

```
clear services ipsec-vpn certificates (all | service-set service-set)
<certificate-cache-entry number>
```

Release Information
Command introduced in Junos OS Release 7.5.

Description
(Adaptive services interfaces only) Delete digital certificates from the IPsec configuration memory cache. Issuing this command also clears the certificate revocation list (CRL) from the cache along with the certificates.

Options
all—Delete digital certificates for all service sets.

service-set *service-set*—Delete digital certificates for the specified service set.

Required Privilege Level
clear

List of Sample Output
clear services ipsec-vpn certificates all on page 1623

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn certificates all

```
user@host> clear services ipsec-vpn certificates all
```

clear services ipsec-vpn ike security-associations

Syntax

```
clear services ipsec-vpn ike security-associations
<peer-address-name>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
service-set option added in Junos OS Release 8.5.

Description

(Adaptive services interfaces only) Clear Internet Key Exchange (IKE) security associations.

Options

peer-address-name—(Optional) Clear only the security association specified by the peer address.

service-set *service-set-name*—(Optional) Clear only the security association specified by the service-set name.

Required Privilege Level

view

RELATED DOCUMENTATION

show services ipsec-vpn ike security-associations | 1872

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ike security-associations

```
user@host> clear services ipsec-vpn ike security-associations
```

clear services ipsec-vpn ipsec security-associations

Syntax

```
clear services ipsec-vpn security-associations
<peer-address-name>
<remote-gateway remote-gateway-address>
<service-set-name>
<tunnel-index tunnel-index-number>
```

Release Information

Command introduced before Junos OS Release 7.4.
remote-gateway, ***service-set-name***, and **tunnel-index** options added in Junos OS Release 8.4.

Description

(Adaptive services interfaces only) Clear IP Security (IPsec) security associations. You can combine the options for greater specificity.

Options

peer-address-name—(Optional) Clear only the security association specified by the peer address.

remote-gateway *remote-gateway-address*—(Optional) Clear only the security association specified by the remote gateway address.

service-set-name—(Optional) Clear only the security association specified by the service-set name.

tunnel-index *tunnel-index-number*—(Optional) Clear only the security association specified by the tunnel index number.

Required Privilege Level

view

RELATED DOCUMENTATION

show services ipsec-vpn ipsec security-associations | 1878

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec security-associations

```
user@host> clear services ipsec-vpn ipsec security-associations
```

clear services ipsec-vpn ipsec statistics

Syntax

```
clear services ipsec-vpn ipsec statistics
<remote-gateway address>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 8.1.

Description

(Adaptive services interface only) Clear IP Security (IPsec) statistics.

Options

remote-gateway *address*—(Optional) Clear statistics for the specified remote system.

service-set *service-set-name*—(Optional) Clear statistics for the specified service set.

Required Privilege Level

view

RELATED DOCUMENTATION

show services ipsec-vpn ipsec statistics | 1885

List of Sample Output

clear services ipsec-vpn ipsec statistics on page 1627

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec statistics

```
user@host> clear services ipsec-vpn ipsec statistics
```

clear services l2tp destination

Syntax

```
clear services l2tp destination
<all | local-gateway gateway-address | peer-gateway gateway-address>
```

Release Information

Command introduced in Junos OS Release 10.4.

Description

Clear all Layer 2 Tunneling Protocol (L2TP) destinations and all tunnels and sessions that belong to the destinations. This command is available only for LAC on MX Series routers.

NOTE: You cannot issue the **clear services l2tp destination** command in parallel with statistics-related **show services l2tp** commands from separate terminals. If this **clear** command is running, then you must press Ctrl+c to make the command run in the background before issuing any of the **show** commands listed in the following table:

show services l2tp destination extensive	**show services l2tp summary statistics**
show services l2tp destination statistics	**show services l2tp tunnel extensive**
show services l2tp session extensive	**show services l2tp tunnel statistics**
show services l2tp session statistics	

Options

all—Close all L2TP destinations.

BEST PRACTICE: The **all** option is not intended to be used as a means to perform a bulk logout of L2TP subscribers. We recommend that you do not use the **all** option in a production environment. Instead of clearing all subscribers at once, consider clearing subscribers in smaller group, based on interface, tunnel, or destination end point.

local-gateway *gateway-address*—Clear only the L2TP destinations and all tunnels and sessions associated with the specified local gateway address.

peer-gateway *gateway-address*—Clear only the L2TP destinations and all tunnels and sessions associated with the peer gateway with the specified address.

Required Privilege Level
clear

RELATED DOCUMENTATION

show services l2tp destination

List of Sample Output
clear services l2tp destination all on page 1629

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp destination all

```
user@host> clear services l2tp destination all

   Destination 2 closed
```

clear services l2tp destination statistics

Syntax

```
clear services l2tp destination statistics
<all | local-gateway gateway-address | peer-gateway gateway-address >
```

Release Information

Command introduced in Junos OS Release 13.1.

Description

Clear all statistics associated with the Layer 2 Tunneling Protocol (L2TP) destinations and all tunnels and sessions that belong to the destinations. This command is available only for LAC on MX Series routers.

Options

all—Clear all statistics associated with the L2TP destinations.

local-gateway *gateway-address*—Clear statistics related to L2TP destination and all tunnels and sessions associated with the specified local gateway address.

peer-gateway *gateway-address*—Clear statistics related to L2TP destination and all tunnels and sessions associated with the specified peer gateway address.

Required Privilege Level

clear

RELATED DOCUMENTATION

show services l2tp destination

List of Sample Output

clear services l2tp destination statistics on page 1630

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp destination statistics

```
user@host>clear services l2tp destination statistics all
```

```
Destination 1 statistics cleared
```

clear services l2tp multilink

Syntax

```
clear services l2tp multilink (all <statistics> | bundle-id number <statistics> | statistics (all | bundle-id number))
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Close Layer 2 Tunneling Protocol (L2TP) multilink sessions or clear session statistics.

Options

all <statistics>—Close all L2TP multilink sessions or clear statistics for all L2TP multilink sessions.

bundle-id *number* <statistics>—L2TP multilink bundle ID. The value is an internally generated number from 1 to 65535. Close the specified L2TP multilink session, or using the **statistics** keyword with this option, clear statistics for the specified session.

statistics (all | bundle-id *number*)—Clear all session statistics or clear statistics for the specified multilink bundle ID.

Required Privilege Level

view

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- show services l2tp multilink | **1897**

List of Sample Output

clear services l2tp multilink statistics all on page 1633

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp multilink statistics all

```
user@host> clear services l2tp multilink statistics all

   Multilink 1 statistics cleared
```

clear services l2tp session

Syntax

clear services l2tp session (all | interface *interface-name* | local-gateway *gateway-address* | local-gateway-name *gateway-name* | local-session-id *session-id* | local-tunnel-id *tunnel-id* | peer-gateway *gateway-address* | peer-gateway-name *gateway-name* | tunnel-group *group-name* | user *username*)

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Clear Layer 2 Tunneling Protocol (L2TP) sessions on LNS.

(MX Series routers only) Clear L2TP sessions on LAC and LNS.

NOTE: On MX Series routers, you cannot issue the **clear services l2tp session** command in parallel with statistics-related **show services l2tp** commands from separate terminals. If this **clear** command is running, then you must press Ctrl+c to make the command run in the background before issuing any of the **show** commands listed in the following table:

show services l2tp destination extensive	**show services l2tp summary statistics**
show services l2tp destination statistics	**show services l2tp tunnel extensive**
show services l2tp session extensive	**show services l2tp tunnel statistics**
show services l2tp session statistics	

Options

all—Close all L2TP sessions.

BEST PRACTICE: The **all** option is not intended to be used as a means to perform a bulk logout of L2TP subscribers. We recommend that you do not use the **all** option in a production environment. Instead of clearing all subscribers at once, consider clearing subscribers in smaller group, based on interface, tunnel, or destination end point.

interface *interface-name*—Clear only the L2TP sessions using the specified adaptive services or inline services interface. The interface type depends on the line card as follows:

- **si-*fpc/pic/port***—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.
- **sp-*fpc/pic/port***—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—Clear only the L2TP sessions associated with the specified local gateway address.

local-gateway-name *gateway-name*—Clear only the L2TP sessions associated with the specified local gateway name.

local-session-id *session-id* —Clear only the L2TP sessions with this identifier for the local endpoint of the L2TP session.

local-tunnel-id *tunnel-id*—Clear only the L2TP sessions associated with the specified local tunnel identifier.

peer-gateway *gateway-address*—Clear only the L2TP sessions associated with the peer gateway with the specified address.

peer-gateway-name *gateway-name*—Clear only the L2TP sessions associated with the peer gateway with the specified name.

tunnel-group *group-name*—Clear only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

user *username* —(M Series routers only) Clear only the L2TP sessions for the specified username.

Required Privilege Level
clear

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**

L2TP Minimum Configuration | **1038**

clear services l2tp session statistics | **1637**

show services l2tp session | **1910**

List of Sample Output

clear services l2tp session on page 1636
clear services l2tp session interface on page 1636

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp session

```
user@host> clear services l2tp session 31694

   Session 31694 closed
```

Sample Output

clear services l2tp session interface

```
user@host> show services l2tp session Tunnel local ID: 17185

Local  Remote   State               Interface         Interface
  ID     ID                           unit              Name
  5117   1        Established         1073741828        si-2/0/0
  34915  2        Established         1073741829        si-2/1/0
  6454   3        Established         1073741830        si-2/0/0
  46142  4        Established         1073741831        si-2/1/0
```

```
user@host> clear services l2tp session interface si-2/0/0

   Session  5117 closed
   Session  6454 closed
```

```
user@host> show services l2tp session Tunnel local ID: 17185

   Local  Remote   State               Interface         Interface
   ID     ID                           unit              Name
   34915  2        Established         1073741829        si-2/1/0
   46142  4        Established         1073741831        si-2/1/0
```

clear services l2tp session statistics

Syntax

clear services l2tp session statistics (all | interface *interface-name* | local-gateway *gateway-address* | local-gateway-name *gateway-name* | local-session-id *session-id* | local-tunnel-id *tunnel-id* | peer-gateway *gateway-address* | peer-gateway-name *gateway-name* | tunnel-group *group-name* | user *username*)

Release Information

Command introduced before Junos OS Release 7.4.
Support for MX Series routers added in Junos OS Release 10.4.

Description

(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Clear statistics for Layer 2 Tunneling Protocol (L2TP) sessions.

Options

all—Clear statistics for all L2TP sessions.

interface *interface-name*—Clear only the L2TP sessions using the specified adaptive services or inline services interface. The interface type depends on the line card as follows:

- **si-*fpc/pic/port***—MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.
- **sp-*fpc/pic/port***—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—Clear statistics for only the L2TP sessions associated with the local gateway with the specified address.

local-gateway-name *gateway-name*—Clear statistics for only the L2TP sessions associated with the local gateway with the specified name.

local-session-id *session-id* —Clear statistics for only the L2TP sessions with this identifier for the local endpoint of the L2TP session.

local-tunnel-id *tunnel-id*—Clear statistics for only the L2TP sessions associated with the specified local tunnel identifier.

peer-gateway *gateway-address*—Clear statistics for only the L2TP sessions associated with the peer gateway with the specified address.

peer-gateway-name *gateway-name*—Clear statistics for only the L2TP sessions associated with the peer gateway with the specified name.

tunnel-group *group-name*—Clear statistics for only the L2TP sessions associated with the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

user *username* —Clear statistics for only the L2TP sessions for the specified username. This option is not available for L2TP LAC on MX Series routers.

Required Privilege Level
view

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- clear services l2tp session | **1634**
- show services l2tp session | **1910**

List of Sample Output
clear services l2tp session statistics all on page 1638

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp session statistics all

```
user@host> clear services l2tp session statistics all

   Session 26497 statistics cleared
```

clear services l2tp tunnel

Syntax

clear services l2tp tunnel (all | interface sp-*fpc/pic/port* | local-gateway *gateway-address* | local-gateway-name *gateway-name* | local-tunnel-id *tunnel-id* | peer-gateway *gateway-address* | peer-gateway-name *gateway-name* | tunnel-group *group-name*)

Release Information

Command introduced before Junos OS Release 7.4.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description

(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Clear Layer 2 Tunneling Protocol (L2TP) tunnels.

NOTE: On MX Series routers, you cannot issue the **clear services l2tp tunnel** command in parallel with statistics-related **show services l2tp** commands from separate terminals. If this **clear** command is running, then you must press Ctrl+c to make the command run in the background before issuing any of the **show** commands listed in the following table:

show services l2tp destination extensive	**show services l2tp summary statistics**
show services l2tp destination statistics	**show services l2tp tunnel extensive**
show services l2tp session extensive	**show services l2tp tunnel statistics**
show services l2tp session statistics	

Options

all—Clear all L2TP tunnels.

BEST PRACTICE: The **all** option is not intended to be used as a means to perform a bulk logout of L2TP subscribers. We recommend that you do not use the **all** option in a production environment. Instead of clearing all subscribers at once, consider clearing subscribers in smaller group, based on interface, tunnel, or destination end point.

sp-*fpc/pic/port*—(Optional) Clear only the L2TP tunnels using the specified adaptive services interface. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—Clear only the L2TP tunnels associated with the local gateway with the specified address.

local-gateway-name *gateway-name*—Clear only the L2TP tunnels associated with the local gateway with the specified name.

local-tunnel-id *tunnel-id*—Clear only the L2TP tunnels that have the specified local tunnel identifier.

peer-gateway *gateway-address*—Clear only the L2TP tunnels associated with the peer gateway with the specified address.

peer-gateway-name *gateway-name*—Clear only the L2TP tunnels associated with the peer gateway with the specified name.

tunnel-group *group-name*—Clear only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

Required Privilege Level
view

RELATED DOCUMENTATION

- L2TP Services Configuration Overview | **1037**
- L2TP Minimum Configuration | **1038**
- clear services l2tp tunnel statistics | **1642**
- show services l2tp tunnel | **1929**

List of Sample Output
clear services l2tp tunnel on page 1640

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp tunnel

```
user@host> clear services l2tp tunnel 17185
```

```
Tunnel 17185 closed
```

clear services l2tp tunnel statistics

Syntax

clear services l2tp tunnel statistics (all | interface sp-*fpc/pic/port* | local-gateway *gateway-address* | local-gateway-name *gateway-name* | local-tunnel-id *tunnel-id* | peer-gateway *gateway-address* | peer-gateway-name *gateway-name* | tunnel-group *group-name*)

Release Information

Command introduced before Junos OS Release 7.4.
Support for MX Series routers added in Junos OS Release 10.4.

Description

(M10i and M7i routers: LNS only. MX Series routers: LAC only.) Clear statistics for Layer 2 Tunneling Protocol (L2TP) tunnels.

Options

all—Clear statistics for all L2TP tunnels.

interface sp-*fpc/pic/port*—Clear statistics for only the L2TP tunnels using the specified adaptive services interface. This option is not available for L2TP LAC on MX Series routers.

local-gateway *gateway-address*—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified address.

local-gateway-name *gateway-name*—Clear statistics for only the L2TP tunnels associated with the local gateway with the specified name.

local-tunnel-id *tunnel-id*—Clear statistics for only the L2TP tunnels that have the specified local tunnel identifier.

peer-gateway *gateway-address*—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified address.

peer-gateway-name *gateway-name*—Clear statistics for only the L2TP tunnels associated with the peer gateway with the specified name.

tunnel-group *group-name*—Clear statistics for only the L2TP tunnels in the specified tunnel group. This option is not available for L2TP LAC on MX Series routers.

Required Privilege Level

clear

RELATED DOCUMENTATION

L2TP Services Configuration Overview | 1037

L2TP Minimum Configuration | 1038

clear services l2tp tunnel | 1639

show services l2tp tunnel | 1929

List of Sample Output

clear services l2tp tunnel statistics all on page 1643

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services l2tp tunnel statistics all

```
user@host> clear services l2tp tunnel statistics all

   Tunnel  9933 statistics cleared
```

clear services nat flows

Syntax

```
clear services nat flows
<b4address b4address>
<service-set service-set>
<subscriber subscriber-address>
```

Release Information

Command introduced in Junos OS Release 14.1.

Description

Clear NAT flows.

Options

none—Clear all NAT flows.

b4address *b4address*—(Optional) Clear NAT flows for a particular B4 address.

service-set *service-set*—(Optional) Clear NAT flows for a particular service set.

subscriber *ip*—(Optional) Clear NAT flows for a particular subscriber, identified by IPv4 address.

Required Privilege Level

view

RELATED DOCUMENTATION

List of Sample Output

clear services nat flows subscriber (IPv4 address) on page 1645

Output Fields

Table 40 on page 1644 lists the output fields for the **clear services nat flows** command. Output fields are listed in the approximate order in which they appear.

Table 40: clear services nat flows Output Fields

Field Name	Field Description
Interface	Name of a services interface.
Service set	Name of the service set from which flows are being cleared.

Table 40: clear services nat flows Output Fields *(continued)*

Field Name	Field Description
Flows removed	Number of flows removed.

Sample Output

clear services nat flows subscriber (IPv4 address)

`user@host>` **clear services nat flows subscriber ip 198.51.100.3**

```
Interface   Service set  Flows removed

sp-2/0/0    ss1             0
```

Sample Output

clear services nat mappings

Syntax

```
clear services nat mappings
<app>
<eim>
<pcp>
<service-set service-set>
```

Release Information

Command introduced in Junos OS Release 14.1.

Description

Clear NAT mappings.

Options

none—Clear all NAT mappings.

app—(Optional) Clear address-pooling paired NAT mappings.

eim—(Optional) Clear endpoint-independent NAT mappings.

pcp—(Optional) Clear Port Control Protocol NAT mappings.

service-set *service-set*—(Optional) Clear NAT mappings for a specified service set..

Required Privilege Level

clear

RELATED DOCUMENTATION

- show services nat source mappings address-pooling-paired | 1949
- clear services nat mappings app | 1648
- clear services nat mappings eim | 1650
- clear services nat mappings pcp | 1652

List of Sample Output

clear services nat mappings on page 1647

Output Fields

Table 41 on page 1647 lists the output fields for the **clear services nat mappings** command. Output fields are listed in the approximate order in which they appear.

Table 41: clear services nat mappings Output Fields

Field Name	Field Description
Interface	Name of a services interface.
Service set	Name of the service set from which flows are being cleared.
Mappings removed	Number of mappings removed.
Flows removed	Number of flows removed.

Sample Output

clear services nat mappings

```
user@host> clear services nat mappings
```

```
Interface   Service set                         Mappings removed   Flows removed
sp-2/0/0    ss1                                                0               0
```

clear services nat mappings app

Syntax

```
clear services nat mappings app
<b4address b4address/prefix>
<service-set service-set>
<subscriber subscriber-ipv4-address>
```

Release Information

Command introduced in Junos OS Release 14.1.

Description

Clear NAT mappings for address pooling paired (app).

Options

none—Clear all NAT app mappings.

b4address *b4address/prefix*—(Optional) Clear NAT APP mappings for a particular subscriber b4address/prefix

service-set *service-set*—(Optional) Clear NAT APP mappings for a specified service set..

subscriber *subscriber-ipv4-address/prefix*—(Optional) Clear NAT APP mappings for a particular subscriber ipv4-address/prefix

Required Privilege Level

clear

RELATED DOCUMENTATION

show services nat source mappings address-pooling-paired | 1949

List of Sample Output

clear services nat mappings app on page 1649

Output Fields

Table 42 on page 1648 lists the output fields for the **clear services nat mappings app** command. Output fields are listed in the approximate order in which they appear.

Table 42: clear services nat mappings app Output Fields

Field Name	Field Description
Interface	Name of a services interface.

Table 42: clear services nat mappings app Output Fields *(continued)*

Field Name	Field Description
Service set	Name of the service set from which flows are being cleared.
Mappings removed	Number of mappings removed.
Flows removed	Number of flows removed.

Sample Output

clear services nat mappings app

```
user@host> clear services nat mappings app

Interface   Service set                          Mappings removed   Flows removed
sp-2/0/0    ss1                                                 0               0
```

clear services nat mappings eim

Syntax

```
clear services nat mappings eim
<b4address b4address/prefix>
<subscriber subscriber-ipv4-address>
```

Release Information

Command introduced in Junos OS Release 14.1.

Description

Clear endpoint independent (EIM) and port control protocol (PCP) mappings .

Options

none—Clear all EIM and PCP mappings.

b4address *b4address/prefix*—(Optional) Clear EIM and PCP mappings for a particular subscriber b4address/prefix

internal-host *ipv4address/prefix*—(Optional) Clear EIM and PCP mappings matching the specified b4address and internal-host..

port *port*—(Optional) Clear EIM and PCP mappings matching the specified b4address, internal host, and port.

service-set *service-set*—(Optional) Clear EIM and PCP mappings for the specified service set.

subscriber *subscriber-ipv4-address/prefix*—(Optional) Clear EIM and PCP mappings for a particular subscriber ipv4-address/prefix

- **port *port***—(Optional) Clear EIM and PCP mappings matching the specified ipv4-address/prefix and port.
- **service-set *service-set***—(Optional) Clear EIM and PCP mappings for the specified service set.

Required Privilege Level

clear

RELATED DOCUMENTATION

show services nat source mappings address-pooling-paired | 1949

List of Sample Output

clear services nat mappings eim on page 1651

Output Fields

Table 43 on page 1651 lists the output fields for the **clear services nat mappings eim** command. Output fields are listed in the approximate order in which they appear.

Table 43: clear services nat mappings eim Output Fields

Field Name	Field Description
Interface	Name of a services interface.
Service set	Name of the service set from which flows are being cleared.
Mappings removed	Number of mappings removed.
Flows removed	Number of flows removed.

Sample Output

clear services nat mappings eim

```
user@host> clear services nat mappings eim
```

```
Interface   Service set                         Mappings removed   Flows removed
sp-2/0/0    ss1                                                0               0
```

clear services nat mappings pcp

Syntax

```
clear services nat mappings pcp
<b4address b4address/prefix>
<subscriber subscriber-ipv4-address>
```

Release Information

Command introduced in Junos OS Release 14.1.

Description

Clear NAT mappings for Port Control Protocol (PCP).

Options

none—Clear all NAT PCP mappings.

b4address *b4address/prefix*—(Optional) Clear NAT PCP mappings for a particular subscriber b4address/prefix

port *port*—(Optional) Clear NAT PCP mappings matching the specified b4address internal host, and port.

service-set *service-set*—(Optional) Clear NAT PCP mappings for the specified service set.

subscriber *ipv4-address/prefix*—(Optional) Clear NAT PCP mappings for a particular subscriber ipv4-address/prefix

port *port*—(Optional) Clear NAT PCP mappings matching the specified ipv4-address/prefix, and port.

Required Privilege Level

clear

RELATED DOCUMENTATION

show services nat source mappings address-pooling-paired | 1949

List of Sample Output

clear services nat mappings pcp on page 1653

Output Fields

Table 44 on page 1653 lists the output fields for the **clear services nat mappings pcp** command. Output fields are listed in the approximate order in which they appear.

Table 44: clear services nat mappings pcp Output Fields

Field Name	Field Description
Interface	Name of a services interface.
Service set	Name of the service set from which flows are being cleared.
Mappings removed	Number of mappings removed.
Flows removed	Number of flows removed.

Sample Output

clear services nat mappings pcp

```
user@host> clear services nat mappings pcp

Interface   Service set                          Mappings removed   Flows removed
sp-2/0/0    ss1                                                0               0
```

clear services redundancy-set last-saved-state id

Syntax

```
clear services redundancy-set last-saved-state id
(redundancy-set{x | all})
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-MX-SPC3 services card.

Description

Clear the last saved state of a redundancy set or of all redundancy sets.

You can clear the warnings on the standby after inspection by issuing the **clear services redundancy-set {x|all} standby-warning** command on it. The command will also send an update notification regarding this peer's clean state to all the other peers in that redundancy set.

clear security pki ca-certificate

Syntax

```
clear security pki ca-certificate (all | ca-profile ca-profile-name)
```

Release Information
Command introduced in Junos OS Release 7.5.

Description
Delete certificate authority (CA) digital certificates from the router.

Options
all—Delete all CA digital certificates from the router.

ca-profile *ca-profile-name*—Delete the specified CA profile.

Required Privilege Level
clear

RELATED DOCUMENTATION

request security pki ca-certificate enroll | **1687**
request security pki ca-certificate load | **1689**
show security pki ca-certificate | **1789**

List of Sample Output
clear security pki ca-certificate all on page 1655

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki ca-certificate all

```
user@host> clear security pki ca-certificate all
```

clear security pki certificate-request

Syntax

```
clear security pki certificate-request (all | certificate-id certificate-id-name)
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Delete manually generated local digital certificate requests from the router.

Options

all—Delete all local digital certificate requests from the router.

certificate-id *certificate-id-name*—Delete the specified local digital certificate and corresponding public/private key pair.

Required Privilege Level

clear

RELATED DOCUMENTATION

show security pki certificate-request | 1794

List of Sample Output

clear security pki certificate-request all on page 1656

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki certificate-request all

```
user@host> clear security pki certificate-request all
```

clear security pki crl

Syntax

```
clear security pki crl (all | ca-profile ca-profile-name)
```

Release Information
Command introduced in Junos 8.1

Description
Delete certificate revocation lists (CRLs) from the router.

Options
all—Delete all CRLs from the router.

ca-profile *ca-profile-name*—Delete CRLs associated with the specified CA profile.

Required Privilege Level
clear

List of Sample Output
clear security pki crl ca-profile all on page 1657

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki crl ca-profile all

```
user@host> clear security pki crl ca-profile all
```

clear security pki key-pair

Syntax

```
clear security pki key-pair (all | certificate-id certificate-id-name)
```

Release Information

Command introduced in Junos OS Release 8.5.

Description

Clear public key infrastructure (PKI) key pair information for local digital certificates from the router.

Options

all—Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

certificate-id *certificate-id-name*—Delete the specified local digital certificate and corresponding public/private key pair.

Required Privilege Level

clear

RELATED DOCUMENTATION

request security pki local-certificate enroll | 1695

show security pki local-certificate | 1800

Output Fields

This command produces no output.

Sample Output

```
user@host> clear security pki key pair
```

clear security pki local-certificate

Syntax

```
clear security pki local-certificate
<all | certificate-id certificate-id-name | system-generated>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the router.

Options

all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

certificate-id *certificate-id-name*—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.

system-generated—(Optional) Auto-generated self-signed certificate.

Required Privilege Level

clear

RELATED DOCUMENTATION

request security pki local-certificate enroll | 1695

show security pki local-certificate | 1800

List of Sample Output

clear security pki local-certificate all on page 1659

Output Fields

This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

clear services service-set statistics ids drops

Syntax

```
clear services service-set statistics ids drops
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 17.1 on MX Series.

Description

Clear statistics for packet drops resulting from header-integrity, suspicious packet pattern, and session-limit checks performed by an MS-MPC or MS-MIC.

Options

none—Clear statistics for all configured services interfaces and service sets.

interface *interface-name*—(Optional) Clear statistics for the specified services interface.

service-set *service-set-name* —(Optional) Clear statistics for the specified service set.

Required Privilege Level

network

RELATED DOCUMENTATION

show services service-set statistics ids drops | 1983

List of Sample Output

clear services service-set statistics ids drops on page 1660

Sample Output

clear services service-set statistics ids drops

```
user@host> clear services service-set statistics ids drops
```

clear services service-sets statistics ids session-limits counters

Syntax

```
clear services service-sets statistics ids session-limits counters
<interface interface-name>
```

Release Information
Command introduced in Junos OS Release 17.1 on MX Series.

Description
Clear counters for session drops and packet drops resulting from session-limit checks performed by an IDS rule on an MS-MPC or MS-MIC.

Options
none—Clear counters for all configured services interfaces.

interface *interface-name*—(Optional) Clear counters for the specified services interface.

Required Privilege Level
network

RELATED DOCUMENTATION

show services service-sets statistics ids session-limits counters | 1993

List of Sample Output
clear services service-sets statistics ids session-limits counters on page 1661

Sample Output

clear services service-sets statistics ids session-limits counters

```
user@host> clear services service-sets statistics ids session-limits counters
```

clear services service-sets statistics integrity-drops

Syntax

```
clear services service-sets statistics integrity-drops
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 13.3

Description

Clear integrity-drops statistics for one adaptive services interface, for all adaptive services interfaces, or for one service-set.

Options

none—Clear integrity-drops statistics for all configured adaptive service interfaces/ service-set.

Service-set *service-set-name* —(Optional) Clear integrity-drops statistics for the specified service-set

interface *interface-name*—(Optional) Clear integrity-drops statistics for the specified adaptive services interface.

Required Privilege Level

network

RELATED DOCUMENTATION

show services service-sets statistics packet-drops | 2006

clear services service-sets statistics packet-drops

Syntax

```
clear services service-sets statistics packet-drops
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 7.4.

Description

Clear dropped-packet statistics for one adaptive services interface or for all adaptive services interfaces.

Options

none—Clear dropped-packet statistics for all configured adaptive services interfaces.

interface *interface-name*—(Optional) Clear dropped-packet statistics for the specified adaptive services interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port*** or **rsp*number***.

Required Privilege Level

network

RELATED DOCUMENTATION

show services service-sets statistics packet-drops | 2006

List of Sample Output

clear services service-sets statistics packet-drops on page 1663

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services service-sets statistics packet-drops

```
user@host> clear services service-sets statistics packet-drops interface sp-5/0/0
```

```
Flow collector interface: cp-5/0/0
Interface state: Collecting flows
Statistics cleared successfully
```

clear services service-sets statistics syslog

Syntax

```
clear services service-sets statistics syslog
<service-set service-set-name>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 11.1.

Description

Clear system log statistics for one services interface or for all services interfaces, and for one named service set or all service sets on the interface or interfaces.

Options

none—Clear system log for all configured services interfaces and their service sets.

interface *interface-name*—(Optional) Clear system log statistics for the specified services interface. On M Series, MX Series, and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***.

service-set *service-set-name*—(Optional) Clear system log statistics for the specified services interface.

Required Privilege Level

network

RELATED DOCUMENTATION

show services service-sets statistics syslog | **2008**

List of Sample Output

clear services service-sets statistics syslog on page 1665

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services service-sets statistics syslog

```
user@host> clear services service-sets statistics syslog interface sp-5/0/0
```

```
Flow collector interface: cp-5/0/0
Interface state: Collecting flows
Statistics cleared successfully
```

clear services sessions

Syntax

```
clear services sessions
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<ip-action>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Command introduced in Junos OS Release 13.1.

Description

Clear services sessions currently active on the embedded PIC or MIC. When you enter this command, the sessions are marked for deletion and are cleared thereafter. The time that is taken to clear the currently active sessions varies, depending on the scaled nature of the environment.

Options

none—Clear all sessions.

application-protocol *protocol*—(Optional) Clear sessions for one of the following application protocols:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **exec**—Exec
- **ftp**—File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **ip**—IP
- **login**—Login

- **netbios**—NetBIOS
- **netshow**—NetShow
- **pptp**—Point-to-Point Tunneling Protocol
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **talk**—Talk Program
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

destination-port *destination-port*—(Optional) Clear sessions for the specified destination port. The range of values is from 0 to 65535.

destination-prefix *destination-prefix*—(Optional) Clear sessions for the specified destination prefix.

interface *interface-name*—(Optional) Clear sessions for the specified interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc/ pic/ port*** or **rspn*umber***.

ip-action—(Optional) Clear **ip-action** entries generated by the router to log, drop, or block traffic based on previous matches. The IP action options and targets are configured at the **{edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* then]** hierarchy level.

protocol *protocol*—(Optional) Clear sessions for 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

- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP Encapsulation Protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Clear sessions for the specified service set.

source-port *source-port*—(Optional) Clear sessions for the specified source port. The range of values is from 0 through 65535.

source-prefix *source-prefix*—(Optional) Clear sessions for the specified source prefix.

Required Privilege Level
clear

RELATED DOCUMENTATION

show services sessions | 2022

List of Sample Output
clear services sessions on page 1670

Output Fields
Table 45 on page 1669 lists the output fields for the **clear services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 45: clear services sessions Output Fields

Field Name	Field Description
Interface	Name of an interface.
Service set	Name of the service set from which sessions are being cleared.

Table 45: clear services sessions Output Fields *(continued)*

Field Name	Field Description
Sessions marked for deletion	Number of sessions that are marked for deletion and are subsequently cleared.

Sample Output

clear services sessions

`user@host>` **clear services sessions**

```
Interface   Service set          Sessions marked for deletion
ms-0/0/0    sset                 10
```

clear services stateful-firewall flows

Syntax

```
clear services stateful-firewall flows
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear stateful firewall flows. Issue this command to clear the stateful firewall flows for the specified option. The default option is "none", that is, to close all stateful firewall flows unless another option is specified.

Starting in Junos Release 14.1, the method for closing flows has changed. With the change, even for peak flows, the command prompt now returns to an active state after 30 seconds and the clear command completes in 90 to 120 seconds. In previous releases, closing peak flows could take as long as 4 minutes, after which the command prompt would return. Note too that during the first 30 seconds of issuing the command, the flows to be deleted remain visible in the **show services stateful-firewall flows** command output.

Options

none—Clear all stateful firewall flows.

destination-port *destination-port*—(Optional) Clear stateful firewall flows for a particular destination port. The range of values is 0 to 65535.

destination-prefix *destination-prefix*—(Optional) Clear stateful firewall flows for a particular destination prefix.

interface *interface-name*—(Optional) Clear stateful firewall flows for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port*** or **rsp*number***.

protocol—(Optional) Clear stateful firewall flows for 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-over-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) Clear stateful firewall flows for a particular service set.

source-port *source-port*—(Optional) Clear stateful firewall flows for a particular source port. The range of values is from 0 through 65535.

source-prefix *source-prefix*—(Optional) Clear stateful firewall flows for a particular source prefix.

Required Privilege Level
view

RELATED DOCUMENTATION

show services stateful-firewall flows | 2078

List of Sample Output
clear services stateful-firewall flows on page 1673

Output Fields
Table 46 on page 1672 lists the output fields for the **clear services stateful-firewall flows** command. Output fields are listed in the approximate order in which they appear.

Table 46: clear services stateful-firewall flows Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.

Table 46: clear services stateful-firewall flows Output Fields *(continued)*

Field Name	Field Description
Service set	Name of the service set from which flows are being cleared.
Conv removed	Number of conversations removed.

Sample Output

clear services stateful-firewall flows

`user@host>` **clear services stateful-firewall flows**

```
Interface   Service set                                          Conv removed
ms-0/3/0    svc_set_trust                                                   0
ms-0/3/0    svc_set_untrust                                                 0
```

clear services stateful-firewall sip-call

Syntax

```
clear services stateful-firewall sip-call
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Command introduced in Junos OS Release 7.4.

Description

Clear Session Initiation Protocol (SIP) call information in stateful firewall flows.

Options

none—Clear stateful firewall statistics for all interfaces and all service sets.

application-protocol—(Optional) Clear information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio

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

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

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

interface *interface-name*—(Optional) Clear information for a particular adaptive services interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

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

- **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
- **ipv6**—IPv6 within IP
- **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) Clear information for a particular service set.

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

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

Required Privilege Level
view

RELATED DOCUMENTATION

show services stateful-firewall sip-call | 2085

List of Sample Output
clear services stateful-firewall sip-call on page 1676

Output Fields
Table 47 on page 1676 lists the output fields for the **clear services stateful-firewall sip-call** command. Output fields are listed in the approximate order in which they appear.

Table 47: clear services stateful-firewall sip-call Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of the service set from which flows are being cleared.
SIP calls removed	Number of SIP calls removed.

Sample Output

clear services stateful-firewall sip-call

```
user@host> clear services stateful-firewall sip-call

Interface   Service set                                    SIP calls removed
sp-0/3/0    test_sip_777                                                 1
```

clear services stateful-firewall sip-register

Syntax

```
clear services stateful-firewall sip-register
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Command introduced in Junos OS Release 7.4.

Description

Clear Session Initiation Protocol (SIP) register information in stateful firewall flows.

Options

application-protocol—(Optional) Clear information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol
- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol

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

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

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

interface ***interface***—(Optional) Clear information about a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

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

- **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
- **ipv6**—IPv6 within IP
- **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) Clear information for a particular service set.

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

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

Required Privilege Level
view

RELATED DOCUMENTATION

show services stateful-firewall sip-register | 2091

List of Sample Output
clear services stateful-firewall sip-register on page 1679

Output Fields
Table 48 on page 1679 lists the output fields for the **clear services stateful-firewall sip-register** command. Output fields are listed in the approximate order in which they appear.

Table 48: clear services stateful-firewall sip-register Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of the service set from which flows are being cleared.
SIP registration removed	Number of SIP registers removed.

Sample Output

clear services stateful-firewall sip-register

```
user@host> clear services stateful-firewall sip-register

Interface   Service set                              SIP registration removed
sp-0/3/0    test_sip_777                                                   1
```

clear services stateful-firewall statistics

Syntax

```
clear services stateful-firewall statistics
<interface interface-name>
<service-set service-set>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Clear stateful firewall statistics.

Options

none—Clear stateful firewall statistics for all interfaces and all service sets.

interface *interface-name*—(Optional) Clear stateful firewall statistics for the specified interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc/pic/port*** or **rsp*number***.

service-set *service-set*—(Optional) Clear stateful firewall statistics for the specified service set.

Required Privilege Level

view

RELATED DOCUMENTATION

show services stateful-firewall statistics | 2095

List of Sample Output

clear services stateful-firewall statistics on page 1680

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services stateful-firewall statistics

```
user@host> clear services stateful-firewall statistics
```

clear services web-filter statistics profile

Syntax

```
clear services web-filter statistics profile profile-name
<dns-filter-template template-name>
<fpc-slot fpc-slot pic-slot pic-slot>
<url-filter-template template-name>
```

Release Information

Command introduced in Junos OS Release 18.3R1.

Description

Clear statistics for DNS request filtering or URL filtering for the specified filter profile.

Options

dns-filter-template *template-name*—(Optional) Name of the DNS filter template for which statistics are cleared.

fpc-slot *fpc-slot* pic-slot *pic-slot*—(Optional) Location of the services PIC for which statistics are cleared.

profile *profile-name*—Name of the filter profile for which statistics are cleared.

url-filter-template *template-name*—(Optional) Name of the URL filter template for which statistics are cleared.

Required Privilege Level

clear

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

Configuring URL Filtering | 55

List of Sample Output

clear services web-filter statistics profile on page 1682

Output Fields

When you enter this command, the statistics for DNS request filtering are cleared. There is no specific output.

Sample Output

clear services web-filter statistics profile

```
user@host> clear services web-filter statistics profile profile1
```

request interface revert

Syntax

```
request interface revert interface interface-name
```

Release Information

Statement introduced in Junos OS Release 17.2 on MX Series.

Description

Revert from the secondary to the primary interface in the specified warm standby AMS interface.

Options

interface *interface-name*—Name of the AMS interface in which you want to revert from the secondary to the primary interface.

Required Privilege Level

view

List of Sample Output

request interface revert interface on page 1683

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request interface revert interface

```
user@host> request interface revert interface ams1
```

request interface (revert | switchover) (Adaptive Services)

Syntax

```
request interface (revert | switchover) (rsp<number> | rlsq<number>)
```

Release Information

Command introduced before Junos OS Release 7.4.
Support for **rlsq** interfaces added in Junos OS Release 7.6.

Description

(M Series and T Series routers only) Manually revert to the primary adaptive services interface or link services IQ interface, or to switch from the primary to the secondary interface.

> **NOTE:** All **rlsq** switchover or revert operations are allowed from the **rlsq*number*** level only and not for individual channelized interfaces (**rlsq*number*:*unit***).

On an aggregated Ethernet interface with link protection enabled, use the **request interface (revert | switchover)** (Aggregated Ethernet Link Protection) operational command to manually revert egress traffic from the designated backup link to the designated primary link, or to manually switch egress traffic from the primary link to the backup link. For information about this command, see *request interface (revert | switchover) (Aggregated Ethernet Link Protection)*.

Options

(revert | switchover)—The **revert** keyword restores active processing to the primary adaptive services (sp) or link services IQ (lsq) interface. The **switchover** keyword transfers active processing to the secondary (backup) interface.

rsp*number*—Redundant adaptive services interface name.

rlsq*number*—Redundant link services IQ interface name.

Required Privilege Level

view

List of Sample Output

request interface revert on page 1685
request interface switchover on page 1685

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request interface revert

```
user@host> request interface revert rlsq0
```

```
request succeeded
```

request interface switchover

```
user@host> request interface switchover rlsq0
```

```
error: rlsq0: already on secondary
```

request interface switchover

Syntax

```
request interface switchover interface interface-name
```

Release Information

Statement introduced in Junos OS Release 17.2 on MX Series.

Description

Switch over from the primary to the secondary (backup) interface in the specified warm standby AMS interface. If the secondary interface is already in use, then the operation fails.

Options

interface *interface-name*—Name of the AMS interface in which you want to switchover from the primary to the secondary interface.

Required Privilege Level

view

List of Sample Output

request interface switchover interface on page 1686

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request interface switchover interface

```
user@host> request interface switchover interface ams1
```

request security pki ca-certificate enroll

Syntax

```
request security pki ca-certificate enroll ca-profile ca-profile-name
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Request a digital certificate from a certificate authority (CA) online by using the Simple Certificate Enrollment Protocol (SCEP).

Options

ca-profile *ca-profile-name*—CA profile name.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

clear security pki ca-certificate | 1655

show security pki ca-certificate | 1789

List of Sample Output

request security pki ca-certificate enroll on page 1687

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate enroll

```
user@host> request security pki ca-certificate enroll ca-profile entrust
```

```
Received following certificates:
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
  Certificate: C=us, O=juniper, CN=First Officer
```

```
    Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
  Certificate: C=us, O=juniper
    Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

request security pki ca-certificate load

Syntax

```
request security pki ca-certificate load ca-profile ca-profile-name filename path/filename
```

Release Information
Command introduced in Junos OS Release 7.5.

Description
Manually load a certificate authority (CA) digital certificate from a specified location.

Options
ca-profile *ca-profile-name*—Load the specified CA profile.

filename *path/filename*—Directory location and filename of the CA digital certificate.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

clear security pki ca-certificate | 1655
show security pki ca-certificate | 1789

List of Sample Output
request security pki ca-certificate load on page 1689

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate load

```
user@host> request security pki ca-certificate load ca-profile ca-private filename pki-file
```

request security pki ca-certificate verify

Syntax

```
request security pki ca-certificate verify ca-profile ca-profile-name
```

Release Information
Command introduced in Junos OS Release 8.5.

Description
Verify the digital certificate installed for the specified certificate authority (CA).

Options
ca-profile *ca-profile-name*—Name of the local digital certificate identifier.

Required Privilege Level
maintenance

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)
```

```
user@host> request security pki ca-certificate verify ca-profile ca1
```

```
CA certificate ca1: CRL verification in progress. Please check the PKId debug logs
 for completion status
```

request security pki crl load

Syntax

```
request security pki crl load ca-profile ca-profile-name  filename path/filename
```

Release Information
Command introduced in Junos OS Release 8.1.

Description
Manually install a certificate revocation list (CRL) on the router from a specified location.

Options
ca-profile *ca-profile-name* —Load the specified certificate authority (CA) profile.

filename *path/filename* —Directory location and filename of the CRL.

Required Privilege Level
maintenance

List of Sample Output
request security pki crl load on page 1691

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki crl load

```
user@host> request security pki crl load ca-profile ca-private filename pki-file
```

request security pki generate-certificate-request

Syntax

```
request security pki generate-certificate-request certificate-id certificate-id-name domain-name domain-name
    subject subject-distinguished-name
<email email-address>
<filename (path | terminal)>
<ip-address ip-address>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format.

Options

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

domain-name *domain-name*—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

subject *subject-distinguished-name*—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

email *email-address*—(Optional) E-mail address of the certificate holder.

filename (*path* | terminal)—(Optional) Location where the local digital certificate request should be placed or the login terminal.

ip-address *ip-address*—(Optional) IP address of the router.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

- clear security pki certificate-request | 1656
- show security pki certificate-request | 1794

List of Sample Output

request security pki generate-certificate-request on page 1693

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-certificate-request

`user@host>` **request security pki generate-certificate-request certificate-id local-entrust2 domain-name router2.example.net filename entrust-req2 subject cn=router2.example.net**

```
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ70fO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

request security pki generate-key-pair

Syntax

```
request security pki generate-key-pair certificate-id certificate-id-name
<size (512 | 1024 | 2048)>
```

Release Information
Command introduced in Junos OS Release 7.5.

Description
Generate a Public Key Infrastructure (PKI) public and private key pair for a local digital certificate.

Options
certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

size—(Optional) Key pair size. The key pair size can be **512**, **1024**, or **2048** bits.

Required Privilege Level
maintenance

List of Sample Output
request security pki generate-key-pair on page 1694

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

`user@host>` **request security pki generate-key-pair certificate-id billy size 2048**

```
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate enroll

Syntax

```
request security pki local-certificate enroll ca-profile ca-profile-name certificate-id certificate-id-name
   challenge-password password  domain-name domain-name subject subject-distinguished-name
<email email-address>
<ip-address ip-address>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Request that a certificate authority (CA) enroll and install a local digital certificate online by using the Simple Certificate Enrollment Protocol (SCEP).

Options

ca-profile *ca-profile-name*—CA profile name.

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

challenge-password *password*—Password set by the administrator and normally obtained from the SCEP enrollment webpage of the CA. The password is 16 characters in length.

domain-name *domain-name*—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

subject *subject-distinguished-name*—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

email *email-address*—(Optional) E-mail address of the certificate holder.

ip-address *ip-address*—(Optional) IP address of the router.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

show security pki local-certificate | 1800

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

`user@host>` **request security pki local-certificate enroll certificate-id r3-entrust-scep ca-profile entrust domain-name router3.example.net subject "CN=router3,OU=Engineering,O=juniper,C=US" challenge-password 123**

```
Certificate enrollment has started. To view the status of your enrollment, check
the public key infrastructure log (pkid) log file at /var/log/pkid. Please save
the challenge-password for revoking this certificate in future.  Note that this
password is not stored on the router.
```

request security pki local-certificate generate-self-signed

Syntax

request security pki local-certificate generate-self-signed certificate-id *certificate-id-name* domain-name *domain-name* ip-address *ip-address* email *email-address* subject *subject-distinguished-name*

Release Information

Command introduced in Junos OS Release 9.1.

Description

Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

domain-name *domain-name*—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

email *email-address*—E-mail address of the certificate holder.

ip-address *ip-address*—IP address of the router.

subject *subject-distinguished-name*—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

Required Privilege Level

maintenance
security

RELATED DOCUMENTATION

Requesting for and Installing a Digital Certificates on Your Router | 757

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

`user@host>` **request security pki local-certificate generate-self-signed certificate-id self-cert subject cn=abc domain-name example.net email user1@example.net**

```
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate load

Syntax

```
request security pki local-certificate load certificate-id certificate-id-name  filename path
```

Release Information
Command introduced in Junos OS Release 7.5.

Description
Manually load a local digital certificate from a specified location.

Options
certificate-id *certificate-id-name*—Name of the public/private key pair mapped to the local digital certificate.

filename *path/filename*—Directory location and filename of the local digital certificate provided by the CA.

Required Privilege Level
maintenance

List of Sample Output
request security pki local-certificate load on page 1699

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate load

`user@host>` **request security pki local-certificate load filename /tmp/router2-cert certificate-id local-entrust2**

```
Local certificate local-entrust2 loaded successfully
```

request security pki local-certificate verify

Syntax

```
request security pki local-certificate verify certificate-id certificate-id-name
```

Release Information
Command introduced in Junos OS Release 8.5.

Description
Verify the validity of the local digital certificate identifier.

Options
certificate-id *certificate-id-name* —Display the specified certificate identifier name.

Required Privilege Level
maintenance

RELATED DOCUMENTATION

show security pki local-certificate | 1800

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate-id bme1 (not
downloaded)
```

```
user@host> request security pki local-certificate verify certificate-id bme1
```

```
Local certificate bme1: CRL verification in progress. Please check the PKId debug
 logs for completion status
```

You receive the following response after the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate bme1 (downloaded)
```

```
user@host> request security pki local-certificate verify certificate-id bme1
```

```
Local certificate bme1 verification success
```

request services ipsec-vpn ipsec switch tunnel

Syntax

request services ipsec-vpn ipsec switch tunnel local-gateway *address* remote-gateway *address* <routing-instance *instance-name*>

Release Information

Command introduced before Junos OS Release 7.4.
routing-instance option added in Release 8.1.

Description

(Adaptive services interface only) Manually switch between primary and backup IP Security (IPsec) tunnels.

Options

local-gateway *address*—Gateway address of the local system.

remote-gateway *address*—Gateway address of the remote system.

routing-instance *instance-name*—(Optional) VRF instance associated with local gateway address.

Required Privilege Level

view

RELATED DOCUMENTATION

show services ipsec-vpn ipsec security-associations | 1878

List of Sample Output

request services ipsec-vpn ipsec switch tunnel on page 1702

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services ipsec-vpn ipsec switch tunnel

```
user@host> request services ipsec-vpn ipsec switch tunnel local-gateway 10.1.1.1 remote gateway
10.100.10.1
```

request services redundancy-set trigger

Syntax

```
request services redundancy-set (redundancy-set |all) trigger redundancy-event
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.

Description

Manually trigger a redundancy event for the specified redundancy set or all sets on the current gateway.

request services url-filter delete gencfg-data

Syntax

```
request services url-filter delete gencfg-data
```

Release Information

Command introduced in Junos OS Release 17.2.

Description

Delete url-filterd–ased objects. This is historical information.

WARNING: Do not use this command unless explicitly instructed to do so.

NOTE: Starting in Junos OS Release 18.3R1, the **request services url-filter delete gencfg-data** command is deprecated and has been replaced by the **request services web-filter delete gencfg-data** command.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services url-filter force dns-resolution | 1705
- request services url-filter update url-filter-database file | 1707
- request services url-filter validate | 1708
- Configuring URL Filtering | 55

request services url-filter force dns-resolution

Syntax

```
request services url-filter force dns-resolution (all | profile profile-name)
<template template-name>
```

Release Information

Command introduced in Junos OS Release 17.2.

Description

Force the domain name system (DNS) resolution request.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **request services url-filter force dns-resolution** command is deprecated and has been replaced by the **request services web-filter force dns-resolution** command.

Options

all—Force a DNS resolution request for all profiles.

profile *profile-name*—Force a DNS resolution request for the profile (all templates).

template *template-name*—Force a DNS resolution request for the template.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services url-filter delete gencfg-data | 1704
- request services url-filter update url-filter-database file | 1707
- request services url-filter validate | 1708
- Configuring URL Filtering | 55

List of Sample Output

Sample Output

request services url-filter force dns-resolution profile profile1

```
user@host> request services url-filter force dns-resolution profile profile1
```

```
STATUS: DNS resolution is triggered for profile profile1
```

request services url-filter force dns-resolution profile profile1 template template1

```
user@host> request services url-filter force dns-resolution profile profile1 template template1
```

```
STATUS: DNS resolution is triggered for template template1 in profile profile1
```

request services url-filter force dns-resolution all

```
user@host> request services url-filter force dns-resolution all
```

```
STATUS: DNS resolution has been triggered for all profiles
```

request services url-filter update url-filter-database file

Syntax

```
request services url-filter update url-filter-database file filename
```

Release Information

Command introduced in Junos OS Release 17.2.

Description

Update the URL filter database. If you change the database file, run this command. It sends a request to the DNS server for only the new hostnames that were not in the previous version of URL database file.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **request services url-filter update url-filter-database file** command is deprecated and has been replaced by the **request services web-filter update url-filter-database file** command.

Options

filename—Use the database filename.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services url-filter delete gencfg-data | 1704
- request services url-filter force dns-resolution | 1705
- request services url-filter validate | 1708
- Configuring URL Filtering | 55

request services url-filter validate

Syntax

```
request services url-filter validate (all | file-name filename)
```

Release Information

Command introduced in Junos OS Release 17.2.

Description

Validate the URL filter database to ensure the database is correct.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **request services url-filter validate** command is deprecated and has been replaced by the **request services web-filter validate url-filter-file-name** command.

Options

all—Validate the URL filter database for all profiles.

file-name *filename*—Validate the URL filter database for the database file specified.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services url-filter delete gencfg-data | 1704
- request services url-filter force dns-resolution | 1705
- request services url-filter update url-filter-database file | 1707
- Configuring URL Filtering | 55

request services web-filter delete gencfg-data

Syntax

```
request services web-filter delete gencfg-data
```

Release Information

Command introduced in Junos OS Release 18.3R1.

Description

Delete url-filterd–ased objects. This is historical information.

WARNING: Do not use this command unless explicitly instructed to do so.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services web-filter force dns-resolution | 1711
- request services web-filter update url-filter-database file | 1712
- request services web-filter validate url-filter-file-name | 1714
- Configuring URL Filtering | 55

request services web-filter update dns-filter-database

Syntax

```
request services web-filter update dns-filter-database filename
```

Release Information

Command introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

When you make changes to the domain filter database file, which is used in filtering DNS requests for disallowed domains, apply the changes.

Options

filename—File name of the database file.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

request services web-filter force dns-resolution

Syntax

```
request services web-filter force dns-resolution (all | profile profile-name)
<template template-name>
```

Release Information

Command introduced in Junos OS Release 18.3R1.

Description

Force the domain name system (DNS) resolution request.

Options

all—Force a DNS resolution request for all profiles.

profile *profile-name*—Force a DNS resolution request for the profile (all templates).

template *template-name*—Force a DNS resolution request for the template.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services web-filter delete gencfg-data | 1709
- request services web-filter update url-filter-database file | 1712
- request services web-filter validate url-filter-file-name | 1714
- Configuring URL Filtering | 55

request services web-filter update url-filter-database file

Syntax

```
request services web-filter update url-filter-database file filename
```

Release Information

Command introduced in Junos OS Release 18.3R1.

Description

Update the URL filter database. If you change the database file, run this command. It sends a request to the DNS server for only the new hostnames that were not in the previous version of the URL database file.

Options

filename—Use the database filename.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services web-filter delete gencfg-data | 1709
- request services web-filter force dns-resolution | 1711
- request services web-filter validate url-filter-file-name | 1714
- Configuring URL Filtering | 55

request services web-filter validate dns-filter-file-name

Syntax

```
request services web-filter validate dns-filter-file-name filename hash-key key-string hash-method hash-method-name
```

Release Information

Command introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Validate the file format of the domain filter database file, which is used in filtering DNS requests for disallowed domains.

Options

filename—File name of the database file.

hash-method-name—Hash method you used to produce the hashed domain name values in the database file.

key-string—Hash key you used to produce the hashed domain name values in the database file.

Required Privilege Level

maintenance

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43

request services web-filter validate url-filter-file-name

Syntax

```
request services web-filter validate (all | url-filter-file-name filename)
```

Release Information

Command introduced in Junos OS Release 18.3R1.

Description

Validate the URL filter database to ensure the database is correct.

Options

all—Validate the URL filter database for all profiles.

url-filter-file-name *filename*—Validate the URL filter database for the database file specified.

Required Privilege Level

view

RELATED DOCUMENTATION

- request services web-filter delete gencfg-data | 1709
- request services web-filter force dns-resolution | 1711
- request services web-filter update url-filter-database file | 1712
- Configuring URL Filtering | 55

show interfaces (Adaptive Services)

Syntax

```
show interfaces interface-type
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display status information about the specified adaptive services interface.

Options

interface-type—On M Series and T Series routers, the interface type is **sp-** ***fpc/pic/port***.

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

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index ***snmp-index***—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces (Adaptive Services) on page 1719
show interfaces brief (Adaptive Services) on page 1720
show interfaces detail (Adaptive Services) on page 1720
show interfaces extensive (Adaptive Services) on page 1721

Output Fields

Table 49 on page 1716 lists the output fields for the **show interfaces** (adaptive services and redundant adaptive services) command. Output fields are listed in the approximate order in which they appear.

Table 49: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields

Field Name	Field Description
Physical Interface	
Physical interface	Name of the physical interface.
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under *Fields Description*.
Interface index	Physical interface's index number, which reflects its initialization sequence.
SNMP ifIndex	SNMP index number for the physical interface.
Generation	Unique number for use by Juniper Networks technical support only.
Type	Encapsulation being used on the interface.
Link-level type	Encapsulation being used on the physical interface.
MTU	MTU size on the physical interface.
Clocking	Reference clock source: can be **Internal** or **External**.
Speed	Speed at which the interface is running.
Device flags	Information about the physical device. Possible values are described in the “Device Flag *Common Output Fields Description*.
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” sect *Output Fields Description*.
Link type	Physical interface link type: **Full-Duplex** or **Half-Duplex**.
Link flags	Information about the link. Possible values are described in the “Link Flags” section und *Fields Description*.
Physical info	Information about the physical interface.
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.
Current address	Configured MAC address.
Hardware address	MAC address of the hardware.

Table 49: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description
Alternate link address	Backup address of the link.
Last flapped	Date, time, and how long ago the interface went from down to up. The format is **Last fla** ***year-month-day hour:minute:second timezone* (*hour:minute:second* ago)**. For example, **Last fla 10:52:40 PDT (04:33:20 ago)**.
Input Rate	Input rate in bits per second (bps) and packets per second (pps).
Output Rate	Output rate in bps and pps.
Statistics last cleared	Time when the statistics for the interface were last set to zero.
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interfac **NOTE:** With static NAT configured as basic NAT44 or destination NAT44 on MX Series rou and MS-MPCs, the Input bytes field might show 16 more bytes than the Output bytes f by the accounting of 16 bytes of the Juniper Forwarding Module cookie. • **Input bytes**—Number of bytes received on the interface. • **Output bytes**—Number of bytes transmitted on the interface. • **Input packets**—Number of packets received on the interface. • **Output packets**—Number of packets transmitted on the interface.
Input errors	Input errors on the interface. The following paragraphs explain the counters whose mea obvious: • **Errors**—Sum of the incoming frame aborts and FCS errors. • **Drops**—Number of packets dropped by the input queue of the I/O Manager ASIC. If t saturated, this number increments once for every packet that is dropped by the ASIC' • **Framing errors**—Number of packets received with an invalid frame checksum (FCS). • **Runts**—Frames received smaller than the runt threshold. • **Giants**—Frames received larger than the giant threshold. • **Policed discards**—Number of frames that the incoming packet match code discarded not recognized or not of interest. Usually, this field reports protocols that the Junos C • **Resource errors**—Sum of transmit drops.

Table 49: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description
Output errors	Output errors on the interface. The following paragraphs explain the counters whose me obvious: • **Carrier transitions**—Number of times the interface has gone from **down** to **up**. This nu normally increment quickly, increasing only when the cable is unplugged, the far-end down and then up, or another problem occurs. If the number of carrier transitions inc (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunc • **Errors**—Sum of the outgoing frame aborts and FCS errors. • **Drops**—Number of packets dropped by the output queue of the I/O Manager ASIC. If saturated, this number increments once for every packet that is dropped by the ASIC' • **MTU errors**—Number of packets larger than the MTU threshold. • **Resource errors**—Sum of transmit drops.
Logical Interface	
Logical interface	Name of the logical interface.
Index	Logical interface index number, which reflects its initialization sequence.
SNMP ifIndex	SNMP interface index number.
Generation	Unique number for use by Juniper Networks technical support only.
Flags	Information about the logical interface. Possible values are described in the "Logical Inter under *Common Output Fields Description*.
Encapsulation	Encapsulation on the logical interface.
Input packets	Number of packets received on the logical interface.
Output packets	Number of packets transmitted on the logical interface.
Traffic statistics	Number and rate of bytes and packets received and transmitted on the logical interface • **Input bytes**—Number of bytes received on the interface. • **Output bytes**—Number of bytes transmitted on the interface. • **Input packets**—Number of packets received on the interface. • **Output packets**—Number of packets transmitted on the interface.
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst o the value in the output packet rate field might briefly exceed the peak cell rate. It takes less than 1 second) for this counter to stabilize.

Table 49: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in rate field might briefly exceed the peak cell rate. It takes generally less than 1 second fo stabilize.
protocol-family	Protocol family configured on the logical interface. If the protocol is **inet**, the IP address also displayed.
Protocol	Protocol family configured on the logical interface, such as **iso**, **inet6**, **mpls**.
MTU	MTU size on the logical interface.
Generation	Unique number for use by Juniper Networks technical support only.
Route table	Routing table in which the logical interface address is located. For example, **0** refers to t inet.0.
Flags	Information about the protocol family flags. Possible values are described in the "Family F *Common Output Fields Description*.
Addresses, Flags	Information about the address flags. Possible values are described in the "Addresses Fla *Common Output Fields Description*.
Destination	IP address of the remote side of the connection.
Local	IP address of the logical interface.
Broadcast	Broadcast address.
Generation	Unique number for use by Juniper Networks technical support only.

Sample Output

show interfaces (Adaptive Services)

```
user@host> show interfaces sp-1/2/0
```

```
Physical interface: sp-1/2/0, Enabled, Physical link is Up
  Interface index: 147, SNMP ifIndex: 72
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: 9192,
```

```
  Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
  Link flags     : None
  Last flapped   : 2006-03-06 11:37:18 PST (00:57:29 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

  Logical interface sp-1/2/0.16383 (Index 68) (SNMP ifIndex 73)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
    Input packets : 3057
    Output packets: 3044
    Protocol inet, MTU: 9192
      Flags: Receive-options, Receive-TTL-Exceeded
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.0.0.34, Local: 10.0.0.1
```

show interfaces brief (Adaptive Services)

user@host> **show interfaces sp-1/2/0 brief**

```
Physical interface: sp-1/2/0, Enabled, Physical link is Up
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: 9192,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000

  Logical interface sp-1/2/0.16383
    Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
    inet  10.0.0.1         --> 10.0.0.34
```

show interfaces detail (Adaptive Services)

user@host> **show interfaces sp-1/2/0 detail**

```
Physical interface: sp-1/2/0, Enabled, Physical link is Up
  Interface index: 147, SNMP ifIndex: 72, Generation: 30
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: 9192,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Link type      : Full-Duplex
```

```
  Link flags     : None
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped   : 2006-03-06 11:37:18 PST (00:57:56 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :               125147                  0 bps
   Output bytes  :              1483113                  0 bps
   Input  packets:                 3061                  0 pps
   Output packets:                 3048                  0 pps

  Logical interface sp-1/2/0.16383 (Index 68) (SNMP ifIndex 73) (Generation 7)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
    Traffic statistics:
     Input  bytes  :               125147
     Output bytes  :              1483113
     Input  packets:                 3061
     Output packets:                 3048
    Local statistics:
     Input  bytes  :               125147
     Output bytes  :              1483113
     Input  packets:                 3061
     Output packets:                 3048
    Transit statistics:
     Input  bytes  :                    0                    0 bps
     Output bytes  :                    0                    0 bps
     Input  packets:                    0                    0 pps
     Output packets:                    0                    0 pps
    Protocol inet, MTU: 9192, Generation: 20, Route table: 1
      Flags: Receive-options, Receive-TTL-Exceeded
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.0.0.34, Local: 10.0.0.1, Broadcast: Unspecified,
        Generation: 22
```

show interfaces extensive (Adaptive Services)

`user@host>` **show interfaces sp-1/2/0 extensive**

```
Physical interface: sp-1/2/0, Enabled, Physical link is Up
  Interface index: 147, SNMP ifIndex: 72, Generation: 30
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: 9192,
  Clocking: Unspecified, Speed: 800mbps
```

```
Device flags   : Present Running
Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
Link type      : Full-Duplex
Link flags     : None
Physical info  : Unspecified
Hold-times     : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Last flapped   : 2006-03-06 11:37:18 PST (00:58:40 ago)
Statistics last cleared: Never
Traffic statistics:
 Input  bytes  :               125547                   0 bps
 Output bytes  :              1483353                   0 bps
 Input  packets:                 3065                   0 pps
 Output packets:                 3052                   0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
  Policed discards: 0, Resource errors: 0
Output errors:
  Carrier transitions: 2, Errors: 0, Drops: 0, MTU errors: 0,
  Resource errors: 0

Logical interface sp-1/2/0.16383 (Index 68) (SNMP ifIndex 73) (Generation 7)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
  Traffic statistics:
   Input  bytes  :               125547
   Output bytes  :              1483353
   Input  packets:                 3065
   Output packets:                 3052
  Local statistics:
   Input  bytes  :               125547
   Output bytes  :              1483353
   Input  packets:                 3065
   Output packets:                 3052
  Transit statistics:
   Input  bytes  :                    0                   0 bps
   Output bytes  :                    0                   0 bps
   Input  packets:                    0                   0 pps
   Output packets:                    0                   0 pps
  Protocol inet, MTU: 9192, Generation: 20, Route table: 1
    Flags: Receive-options, Receive-TTL-Exceeded
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.0.0.34, Local: 10.0.0.1, Broadcast: Unspecified,
      Generation: 22
```

show interfaces (Link Services IQ)

Syntax

```
show interfaces lsq-fpc/pic/port
<brief | detail | extensive | terse>
<descriptions>
<l2-statistics>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.
l2-statistics option introduced with Junos OS Release 12.1.

Description

(M Series, MX Series, and T Series routers only) Display status information about the specified link services intelligent queuing (IQ) interface.

Options

lsq-*fpc/pic/port*—Display standard status information about the specified link services IQ interface.

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

descriptions—(Optional) Display interface description strings.

l2-statistics—(Optional) Display Layer 2 queue statistics for Multilink Point-to-Point Protocol (MLPPP), FRF.15, and FRF.16 bundles.

media—(Optional) Display media-specific information about network interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Additional Information

Link services IQ interfaces are similar to link services interfaces. The important difference is that link services IQ interfaces fully support Junos OS class-of-service (CoS) components.

Required Privilege Level

view

RELATED DOCUMENTATION

Link and Multilink Services Overview

Multilink Interfaces on Channelized MICs Overview

List of Sample Output

show interfaces extensive (MLPPP on Link Services IQ) on page 1745
show interfaces extensive (Multiclass MLPPP on Link Services IQ) on page 1747
show interfaces extensive (MLPPP on Link Services IQ Bundle) on page 1749
show interfaces extensive (MFR on Link Services IQ Bundle) on page 1751
show interfaces extensive (Multiclass MLPPP on Link Services IQ) on page 1754

Output Fields

Table 50 on page 1724 lists the output fields for the **show interfaces** (link services IQ) command. Output fields are listed in the approximate order in which they appear.

Table 50: show interfaces (Link Services IQ) Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the "Enabled Field" section under *Common Output Fields Description*.	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	SNMP index number for the physical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
Link-level type	Encapsulation being used on the physical interface: **Multilink-Frame-Relay-UNI-NNI Multilink-Frame-Relay-UNI-NNI** (default), **LinkService**, **Frame-relay**, **Frame-relay-ccc**, or **Frame-relay-tcc**.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under *Common Output Fields Description*.	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under *Common Output Fields Description*.	All levels

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Last flapped	Date, time, and how long ago the interface went from down to up. The format is **Last flapped: *year-month-day hour:minute:second timezone* (*hour:minute:second* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.	**detail extensive** none

Multilink Frame Relay UNI NNI bundle options	(Multilink Frame Relay UNI NNI only) Configured information about Multilink Frame Relay bundle options.
	• **Device type**—DCE (data communication equipment) or DTE (data terminal equipment).
	• **MRRU**—Configured size of the maximum received reconstructed unit (MRRU): 1500 to 4500 bytes. The default is 1524 bytes.
	• **Bandwidth**—Speed at which the interface is running.
	• **Fragmentation threshold**—Configured fragmentation threshold: 128 through 16,320 bytes, in integer multiples of 64 bytes. The default setting is 0, which disables fragmentation.
	• **Red differential delay limit**—Red differential delay limit among bundle links has been reached, indicating an action will occur.
	• **Yellow differential delay limit**—Yellow differential delay among bundle links has been reached, indicating a warning will occur.
	• **Red differential delay action**—Type of actions taken when the red differential delay exceeds the red limit: *Disable link transmit* or *Remove link from service*.
	• **Link layer overhead**—Percentage of bundle bandwidth to be set aside for link layer overhead.
	• **Reassembly drop timer**—Drop timeout value to provide a recovery mechanism if individual links in the link services bundle drop one or more packets: 1 through 127 milliseconds. By default, the drop timeout parameter is 0 (disabled). A value under 5 ms is not recommended.
	• **Links needed to sustain bundle**—Minimum number of links to sustain the bundle: 1 through 8.
	• **LIP Hello timer**—Link Interleaving Protocol hello timer: 1 through 180 seconds.
	  ◦ **Acknowledgement timer**—Maximum period to wait for an add link acknowledgement, hello acknowledgement, or remove link acknowledgement: 1 through 10 seconds.
	  ◦ **Acknowledgement retries**—Number of retransmission attempts to be made for consecutive hello or remove link messages after the expiration of the acknowledgement timer: 1through 5.
		detail extensive none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output

Multilink Frame Relay UNI NNI bundle options (continued)	• **Bundle class**—Bundle class ID.
	• **LMI type**—Multilink Frame Relay UNI NNI LMI type: **ANSI**, **Q.933 ANNEX A**, or **Consortium**.
	  ◦ **T391 LIV polling timer**—Multilink Frame Relay UNI NNI Full status polling counter: 1 through 255, with a default value of 6.
	  ◦ **T392 polling verification timer**—Multilink Frame Relay UNI NNI LMI error threshold. The number of errors required to bring down the link, within the event count specified by *N393*. The range is 1 through 10, with a default value of 3.
	  ◦ **N391 full status polling count**—Multilink Frame Relay UNI NNI Full status polling counter: 1 through 255.
	  ◦ **N392 error threshold**—Multilink Frame Relay UNI NNI LMI error threshold: 1 through 10.
	• **N393 monitored event count**—Multilink Frame Relay UNI NNI LMI monitored event count: 1 through 10, with a default value of 4.
	• **Consortium LMI Settings**
	  ◦ **n391dte**—DTE full status polling interval in seconds: 1 through 255.
	  ◦ **n392dce**—DCE error threshold: 1 through 10.
	  ◦ **n392dte**—DTE error threshold: 1 through 10.
	  ◦ **n393dce**—DCE monitored event count: 1 through 10.
	n393dte—DTE monitored event count: 1 through 10.
	  ◦ **t391dte**—DTE polling verification timer (in seconds): 5 through 30.
	  ◦ **t392dce**—DCE polling verification timer (in seconds): 5 through 30.
		detail extensive none

LMI	Local Managment Interface packet statistics: • **Input**—Number of packets arriving on the interface (nn) and timestamp of the most recent packet arrival, in the format: **Input: *nn* (last seen *hh:mm:ss ago*)** **Output**—Number of packets sent out on the interface (nn) and how much time has passed since the last packet was sent, in the format: **Output: *nn* (last seen *hh:mm:ss ago*)**	**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
DTE Statistics	Statistics about information transferred from the data terminal equipment (DTE) to the data communications equipment (DCE). • **Enquiries sent**—Number of link status enquiries sent from the DTE to the DCE. • **Full enquiries sent**—Number of full enquiries sent from the DTE to the DCE. • **Enquiry responses received**—Number of enquiry responses received by the DCE from the DTE. • **Full enquiry responses received**—Number of full enquiry responses received by DCE from the DTE.	**detail extensive** none
DCE Statistics	Statistics about information transferred from the DCE to the DTE. • **Enquiries received**—Number of enquiries received by the DCE from the DTE. • **Full enquiries received**—Number of full enquiries received by the DCE from the DTE. • **Enquiry responses sent**—Number of enquiry responses sent from the DCE to the DTE. • **Full enquiry responses sent**—Number of full enquiry responses sent from the DCE to the DTE.	**detail extensive** none
Common Statistics	Statistics about messages snet between the DTE and the DCE. • **Unknown messages received**—Number of received packets that do not fall into any other category. • **Asynchronouts updates received**—Number of link status peer changes received. • **Out-of-sequence packets received**—Number of packets for which the sequence of the packets received is different from the expected sequence. • **Keepalive responses timed out**—Number of keepalive responses that time out when no Local Management Interface (LMI) packet was reported for **n392dte** or **n393dce** intervals. (See *LMI settings*.)	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. All references to traffic direction (input or output) are defined with respect to the Packet Forwarding Engine (PFE). Input traffic refers to the fragments received by the ingress PFE, which get assembled into Layer 3 input packets. Output packets refer to the IP packets transmitted out of the ingress PFE to the LSQ, which get segmented into output fragments.	**detail extensive**

DLCI*nn*	Data-link connection identifier (DLCI) number of the logicial interview. The following information is displayed.
	• **Flags**—Values are:
	  • **Active**—Set when the link is active and the DTE and DCE are exchanging information.
	  • **Down**—Set when the link is active, but no information is received from the DTE.
	  • **DCE unconfigured**—Set when the corresponding DCLI in the DCE is not configured.
	  • **Configured**—Set when the correspondening DLCCI is configured.
	  • **DCE-Configured**—Displayed when the command is issued from the DTE.	

DLCI Statistics	(Frame Relay) Data-link connection identifier (DLCI) statistics. • **Active DLCI**—Number of active DLCIs. • **Inactive DLCI**—Number of inactive DLCIs.	
Input rate	(Redundant LSQ) Rate of bits and packets received on the interface.	None specified
Output rate	(Redundant LSQ) Rate of bits and packets transmitted on the interface.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	**detail extensive**
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. All references to traffic direction (input or output) are defined with respect to the router. Input fragments received by the router are assembled into input packets; output packets are segmented into output fragments for transmission out of the router.	**detail extensive**

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Frame exceptions	Information about framing exceptions. Includes events recorded under **Exception Events** for each logical interface. • **Oversized frames**—Number of frames received that exceed maximum frame length. Maximum length is 4500 Kb (kilobits). • **Errored input frames**—Number of input frame errors. • **Input on disabled link/bundle**—Number of frames received on disabled links. These frames can result either from an inconsistent configuration, or from a bundle or link being brought up or down with traffic actively flowing through it. • **Output for disabled link/bundle**—Number of frames sent for a disabled or unavailable link. These frames can result either from an inconsistent configuration, or from a bundle being brought up or down while traffic is flowing through it. • **Queuing drops**—Total number of packets dropped before traffic enters the link services IQ interface. Indicates that the interface is becoming oversubscribed.	**extensive**
Buffering exceptions	Information about buffering exceptions. Includes events recorded under **Exception Events** for each logical interface: • **Packet data buffer overflow**—Packet buffer memory is full. This overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity. Check the logical interface exception event counters to determine which bundle is responsible.	**extensive**

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Assembly exceptions		**extensive**

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	(Multilink Frame Relay end-to-end only) Information about assembly exceptions. Includes events recorded under **Exception Events** for each logical interface. An assembly exception does not necessarily indicate an operational problem with the physical link services IQ interface itself. If multilink-encapsulated traffic is dropped or reordered after a sequence number has been assigned, the interface records one or more exception events. The physical interface can drop multilink-encapsulated fragments itself as a result. Any multilink packets or fragments dropped by the interface itself result in packet or fragment drop counts on individual logical interfaces. If the logical interface drop counts are zero, but exception events are seen, the most likely cause is a problem with the individual link interfaces. Even if the logical interface fragment drop counts are nonzero, excess differential delay or traffic losses on individual interfaces can be the root cause. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. These events do not necessarily indicate any problem with the operation of the physical link services IQ interface itself, but can occur when one or more individual links drop traffic. Check the logical interface exception event counters to determine which bundle is responsible. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. These events do not necessarily indicate any problem with the operation of the physical link services IQ interface itself, but can occur when one or more individual links drop traffic. Check the logical interface exception event counters to determine which bundle is responsible. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers within a single link. This event indicates that an individual link within a bundle reordered traffic, making the link services IQ interface unable to correctly process the resulting stream. Check the logical interface exception event counters to determine which bundle is responsible. • **Out-of-range sequence number**—Received a frame with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	events can occur when the far end of a bundle is taken down or brought up. Check the logical interface exception event counters to determine which bundle is responsible.	
Hardware errors (sticky)	(Multilink Frame Relay end-to-end only) Information about hardware errors: • **Data memory error**—A memory error was detected on the interface DRAM. Indicates possible hardware failure. Contact Juniper Networks technical support. • **Control memory error**—A memory error was detected on the interface DRAM. Indicates possible hardware failure. Contact Juniper Networks technical support.	**extensive**
Egress queues	Total number of egress queues supported on the specified interface.	**detail extensive** none
Queue counters	Queue number and its associated user-configured forwarding class name. • **Queued packets**—Number of queued packets. • **Transmitted packets**—Number of transmitted packets. • **Dropped packets**—Number of packets dropped by the ASIC's RED mechanism.	**detail extensive** none
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	Logical interface SNMP interface index number.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
Flags	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under *Common Output Fields Description*.	All levels
Encapsulation	Encapsulation being used: PPP or Multilink PPP.	All levels
Bandwidth	Speed at which the interface is running.	All levels

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle options	(Multilink Frame Relay end-to-end interfaces only) • **MRRU**—Configured size of the maximum received reconstructed unit (MRRU): 1500 through 4500 bytes. The default is 1504 bytes. • **Drop timer period**—Drop timeout value to provide a recovery mechanism if individual links in link services bundle drop one or more packets: 0 though 2000 milliseconds. Values under 5 ms are not recommended. The default setting is 0, which disables the timer. • **Sequence number format**—Short sequence number header format (MLPPP only). • **Fragmentation threshold**—Configured fragmentation threshold: 64 through 16,320 bytes, in integer multiples of 64 bytes. The default setting is 0, which disables fragmentation. • **Links needed to sustain bundle**—Minimum number of links to sustain the bundle: 1 through 8. • **Multilink classes**—Number of multilink classes negotiated. • **Link layer overhead**—Percentage of bundle bandwidth to be set aside for link-layer overhead.	**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle status (MLPPP) or **Multilink class status** (Multiclass MLPPP)		**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	Information about bundle status: • **Remote MRRU**—MRRU value received from remote peer. If negotiation has not been initiated, the default value is displayed. • **Received sequence number**—Sequence number for received packets. • **Transmitted sequence number**—Sequence number for transmitted packets. • **Packet drops**—Number and byte count of output packets that were dropped, rather than being encapsulated and sent out of the router as fragments. The packet drop counter is incremented if there is a temporary shortage of packet memory on the AS PIC, which causes packet fragmentation to fail. • **Fragment drops**—Number and byte count of input fragments that were dropped, rather than being reassembled and handled by the router as packets. This counter also includes fragments that have been received successfully, but had to be dropped because not all fragments that constituted a packet had been received. The fragment drop counter is incremented when a fragment received on constituent links is dropped. Drop fragments can be triggered by sequence ordering errors, duplicate fragments, timed-out fragments, and bad multilink headers. • **MRRU exceeded**—Number of reassembled packets exceeding the MRRU. This counter is not implemented in this release. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers within a single link. This event indicates that an individual link within a bundle reordered traffic, making the multilink interface unable to correctly process the resulting stream. • **Out-of-range sequence number**—Received a frame with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these events can occur when the far end of a bundle is taken down or brought up. • **Packet data buffer overflow**—Packet buffer memory is full. This	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity.	

Statistics	Information about fragments and packets received and sent by the router. All references to traffic direction (input or output) are defined with respect to the router. Input fragments received by the router are assembled into input packets; output packets are segmented into output fragments for transmission out of the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	• **Bundle**—Information for each active bundle link.
	  ◦ **Fragments: Input and Output**—Total number and rate of fragments received and transmitted.
	  ◦ **Packets: Input and Output**—Total number and rate of packets received and transmitted.
	  ◦ **Multilink class**—(Multiclass MLPPP only) Information about multiclass links used in the multilink operation.
	• **Link**—Information about links used in the multilink operation.
	  ◦ **Link name**—Interface name of the link services IQ channel and state information (physical link **up** or **down**).
	  ◦ **Input and Output**—Total number and rate of fragments and packets received and transmitted.
		detail extensive

NCP state	(PPP) Network Control Protocol state. • **Conf-ack-received**—Acknowledgement was received. • **Conf-ack-sent**—Acknowledgement was sent. • **Conf-req-sent**—Request was sent. • **Down**—NCP negotiation is incomplete (not yet completed or has failed). • **Not-configured**—NCP is not configured on the interface. • **Opened**—NCP negotiation is successful.	**detail extensive** none
Protocol	Protocol family configured on the logical interface.	**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
MTU	MTU size on the logical interface. If the MTU value is negotiated down to meet the MRRU requirement on the remote side, this value is marked **Adjusted**.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Route Table	Routing table in which this address exists. For example, **Route table:0** refers to inet.0.	**detail extensive**
Flags	Information about the protocol family flags. Possible values are described in the "Family Flags" section under *Common Output Fields Description*.	**detail extensive** none
Addresses, Flags	Information about the addresses configured on the logical interface. Possible values are described in the "Addresses Flags" section under *Common Output Fields Description*.	**detail extensive** none
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none
Broadcast	Broadcast address on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
MLPPP Bundle Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	Logical interface SNMP interface index number.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under *Common Output Fields Description*.	All levels
SNMP-Traps	SNMP trap notifications are enabled.	All levels
Encapsulation	Encapsulation being used: PPP, Multilink PPP, or Multilink-FR.	All levels

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Last flapped	Date, time, and how long ago the interface went from down to up. The format is **Last flapped: *year-month-day hour:minute:second timezone* (*hour:minute:second* ago)**. For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.	**detail extensive** none
Bandwidth	Speed at which the interface is running.	All levels
Bundle links linformation	Information about the bundled links. • **Active bundle links**—Number of active links. • **Removed bundle links**—Information about links used in the multilink operation. • **Disabled bundle links**—Number of disabled links.	**detail extensive** none
Bundle options	(Multilink Frame Relay end-to-end interfaces only) • **MRRU**—Configured size of the maximum received reconstructed unit (MRRU): 1500 through 4500 bytes. The default is 1504 bytes. • **Drop timer period**—Drop timeout value to provide a recovery mechanism if individual links in link services bundle drop one or more packets: 0 though 2000 milliseconds. Values under 5 ms are not recommended. The default setting is 0, which disables the timer. • **Inner PPP Protocol field compression**—Inner PPP protocol compression is enabled or disabled. • **Sequence number format**—Short sequence number header format (MLPPP only). • **Fragmentation threshold**—Configured fragmentation threshold: 64 through 16,320 bytes, in integer multiples of 64 bytes. The default setting is 0, which disables fragmentation. • **Links needed to sustain bundle**—Minimum number of links to sustain the bundle: 1 through 8. • **Multilink classes**—Number of multilink classes negotiated. • **Link layer overhead**—Percentage of bundle bandwidth to be set aside for link-layer overhead.	**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle status (MLPPP)		**detail extensive** none

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	Information about bundle status: • **Received sequence number**—Sequence number for received packets. • **Transmit sequence number**—Sequence number for transmitted packets. • **Packet drops**—Number and byte count of output packets that were dropped, rather than being encapsulated and sent out of the router as fragments. The packet drop counter is incremented if there is a temporary shortage of packet memory on the AS PIC, which causes packet fragmentation to fail. • **Fragment drops**—Number and byte count of input fragments that were dropped, rather than being reassembled and handled by the router as packets. This counter also includes fragments that have been received successfully but had to be dropped because not all fragments that constituted a packet had been received. The fragment drop counter is incremented when a fragment received on constituent links is dropped. Drop fragments can be triggered by sequence ordering errors, duplicate fragments, timed-out fragments, and bad multilink headers. • **MRRU exceeded**—Number of reassembled packets exceeding the MRRU. This counter is not implemented in this release. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers occurred within a single link. This event indicates that an individual link within a bundle reordered traffic, making the multilink interface unable to correctly process the resulting stream. • **Out-of-range sequence number**—A frame was received with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these events can occur when the far end of a bundle is taken down or brought up. • **Packet data buffer overflow**—Packet buffer memory is full. This overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity.	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Statistics		**extensive**

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output

	Information about frames, bytes, and bits per second received and sent by the router. All references to traffic direction (input or output) are defined with respect to the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	
	The bundle, multilink, and network statistics are reported by the Packet Forwarding Engine (PFE). The Multi Link Detail statistics like fragments, non-fragments and LFI are reported by the PIC.
	
	However, the PFE reports an extra overhead of 2 bytes in the output when compared with the Multilink Detail Statistics. This is due to the service-cookie in the PFE which does the link demux for the ML header.
	
	The difference in the bytes received and transmitted from Network and Multilink interfaces and Multilink statistics for each member link is divided between the ML and the PPP headers. For example the header counter for a long sequence configuration would be as follows.
	
	• Input side - Total overhead = 6 bytes.
	  ◦ ML: 4 bytes of ML header = 1 byte of Flag + 3 bytes of long sequence number.
	  ◦ PPP: 2 bytes of protocol field.
	• Output side - Total overhead = 11 bytes.
	  ◦ ML: 4 bytes of ML Header = 1 byte of Flag + 3 bytes of Long sequence number.
	  ◦ PPP: 5 bytes = 4 bytes of header + 1 byte of Idle flag.
	  ◦ 2 bytes of Service Cookie.
	• **Bundle**—Information for each active bundle link.
	  ◦ **Multilink: Input and Ouput**—Total number and rate of multilink frames, bytes, and bits per second received and transmitted. It is a module connecting LSQ PIC and its member link. Multilink Input displays L2 fragments received from the member link to the LSQ PIC. Multilink Output displays the L2 fragments transmitted from LSQ PIC to the member links.
	  ◦ **Network: Input and Output**—Total number of network frames, bytes, and bits per second received and transmitted. It refers to the packets transmitted from an ingress interface to the PFE and then to the LSQ PIC. Network Input displays the L3 packets received from the LSQ PIC to the PFE. Network Output displays the L3 packets transmitted from PFE to LSQ PIC.	

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output

	• **Link**—Information about links used in the multilink operation.
	  • **Link name**—The interface name of the link services IQ channel and state information (physical link *up* or *down*) and up time.
	  • **Input and Output**—Total number and rate of frames, bytes, and bits per second received and transmitted.	

Multilink detail statistics	Frames, bytes, and bits per second received and sent by the bundle. All references to traffic direction (input or output) are defined with respect to the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	
	The difference in the bytes received and transmitted from the bundle is divided between the ML and the PPP headers. For example the header counter for a long sequence configuration would be as follows:
	
	• Input side - Total overhead = 6 bytes.
	  • ML: 4 bytes of ML header = 1 byte of Flag + 3 bytes of long sequence number.
	  • PPP: 2 bytes of protocol field.
	• Output side - Total overhead = 9 bytes.
	  • ML: 4 bytes of ML Header = 1 byte of Flag + 3 bytes of Long sequence number.
	  • PPP: 5 bytes = 4 bytes of header + 1 byte of Idle flag.
	• **Bundle**—Information for the bundle link.
	  • **Fragments: Input and Output**—Total number and rate of multilink fragments received and transmitted.
	  • **Non-fragments: Input and Output**—Total number and rate of nonfragmented multilink frames received and transmitted.
	  • **LFI: Input and Output**—Total number and rate of link fragmented and interleaved frames and bytes.
		extensive

Protocol	Protocol family configured on the logical interface.	**detail extensive** none
MTU	MTU size on the logical interface. If the MTU value is negotiated down to meet the MRRU requirement on the remote side, this value is marked *Adjusted*.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

Table 50: show interfaces (Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Route Table	Routing table in which this address exists. For example, **Route table:0** refers to inet.0.	**detail extensive**
Addresses, Flags	Information about the addresses configured on the logical interface. Possible values are described in the "Addresses Flags" section under *Common Output Fields Description*.	**detail extensive** none
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none
Broadcast	Broadcast address on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**

Sample Output

show interfaces extensive (MLPPP on Link Services IQ)

`user@host>` **show interfaces lsq-0/2/0 extensive**

```
Physical interface: lsq-0/2/0, Enabled, Physical link is Up
  Interface index: 140, SNMP ifIndex: 25, Generation: 23
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2005-06-02 08:54:36 PDT (00:05:45 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              8872424                229080 bps
   Output bytes  :              9856960                234448 bps
   Input  packets:                38202                   117 pps
   Output packets:                39453                   117 pps
  Frame exceptions:
    Oversized frames                 0
    Errored input frames             0
    Input on disabled link/bundle    0
    Output for disabled link/bundle  0
    Queuing drops                    0
```

```
Buffering exceptions:
  Packet data buffer overflow       0
  Fragment data buffer overflow     0
Assembly exceptions:
  Fragment timeout                  0
  Missing sequence number           0
  Out-of-order sequence number      0
  Out-of-range sequence number      0
Hardware errors (sticky):
  Data memory error                 0
  Control memory error              0
Queue counters:       Queued packets  Transmitted packets      Dropped packets
  0 be                             0                    0                    0
  1 ef                             0                    0                    0
  2 af                             0                    0                    0
  3 nc                             0                    0                    0
Logical interface lsq-0/2/0.0 (Index 66) (SNMP ifIndex 26) (Generation 5)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Multilink-PPP
  Bandwidth: 256kbps
  Bundle options:
    MRRU                            1504
    Drop timer period               2000
    Sequence number format          long (24 bits)
    Fragmentation threshold         0
    Links needed to sustain bundle  1
    Multilink classes               0
    Link layer overhead             4.0 %
  Bundle status:
    Remote MRRU                     1500
    Received sequence number        0x0
    Transmit sequence number        0x0
    Packet drops                    0 (0 bytes)
    Fragment drops                  9 (1401 bytes)
    MRRU exceeded                   0
    Fragment timeout                0
    Missing sequence number         0
    Out-of-order sequence number    4
    Out-of-range sequence number    0
    Packet data buffer overflow     0
    Fragment data buffer overflow   0
  Statistics         Frames        fps         Bytes          bps
  Bundle:
    Multilink:
      Input :         79827        239       9593009       232288
```

```
      Output:         77533        234       9811743       238056
    Network:
      Input :         38202        117       8872424       229080
      Output:         39453        117       9856960       234448
  Link:
    ds-1/0/2:1:1.0 <-- up
      Input :          1114         87        180183       113608
      Output:          1577        118        199215       119064
    ds-1/0/2:1:2.0 <-- down
      Input :          1941        152        187948       118680
      Output:          1574        116        199494       118992
  Protocol inet, MTU: 1500 [Adjusted]
    Flags: User-MTU, MTU-Protocol-Adjusted
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 10.74.11/24, Local: 10.74.11.10
  Protocol iso, MTU: 1500 [Adjusted]
    Flags: User-MTU, MTU-Protocol-Adjusted
  Protocol mpls, MTU: 1488 [Adjusted], Maximum labels: 3
    Flags: User-MTU, MTU-Protocol-Adjusted
```

show interfaces extensive (Multiclass MLPPP on Link Services IQ)

`user@host>` **show interfaces extensive lsq-0/2/0**

```
Physical interface: lsq-0/2/0, Enabled, Physical link is Up
  Interface index: 140, SNMP ifIndex: 25, Generation: 23
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2005-06-02 08:54:36 PDT (00:02:25 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :              3474024                223704 bps
   Output bytes  :              4193992                233888 bps
   Input  packets:                15809                   116 pps
   Output packets:                16788                   117 pps
  Frame exceptions:
    Oversized frames                 0
    Errored input frames             0
    Input on disabled link/bundle    0
    Output for disabled link/bundle  0
    Queuing drops                    0
  Buffering exceptions:
    Packet data buffer overflow      0
```

```
  Fragment data buffer overflow     0
Assembly exceptions:
  Fragment timeout                  0
  Missing sequence number           0
  Out-of-order sequence number      0
  Out-of-range sequence number      0
Hardware errors (sticky):
  Data memory error                 0
  Control memory error              0
Queue counters:       Queued packets  Transmitted packets      Dropped packets
  0 be                             0                    0                    0
  1 ef                             0                    0                    0
  2 af                             0                    0                    0
  3 nc                             0                    0                    0
Logical interface lsq-0/2/0.0 (Index 66) (SNMP ifIndex 26) (Generation 5)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Multilink-PPP
  Bandwidth: 256kbps
  Bundle options:
    MRRU                            1504
    Drop timer period               2000
    Sequence number format          long (24 bits)
    Fragmentation threshold         0
    Links needed to sustain bundle  1
    Multilink classes               2
    Link layer overhead             4.0 %
  Multilink class 0 status:
    Received sequence number        0x4c38
    Transmit sequence number        0x4890
    Packet drops                    0 (0 bytes)
    Fragment drops                  2551 (397084 bytes)
    MRRU exceeded                   0
    Fragment timeout                52
    Missing sequence number         0
    Out-of-order sequence number    953
    Out-of-range sequence number    0
    Packet data buffer overflow     0
    Fragment data buffer overflow   0
  Multilink class 1 status:
    Received sequence number        0xffffff
    Transmit sequence number        0x3710
    Packet drops                    0 (0 bytes)
    Fragment drops                  0 (0 bytes)
    MRRU exceeded                   0
    Fragment timeout                0
```

```
  Missing sequence number         0
  Out-of-order sequence number    0
  Out-of-range sequence number    0
  Packet data buffer overflow     0
  Fragment data buffer overflow   0
Statistics         Frames        fps         Bytes          bps
Bundle:
  Fragments:
    Input :         33719        239       4041763       231632
    Output:         32371        234       4096545       237488
  Packets:
    Input :         15809        116       3474024       223704
    Output:         16788        117       4193992       233888
Multilink class 0:
  Fragments:
    Input :         19331          0             0            0
    Output:             0          0             0            0
  Packets:
    Input :          2064          0             0            0
    Output:          1864          0             0            0
Multilink class 1:
  Fragments:
    Input :             0          0             0            0
    Output:         14096          0             0            0
  Packets:
    Input :         14096          0             0            0
    Output:             0          0             0            0
Link:
  ds-1/0/2:1:1.0, Enabled, Physical link is Up
    Input :         20972        151       2030595       118080
    Output:         16184        116       2048468       118488
  ds-1/0/2:1:2.0, Enabled, Physical link is Up
    Input :         12747         88       2011168       113552
    Output:         16187        118       2048077       119000
Protocol inet, MTU: 1500 [Adjusted], Generation: 14, Route table: 0
  Flags: User-MTU, MTU-Protocol-Adjusted
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.1.0/30, Local: 10.0.1.2, Broadcast: Unspecified,
    Generation: 18
```

show interfaces extensive (MLPPP on Link Services IQ Bundle)

`user@host>` **show interfaces lsq-7/1/0.0 extensive**

```
Logical interface lsq-7/1/0.0 (Index 88) (SNMP ifIndex 114) (Generation 188)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-FR
    Last flapped: Never
    Bandwidth: 256kbps
    Bundle links information:
      Active bundle links       2
      Removed bundle links      0
      Disabled bundle links     0
    Bundle options:
      MRRU                                1504
      Drop timer period                   1500
      Inner PPP Protocol field compression enabled
      Sequence number format              short (12 bits)
      Fragmentation threshold             0
      Links needed to sustain bundle      1
      Multilink classes                   0
      Link layer overhead                 4.0 %
    Bundle status:
      Received sequence number        0xb74
      Transmit sequence number        0xb74
      Packet drops                    0 (0 bytes)
      Fragment drops                  0 (0 bytes)
      MRRU exceeded                   0
      Fragment timeout                0
      Missing sequence number         0
      Out-of-order sequence number    0
      Out-of-range sequence number    0
      Packet data buffer overflow     0
      Fragment data buffer overflow   0
    Statistics         Frames        fps         Bytes          bps
    Bundle:
      Multilink:
        Input :        315381          0      42757818            0
        Output:        315381          0      43388580            0
      Network:
        Input :        315381          0      40952064            0
        Output:        315381          0      40952064            0
    Link:
      ds-6/0/0:1:1.0
        Up time: Up since boot
        Input :         63794          0      25146728            0
        Output:         63778          0      25273164            0
      ds-6/0/0:1:2.0
        Up time: Up since boot
```

```
        Input :        251587          0      17611090           0
        Output:        251603          0      18115416           0
    Multilink detail statistics:
    Bundle:
      Fragments:
        Input :             0          0             0           0
        Output:             0          0             0           0
      Non-fragments:
        Input :        293748          0      19387368           0
        Output:        293748          0      20562360           0
      LFI:
        Input :         21633          0      22152192           0
        Output:         21633          0      22325256           0
    Protocol inet, MTU: 1500, Generation: 204, Route table: 0
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.0.1.0/30, Local: 10.0.1.2, Broadcast:
Unspecified, Generation: 214
```

show interfaces extensive (MFR on Link Services IQ Bundle)

`user@host>` **show interfaces lsq-1/0/0:0 extensive**

```
Physical interface: lsq-1/0/0:0, Enabled, Physical link is Up
  Interface index: 179, SNMP ifIndex: 746, Generation: 182
  Link-level type: Multilink-FR-UNI-NNI, MTU: 1508
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Internal: 0x4000
  Last flapped   : 2010-11-15 01:11:00 PST (00:31:58 ago)
  Statistics last cleared: Never
  Hold-times     : Up 0 ms, Down 0 ms
  Multilink Frame Relay UNI NNI bundle options:
    Device type                       DCE
    MRRU                              1508
    Bandwidth                         1536kbps
    Fragmentation threshold           0
    Red differential delay limit      120
    Yellow differential delay limit   72
    Red differential delay action     Remove link
    Reassembly drop timer             65535
    Links needed to sustain bundle    1
    Link layer overhead               4.0 %
    LIP Hello timer                   10
        Acknowledgement timer         4
```

```
      Acknowledgement retries       2
  Bundle class                      A
  LMI type                          Consortium
    T391 LIV polling timer          10
    T392 polling verification timer 15
    N391 full status polling count  6
    N392 error threshold            3
    N393 monitored event count      4
Consortium LMI settings: n392dce 3, n393dce 4, t392dce 15 seconds
LMI statistics:
  Input : 188 (last seen 00:00:01 ago)
  Output: 189 (last sent 00:00:01 ago)
DTE statistics:
  Enquiries sent                    : 0
  Full enquiries sent               : 0
  Enquiry responses received        : 0
  Full enquiry responses received   : 0
DCE statistics:
  Enquiries received                : 157
  Full enquiries received           : 31
  Enquiry responses sent            : 158
  Full enquiry responses sent       : 31
Common statistics:
  Unknown messages received         : 0
  Asynchronous updates received     : 0
  Out-of-sequence packets received  : 0
  Keepalive responses timedout      : 0
Traffic statistics:
 Input  bytes  :                    0                    0 bps
 Output bytes  :                    0                    0 bps
 Input  packets:                    0                    0 pps
 Output packets:                    0                    0 pps
 IPv6 transit statistics:
  Input  bytes  :                   0
  Output bytes  :                   0
  Input  packets:                   0
  Output packets:                   0
Multilink Frame Relay UNI NNI bundle errors:
  Packet drops                    0 (0 bytes)
  Fragment drops                  0 (0 bytes)
  MRRU exceeded                   0
  Exception events                0
Multilink Frame Relay UNI NNI bundle statistics:
                   Frames        fps         Bytes          bps
```

```
  Multilink:
    Input :             0          0             0            0
    Output:             0          0             0            0
  Network:
    Input :             0          0             0            0
    Output:             0          0             0            0
Multilink Frame Relay UNI NNI bundle links information:
    Active bundle links       1
    Removed bundle links      0
    Disabled bundle links     0
Multilink Frame Relay UNI NNI active bundle links statistics:
                   Frames        fps         Bytes          bps
  t1-7/0/0:1:3.0
    Up time: 00:31:24
    Input :             0          0             0            0
    Output:             0          0             0            0
    Current differential delay       0.0 ms
    Recent high differential delay   0.0 ms
    Times over red diff delay        0
    Times over yellow diff delay     0
    LIP:add_lnk lnk_ack lnk_rej    hello hel_ack lnk_rem rem_ack
    Rcv:      2       2       0        0     189       0       0
    Xmt:      2       1       0      189       0       0       0

Logical interface lsq-1/0/0:2.0 (Index 77) (SNMP ifIndex 751) (Generation 142)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Multilink-FR-UNI-NNI
  Last flapped: 2010-11-15 01:11:40 PST (00:31:18 ago)
  Bundle status:
    Received sequence number        0xfff
    Transmit sequence number        0x0
    Packet drops                    0 (0 bytes)
    Fragment drops                  0 (0 bytes)
    MRRU exceeded                   0
    Fragment timeout                0
    Missing sequence number         0
    Out-of-order sequence number    0
    Out-of-range sequence number    0
    Packet data buffer overflow     0
    Fragment data buffer overflow   0
  Statistics         Frames        fps         Bytes          bps
  Bundle:
    Multilink:
      Input :             0          0             0            0
```

```
        Output:             0          0             0           0
      Network:
        Input :             0          0             0           0
        Output:             0          0             0           0
    Link:
      t1-7/0/0:1:3.0
        Up time: 00:31:24
        Input :             0          0             0           0
        Output:             0          0             0           0
    Multilink detail statistics:
    Bundle:
      Fragments:
        Input :             0          0             0           0
        Output:             0          0             0           0
      Non-fragments:
        Input :             0          0             0           0
        Output:             0          0             0           0
    Protocol inet, MTU: 1500, Generation: 153, Route table: 0
      Flags: Sendbcast-pkt-to-re
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 10.0.1.8/30, Local: 10.0.1.9, Broadcast: Unspecified,
Generation: 154
    DLCI 12
      Flags: Active
      Total down time: 00:00:32 sec, Last down: 00:31:50 ago
      Traffic statistics:
       Input  bytes  :                   0
       Output bytes  :                   0
       Input  packets:                   0
       Output packets:                   0
  DLCI statistics:
    Active DLCI  :1  Inactive DLCI  :0
```

show interfaces extensive (Multiclass MLPPP on Link Services IQ)

`user@host>` **show interfaces extensive lsq-0/2/0**

```
Physical interface: lsq-0/2/0, Enabled, Physical link is Up
  Interface index: 140, SNMP ifIndex: 25, Generation: 23
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Last flapped   : 2005-06-02 08:54:36 PDT (00:02:25 ago)
  Statistics last cleared: Never
```

```
Traffic statistics:
 Input  bytes  :              3474024                223704 bps
 Output bytes  :              4193992                233888 bps
 Input  packets:                15809                   116 pps
 Output packets:                16788                   117 pps
Frame exceptions:
  Oversized frames                  0
  Errored input frames              0
  Input on disabled link/bundle     0
  Output for disabled link/bundle   0
  Queuing drops                     0
Buffering exceptions:
  Packet data buffer overflow       0
  Fragment data buffer overflow     0
Assembly exceptions:
  Fragment timeout                  0
  Missing sequence number           0
  Out-of-order sequence number      0
  Out-of-range sequence number      0
Hardware errors (sticky):
  Data memory error                 0
  Control memory error              0
Queue counters:       Queued packets  Transmitted packets      Dropped packets
  0 be                             0                    0                    0
  1 ef                             0                    0                    0
  2 af                             0                    0                    0
  3 nc                             0                    0                    0
Logical interface lsq-0/2/0.0 (Index 66) (SNMP ifIndex 26) (Generation 5)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Multilink-PPP
  Bandwidth: 256kbps
  Bundle options:
    MRRU                            1504
    Drop timer period               2000
    Sequence number format          long (24 bits)
    Fragmentation threshold         0
    Links needed to sustain bundle  1
    Multilink classes               2
    Link layer overhead             4.0 %
  Multilink class 0 status:
    Received sequence number        0x4c38
    Transmit sequence number        0x4890
    Packet drops                    0 (0 bytes)
    Fragment drops                  2551 (397084 bytes)
    MRRU exceeded                   0
```

```
  Fragment timeout                52
  Missing sequence number         0
  Out-of-order sequence number    953
  Out-of-range sequence number    0
  Packet data buffer overflow     0
  Fragment data buffer overflow   0
Multilink class 1 status:
  Received sequence number        0xffffff
  Transmit sequence number        0x3710
  Packet drops                    0 (0 bytes)
  Fragment drops                  0 (0 bytes)
  MRRU exceeded                   0
  Fragment timeout                0
  Missing sequence number         0
  Out-of-order sequence number    0
  Out-of-range sequence number    0
  Packet data buffer overflow     0
  Fragment data buffer overflow   0
Statistics         Frames        fps         Bytes          bps
Bundle:
  Fragments:
    Input :         33719        239       4041763       231632
    Output:         32371        234       4096545       237488
  Packets:
    Input :         15809        116       3474024       223704
    Output:         16788        117       4193992       233888
Multilink class 0:
  Fragments:
    Input :         19331          0             0            0
    Output:             0          0             0            0
  Packets:
    Input :          2064          0             0            0
    Output:          1864          0             0            0
Multilink class 1:
  Fragments:
    Input :             0          0             0            0
    Output:         14096          0             0            0
  Packets:
    Input :         14096          0             0            0
    Output:             0          0             0            0
Link:
  ds-1/0/2:1:1.0, Enabled, Physical link is Up
    Input :         20972        151       2030595       118080
    Output:         16184        116       2048468       118488
```

```
  ds-1/0/2:1:2.0, Enabled, Physical link is Up
    Input :         12747         88       2011168       113552
    Output:         16187        118       2048077       119000
Protocol inet, MTU: 1500 [Adjusted], Generation: 14, Route table: 0
  Flags: User-MTU, MTU-Protocol-Adjusted
  Addresses, Flags: Is-Preferred Is-Primary
    Destination: 10.0.1.0/30, Local: 10.0.1.2, Broadcast: Unspecified,
    Generation: 18
```

show interfaces (Redundant Adaptive Services)

Syntax

```
show interfaces rspnumber
<brief | detail | extensive | terse>
<descriptions>
<media>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M Series and T Series routers only) Display status information about the specified redundant adaptive services configuration.

Options

rsp*number*—Display standard status information about the specified redundant adaptive services configuration.

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

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces extensive (Redundant Adaptive Services) on page 1759

Output Fields

See the output field table for the **show interfaces (Adaptive Services)** command.

Sample Output

show interfaces extensive (Redundant Adaptive Services)

user@host> **show interfaces rsp0 extensive**

```
Physical interface: rsp0, Enabled, Physical link is Up
  Interface index: 150, SNMP ifIndex: 40, Generation: 44
  Type: Adaptive-Services, Link-level type: Adaptive-Services, MTU: 9192,
  Clocking: Unspecified, Speed: 800mbps
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps Redundancy-Device 16384
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped   : 2005-03-11 18:36:37 UTC (00:00:08 ago)
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                   0                   0 bps
   Output bytes  :                   0                   0 bps
   Input  packets:                   0                   0 pps
   Output packets:                   0                   0 pps
  Input errors:
    Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
    Policed discards: 0, Resource errors: 0
  Output errors:
    Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
    Resource errors: 0

  Logical interface rsp0.0 (Index 68) (SNMP ifIndex 42) (Generation 30)
    Flags: Point-To-Point SNMP-Traps Encapsulation: Adaptive-Services
    Traffic statistics:
     Input  bytes  :                   0
     Output bytes  :                   0
     Input  packets:                   0
     Output packets:                   0
    Local statistics:
     Input  bytes  :                   0
     Output bytes  :                   0
     Input  packets:                   0
     Output packets:                   0
    Transit statistics:
```

```
  Input  bytes  :                    0                    0 bps
  Output bytes  :                    0                    0 bps
  Input  packets:                    0                    0 pps
  Output packets:                    0                    0 pps
Protocol inet, MTU: 9192, Generation: 37, Route table: 0
   Flags: Receive-options, Receive-TTL-Exceeded
```

show interfaces (Redundant Link Services IQ)

Syntax

```
show interfaces rlsq<number>
<brief | detail | extensive | terse>
<descriptions>
<media>
<queue>
<routing>
<snmp-index snmp-index>
<statistics>
```

Release Information

Command introduced in Junos OS Release 7.6.

Description

(M Series and T Series routers only) Display status information about the specified redundant link services intelligent queuing (IQ) configuration.

Options

rlsq*number*—Redundant link services IQ interface name. The logical interface number range of values is **0** through **127**.

none—Display standard status information about the specified redundant link services IQ configuration.

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

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

queue—(Optional) Display queue information about network interfaces.

routing—(Optional) Display routing information about network interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level

view

List of Sample Output

show interfaces (Redundant Link Services IQ) on page 1776
show interfaces brief (Redundant Link Services IQ) on page 1777
show interfaces detail (Redundant Link Services IQ) on page 1777

show interfaces extensive (Redundant Link Services IQ) on page 1779

Output Fields

Table 51 on page 1762 lists the output fields for the **show interfaces** (redundant link services IQ) command. Output fields are listed in the approximate order in which they appear.

Table 51: show interfaces (Redundant Link Services IQ) Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the "Enabled Field" section under *Common Output Fields Description*.	All levels
Interface index	Physical interface's index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	SNMP index number for the physical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
Link-level type	Encapsulation being used on the physical interface: **Multilink-Frame-Relay-UNI-NNI** (default), **LinkService**, **Frame-relay**, **Frame-relay-ccc**, or **Frame-relay-tcc**.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under *Common Output Fields Description*.	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under *Common Output Fields Description*.	All levels
Last flapped	Date, time, and how long ago the interface went from down to up. The format is **Last flapped: *year-month-day hour:minute:second timezone* (*hour:minute:second* ago)** . For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.	**detail extensive** none
Input rate	(Redundant LSQ) Rate of bits and packets received on the interface.	None specified
Output rate	(Redundant LSQ) Rate of bits and packets transmitted on the interface.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	**detail extensive**

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Traffic statistics	Number and rate of bytes and packets received and transmitted on the physical interface. All references to traffic direction (input or output) are defined with respect to the router. Input fragments received by the router are assembled into input packets; output packets are segmented into output fragments for transmission out of the router.	**detail extensive**
Frame exceptions	Information about framing exceptions. Includes events recorded under **Exception Events** for each logical interface. • **Oversized frames**—Number of frames received that exceed maximum frame length. Maximum length is 4500 Kb (kilobits). • **Errored input frames**—Number of input frame errors. • **Input on disabled link/bundle**—Number of frames received on disabled links. These frames can result either from an inconsistent configuration, or from a bundle or link being brought up or down with traffic actively flowing through it. • **Output for disabled link/bundle**—Number of frames sent for a disabled or unavailable link. These frames can result either from an inconsistent configuration, or from a bundle being brought up or down while traffic is flowing through it. • **Queuing drops**—Total number of packets dropped before traffic enters the link services IQ interface. Indicates that the interface is becoming oversubscribed.	**extensive**
Buffering exceptions	Information about buffering exceptions. Includes events recorded under **Exception Events** for each logical interface: • **Packet data buffer overflow**—Packet buffer memory is full. This overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity. Check the logical interface exception event counters to determine which bundle is responsible.	**extensive**

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Assembly exceptions		**extensive**

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	(Multilink Frame Relay end-to-end only) Information about assembly exceptions. Includes events recorded under **Exception Events** for each logical interface. An assembly exception does not necessarily indicate an operational problem with the physical link services IQ interface itself. If multilink-encapsulated traffic is dropped or reordered after a sequence number has been assigned, the interface records one or more exception events. The physical interface can drop multilink-encapsulated fragments itself as a result. Any multilink packets or fragments dropped by the interface itself result in packet or fragment drop counts on individual logical interfaces. If the logical interface drop counts are zero, but exception events are seen, the most likely cause is a problem with the individual link interfaces. Even if the logical interface fragment drop counts are nonzero, excess differential delay or traffic losses on individual interfaces can be the root cause. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. These events do not necessarily indicate any problem with the operation of the physical link services IQ interface itself, but can occur when one or more individual links drop traffic. Check the logical interface exception event counters to determine which bundle is responsible. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. These events do not necessarily indicate any problem with the operation of the physical link services IQ interface itself, but can occur when one or more individual links drop traffic. Check the logical interface exception event counters to determine which bundle is responsible. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers within a single link. This event indicates that an individual link within a bundle reordered traffic, making the link services IQ interface unable to correctly process the resulting stream. Check the logical interface exception event counters to determine which bundle is responsible. • **Out-of-range sequence number**—Received a frame with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these	

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	events can occur when the far end of a bundle is taken down or brought up. Check the logical interface exception event counters to determine which bundle is responsible.	
Hardware errors (sticky)	(Multilink Frame Relay end-to-end only) Information about hardware errors: • **Data memory error**—A memory error was detected on the interface DRAM. Indicates possible hardware failure. Contact Juniper Networks technical support. • **Control memory error**—A memory error was detected on the interface DRAM. Indicates possible hardware failure. Contact Juniper Networks technical support.	**extensive**
Egress queues	Total number of egress queues supported on the specified interface.	**detail extensive** none
Queue counters	Queue number and its associated user-configured forwarding class name. • **Queued packets**—Number of queued packets. • **Transmitted packets**—Number of transmitted packets. • **Dropped packets**—Number of packets dropped by the ASIC's RED mechanism.	**detail extensive** none
Logical Interface		
Logical interface	Name of the logical interface	All levels
Index	Logical interface index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	Logical interface SNMP interface index number.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support	**detail extensive**
Flags	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under *Common Output Fields Description*.	All levels
Encapsulation	Encapsulation being used: PPP or Multilink PPP.	All levels
Bandwidth	Speed at which the interface is running.	All levels

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle options	(Multilink Frame Relay end-to-end interfaces only) • **MRRU**—Configured size of the maximum received reconstructed unit (MRRU): **1500** through **4500** bytes. The default is **1504** bytes. • **Drop timer period**—Drop timeout value to provide a recovery mechanism if individual links in link services bundle drop one or more packets: **0** though **2000** milliseconds. Values under 5 ms are not recommended. The default setting is **0**, which disables the timer. • **Sequence number format**—Short sequence number header format (MLPPP only). • **Fragmentation threshold**—Configured fragmentation threshold: **64** through **16,320** bytes, in integer multiples of **64** bytes. The default setting is **0**, which disables fragmentation. • **Links needed to sustain bundle**—Minimum number of links to sustain the bundle: **1** through **8**. • **Multilink classes**—Number of multilink classes negotiated. • **Link layer overhead**—Percentage of bundle bandwidth to be set aside for link-layer overhead.	**detail extensive** none

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle status (MLPPP) or **Multilink class status** (MC-MLPPP)		**detail extensive** none

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	Information about bundle status: • **Remote MRRU**—MRRU value received from remote peer. If negotiation has not been initiated, the default value is displayed. • **Received sequence number**—Sequence number for received packets. • **Transmitted sequence number**—Sequence number for transmitted packets. • **Packet drops**—Number and byte count of output packets that were dropped, rather than being encapsulated and sent out of the router as fragments. The packet drop counter is incremented if there is a temporary shortage of packet memory on the AS PIC, which causes packet fragmentation to fail. • **Fragment drops**—Number and byte count of input fragments that were dropped, rather than being reassembled and handled by the router as packets. This counter also includes fragments that have been received successfully but had to be dropped because not all fragments that constituted a packet had been received. The fragment drop counter is incremented when a fragment received on constituent links is dropped. Drop fragments can be triggered by sequence ordering errors, duplicate fragments, timed-out fragments, and bad multilink headers. • **MRRU exceeded**—Number of reassembled packets exceeding the MRRU. This counter is not implemented in this release. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers within a single link. This event indicates that an individual link within a bundle reordered traffic, making the multilink interface unable to correctly process the resulting stream. • **Out-of-range sequence number**—Received a frame with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these events can occur when the far end of a bundle is taken down or brought up. • **Packet data buffer overflow**—Packet buffer memory is full. This	

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity.	

Statistics	Information about fragments and packets received and sent by the router. All references to traffic direction (input or output) are defined with respect to the router. Input fragments received by the router are assembled into input packets; output packets are segmented into output fragments for transmission out of the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	• **Bundle**—Information for each active bundle link.
	  ◦ **Fragments: Input and Output**—Total number and rate of fragments received and transmitted.
	  ◦ **Packets: Input and Output**—Total number and rate of packets received and transmitted.
	  ◦ **Multilink class**—(MC-MLPPP only) Information about multiclass links used in the multilink operation.
	• **Link**—Information about links used in the multilink operation.
	  ◦ **Link name**—Interface name of the link services IQ channel and state information (physical link **up** or **down**).
	  ◦ **Input and Output**—Total number and rate of fragments and packets received and transmitted.
		detail extensive

NCP state	(PPP) Network Control Protocol state. • **Conf-ack-received**—Acknowledgement was received. • **Conf-ack-sent**—Acknowledgement was sent. • **Conf-req-sent**—Request was sent. • **Down**—NCP negotiation is incomplete (not yet completed or has failed). • **Not-configured**—NCP is not configured on the interface. • **Opened**—NCP negotiation is successful.	**detail extensive** none
Protocol	Protocol family configured on the logical interface.	**detail extensive** none

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
MTU	MTU size on the logical interface. If the MTU value is negotiated down to meet the MRRU requirement on the remote side, this value is marked **Adjusted**.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Route Table	Routing table in which this address exists. For example, **Route table:0** refers to inet.0.	**detail extensive**
Flags	Information about the protocol family flags. Possible values are described in the "Family Flags" section under *Common Output Fields Description*.	**detail extensive** none
Addresses, Flags	Information about the addresses configured on the logical interface. Possible values are described in the "Addresses Flags" section under *Common Output Fields Description*.	**detail extensive** none
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none
Broadcast	Broadcast address on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
MLPPP Bundle Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	**detail extensive** none
SNMP ifIndex	Logical interface SNMP interface index number.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under *Common Output Fields Description*.	All levels
SNMP-Traps	SNMP trap notifications are enabled.	All levels
Encapsulation	Encapsulation being used: PPP, Multilink PPP or Multilink-FR.	All levels

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Last flapped	Date, time, and how long ago the interface went from down to up. The format is **Last flapped: *year-month-day hour:minute:second timezone* (*hour:minute:second* ago)** . For example, **Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago)**.	**detail extensive** none
Bandwidth	Speed at which the interface is running.	All levels
Bundle links linformation	Information about the bundled links. • **Active bundle links**—Number of active links. • **Removed bundle links**—Information about links used in the multilink operation. • **Disabled bundle links**—Number of disabled links.	**detail extensive** none
Bundle options	(Multilink Frame Relay end-to-end interfaces only) • **MRRU**—Configured size of the maximum received reconstructed unit (MRRU): **1500** through **4500** bytes. The default is **1504** bytes. • **Drop timer period**—Drop timeout value to provide a recovery mechanism if individual links in link services bundle drop one or more packets: **0** though **2000** milliseconds. Values under 5 ms are not recommended. The default setting is **0**, which disables the timer. • **Inner PPP Protocol field compression**—Inner PPP protocol compression is enabled or disabled. • **Sequence number format**—Short sequence number header format (MLPPP only). • **Fragmentation threshold**—Configured fragmentation threshold: **64** through **16,320** bytes, in integer multiples of **64** bytes. The default setting is **0**, which disables fragmentation. • **Links needed to sustain bundle**—Minimum number of links to sustain the bundle: **1** through **8**. • **Multilink classes**—Number of multilink classes negotiated. • **Link layer overhead**—Percentage of bundle bandwidth to be set aside for link-layer overhead.	**detail extensive** none

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Bundle status (MLPPP)		**detail extensive** none

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	Information about bundle status: • **Received sequence number**—Sequence number for received packets. • **Transmit sequence number**—Sequence number for transmitted packets. • **Packet drops**—Number and byte count of output packets that were dropped, rather than being encapsulated and sent out of the router as fragments. The packet drop counter is incremented if there is a temporary shortage of packet memory on the AS PIC, which causes packet fragmentation to fail. • **Fragment drops**—Number and byte count of input fragments that were dropped, rather than being reassembled and handled by the router as packets. This counter also includes fragments that have been received successfully but had to be dropped because not all fragments that constituted a packet had been received. The fragment drop counter is incremented when a fragment received on constituent links is dropped. Drop fragments can be triggered by sequence ordering errors, duplicate fragments, timed-out fragments, and bad multilink headers. • **MRRU exceeded**—Number of reassembled packets exceeding the MRRU. This counter is not implemented in this release. • **Fragment timeout**—The drop timer expired while a fragment sequence number was outstanding. Occurs only if the drop timer is enabled. This timeout can occur if the differential delay across the links in a bundle exceeds the drop-timer setting, or if a multilink packet is lost in transit while the drop timer is enabled. • **Missing sequence number**—A gap was detected in the sequence numbers of fragments on a bundle. • **Out-of-order sequence number**—Two frames with out-of-order sequence numbers occurred within a single link. This event indicates that an individual link within a bundle reordered traffic, making the multilink interface unable to correctly process the resulting stream. • **Out-of-range sequence number**—A frame was received with an out-of-range sequence number. These events can occur when a large amount of multilink-encapsulated traffic is lost or the multilink peer is reset, so that a large jump in sequence numbers results. A small number of these events can occur when the far end of a bundle is taken down or brought up. • **Packet data buffer overflow**—Packet buffer memory is full. This overflow can occur when the aggregate data rate exceeds the physical link services IQ interface capacity. • **Fragment data buffer overflow**—Fragment buffer memory is full. This	

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
	overflow can occur when excessive differential delay is experienced across the links within a single bundle, or when the aggregate data rate exceeds the physical link services IQ capacity.	

Statistics	Information about frames, bytes, and bits per second received and sent by the router. All references to traffic direction (input or output) are defined with respect to the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	• **Bundle**—Information for each active bundle link.
	  ◦ **Multilink: Input and Ouput**—Total number and rate of multilink frames, bytes, and bits per second received and transmitted.
	  ◦ **Network: Input and Output**—Total number of multilink frames, bytes, and bits per second received and transmitted.
	• **Link**—Information about links used in the multilink operation.
	  ◦ **Link name** is the interface name of the link services IQ channel and state information (physical link **up** or **down**) and up time.
	  ◦ **Input and Output**—Total number and rate of frames, bytes, and bits per second received and transmitted.
		extensive

Multilink detail statistics	Frames, bytes, and bits per second received and sent by the bundle. All references to traffic direction (input or output) are defined with respect to the router. Each field has columns that indicate the number of frames received and transmitted, frames per second (fps), the number of bytes received and transmitted, and bits per second (bps).
	• **Bundle**—Information for the bundle link.
	  ◦ **Fragments: Input and Output**—Total number and rate of multilink fragments received and transmitted.
	  ◦ **Non-fragments: Input and Output**—Total number and rate of nonfragmented multilink frames received and transmitted.
	  ◦ **LFI: Input and Output**—Total number and rate of link fragmented and interleaved frames and bytes.
		extensive

Protocol	Protocol family configured on the logical interface.	**detail extensive** none
MTU	MTU size on the logical interface. If the MTU value is negotiated down to meet the MRRU requirement on the remote side, this value is marked **Adjusted**.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

Table 51: show interfaces (Redundant Link Services IQ) Output Fields *(continued)*

Field Name	Field Description	Level of Output
Route Table	Routing table in which this address exists. For example, **Route table:0** refers to inet.0.	**detail extensive**
Addresses, Flags	Information about the addresses configured on the logical interface. Possible values are described in the "Addresses Flags" section under *Common Output Fields Description*.	**detail extensive** none
Destination	IP address of the remote side of the connection.	**detail extensive** none
Local	IP address of the logical interface.	**detail extensive** none
Broadcast	Broadcast address on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support.	**detail extensive**

Sample Output

show interfaces (Redundant Link Services IQ)

`user@host>` **show interfaces rlsq0**

```
Physical interface: rlsq0, Enabled, Physical link is Up
  Interface index: 196, SNMP ifIndex: 27
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Last flapped   : Never
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

  Logical interface rlsq0.0 (Index 72) (SNMP ifIndex 88)
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
    Bandwidth: 0
    Statistics        Frames        fps         Bytes          bps
    Bundle:
      Fragments:
        Input :            3          0           255            0
        Output:            3          0           264            0
      Packets:
```

```
        Input :             3          0           252            0
        Output:             0          0             0            0
    Link:
      t1-1/3/0:1.0
        Input :             3          0           255            0
        Output:             0          0             0            0
      t1-1/3/0:2.0
        Input :             0          0             0            0
        Output:             3          0           264            0
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured,
  mpls: Not-configured
    Protocol inet, MTU: 1500
      Flags: None
      Addresses, Flags: Is-Preferred Is-Primary
        Destination: 192.0.2.0/30, Local: 192.0.2.1
```

show interfaces brief (Redundant Link Services IQ)

`user@host>` **show interfaces rlsq0 brief**

```
Physical interface: rlsq0, Enabled, Physical link is Up
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000

  Logical interface rlsq0.0
    Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
    inet  192.0.2.1/30
```

show interfaces detail (Redundant Link Services IQ)

`user@host>` **show interfaces rlsq0 detail**

```
Physical interface: rlsq0, Enabled, Physical link is Up
  Interface index: 196, SNMP ifIndex: 27, Generation: 144
  Link-level type: LinkService, MTU: 1504
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Last flapped   : Never
  Statistics last cleared: Never
  Traffic statistics:
   Input  bytes  :                 252                   0 bps
   Output bytes  :                 276                   0 bps
```

```
 Input  packets:                    3                    0 pps
 Output packets:                    3                    0 pps
Frame exceptions:
  Oversized frames                  0
  Errored input frames              0
  Input on disabled link/bundle     0
  Output for disabled link/bundle   0
  Queuing drops                     0
Buffering exceptions:
  Packet data buffer overflow       0
  Fragment data buffer overflow     0
Assembly exceptions:
  Fragment timeout                  0
  Missing sequence number           0
  Out-of-order sequence number      0
  Out-of-range sequence number      0
Hardware errors (sticky):
  Data memory error                 0
  Control memory error              0
Egress queues: 8 supported, 4 in use
Queue counters:       Queued packets  Transmitted packets      Dropped packets
  0 be                             0                    0                    0
  1 expedited-fo                   0                    0                    0
  2 assured-forw                   0                    0                    0
  3 network-cont                   0                    0                    0

Logical interface rlsq0.0 (Index 72) (SNMP ifIndex 88) (Generation 31)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: Multilink-PPP
  Bandwidth: 0
  Bundle options:
    MRRU                            1504
    Remote MRRU                     N/A
    Drop timer period               2000
    Sequence number format          long (24 bits)
    Fragmentation threshold         0
    Links needed to sustain bundle  1
    Multilink classes               0
    Link layer overhead             4.0 %
  Bundle status:
    Received sequence number        0xffffff
    Transmit sequence number        0x0
    Packet drops                    0 (0 bytes)
    Fragment drops                  0 (0 bytes)
    MRRU exceeded                   0
```

```
    Fragment timeout                0
    Missing sequence number         0
    Out-of-order sequence number    0
    Out-of-range sequence number    0
    Packet data buffer overflow     0
    Fragment data buffer overflow   0
  Statistics         Frames        fps         Bytes          bps
  Bundle:
    Fragments:
      Input :             3          0           255            0
      Output:             3          0           264            0
    Packets:
      Input :             3          0           252            0
      Output:             0          0             0            0
  Link:
    t1-1/3/0:1.0
      Input :             3          0           255            0
      Output:             0          0             0            0
    t1-1/3/0:2.0
      Input :             0          0             0            0
      Output:             3          0           264            0
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
  Protocol inet, MTU: 1500, Generation: 43, Route table: 0
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 192.0.2.0/30, Local: 2.2.2.1, Broadcast: Unspecified,
      Generation: 45
```

show interfaces extensive (Redundant Link Services IQ)

The output for the **show interfaces rlsq extensive** command is identical to that for the **show interfaces rlsq detail** command. For sample output, see show interfaces detail (Redundant Link Services IQ) on page 1777.

show interfaces load-balancing (Aggregated Multiservices)

Syntax

```
show interfaces load-balancing
<detail>
<interface-name>
```

Release Information

Command introduced in Junos OS Release 11.4.
interface-name option added in Junos OS Release 16.1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display information about the aggregated multiservices interface (AMS) as well as its individual member interfaces and the status of the replication state.

Options

none—Display standard information about status of all AMS interfaces.

detail—(Optional) Display detailed status of all AMS interfaces.

interface-name—(Optional) Name of the aggregated multiservices interface (**ams**). If this is omitted, then the information for all the aggregated multiservices interfaces, including those used in control plane redundancy and high availability (HA) for service applications, is displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces | **994**

Understanding Aggregated Multiservices Interfaces for Next Gen Services

Example: Configuring an Aggregated Multiservices Interface (AMS) | **1009**

List of Sample Output

show interfaces load-balancing on page 1782
show interfaces load-balancing detail on page 1783
show interfaces load-balancing detail (Specific Interface) on page 1783

Output Fields

Table 52 on page 1781 lists the output fields for the **show interfaces load-balancing** (aggregated multiservices interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 52: Aggregated Multiservices show interfaces load-balancing Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices (AMS) interface.	**detail** none
State	Status of AMS interfaces: • **Coming Up**—Interface is becoming operational. • **Members Seen**—Member interfaces (mams) are available. • **Up**—Interface is configured and operational. • **Wait for Members**—Member interfaces (mams) are not available. • **Wait Timer**—Interface is waiting for member interfaces (mams) to come online.	**detail** none
Last change	Time (in *hh:mm:ss* [*hours:minutes:seconds*] format) when the state last changed.	**detail** none
Members	Number of member interfaces (mams-).	none specified
Member count	Number of member PICs (mams) that are part of the aggregated interface.	**detail** none
HA Model	High availability (HA) model supported on the interface. • **Many-to-One**—The preferred backup Multiservices PIC, in hot standby mode, backs up one or more (N) active Multiservices PICs. • **One-to-One**—–The preferred backup Multiservices PIC, in hot standby mode, backs up only one active Multiservices PIC. NOTE: **One-to-One** is not supported on MX-SPC3 cards.	**detail** none

Table 52: Aggregated Multiservices show interfaces load-balancing Output Fields *(continued)*

Field Name	Field Description	Level of Output

Members	Information about the member interfaces:
	• **Interface**—Name of the member interface.
	• **Weight**—Not applicable for the current release.
	• **State**—State of the member interface (mams-).
	  ◦ **Active**—Member is an active member.
	  ◦ **Backup**—Member is a backup.
	  ◦ **Discard**—Member has not yet rejoined the ams interface after failure.
	  ◦ **Down**—Member has not yet powered on.
	  ◦ **Inactive**—Member has failed to rejoin the ams interface within the configured **rejoin-timeout**.
	  ◦ **Invalid**—Multiservices PIC corresponding to the member interface has been configured but is not physically present in the chassis.
		detail

Sync-state	Synchronization (sync) status of the control plane redundancy. The sync state is displayed only when the ams interface is **Up**.
	• **Interface**—Name of the member interface.
	• **Status**—Synchronization status of the member interfaces.
	  ◦ **In progress**—The active member is currently synchronizing its state information with the backup member.
	  ◦ **In sync**—The active member has finished synchronizing its state information with the backup and the backup is ready to take over if the active member fails.
	  ◦ **NA (Not applicable)**—The backup member is not yet ready to synchronize with the active (primary) member. This condition may occur if the backup is still powered off or still booting.
	  ◦ **Unknown**—The daemons are still initializing and the state information is unavailable.
		detail

Sample Output

show interfaces load-balancing

```
user@host> show interfaces load-balancing
```

```
Interface  State       Last change  Members  HA Model
ams0       Up          00:10:02     4        Many-to-One
```

show interfaces load-balancing detail

`user@host>` **show interfaces load-balancing detail**

```
Load-balancing interfaces detail
Interface        : ams0
  State          : Up
  Last change    : 00:10:23
  Member count   : 4
  HA Model       : Many-to-One
  Members        :
      Interface    Weight   State
      mams-4/0/0   10       Active
      mams-4/1/0   10       Active
      mams-5/0/0   10       Active
      mams-5/1/0   10       Backup
  Sync-state     :
      Interface    Status
      mams-4/0/0   Unknown
      mams-4/1/0   Unknown
      mams-5/0/0   Unknown
```

show interfaces load-balancing detail (Specific Interface)

`user@host>` **show interfaces load-balancing ams0 detail**

```
Load-balancing interfaces detail
Interface        : ams0
  State          : Up
  Last change    : 00:11:28
  Member count   : 4
  HA Model       : Many-to-One
  Members        :
      Interface    Weight   State
      mams-4/0/0   10       Active
      mams-4/1/0   10       Active
      mams-5/0/0   10       Active
      mams-5/1/0   10       Backup
```

```
Sync-state     :
    Interface    Status
    mams-4/0/0   Unknown
    mams-4/1/0   Unknown
    mams-5/0/0   Unknown
```

show interfaces redundancy

Syntax

```
show interfaces redundancy
<brief | detail>
```

Release Information

Command introduced before Junos OS Release 7.4.
detail option added in Junos OS Release 10.0.

Description

(M Series, T Series, and MX Series routers only) Display general information about redundancy for aggregated multiservices (AMS) interfaces configured for warm standby, adaptive services and link services intelligent queuing (IQ) interfaces, aggregated Ethernet interfaces redundancy, and LNS aggregated inline service interfaces.

> **NOTE:** When you run the **show interfaces redundancy** command on an MX80 router, it displays the error message, **error:the redundancy-interface-process subsystem is not running**. This is because an MX80 router does not have a redundant FPC and does not support link protection.

Options

brief | detail—(Optional) Display the specified level of output.

Required Privilege Level

view

List of Sample Output

show interfaces redundancy on page 1786
show interfaces redundancy (Aggregated Ethernet) on page 1787
show interfaces redundancy (Aggregated Inline Service Interface) on page 1787
show interfaces redundancy detail on page 1787

Output Fields

Table 53 on page 1786 lists the output fields for the **show interfaces redundancy** command. Output fields are listed in the approximate order in which they appear.

Table 53: show interfaces redundancy Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the AMS interface, redundant adaptive services, link services IQ interfaces, aggregated Ethernet interfaces, or LNS aggregated inline service interfaces.	All levels
State	State of the redundant interface: **Not present**, **On primary**, **On secondary**, or **Waiting for primary MS PIC**.	All levels
Last Change	Timestamp for the last change in status. This value resets after a master Routing Engine switchover event if any of the following conditions is met: • GRES is not configured on the router. • The **rlsq** interface is configured without the **hot-standby** or **warm-standby** statements and the backup **lsq** interface was active before the switchover. • No logical interfaces are configured or all of the configured logical interfaces are down at the time of the switchover.	All levels
Primary	Name of the interface configured to be the primary interface.	All levels
Secondary	Name of the interface configured to be the backup interface.	All levels
Current Status	Physical status of the primary and secondary interfaces.	All levels
Mode	Standby mode.	**detail**

Sample Output

show interfaces redundancy

`user@host>` **show interfaces redundancy**

```
Interface  State         Last change  Primary    Secondary  Current status
rsp0       Not present                sp-1/0/0   sp-0/2/0   both down
rsp1       On secondary  1d 23:56     sp-1/2/0   sp-0/3/0   primary down
rsp2       On primary    10:10:27     sp-1/3/0   sp-0/2/0   secondary down
rlsq0      On primary    00:06:24     lsq-0/3/0  lsq-1/0/0  both up
ams0       On primary    00:39:51     mams-5/0/0 mams-5/1/0 both up
```

show interfaces redundancy (Aggregated Ethernet)

```
user@host> show interfaces redundancy
```

```
Interface  State           Last change  Primary      Secondary    Current status
rlsq0      On secondary    00:56:12     lsq-4/0/0    lsq-3/0/0    both up
ae0
ae1
ae2
ae3
ae4
```

show interfaces redundancy (Aggregated Inline Service Interface)

```
user@host> show interfaces redundancy asi0
```

```
Interface  State          Last change  Primary      Secondary    Current status
asi0       On primary     00:00:09     si-1/0/0     si-0/0/0     both up
```

show interfaces redundancy detail

```
user@host> show interfaces redundancy detail
```

```
Interface        : rlsq0
  State          : On primary
  Last change    : 00:45:47
  Primary        : lsq-0/2/0
  Secondary      : lsq-1/2/0
  Current status : both up
  Mode           : hot-standby

Interface        : rlsq0:0
  State          : On primary
  Last change    : 00:45:46
  Primary        : lsq-0/2/0:0
  Secondary      : lsq-1/2/0:0
  Current status : both up
  Mode           : warm-standby

Interface        : asi0
  State          : On primary
  Last change    : 00:03:42
  Primary        : si-1/0/0
  Secondary      : si-0/0/0
```

```
  Mode           : hot-standby
  Current status : both up

Interface        :ams0
  State : On primary
  Last change : 00:39:52
  Primary : mams-5/0/0
  Secondary : mams-5/1/0
  Mode : warm-standby
  Current status : both up
  Replication state : Disconnected
```

show security pki ca-certificate

Syntax

```
show security pki ca-certificate
<brief | detail>
<ca-profile ca-profile-name>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Display information about certificate authority (CA) digital certificates installed in the router.

Options

none—(Same as brief) Display information about all CA digital certificates.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display information about only the specified CA profile.

Required Privilege Level

view

List of Sample Output

show security pki ca-certificate on page 1791
show security pki ca-certificate detail on page 1791

Output Fields

Table 54 on page 1789 lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 54: show security pki ca-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	**none brief**

Table 54: show security pki ca-certificate Output Fields *(continued)*

Field Name	Field Description	Level of Output
Issued to	Device that was issued the digital certificate.	**none brief**
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the requestor. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption(1024 bits)**.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki ca-certificate

user@host> **show security pki ca-certificate**

```
Certificate identifier: abc
  Issued to: example, Issued by: exmple
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier: entrust
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier:abe
  Issued to: First Officer, Issued by: example
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
```

show security pki ca-certificate detail

user@host> **show security pki ca-certificate detail**

```
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
```

```
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: example, Country: us
  Subject:
    Organization: example, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
    23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925b
  Issuer:
    Organization: example, Country: us
```

```
Subject:
  Organization: example, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
  ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
  d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
  00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
  e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
  90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
  b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
  af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=example, CN=CRL1
  http://CA-1/CRL/example_us_crlfile.crl
Use for key: Digital signature
```

show security pki certificate-request

Syntax

```
show security pki certificate-request
<brief | detail>
<certificate-id certificate-id-name>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Display information about manually generated local digital certificate requests that are stored in the router.

Options

none—(same as brief) Display information about all local digital certificate requests.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified local digital certificate request

Required Privilege Level

view

RELATED DOCUMENTATION

clear security pki certificate-request | **1656**

List of Sample Output

show security pki certificate-request on page 1795
show security pki certificate-request detail on page 1796

Output Fields

Table 55 on page 1794 lists the output fields for the **show security pki certificate-request** command. Output fields are listed in the approximate order in which they appear.

Table 55: show security pki certificate-request Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels

Table 55: show security pki certificate-request Output Fields *(continued)*

Field Name	Field Description	Level of Output
Certificate version	Revision number of the digital certificate.	**detail**
Issued to	Device that was issued the digital certificate.	**none brief**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption(1024 bits)**.	All levels
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.	All levels
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki certificate-request

```
user@host> show security pki certificate-request
```

```
Certificate identifier: local-microsoft-2
  Issued to: router2.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

show security pki certificate-request detail

user@host> **show security pki certificate-request detail**

```
Certificate identifier: local-entrust3
  Certificate version: 3
  Subject:
    Common name: router3.example.com
  Alternate subject: router3.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
    fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
    d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
    23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
    ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
    7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
    72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
    79:54:da:4f:d3:6f:52:1f
  Fingerprint:
    7c:e8:f9:45:93:8d:a3:92:7f:18:29:02:f1:c8:e2:85:3d:ad:df:1f (sha1)
    00:4e:df:a0:6b:ad:8c:50:da:7c:a1:cf:5d:37:b0:ea (md5)
  Use for key: Digital signature
```

show security pki crl

Syntax

```
show security pki crl
<brief | detail>
<ca-profile ca-profile-name>
```

Release Information

Command introduced in Junos OS Release 8.1.

Description

Display information about the certificate revocation lists (CRLs) that are stored in the router.

Options

none—(same as brief) Display information about all CRLs.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display CRL information about only the specified CA profile.

Required Privilege Level

view

RELATED DOCUMENTATION

clear security pki crl | **1657**

List of Sample Output

show security pki crl on page 1798
show security pki crl detail on page 1799

Output Fields

Table 56 on page 1797 shows the output fields for the **show security pki crl** command. Output fields are listed in the approximate order in which they appear.

Table 56: show security pki crl Output Fields

Field Name	Field Description	Level of Output
CA profile	Name of the configured CA profile.	All levels
CRL version	Revision number of the certificate revocation list.	All levels

Table 56: show security pki crl Output Fields *(continued)*

Field Name	Field Description	Level of Output
CRL number	Number of the certificate revocation list	All levels
CRL Issuer	Device that was issued the certificate revocation list.	All levels
Issuer	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Effective date	Date and time the certificate revocation list becomes valid.	All levels
Next update	Date and time the router will download the latest version of the certificate revocation list.	All levels
Revocation List	List of digital certificates that have been revoked before their expiration date. Values are: • **Serial number**—Unique serial number of the digital certificate • **Revocation date**—Date and time that the digital certificate was revoked.	**detail**

Sample Output

show security pki crl

```
user@host> show security pki crl
 CA profile entrust
 CRL version: V2
 CRL number: 24
 CRL issuer: C=CA, O=juniper
 Effective date: 2006 May 31st, 05:35:25 GMT
 Next update: 2006 Jun 1st, 06:35:25 GMT
```

show security pki crl detail

```
user@host> show security pki crl detail
  CA profile: entrust
 CRL version: V2
 CRL number: 24
 Issuer:
  Organization: juniper, Country: ca
 Validity:
  Effective date: 2006 May 31st, 05:35:25 GMT
  Next update: 2006 Jun 1st, 06:35:25 GMT
 Revocation List:
  Serial number      Revocation date
  4451aca3 2006      May 25th, 09:13:38 GMT
  4451aca4 2006      May 25th, 10:11:33 GMT
  4451acb4 2006      May 29th, 11:28:54 GMT
  4451aceb 2006      May 29th, 11:29:01 GMT
  4451acfe 2006      May 29th, 11:29:17 GMT
  4451acff 2006      May 31st, 05:29:55 GMT
```

show security pki local-certificate

Syntax

```
show security pki local-certificate
<brief | detail>
<certificate-id certificate-id-name>
<system-generated>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

Display information about the local digital certificates and the corresponding public keys installed in the router.

Options

none—(same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.

system-generated—(Optional) Auto-generated self-signed certificate.

Required Privilege Level

view

RELATED DOCUMENTATION

clear security pki local-certificate | **1659**

List of Sample Output

show security pki local-certificate on page 1802
show security pki local-certificate detail on page 1802

Output Fields

Table 57 on page 1801 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 57: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	none **brief**
Issued to	Device that was issued the digital certificate.	none **brief**
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption (1024 bits)**.	All levels

Table 57: show security pki local-certificate Output Fields *(continued)*

Field Name	Field Description	Level of Output
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki local-certificate

```
user@host> show security pki local-certificate
```

```
Certificate identifier: local-entrust2
  Issued to: router2.example.com, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

show security pki local-certificate detail

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: local-entrust3
  Certificate version: 3
  Serial number: 4355 94f9
  Issuer:
```

```
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: router3.example.com
Alternate subject: router3.example.com
Validity:
  Not before: 2005 Nov 21st, 23:33:58 GMT
  Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
  fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
  d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
  23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
  ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
  7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
  72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
  79:54:da:4f:d3:6f:52:1f
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
  60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature
```

show services alg conversations

Syntax

```
show services alg conversations
<brief >
<application-protocol protocol>
<extensive>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 10.4.
h323 option introduced in Junos OS Release 17.1.
ike-esp-nat option introduced in Junos OS Release 17.1.

Description

Display ALG information for Junos OS extension-provider packages.

> **NOTE:** In Junos OS releases earlier than 12.3, the extension-provider packages were variously referred to as Junos Services Framework (JSF), MP-SDK, and eJunos.

Options

none—Display standard information about all Junos OS extension-provider packages ALG sessions.

brief —(Optional) Display the specified level of output.

application-protocol—(Optional) Display information about one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **h323**—H323 protocol
- **ike-esp-nat**—IKE ALG
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol

rpc-portmap—Remote Procedure Call protocol portmap service

rtsp—Real-Time Streaming Protocol

rsh—Remote Shell

sip—Session Initiation Protocol

sql—SQLNet

talk—Talk Program

extensive—Display extensive information

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level
view

List of Sample Output
show services alg conversations on page 1806
show services alg conversations brief on page 1806
show services alg conversations extensive on page 1807
show services alg conversations application-protocol on page 1807
show services alg conversations interface on page 1811

Output Fields
Table 58 on page 1805 lists the output fields for the **show services alg conversations** command. Output fields are listed in the approximate order in which they appear.

Table 58: show services alg conversations Output Fields

Field Name	Field Description
Interface	Name of the interface.
ALG	Name of the ALG in use.
Number of conversations	Number of ALG conversations open. A conversation is a group of parent and child sessions.
Group ID	Numeric identifier for the session.
Parent session status	Status of the parent session: • **Active** • **Closed**

Table 58: show services alg conversations Output Fields *(continued)*

Field Name	Field Description
Parent session ID	Numeric identifier for the parent session.
Protocol	Protocol used for the parent session.
Forward Flow	The source and destination prefixes for forward flow.
Reverse Flow	The source and destination prefixes for reverse flow.
Child session status	Status of the child session: • **Active** • **Closed**
Child session ID	Numeric identifier for the child session.
Number of Resources	Total number of active child sessions associated with the parent session.
Resource ID	Numeric identifier for the resources associated with the parent session.
Protocol	Protocol used for the child session.

Sample Output

show services alg conversations

`user@host>` **show services alg conversations**

```
Interface name: ms-2/1/0
ALG : SQLV2 ALG, State : active
Number of conversations: 1
Parent session status: closed
Child session : 1, protocol: TCP
Forward Flow : {10.50.50.2:37244 -> 10.40.40.10:4334}
Reverse Flow : {10.40.40.10:4334 -> 10.11.11.10:37244}
```

show services alg conversations brief

The output for the **show services alg conversations brief** command is identical to that for the **show services alg conversations** command. For sample output, see show services alg conversations on page 1806.

show services alg conversations extensive

user@host> **show services alg conversations extensive**

```
Interface name: ms-1/0/0
ALG : H323 ALG, State : active
Number of conversations: 1
Group ID : 3499913712, State : active
Parent session state: active
Parent session ID: 33554433, protocol : TCP
Forward Flow : {198.51.100.2:30000 -> 192.0.2.2:1720}
Reverse Flow : {192.0.2.2:1720 -> 203.0.113.1:57730}
Number of resources: 4
Resource ID: 3499927656, State: active
Number of sessions: 1
Child session ID: 33554436, protocol : UDP
Forward Flow : {198.51.100.2:5086 -> 192.0.2.2:5090}
Reverse Flow : {192.0.2.2:5090 -> 203.0.113.3:55916}
Resource ID: 3499927376, State: active
Number of sessions: 1
Child session ID: 67108867, protocol : UDP
Forward Flow : {192.0.2:5091 -> 203.0.113.3:55917}
Reverse Flow : {198.51.100.2:5087 -> 192.0.2.2:5091}
Resource ID: 3499926816, State: active
Number of sessions: 1
Child session ID: 33554438, protocol : UDP
Forward Flow : {198.51.100.2:5089 -> 192.0.2.2:5093}
Reverse Flow : {192.0.2.2:5093 -> 203.0.113.2:63435}
Resource ID: 3499926536, State: active
Number of sessions: 1
Child session ID: 33554437, protocol : UDP
Forward Flow : {198.51.100.2:5088 -> 192.0.2.2:5092}
Reverse Flow : {192.0.2.2:5092 -> 203.0.113.2:63434}
ALG : RAS ALG, State : active
Number of conversations: 1
Group ID : 799037592, State : active
Parent session state: closed
Number of resources: 0
```

show services alg conversations application-protocol

This command has the same output for the rpc, dce-rpc, rpc-portmap and dce-rpc-portmap ALGs.

user@router> **show services alg conversations application-protocol rpc**

```
Interface name: ms-1/1/0
ALG : SUNRPC ALG, State : active
  Number of conversations: 2
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:1019 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:1019}
      Child session : 2, protocol: UDP
        Forward Flow : {192.168.203.198:36595 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:36595}
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:954 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:954}
      Child session : 2, protocol: UDP
        Forward Flow : {192.168.203.198:53836 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:53836}
```

user@router> **show services alg conversations application-protocol dns**

```
Interface name: ms-1/1/0
ALG : DNS ALG, State : active
  Number of conversations: 1
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:1019 -> 192.168.203.194:2049}
        Reverse Flow : {192.168.203.194:2049 -> 192.168.203.198:1019}
```

user@router> **show services alg conversations application-protocol ftp**

```
Interface name: ms-1/1/0
ALG : DNS ALG, State : active
  Number of conversations: 1
    Parent session status: closed
      Child session : 1, protocol: UDP
        Forward Flow : {192.168.203.198:53836 -> 192.168.203.194:613}
        Reverse Flow : {192.168.203.194:613 -> 192.168.203.198:53836}
```

user@router> **show services alg conversations application-protocol ike-esp-nat**

```
Interface name: ms-2/2/0
ALG : IKE ALG, State : active
  Number of conversations: 1
    Parent session status: closed
    Child session : 1, protocol: ESP
      Forward Flow : {198.51.100.101:2623 -> 203.0.113.1:46838}
      Reverse Flow : {192.0.2.101:46838 -> 198.51.10.101:2623}
    Child session : 2, protocol: ESP
      Forward Flow : {192.0.2.101:2666 -> 198.51.10.101:57882}
      Reverse Flow : {198.51.10.101:57882 -> 203.0.113.1:2666}
```

user@router> **show services alg conversations application-protocol pptp**

```
Interface name: ms-2/0/0
ALG : PPTP ALG, State : active
  Number of conversations: 1
    Parent session status: active
    Parent session : 1, protocol : TCP
      Forward Flow : {192.0.2.10:1511 -> 198.51.100.10:1723}
      Reverse Flow : {198.51.100.10:1723 -> 192.0.2.10:1511}
      Child session : 1, protocol: GRE
        Forward Flow : {192.0.2.10:0 -> 198.51.100.10:49913}
        Reverse Flow : {198.51.100.10:49913 -> 192.0.2.10:65001}
      Child session : 2, protocol: GRE
        Forward Flow : {198.51.100.10:0 -> 192.0.2.10:0}
        Reverse Flow : {192.0.2.10:0 -> 198.51.100.10:65000}
```

user@router> **show services alg conversations application-protocol rtsp**

```
Interface name: ms-0/1/0
ALG : RTSP ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {198.51.100.2:3985 -> 192.0.2.1:554}
      Reverse Flow : {203.0.113.2:554 -> 198.51.100.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {203.0.113.2:35859 -> 198.51.100.2:38159}
      Reverse Flow : {198.51.100.2:38159 -> 192.0.2.1:35859}
    Child session : 2, protocol: UDP
      Forward Flow : {203.0.113.2:35859 -> 198.51.100.2:37391}
      Reverse Flow : {198.51.100.2:37391 -> 192.0.2.1:35859}
```

user@router> **show services alg conversations application-protocol rsh**

```
Interface name: ms-0/1/0
ALG : RSH ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {198.51.100.2:3985 -> 192.0.2.1:554}
      Reverse Flow : {203.0.113.2:554 -> 198.51.100.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {203.0.113.2:35859 -> 198.51.100.2:38159}
      Reverse Flow : {198.51.100.2:38159 -> 192.0.2.1:35859}
```

user@router> **show services alg conversations application-protocol sip**

```
Interface name: ms-1/1/0
ALG : SIP ALG, State : active
  Number of conversations: 1
    Parent session status: active
    Parent session : 1, protocol : UDP
      Forward Flow : {192.0.2.2:5060 -> 198.51.100.2:5060}
      Reverse Flow : {198.51.100.2:5060 -> 203.0.113.2:5060}
    Child session : 1, protocol: UDP
        Forward Flow : {192.0.2.2:6000 -> 198.51.100.2:12442}
        Reverse Flow : {198.51.100.2:12442 -> 203.0.113.2:6000}
```

user@router> **show services alg conversations application-protocol sql**

```
Interface name: ms-2/0/0
ALG : SQLV2 ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : 0
      Forward Flow : {0.0.0.0:0 -> 0.0.0.0:0}
      Reverse Flow : {0.0.0.0:0 -> 0.0.0.0:0}
    Child session : 1, protocol: TCP
      Forward Flow : {203.0.113.2:19099 -> 198.51.100.10:32773}
      Reverse Flow : {198.51.100.10:32773 -> 192.0.2.1:19099}
```

user@router> **show services alg conversations application-protocol talk**

```
Interface name: ms-0/1/0
ALG : TALK ALG, State : active
  Number of conversations: 1
    Parent session : 1, protocol : TCP
      Forward Flow : {198.51.2:3985 -> 192.0.2.1:554}
```

```
      Reverse Flow : {203.0.113.2:554 -> 198.51.2:3985}
    Child session : 1, protocol: UDP
      Forward Flow : {203.0.113.2:35859 -> 198.51.2:38159}
      Reverse Flow : {198.51.2:38159 -> 192.0.2.1:35859}
```

show services alg conversations interface

user@router> **show services alg conversations interface ms-1/1/0**

```
ALG : FTP ALG, State : active
Number of conversations: 1
Parent session status: active
Parent session : 1, protocol : TCP
Forward Flow : {10.20.20.10:47164 -> 10.30.30.30:21}
```

show services alg statistics

Syntax

```
show services alg statistics
<application-protocol protocol>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 10.4.
h323 option introduced in Junos OS Release 17.1.
ike-esp-nat option introduced in Junos OS Release 17.1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display ALG statistics for Junos OS extension-provider packages.

> **NOTE:** In Junos OS releases earlier than 12.3, the extension-provider packages were variously referred to as Junos Services Framework (JSF), MP-SDK, and eJunos.

Options

application-protocol—(Optional) Display statistics for one of the following application protocols:

- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **ftp**—File Transfer Protocol
- **h323**—H323 protocol
- **ike-esp-nat**—IKE ALG
- **pptp**—Point-to-Point Tunneling Protocol
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol

rsh—Remote Shell

sip—Session Initiation Protocol

sql—SQLNet

talk—Talk Program

tftp—Trivial File Transfer Protocol

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level
view

List of Sample Output
show services alg statistics application-protocol on page 1822
show services alg statistics interface on page 1827

Output Fields
Table 59 on page 1813 lists the output fields for the **show services alg statistics** command. Output fields are listed in the approximate order in which they appear.

Table 59: show services alg statistics Output Fields

Field Name	Field Description
Interface	Name of the interface.
ALG statistics	Name of the ALG for which the statistics are displayed.
Packets with wrong header	Number of packets with wrong header.
Non epm 3.0 packets	Number of non epm 3.0 packets.
Packets with type mismatch	Number of packets with type mismatch.
Packets with id mismatch	Number of packets with id mismatch.
Packets with call mismatch	Number of packets with call mismatch.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Packets fragmented	Number of packets fragmented.
Packets queued	Number of packets queued.
Packets dropped	Number of packets dropped.
Packets released	Number of packets released.
Invalid packets received	Number of invalid packets received.
Reply packets received	Number of reply packets received.
Oversized packets received	Number of oversized packets received.
ALG parser errors	Number of parsing failed errors.
Packets translated	Number of packets translated.
H323 total calls	Total number of audio/video calls that have been established.
H323 active calls	Current number of active H.323 calls.
H323 gate install failed	Number of gate installation failures for child sessions.
H323 pinhole opened too late	Number of H323 parent sessions that released the resources before pinhole creation.
H323 pinhole hit dropped	Number of H323 gate hits that have been dropped.
H323 gate timeout failed	Number of gate timeout failures due to an error.
H323 packets dropped	Number of packets dropped.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
H323 get virtual ctx failed	Number of failures to get the session virtualization ctx information.
H323 obj alloc failed	Number of memory allocation failures for H323 session cookie.
H323 group alloc failed	Number of H323 session resource/group memory allocation failures.
H323 ce alloc failed	Number of H323 session call entity object memory allocation failures.
H323 Q931 decode error	Number of errors in decoding Q931 packets.
H323 H245 decode error	Number of errors in decoding H245 packets.
H323 Q931 process error	Number of errors in processing Q931 packets.
H323 H245 process error	Number of errors in processing H245 packets.
H323 do nat failed	Number of NAT translation failures after packet decode.
H323 do rm failed	Number of H323 vsip table creation failures.
H323 dscp marked	Number of Differentiated Services code point (DSCP) packets marked.
H323 dscp marked error	Number of Differentiated Services code point (DSCP) packets marked as errors.
RAS obj alloc failed	Number of RAS session object memory allocation failures.
RAS group alloc failed	Number of RAS session group memory allocation failures.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
RAS packets dropped	Number of RAS packets dropped.
RAS packet exists in cookie error	Number of times that some packets exist in existing RAS sessions cookie.
RAS decode error	Number of errors in decoding RAS packets.
RAS flood error	Number of gatekeeper requests that were dropped because of too many RAS request messages.
RAS do nat failed	Number of RAS session payload IP translation errors.
PPTP Objects Active	Number of PPTP objects active.
PPTP Objects Total	Number of PPTP objects in total.
PPTP Objects Error	Number of PPTP objects having errors.
PPTP ASL Group Active	Number of PPTP groups active.
PPTP ASL Group Total	Number of PPTP groups in total.
PPTP ASL Group Error	Number of PPTP groups having errors.
PPTP Packets received	Number of PPTP packets received.
PPTP Packets Discarded	Number of PPTP packets discarded.
PPTP Packets Free	Number of PPTP packets freed.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP OCRQ Received	Number of Outgoing Call Requests received.
PPTP OCRQ Discarded	Number of Outgoing Call Requests discarded.
PPTP OCRP Received	Number of Outgoing Call Packets received.
PPTP OCRP Discarded	Number of Outgoing Call Packets discarded.
PPTP WEN(SLI) Received	Number of WEN (SLI) packets received.
PPTP WEN(SLI) Discarded	Number of WEN (SLI) packets discarded.
PPTP CCRQ-CDSN Received	Number of Call Clear Requests received.
PPTP CDSN Received	Number of Call Disconnection Notifications received.
PPTP CCRQ-CDSN Discarded	Number of Call Clear Requests discarded.
PPTP Session Create	Number of PPTP sessions created.
PPTP Session Destroy	Number of PPTP sessions destroyed.
PPTP Gate Create	Number of PPTP gates created.
PPTP Gate Hit	Number of PPTP gates hit.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP Gate Timeout	Number of PPTP gates timed out.
PPTP NAT Events	Number of NAT events.
PPTP DO-NAT Total	Number of DO NATs in total.
PPTP DO-NAT Ok	Number of DO NATs okay.
PPTP DO-NAT Pending	Number of DO NATs pending.
PPTP DO-NAT Fail	Number of DO NATs failed.
PPTP DO-RM Total	Number of DO RMs in total.
PPTP DO-RM Ok	Number of DO RMs okay.
PPTP DO-RM Pending	Number of DO RMs pending.
PPTP DO-RM Fail	Number of DO RMs failed.
PPTP NAT-ASYNC Total	Number of NAT-ASYNCs in total.
PPTP NAT-ASYNC Invalid	Number of NAT-ASYNCs invalid.
PPTP NAT-ASYNC Error1	Number of NAT-ASYNCs error1.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
PPTP NAT-ASYNC Error2	Number of NAT-ASYNCs error2.
PPTP ASL Hole Ok	Number of ASYNC holes okay.
PPTP ASL Hole Error	Number of ASYNC hole errors.
PPTP ASL First Hit	Number of ASYNC holes first hit.
PPTP ASL Hole Timeout	Number of ASYNC holes timed out.
PPTP ASL Invalid	Number of ASYNC holes invalid.
PPTP NAT Ctx Free	Number of NAT Ctxs free.
PPTP Create Resource Error	Number of create resource errors.
PPTP set S2C hole error	Number of server-to-client hole errors.
PPTP set C2S hole error	Number of client-to-server hole errors.
PPTP lnbrk error	Number of PPTP lnbrk errors.
PPTP Mpool Create Error	Number of Mpool create errors.
PPTP RM register client Error	Number of client registration errors.
Call packet with rpcbind2	Number of call packets with rpcbind2.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Call packet with rpcbind3	Number of call packets with rpcbind3.
Call packet with rpcbind4	Number of call packets with rpcbind4.
Invalid rpcbind call	Number of invalid rpcbind calls.
Reply packet with rpcbind2	Number of reply packets with rpcbind2.
Reply packet with rpcbind3	Number of reply packets with rpcbind3.
Reply packet with rpcbind4	Number of reply packets with rpcbind4.
Invalid rpcbind reply	Number of invalid rpcbind replies.
Packets exceeded maximum length	Number of packets exceeding maximum length.
Packets dropped by ALG	Number of packets dropped by the ALG.
Number of describe messages received	Number of describe messages received.
Number of setup messages received	Number of setup messages received.
Number of teardown messages received	Number of teardown messages received.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Total packets dropped	Total number of SIP packets dropped.
Unexpected requests dropped	Number of unexpected requests dropped.
Unexpected responses dropped	Number of unexpected responses dropped.
Packets DSCP marked	Number of Differentiated Services code point (DSCP) packets marked.
Packets DSCP marked error	Number of Differentiated Services code point (DSCP) packets marked as error.
NAT errors	Number of Network Address Translation errors.
RR headers exceeded maximum limits	Number of RR headers exceeded maximum limits.
Contact headers exceeded maximum limits	Number of contact headers exceeded maximum limits.
Invite dropped due to call limit	Number of invites dropped due to call limit.
Messages not processed by sip stack	Number of messages not processed by sip stack.
Unknown packets dropped	Number of unknown packets dropped.
Decoding Errors	Number of decoding errors.
Packets received in out of state	Number of packets received in out of state.

Table 59: show services alg statistics Output Fields *(continued)*

Field Name	Field Description
Packets received	Number of packets received.
Packets freed by ALG	Number of packets freed by ALG.
Gate fail errors	Number of gate fail errors.
Lookup packets	Number of lookup packets.
Announce packets	Number of announce packets.
Delete packets	Number of delete packets.
Number of packets received	Number of packets received.
Number of Invalid packets	Number of invalid packets.
Total number of sessions	Total number of sessions.
Number of actives sessions	Number of active sessions.

Sample Output

show services alg statistics application-protocol

While the statistics are the same for dce-rpc and dce-rpc-portmap, both rpc and rpc-portmap have the same output too.

`user@router>` **show services alg statistics application-protocol dce-rpc**

```
Interface name: ms-1/1/0
  DCE-RPC ALG statistics:
    Packets with wrong header : 0
    Non epm 3.0 packets       : 0
```

```
    Packets with type mismatch: 0
    Packets with id mismatch  : 0
    Packets with call mismatch: 0
    Packets fragmented        : 0
    Packets queued            : 0
    Packets dropped           : 0
    Packets released          : 0
```

user@router> **show services alg statistics application-protocol dns**

```
Interface name: ms-2/0/0
  DNS ALG statistics:
    Invalid packets received   : 0
    Reply packets received     : 3509
    Oversized packets received : 0
```

user@router> **show services alg statistics application-protocol ftp**

```
Interface name: ms-1/1/0
FTP ALG statistics:
Packets dropped           : 0
ALG parser errors         : 0
Packets translated        : 0
```

user@router> **show services alg conversations application-protocol h323**

```
Interface name: ms-1/0/0
H323 ALG statistics:
  H323 total calls: 1
  H323 active calls: 1
  H323 gate install failed: 0
  H323 pinhole opened too late: 0
  H323 pinhole hit dropped: 0
  H323 gate timeout failed: 0
  H323 packets dropped: 0
  H323 get virtual ctx failed: 0
  H323 obj alloc failed: 0
  H323 group alloc failed: 0
  H323 ce alloc failed: 0
  H323 Q931 decode error: 0
  H323 H245 decode error: 0
  H323 Q931 process error: 0
```

```
  H323 H245 process error: 0
  H323 do nat failed: 0
  H323 do rm failed: 0
  H323 dscp marked: 0
  H323 dscp marked error: 0
  RAS obj alloc failed: 0
  RAS group alloc failed: 0
  RAS packets dropped: 0
  RAS packet exists in cookie error: 0
  RAS decode error: 0
  RAS flood error: 0
  RAS do nat failed: 0
```

user@router> **show services alg statistics application-protocol ike-esp-nat**

```
Interface name: ms-4/1/0
  IKE ESP ALG statistics:
    Session interests processed: 2
    Sessions created: 2
    Sessions destroyed: 1
    Control sessions created: 2
    Control sessions destroyed: 1
    Data sessions created: 0
    Data sessions destroyed: 0
    Gates created: 4
    Gate hits: 0
    Gates timedout: 4
```

user@router> **show services alg statistics application-protocol pptp**

```
Interface name: ms-2/0/0
  PPTP ALG statistics:
    PPTP Objects Active  : 1
    PPTP Objects Total  : 1
    PPTP Objects Error  : 0
    PPTP ASL Group Active  : 1
    PPTP ASL Group Total  : 1
    PPTP ASL Group Error  : 0
    PPTP Packets received  : 11
    PPTP Packets Discarded  : 0
    PPTP Packets Free  : 0
    PPTP OCRQ Received  : 1
    PPTP OCRQ Discarded  : 0
```

```
    PPTP OCRP Received  : 1
    PPTP OCRP Discarded  : 0
    PPTP WEN(SLI) Received  : 3
    PPTP WEN(SLI) Discarded  : 0
    PPTP CCRQ-CDSN Received  : 0
    PPTP CDSN Received  : 0
    PPTP CCRQ-CDSN Discarded  : 0
    PPTP Session Create  : 3
    PPTP Session Destroy  : 0
    PPTP Gate Create  : 0
    PPTP Gate Hit  : 2
    PPTP Gate Timeout  : 0
    PPTP NAT Events  : 0
    PPTP DO-NAT Total  : 1
    PPTP DO-NAT Ok  : 1
    PPTP DO-NAT Pending  : 0
    PPTP DO-NAT Fail  : 0
    PPTP DO-RM Total  : 1
    PPTP DO-RM Ok  : 2
    PPTP DO-RM Pending  : 0
    PPTP DO-RM Fail  : 0
    PPTP NAT-ASYNC Total  : 0
    PPTP NAT-ASYNC Invalid  : 0
    PPTP NAT-ASYNC Error1  : 0
    PPTP NAT-ASYNC Error2  : 0
    PPTP ASL Hole Ok  : 2
    PPTP ASL Hole Error  : 0
    PPTP ASL First Hit  : 2
    PPTP ASL Hole Timeout  : 0
    PPTP ASL Invalid  : 0
    PPTP NAT Ctx Free  : 0
    PPTP Create Resource Error  : 0
    PPTP set S2C hole error  : 0
    PPTP set C2S hole error  : 0
    PPTP lnbrk error  : 0
    PPTP Mpool Create Error  : 0
    PPTP RM register client Error  : 0
```

user@router> **show services alg statistics application-protocol rpc**

```
Interface name: ms-1/1/0
  RPC ALG statistics:
    Call packet with rpcbind2 : 2
    Call packet with rpcbind3 : 0
```

```
    Call packet with rpcbind4 : 0
    Invalid rpcbind call      : 0
    Reply packet with rpcbind2: 2
    Reply packet with rpcbind3: 0
    Reply packet with rpcbind4: 0
    Invalid rpcbind reply     : 0
    Packets fragmented        : 0
    Packets dropped           : 0
    Packets released          : 0
```

user@router> **show services alg statistics application-protocol rtsp**

```
Interface name: ms-0/1/0
  RTSP ALG statistics:
    Packets exceeded maximum length : 0
    Packets dropped by ALG : 0
    Number of describe messages received : 8
    Number of setup messages received : 30
    Number of teardown messages received : 7
```

user@router> **show services alg statistics application-protocol rsh**

```
Interface name: ms-2/0/0
  RSH ALG statistics:
    Invalid packets received   : 0
    Packets dropped by ALG   : 0
    ALG parser errors  : 0
    Packets freed by ALG     : 0
```

user@router> **show services alg statistics application-protocol sip**

```
Interface name: ms-2/0/0
  SIP ALG statistics:
    Total packets dropped  : 0
    Unexpected requests dropped : 0
    Unexpected responses dropped : 0
    Packets DSCP marked  : 0
    Packets DSCP marked error  : 0
    NAT errors : 0
    RR headers exceeded maximum limits : 0
    Contact headers exceeded maximum limits  : 0
```

```
    Invite dropped due to call limit : 0
    Messages not processed by sip stack : 0
    Unknown packets dropped  : 0
    Decoding Errors : 0
    Packets received in out of state  : 0
```

user@router> **show services alg statistics application-protocol sql**

```
Interface name: ms-2/0/0
  SQLNET ALG statistics:
    Packets received  : 5
    ALG parser errors  : 0
    Packets freed by ALG : 0
    Gate fail errors  : 0
```

user@router> **show services alg statistics application-protocol talk**

```
Interface name: ms-2/0/0
  TALK ALG statistics:
    Lookup packets  : 5
    Announce packets  : 0
    Delete packets : 0
```

user@router> **show services alg statistics application-protocol tftp**

```
Interface name: ms-0/0/0
  TFTP ALG statistics:
    Number of packets received : 0
    Number of Invalid packets  : 0
    Total number of sessions :   0
    Number of active sessions:   0
```

show services alg statistics interface

user@router> **show services alg statistics interface ms-1/1/0**

```
Interface name: ms-1/1/0
FTP ALG statistics:
Packets dropped           : 0
```

```
ALG parser errors         : 0
Packets translated        : 0
```

show services cos statistics

Syntax

```
show services cos statistics
<brief | detail | extensive>
<diffserv | forwarding-class>
<interface interface-name>
<service-set service-set-name>
<summary>
```

Release Information

Command introduced in Junos OS Release 8.1.

Description

Display the mapping of class-of-service (CoS) code point aliases to corresponding bit patterns and the mapping of forwarding class names to queue numbers as configured in CoS services for the Multiservices PIC, MS-MIC, or MS-MPC.

Options

none—Display all services CoS statistics.

brief | detail | extensive—(Optional) Display the specified level of output.

diffserv | forwarding-class—(Optional) Display only the selected information, either DiffServ codepoints or forwarding classes.

interface *interface-name*—(Optional) Display statistics for the specified interface only.

service-set *service-set-name*—(Optional) Display statistics for the specified service set only.

summary—(Optional) Display summary of statistics on a per-interface basis.

Required Privilege Level

view

List of Sample Output

show services cos statistics on page 1830
show services cos statistics brief on page 1832
show services cos statistics detail on page 1832
show services cos statistics extensive on page 1832

Output Fields

Table 60 on page 1830 describes the output fields for the **show services cos statistics** command. Output fields are listed in the approximate order in which they appear.

Table 60: show services cos statistics Output Fields

Field Name	Field Description	Level of Output
Interface	Name of interface.	All levels
Service set	Name of service set.	All levels
DSCP	DiffServ code point bit pattern.	All levels
Packets in	Number of packets received.	All levels
Packets out	Number of packets transmitted.	All levels
Forwarding class	Forwarding class queue number.	All levels

Sample Output

show services cos statistics

`user@host>` **show services cos statistics**

```
Interface: sp-1/0/0, Service set: scos
DSCP               Packets in          Packets out
000000                      0                    0
000001                      0                    0
000010                      0                    0
000011                      0                    0
000100                      0                    0
000101                      0                    0
000110                      0                    0
000111                      0                    0
001000                      0                    0
001001                      0                    0
001010                      0                    0
001011                      0                    0
001100                      0                    0
001101                      0                    0
001110                      0                    0
001111                      0                    0
010000                      0                    0
010001                      0                    0
```

```
010010                  0                  0
010011                  0                  0
010100                  0                  0
010101                  0                  0
010110                  0                  0
010111                  0                  0
011000                  0                  0
011001                  0                  0
011010                  0                  0
011011                  0                  0
011100                  0                  0
011101                  0                  0
011110                  0                  0
011111                  0                  0
100000                  0                  0
100001                  0                  0
100010                  0                  0
100011                  0                  0
100100                  0                  0
100101                  0                  0
100110                  0                  0
100111                  0                  0
101000                  0                  0
101001                  0                  0
101010                  0                  0
101011                  0                  0
101100                  0                  0
101101                  0                  0
101110                  0                  0
101111                  0                  0
110000                  0                  0
110001                  0                  0
110010                  0                  0
110011                  0                  0
110100                  0                  0
110101                  0                  0
110110                  0                  0
110111                  0                  0
111000                  0                  0
111001                  0                  0
111010                  0                  0
111011                  0                  0
111100                  0                  0
111101                  0                  0
```

```
111110                    0                    0
111111                    0                    0
Forwarding class          Packets in           Packets out
0                                 0                    0
1                                 0                    0
2                                 0                    0
3                                 0                    0
4                                 0                    0
5                                 0                    0
6                                 0                    0
7                                 0                    0
8                                 0                    0
9                                 0                    0
10                                0                    0
11                                0                    0
12                                0                    0
13                                0                    0
14                                0                    0
15                                0                    0
```

show services cos statistics brief

The output for the **show services cos statistics brief** command is identical to that for the **show services cos statistics** command.

show services cos statistics detail

The output for the **show services cos statistics detail** command is identical to that for the **show services cos statistics** command.

show services cos statistics extensive

The output for the **show services cos statistics extensive** command is identical to that for the **show services cos statistics** command.

show services crtp

Syntax

```
show services crtp
<extensive>
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display Compressed Real-Time Transport Protocol (CRTP) extensive output.

Options

none—Display CRTP extensive output for all interfaces.

extensive—(Optional) Display extensive CRTP information.

interface *interface-name*—(Optional) Display CRTP flow statistics for the specified interface. On M Series and T Series routers, a link services IQ (**lsq-*fpc*/*pic*/*port***) or redundant link services IQ (**rlsq-*fpc*/*pic*/*port***) interface.

Required Privilege Level

view

List of Sample Output

show services crtp extensive on page 1835

Output Fields

Table 61 on page 1833 lists the output fields for the **show services crtp** command. Output fields are listed in the approximate order in which they appear.

Table 61: show services crtp Output Fields

Field Name	Field Description
Interface	Name of the physical interface.
Port minimum **Port maximum**	Compression is applied to UDP packets with even ports in the specified range.

Table 61: show services crtp Output Fields *(continued)*

Field Name	Field Description
Maximum UDP compressed sessions	Maximum value of a context identifier in the space of context identifiers allocated for UDP.
CRTP maximum period	Maximum interval between full headers. Suggested value is 256.
CRTP maximum time	Maximum time interval between full headers. Suggested value is 5 seconds.
Compression ratio	Ratio of received packet size to compressed packet size, in percentage. For example, if the packet size is 100 bytes when it is received, and is 40 bytes after compression, the compression ratio is 100 ? 40/100 * 100 = 60%.
Decompression ratio	Ratio of received packet size to decompressed packet size, in percentage. For example, if the packet size is 40 bytes when it is received, and is 100 bytes after compression, the decompression ratio is 100 ? 40/100 * 100 = 60%.
Discards	Number of frames that the incoming packet match code discarded because they were not recognized.
Sessions	Total number of active CRTP sessions.
IP bytes	Number of IP bytes sent and received.
Compressed bytes	Number of compressed IP header bytes sent and received.
CRTP packets	Number of CRTP packets sent and received.
CUDP/CNTCP packets	Number of compressed UDP packets and compressed non-TCP packets sent and received.
Full header packets	Number of full header packets sent and received. Full header packets communicate the uncompressed IP header plus any following headers and data to establish the uncompressed header state in the decompressor for a particular context.

Table 61: show services crtp Output Fields *(continued)*

Field Name	Field Description
Context state packet	Number of context state packets sent and received. Context state packets are sent from the decompressor to the compressor to communicate a list of context IDs for which synchronization is lost or might be lost.
IP packets	Number of IP packets sent and received.
Compressed packets	Number of compressed packets sent and received.

Sample Output

show services crtp extensive

`user@host>` **show services crtp extensive**

```
Interface: lsq-1/1/0.1
  Port minimum: 2000, Port maximum: 64009
  Maximum UDP compressed sessions: 256
  CRTP maximum period: 256, CRTP maximum time: 5
  Compression ratio: 0, Decompression ratio: 0, Discards: 0
  CRTP stats                       Receive         Transmit
  Sessions                               1                1
  IP bytes                              60               60
  Compressed bytes                      61               60
  CRTP packets                           0                0
  CUDP/CNTCP packets                     0                0
  Full header packets                    1                1
  Context state packets                  0                0
  IP packets                             1                1
  Compressed packets                     1                1
```

show services crtp flows

Syntax

```
show services crtp flows
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display Compressed Real-Time Transport Protocol (CRTP) flows.

Options

none—Display CRTP flows for all interfaces.

interface *interface-name*—(Optional) Display CRTP flows for the specified interface. On M Series and T Series routers, a link services IQ (**lsq-*fpc/pic/port***) or redundant link services IQ (**rlsq-*fpc/pic/port***) interface.

Required Privilege Level

view

List of Sample Output

show services crtp flows on page 1837

Output Fields

Table 62 on page 1836 lists the output fields for the **show services crtp flows** command. Output fields are listed in the approximate order in which they appear.

Table 62: show services crtp flows Output Fields

Field Name	Field Description
Interface	Name of the physical interface.
Flow	Received or transmitted flow.
Source	IP source address.
Destination	IP destination address.

Table 62: show services crtp flows Output Fields *(continued)*

Field Name	Field Description
SSRC ID	Synchronization source (SSRC) identifier. One of the fields in the RTP header used to select the context. The SSRC identifier is a randomly chosen value unique within a particular CRTP session.
Ctx ID	Session context ID. Indicates the session context in which to interpret the packet. The decompressor can use the context ID to index its table of stored session contexts directly.

Sample Output

show services crtp flows

`user@host>` **show services crtp flows**

```
Interface: lsq-1/1/0.1
  Flow           Source               Destination          SSRC ID  Ctx ID
  Receive        192.0.2.3:28004      198.51.100.3:26000       123       0
  Transmit       198.51.100.3:26000   192.0.2.3:28004          123       2
```

show services ha detail

Syntax

```
show services ha detail
<interface interface-name>
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series.

Description

Display detailed information for stateful sync processing for a specified interface or for all interfaces.

Options

none—Display detailed information for stateful sync processing for all interfaces.

interface-name—(Optional) Name of a specific interface.

Required Privilege Level

view

RELATED DOCUMENTATION

Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later) | **858**

List of Sample Output

show services ha detail on page 1839

Output Fields

Table 63 on page 1838 lists the output fields for the **show services ha detail** command. Output fields are listed in the approximate order in which they appear.

Table 63: show services ha detail Output Fields

Field Name	Field Description
Interface	Name of the interface for which information is reported.
Inter-chassis	

Table 63: show services ha detail Output Fields *(continued)*

Field Name	Field Description
Role	Role of the interface. • **active**—Active interface. • **backup**–Backup interface.
Connection	Status of the peer connection. • Up • Down
Synchronization	Synchronization state of peers. • Off–Peers are not currently engaged in synchronization.. • Cold–Peers are in a pre-synchronization state. • Hot—Peers are ready for synchronization.
Peers	
Local	Local peer IP address.
Port	Local peer port number.
Remote	Remote peer IP address.
Port	Remote peer port number.

Sample Output

show services ha detail

`user@host>` **show services ha detail**

```
Interface:        ms-7/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 192.0.2.1 Port: 4001, Remote: 192.0.2.2 Port: 4001

Interface:        ms-7/1/0
Inter-chassis:    Role: active, Connection: Down, Synchronization: Off
Peers:           Local: 198.51.100.1 Port: 4001, Remote: 198.51.100.2 Port: 4001
```

```
Interface:        ms-8/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Cold
Peers:            Local: 203.0.113.1 Port: 4001, Remote: 203.0.113.2 Port: 4001

Interface:        ms-8/1/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 10.10.10.1 Port: 4001, Remote: 10.10.10.2 Port: 4001
```

show services ha statistics

Syntax

```
show services ha statistics
<interface interface-name>
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.

Description

Display detailed statistics for stateful sync processing for a specified interface or for all interfaces.

Options

none—Display detailed statistics for stateful sync processing for all interfaces.

interface-name—(Optional) Name of a specific interface.

Required Privilege Level

view

RELATED DOCUMENTATION

> Inter-Chassis Stateful Synchronization for Long Lived NAT and Stateful Firewall Flows (MS-MPC, MS-MIC) Overview (Release 16.1 and later) | **858**

List of Sample Output

show services ha statistics on page 1845

Output Fields

Table 64 on page 1841 lists the output fields for the **show services ha statistics** command. Output fields are listed in the approximate order in which they appear.

Table 64: show services ha statistics Output Fields

Field Name	Field Description
Interface	Interface name.
Inter-chassis	

Table 64: show services ha statistics Output Fields *(continued)*

Field Name	Field Description
Role	Role of the interface. • **active**—Active interface. • **backup**–Backup interface.
Connection	Status of the peer connection. • Up • Down
Synchronization	Synchronization state of peers. • Off–Peers are not currently engaged in synchronization. • Cold–Peers are in a pre-synchronization state. • Hot—Peers are ready for synchronization.
Peers	
Local	Local peer IP address.
Port	Local peer port number.
Remote	Remote peer IP address.
Port	Remote peer port number.
Connection Status	
TCP connection establish	Number of times a TCP connection is established.
TCP connection teardown	Number of times a TCP connection is torn down.
UDP address exchange sent	Number of times a UDP address is sent.
Stateful sync start sent	Number of stateful sync start messages sent by the backup PIC, indicating the start of the cold sync phase.
Stateful sync start received	Number of stateful sync start messages received by active PIC, indicating the start of the cold sync phase.
Cold sync completed count	Number of times the PIC has successfully completed the cold sync phase.
Session Add Statistics	

Table 64: show services ha statistics Output Fields *(continued)*

Field Name	Field Description
Sent	Number of session add statistics sent by the active PIC.
Received	Number of session add statistics received by the backup PIC.
Completed	Number of session adds completed on the active and backup PICs.
rate	Number of sessions currently added per second.
Nack sent	Number of times that a session add failed on the backup PIC, resulting in the sending of a Nack message to the active PIC.
Nack received	Number of Nack messages received from backup PIC due to session add failure.
Add pending	Number of sessions eligible for synchronization, but not yet synchronized.
Session Delete Statistics	
Sent	Number of session deletes sent by the active PIC.
Received	Number of session deletes received by the backup PIC.
Completed	Number of session deletes completed on the active and backup PICs.
rate	Number of sessions currently deleted per second.
Nack sent	Number of times that a session add failed on the backup PIC, resulting in the sending of a Nack message to the active PIC.
Nack received	Number of Nack messages received from backup PIC due to session add failure.
Session not found	Number of sessions not found when session delete was attempted.
Session Error Statistics	
Session attach failures	Number of high-availability extension creation failures on the active PIC.
Session detach failures	Number of high-availability extension deletion failures on the active PIC.
Session extension get failures	Number of times that the high-availability extension is not available when requested.

Table 64: show services ha statistics Output Fields *(continued)*

Field Name	Field Description
Session nullify	Number of times the high-availability session creation failed on the active PIC.
Lookup fail	Number of times session lookup failed because the session has already been released by the infrastructure.
Initiate fail	Number of times session creation failed on the backup PIC.
Activate fail	Number of times session activation failed on the backup PIC.
Illegal flow type	Number of times an illegal flow type occurred on the active and backup PICs.
Illegal service set	Number of times service set extraction failed on backup and active PICs.
Unsupported protocol	Number of times that a session was not backed up because the protocol was neither TCP or UDP.
Send overflow	Number of times buffer overflowed when the high-availability session was created on the active PIC.
Send discard	Number of sessions that not synchronized to the backup, even though they were eligible for synchronization. This occurs whe at least one plugin in the service set indicates that a session should not be synchronized.
Spurious	Number of packets received on the backup PIC for which there are no existing sessions
Process incoming failed	Number of times JMUX header processing failed.
Session ignored	Number of sessions that were eligible for synchronization, but are ignored because stateful sync is not supported for them, such as ALG sessions
JMUX Error Statistics	Synchronization statistics related to the JMUX library.
JMUX begin fail	Number of times that JMUX key verification or header creation failed.
JMUX commit fail	Number of times addition of JMUX data failed.
JMUX flush fail	Number of times a send of JMUX data failed.

Table 64: show services ha statistics Output Fields *(continued)*

Field Name	Field Description
Invalid plugin header	Number of times stateful sync messages were rejected due to an invalid plugin header (internal error).
Invalid plugin name	Number of times stateful sync messages were rejected due to an invalid plugin name (internal error).
Invalid plugin length	Number of times stateful sync messages were rejected due to invalid plugin length (internal error).
Plugin receive error	Number of times installation of plugin information failed on the backup.
Plugin send error	Number of times the plugin failed to pack the extension.
IDL Error Statistics	Statistics concerning encode or decode errors at the backup.
IDL encode fail	Number of times IDL encoding failed on the active and backup PICs.
IDL decode fail	Number of times IDL decoding failed on the active and backup PICs.

Sample Output

show services ha statistics

`user@host>` **show services ha statistics**

```
Interface:        ms-5/0/0
Inter-chassis:    Role: active, Connection: Up, Synchronization: Hot
Peers:            Local: 192.0.2.2 Port: 4001, Remote: 192.0.2.1 Port: 4001
Connection Status:
    TCP connection establish: 8, Teardown: 8
    UDP address exchange sent: 8, Received: 8
    Stateful sync start sent: 0, Received: 8
    Cold sync completed count: 0
Session Add Statistics:
    Sent: 255, Received: 0
    Completed: 255, Rate: 0
    Nack sent: 0, Nack received: 0
    Add pending: 0
Session Delete Statistics:
```

```
    Sent: 255, Received: 0
    Completed: 255, Rate: 0
    Nack sent: 0, Nack received: 0
    Session not found: 0
Session Error Statistics:
   Session attach failures: 0, Session detach failures: 0
    Session extension get failures: 0, Session nullify: 0
    Lookup fail: 0, Initiate fail: 0, Activate fail: 0
    Illegal flow type: 0, Illegal service set: 0
    Unsupported protocol: 0, Send overflow: 0, Send discard: 0
    Spurious: 0, Process incoming failed: 0, Session ignored: 0
JMUX Error Statistics:
    JMUX begin fail: 0, JMUX commit fail: 0, JMUX flush fail: 0
    Invalid plugin header: 0, Invalid plugin name: 0
    Invalid plugin length: 0, Plugin receive error: 0, Plugin send error: 0
IDL Error Statistics:
    IDL encode fail: 0, IDL decode fail: 0
```

show services ids

Syntax

```
show services ids (destination-table | pair-table | source-table)
<brief | extensive | terse>
<destination-prefix destination-prefix-name>
<interface interface-name>
<limit number>
<order  (anomalies | bytes | flows | packets)>
<service-set service-set-name>
<source-prefix source-prefix-name>
<threshold number>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display information about intrusion detection service (IDS) events. All events gathered by IDS are reported as anomalies. For example, events such as **create forward or watch flow**, **FTP passive**, and **FTP active** are genuinely allowed by the stateful firewall but are logged as anomalies to track the rates and number for these events.

Options

destination-table—Display information for an address under possible attack.

pair-table—Display information for a particular suspected attack source and destination address pair.

source-table—Display information for an address that is a suspected attacker.

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

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

interface *interface-name*—(Optional) On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

limit *number*—(Optional) Maximum number of entries to display. By default, all tables display the top 32 entries sorted by the number of events for the criteria chosen. To display additional entries, configure the limit option to set up to 256 entries.

order—(Optional) Display events according to one of the following table-ordering criteria. The default is anomalies.

- **anomalies**—Display information for particular anomalies.
- **bytes**—Order output by number of bytes received.
- **flows**—Order output by number of flows.
- **packets**—Order output by number of packets received.

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

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

threshold *number*—(Optional) Limit the display to events with this number of anomalies, bytes, flows, or packets, whichever criterion you specify for order. For example, to display all events with more than 100 flows, specify order flows and threshold 100.

Required Privilege Level
view

List of Sample Output
show services ids destination-table on page 1852
show services ids destination-table extensive on page 1853
show services ids destination-table extensive order anomalies on page 1853
show services ids pair-table extensive on page 1854
show services ids pair-table extensive limit on page 1854
show services ids source-table extensive on page 1855
show services ids source-table extensive limit on page 1856

Output Fields
Table 65 on page 1848 lists the output fields for the **show services ids** command. Output fields are listed in the approximate order in which they appear.

Table 65: show services ids Output Fields

Field Name	Field Description	Output Level
Interface	Name of an adaptive services interface.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed, but if no service set has any flows, a flow table header is printed for each service set.	All levels
Sorting order	Primary mode to display information: **Anomalies**, **Bytes**, **Flows**, or **Packets**.	All levels
Source address	Name of the source address.	All levels
Dest address	Name of the destination address.	All levels

Table 65: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Time	Total time the information has been in the table.	All levels
Flags	**Flags** can be **Forced**, **F** (terse output only), **SYNcookie**, **S** (terse output only), **Forced+SYNcookie**, and **F+S** (terse output only). The **SYNcookie** flag is visible only in the destination table.	All levels
Application	Configured application, such as **FTP** or **Telnet**.	All levels
Bytes	Total number of bytes sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels
Packets	Total number of packets sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels
Flows	Total number of flows of packets sent from the source to the destination address, in thousands (**k**) or millions (**m**).	All levels
Anomalies	Total number of packets in the anomaly table, in thousands (**k**) or millions (**m**).	All levels

Table 65: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Anomaly description	One or more of the following types of anomalies. For more information, see the detailed descriptions in the stateful firewall section of the System Log Explorer. • **First packet of TCP session not SYN** • **ICMP echo request dropped, because sequence number duplicated** • **ICMP echo reply dropped. No matching sequence number** • **ICMP echo request dropped. Too many echo requests without echo reply** • **ICMP header length check failed** • **ICMP packet length greater than 64K** • **IP fragment assembly timeout** • **IP fragment length error** • **IP fragment overlap** • **IP packet length greater than 64K** • **IP packet too short** • **IP packet with broadcast destination address** • **IP packet with checksum error** • **IP packet with incorrect length** • **IP packet with TTL equal to 0**	**extensive**

Table 65: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Anomaly description (continued)	• **IP packet with version other than 4** • **Land attack (IP src address = dest address)** • **No matching SFW rule; attempting to create discard flow** • **Number of open sessions exceeds IDS limit; packet dropped** • **Packet rate exceeds IDS limit; packet dropped** • **Session creation rate exceeds IDS limit; packet dropped** • **SFW application message too long** • **SFW discard packet contains non-configured IP option types** • **SFW drop packet because of discard flow** • **SFW dropped TCP watch packet** • **SFW rules request FTP active mode data packets to be accepted; attempting to create forward flow** • **SFW rules request FTP passive mode data packets to be accepted; attempting to create forward flow** • **SFW rules request packet to be accepted; attempting to create forward or watch flow** • **SFW rules request packet to be discarded; attempting to create discard flow** • **SFW rules request packet to be rejected; attempting to create reject flow** • **SFW discard flow requires packet to be dropped** • **SFW SYN defense** • **Smurf attack (ping to IP broadcast address)** • **TCP FIN/RST or SYN/(URG|FIN|RST) flags set** • **TCP header length check failed** • **TCP port scan (port not in LISTEN state)** • **TCP seq number zero and FIN/PSH/RST flags set** • **TCP seq number zero and no flags set** • **TCP source or destination port zero** • **TCP SYN flood attack** • **UDP header length check failed** • **UDP port scan (port not in LISTEN state)** • **UDP source or destination port zero**	**extensive**
Count	Number of times that a particular anomaly occurred, in thousands (**k**) or millions (**M**).	**extensive**

Table 65: show services ids Output Fields *(continued)*

Field Name	Field Description	Output Level
Rate (eps)	Anomaly events per second. The IDS subsystem attempts to maintain a weighted average of rates, which might not reflect the exact incoming rate of attack at low rates. However, at high rates exceeding 160 events per second, the rates generally match.	**extensive**
Elapsed	Time since the same type of event last occurred.	**extensive**
Total IDS table entries	Number of entries in the IDS table. This number is not necessarily the sum of all entries displayed.	All levels
Total failed IDS table entry insertions	Number of IDS entries not allowed into the table because the table was full	All levels
Total number of events (closed flows and anomalies detected)	Total number of events since the system was started or since the **show ids services** command was executed.	All levels

Sample Output

show services ids destination-table

`user@host>` **show services ids destination-table**

```
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags            Application

any             ->   10.58.255.146   36m12s SYN cookie
  Bytes:   35.0 m, Packets:  822.0 k, Flows:  274.0 k, Anomalies: 2251.0 k


Total IDS table entries: 87
Total failed IDS table entry insertions 0
Total number of events (closed flows and anomalies detected): 2606018
```

show services ids destination-table extensive

user@host> **show services ids destination-table extensive**

```
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags            Application

any             ->   10.58.255.146   35m52s SYN cookie
  Bytes:   34.0 m, Packets:  798.0 k, Flows:  266.0 k, Anomalies: 2251.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    First packet of TCP session not SYN              160.0 k       0       14s
    TCP source or destination port zero              634.0 k   154.6     3m37s
    UDP source or destination port zero              633.0 k   170.0     3m37s
    ICMP header length check failed                     2875     0.9     3m37s
    IP fragment assembly timeout                     820.0 k    12.8     3m18s
    UDP header length check failed                       385     0.5     3m53s
    TCP header length check failed                       383     0.5     3m53s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2598063
```

show services ids destination-table extensive order anomalies

user@host> **show services ids destination-table extensive order anomalies**

```
Interface: sp-0/2/0, Service set: ss1
IDS sorting order: Anomalies
Source address       Dest address      Time Flags            Application
192.0.2.1        ->  198.51.100.1         1m28s              junos-ftp
  Bytes: 1065, Packets: 18, Flows: 1, Anomalies: 10
   Anomaly description                              Count   Rate(eps)  Elapsed
   creating forward or watch flow                     1     15.6       1m28s
   Number of open sessions exceeds IDS limit          9      0.8         18s

Total IDS table entries:                                3
Total failed IDS table entry insertions                 0
Total number of events (closed flows and anomalies):        11
```

show services ids pair-table extensive

user@host> **show services ids pair-table extensive**

```
Interface: sp-3/2/0, Service set: ss_all_limits
IDS sorting order: Packets
Source address       Dest address      Time Flags             Application
198.51.100.4         198.51.100.4      2m20s                  junos-ftp

  Bytes: 5.7k, Packets: 102.0, Flows: 41.0, Anomalies: 462.0
    Anomaly description                               Count     Rate   Elapsed
    creating forward or watch flow                     41.0      8.8     2m17s

    Packet rate exceeds IDS src limit                  21.0      7.1     2m17s

    Session creation rate exceeds IDS src limit       359.0     99.7     2m16s

    TCP SYN flood attack                               41.0      1.9     1m30s



Total IDS table entries:                                    3
Total failed IDS table entry insertions                     0
Total number of events (closed flows and anomalies):        462
```

show services ids pair-table extensive limit

user@host> **show services ids pair-table extensive limit 3**

```
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application
10.58.255.18    ->   10.58.255.146   38m41s SYN cookie
  Bytes:  286.0 m, Packets: 2823.0 k, Flows:  324.0 k, Anomalies:  387.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    First packet of TCP session not SYN             160.0 k     0.1       25s
    TCP source or destination port zero              69.0 k    14.1     6m26s
    UDP source or destination port zero              68.0 k    12.7     6m26s
    ICMP header length check failed                     318     0.1      7m6s
    IP fragment assembly timeout                     88.0 k     1.3      6m7s
    UDP header length check failed                       39     0.0     6m58s
    TCP header length check failed                       46     0.0     6m45s

10.58.255.23    ->   10.58.255.146   18m48s SYN cookie
  Bytes:  104.0 m, Packets:  421.0 k, Flows:      230, Anomalies:  124.0 k
```

```
    Anomalies                                        Count   Rate(eps) Elapsed
    TCP source or destination port zero               37.0 k     9.8     6m26s
    UDP source or destination port zero               37.0 k     8.4     6m26s
    IP fragment assembly timeout                      48.0 k     1.0      6m7s
    ICMP header length check failed                      190     0.2     6m47s
    UDP header length check failed                        29     0.0     6m51s
    TCP header length check failed                        23     0.0     6m59s

10.58.255.25    ->   10.58.255.146   18m48s SYN cookie
  Bytes:  104.0 m, Packets:  420.0 k, Flows:      232, Anomalies:  123.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    TCP source or destination port zero               37.0 k     9.8      6m26s
    UDP source or destination port zero               37.0 k     8.6      6m26s
    IP fragment assembly timeout                      48.0 k     1.5       6m7s
    ICMP header length check failed                      173     0.1      6m43s
    UDP header length check failed                        24     0.0      6m43s
    TCP header length check failed                        19     0.0      6m56s

Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2659291
```

show services ids source-table extensive

user@host> **show services ids source-table extensive**

```
Interface: sp-3/2/0, Service set: ss_all_limits
IDS sorting order: Packets
Source address       Dest address      Time Flags             Application
198.51.100.4          any              2m43s                  junos-ftp

  Bytes: 5.7k, Packets: 102.0, Flows: 41.0, Anomalies: 462.0
    Anomaly description                               Count     Rate   Elapsed
    creating forward or watch flow                     41.0      8.8     2m40s

    Packet rate exceeds IDS src limit                  21.0      7.1     2m40s

    Session creation rate exceeds IDS src limit       359.0     99.7     2m39s

    TCP SYN flood attack                               41.0      1.9     1m53s
```

```
Total IDS table entries:                                    3
Total failed IDS table entry insertions                     0
Total number of events (closed flows and anomalies):        462
```

show services ids source-table extensive limit

user@host> **show services ids source-table extensive limit 3**

```
Interface: sp-1/3/0, Service set: null-sfw
Sorting order: Packets
Source address       Dest address   Time    Flags             Application

10.58.255.18    ->             any   40m 0s SYN cookie
  Bytes:  250.0 m, Packets: 1978.0 k, Flows:  356.0 k, Anomalies:  387.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    TCP source or destination port zero               37.0 k     9.8     6m26s
    First packet of TCP session not SYN              160.0 k     0.0       40s
    TCP source or destination port zero               69.0 k    62.5     7m45s
    UDP source or destination port zero               68.0 k    56.2     7m45s
    ICMP header length check failed                      319     0.1     7m49s
    IP fragment assembly timeout                      89.0 k     4.4     7m26s
    UDP header length check failed                       39     0.0     8m17s
    TCP header length check failed                       46     0.0      8m4s

10.58.255.30    ->             any   20m 7s SYN cookie
  Bytes:  107.0 m, Packets:  427.0 k, Flows:      264, Anomalies:  125.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    UDP source or destination port zero               38.0 k    65.5     7m45s
    TCP source or destination port zero               37.0 k    38.1     7m45s
    IP fragment assembly timeout                      49.0 k     4.1     7m26s
    TCP header length check failed                       24     0.0     9m23s
    ICMP header length check failed                     165     0.1      8m6s
    UDP header length check failed                       26     0.0     8m13s

10.58.255.17    ->             any   20m10s SYN cookie
  Bytes:  107.0 m, Packets:  426.0 k, Flows:      262, Anomalies:  125.0 k
    Anomalies                                        Count   Rate(eps) Elapsed
    TCP source or destination port zero               38.0 k    55.      7m45s
    UDP source or destination port zero               38.0 k    55.1     7m45s
    ICMP header length check failed                     147     0.1      7m50s
    IP fragment assembly timeout                      49.0 k    2.8      7m26s
    TCP header length check failed                       22     0.0      9m33s
```

```
    UDP header length check failed                        22    0.0       8m1s
Total IDS table entries:
87
Total failed IDS table entry insertions
0
Total number of events (closed flows and anomalies detected):
2691423
Interface: sp-1/3/0, Service set: blue
NAT pool                  Address                   Port         Ports in use
d2-pool             10.59.16.100-10.59.16.100     4000-4002           1
```

show services inline nat pool

Syntax

```
show services inline nat pool
<pool pool--name>
```

Release Information

Command introduced in Junos OS Release 11.4.

Description

Display information about inline Network Address Translation (NAT) pool.

Options

pool-name—Display information about the specified services-inline interface NAT pool.

Required Privilege Level

view

List of Sample Output

show services inline nat pool on page 1859
show services inline nat pool (Network Prefix Translation for IPv6) on page 1859

Output Fields

Table 66 on page 1858 lists the output fields for the **show services inline nat pool** command. Output fields are listed in the order in which they appear.

Table 66: show services inline nat pool Output Fields

Field Name	Field Description
Interface	Name of an **si** interace hosted on a Trio-based line card.
NAT pool	Name of the pool used for address translations.
Translation type	Translation type specified in the applicable NAT rule for the service set.
Address range	Starting and ending public NAT addresses available for translation.
NATed packets	Number of packets translated for the specified pool.
un-NATed packets	Number of received packets that were not translated.

Table 66: show services inline nat pool Output Fields *(continued)*

Field Name	Field Description
deNATed packets	Number of packets that were not translated for the specified service PIC.
Errors	Number of packets with translation errors.

Sample Output

show services inline nat pool

```
user@host> show services inline nat pool p1
```

```
Interface: si-5/0/0, Service set: ss-inat
  NAT pool: p1, Translation type: BASIC NAT44
    Address range: 192.0.2.0-192.0.2.255
    NATed packets: 0, Un-NATed packets: 0, Errors: 0
```

show services inline nat pool (Network Prefix Translation for IPv6)

```
user@host> show services inline nat pool ss_nptv6_pool1
```

```
     Interface: si-4/0/0, Service set: ss_nptv6
           NAT pool: ss_nptv6_pool1, Translation type: NPTV6
                Address range: 2001:db8:3456::/48
                NATed packets: 0, deNATed packets: 0, Errors: 0
```

show services inline nat statistics

Syntax

```
show services inline nat statistics
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 11.4.

Description

Display information about inline Network Address Translation (NAT) address translations.

Options

interface-name—(Optional) Display information about the specified NAT services-inline interface only.

When a specific interface is not specified, statistics for all services-inline interfaces are shown.

Required Privilege Level

view

List of Sample Output

show services inline nat statistics on page 1861
show services inline nat statistics (Network Prefix Translation for IPv6) on page 1862

Output Fields

Table 67 on page 1860 lists the output fields for the **show services inline nat statistics** command. Output fields are listed in the order in which they appear.

Table 67: show services inline nat statistics Output Fields

Field Name	Field Description	Level of Output
Service PIC	Name of an **si** interface hosted on a Trio-based line card.	All levels
Slow path packets received	Number of ICMP exception packets received for NAT translation.	All levels
Slow path packets dropped	Number of received ICMP exception packets that were dropped.	All levels
Service PIC Name	FPC and PIC slots for the service PIC on which NAT processing is performed	All levels
Data Plane Statistics	Information about packets processed by the data plane for NAT operations	All levels

Table 67: show services inline nat statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Control Plane Statistics	Information about packets processed by the control plane for NAT operations	All levels
ICMPv4 errors packets pass through	Number of ICMPv4 error packets that were passed through without being subjected to rules	All levels
ICMPv4 errors packets locally generated	Number of ICMPv4 error packets that were locally generated	All levels
ICMPv6 errors packets pass through	Number of ICMPv6 error packets that were passed through without being subjected to rules	All levels
ICMPv6 errors packets locally generated	Number of ICMPv6 error packets that were locally generated	All levels
Dropped packets	Number of packets dropped during inline NAT processing	All levels
NATed packets	Number of packets translated for the specified service PIC.	All levels
deNATed packets	Number of packets that were not translated for the specified service PIC.	All levels
Errors	Number of packets with translation errors.	All levels

Sample Output

show services inline nat statistics

`user@host>` **show services inline nat statistics**

```
Service PIC Name                                    :si-5/0/0

     Slow path packets received                        :0
     Slow path packets dropped                         :0
```

show services inline nat statistics (Network Prefix Translation for IPv6)

```
user@host> show services inline nat statistics
```

```
Service PIC Name                                                  :si-4/0/0


 Control Plane Statistics
     ICMPv4 errors packets pass through                                :0
     ICMPv4 errors packets locally generated                           :0
     ICMPv6 errors packets pass through                                :0
     ICMPv6 errors packets locally generated                           :0
     Dropped packets                                                   :0

  Data Plane Statistics
     NATed packets                                                     :0
     deNATed packets                                                   :0
     Errors                                                            :0

Service PIC Name                                                    :si-4/1/0


 Control Plane Statistics
     ICMPv4 errors packets pass through                                :0
     ICMPv4 errors packets locally generated                           :0
     ICMPv6 errors packets pass through                                :0
     ICMPv6 errors packets locally generated                           :0
     Dropped packets                                                   :0

  Data Plane Statistics
     NATed packets                                                     :0
     deNATed packets                                                   :0
     Errors                                                            :0
```

show services inline softwire statistics

Syntax

```
show services inline softwire statistics
<interface interface-name>
<mape name>
<v6rd>
```

Release Information

Command introduced in Junos OS Release 13.3R3.
map-e option introduced in Junos OS Release 18.2R1 for MX Series Routers with MPC and MIC interfaces.
map-e option introduced in Junos OS Release 20.2R1 for Next Gen Services on MX240, MX480 and MX960 routers.

Description

Display information about inline softwire activity.

Options

interface *interface-name*—(Optional) Display information about the specified services-inline interface only.
When a specific interface is not specified, statistics for all services-inline interfaces are shown.

mape *name*—(Optional) Display information on per physical service interface basis.

v6rd—(Optional) Display information for 6rd.

Required Privilege Level

view

List of Sample Output

show services inline softwire statistics on page 1865
show services inline softwire statistics mape (Adaptive Services si- interfaces) on page 1866
show services inline softwire statistics mape (Next Gen Services si- interfaces) on page 1867

Output Fields

Table 68 on page 1863 lists the output fields for the **show services inline softwire statistics** command. Output fields are listed in the order in which they appear.

Table 68: show services inline softwire statistics Output Fields

Field Name	Field Description
Service PIC Name	Name of the service PIC for which statistics are displayed.

Table 68: show services inline softwire statistics Output Fields *(continued)*

Field Name	Field Description
Control Plane Statistics	Statistics on the control plane.
ICMPv4 echo requests to softwire concentrator	Number of ICMPv4 echo received by the softwire concentrator. IPv6 ICMP type = 128, code =0. destined to BR IPv6 address
ICMPv4 echo responses from softwire concentrator	Number of ICMPv4 echo responses sent from the softwire concentrator or BR. IPv6 ICMP type = 129
Dropped ICMPv4 packets to softwire concentrator	Number of ICMP packets (except ICMP request) received by the softwire concentrator or BR. All these packets are dropped in by the packet forwarding engine Ukernel.
Trace route UDP packets to softwire concentrator	Number of UDP trace route packets (port numbers 33434 through 33534) received by the softwire concentrator.
ICMPv4 Port unreachable errors sent from softwire concentrator	Number of ICMP port unreachable errors sent by the softwire concentrator after receiving the UDP trace route packets.
Other dropped IPv4 packets to softwire concentrator	Number of non-ICMPpackets that were received and dropped because of fragmentation during encapsulation or decapsulation.
Data Plane Statistics	Statistics of the data plane.
6rd decaps	Number of 6rd decapsulated packets and bytes in the data plane. Decapsulation includes removing the outer IPv4 header and routing the inner IPv6 packet.
6rd encaps	Number of 6rd encapsulted (IPv4) packets and bytes in the data plane.

Table 68: show services inline softwire statistics Output Fields *(continued)*

Field Name	Field Description
6rd decap errors	Number of all the packets and bytes that are not IPv4-IPv6, IPv4-UDP, or IPV4-ICMP packets.
6rd decap fragment errors	Number of IPv4 fragmented packets and bytes.
6rd decap spoof attacks	Number of spoof attack packets and bytes, which includes packets for which the 6rd derived IPv4 address does not match with the source IPv4 address and packets for which the source IPv6 prefix does not match the 6rd IPv6 prefix.
6rd encap v4 mtu errors	Count of packets and bytes with IPv4 encapsulation MTU errors. For downlink packets after encapsulating with an IPv4 header, if the packet length is more than Tunnel MTU then it is dropped as v4 MTU errors. For these packet drops, an ICMPv6 packet too big error is sent back to the sender.
Data Plane Statistics (MAP-E upstream)	
MAPE decaps	IPv6 packets successfully decapsulated by BR (includes reassembled IPv6)
MAPE ICMP decap errors	IPv6 packets dropped due to unsupported type/code of inner ICMPv4
MAPE decap spoof errors	IPv6 Packets that failed MAPE spoof check

Sample Output

show services inline softwire statistics

`user@host>` **show services inline softwire statistics**

```
Border Router v6rd statistics:

 Service PIC Name                                    si-0/0/0
```

```
Control Plane Statistics
    ICMPv4 echo requests to softwire concentrator                    0
    ICMPv4 echo responses from softwire concentrator                 0
    Dropped ICMPv4 packets to softwire concentrator                  0
    Trace route UDP packets to softwire concentrator                 0
    ICMPv4 Port unreachable errors sent from softwire concentrator   0
    Other dropped IPv4 packets to softwire concentrator              0

 Data Plane Statistics           Packets                  Bytes
   6rd decaps                    32222173891              3061106519645
   6rd encaps                    415480622                28252710148
   6rd decap errors              0                        0
   6rd decap fragment errors     0                        0
   6rd decap spoof attacks       0                        0


Service PIC Name                                    si-0/2/0

Control Plane Statistics
    ICMPv4 echo requests to softwire concentrator                    0
    ICMPv4 echo responses from softwire concentrator                 0
    Dropped ICMPv4 packets to softwire concentrator                  0
    Trace route UDP packets to softwire concentrator                 0
    ICMPv4 Port unreachable errors sent from softwire concentrator   0
    Other dropped IPv4 packets to softwire concentrator              0

Data Plane Statistics           Packets                  Bytes
    6rd decaps                    0                        0
    6rd encaps                    0                        0
    6rd decap errors              0                        0
    6rd decap fragment errors     0                        0
    6rd decap spoof attacks       0                        0
    6rd encap v4 mtu errors       0                        0
```

show services inline softwire statistics mape (Adaptive Services si- interfaces)

`user@host>` **show services inline softwire statistics mape**

```
Service PIC Name                                    si-0/0/0

Statistics              Packets                 Bytes

     MAP-E  decaps                  0                     0
```

```
    MAP-E  encaps                    0                    0

    MAP-E  decap errors              0                    0

    MAP-E  encap errors              0                    0

    MAP-E decap spoof attacks         0                    0

    MAP-E decap v4 fragmented        0                    0

    MAP-E decap v4 reassembled       0                    0

    MAP-E encap v4 mtu errors         0                    0
```

show services inline softwire statistics mape (Next Gen Services si- interfaces)

`user@host>` **show services inline softwire statistics mape**

```
Service PIC Name                                    si-2/0/0

 Control Plane Statistics
     MAPE ICMPv6 echo requests to softwire concentrator          0
     MAPE ICMPv6 echo responses from softwire concentrator       0
     MAPE Dropped ICMPv6 packets to softwire concentrator        0

 Data Plane Statistics (v6-to-v4)      Packets                 Bytes
     MAPE decaps                        0                      0
     MAPE ICMP decap errors             0                      0
     MAPE decap spoof errors            0                      0
     MAPE v6 reassembled                0                      0
     MAPE dropped v6 fragments          0                      0
     MAPE v6 unsupp protocol drops      0                      0


 Data Plane Statistics (v4-to-v6)      Packets                 Bytes
     MAPE encaps                        0                      0
     MAPE ICMP encap errors             0                      0
     MAPE v6 mtu errors                 0                      0
     MAPE v4 reassembled                0                      0
     MAPE dropped v4 fragments          0                      0
```

show services ipsec-vpn certificates

Syntax

```
show services ipsec-vpn certificates
<brief | detail>
<service-set service-set>
```

Release Information

Command introduced in Junos OS Release 7.5.

Description

(Adaptive services interfaces only) Display local and remote certificates installed in the IPsec configuration memory cache that are used for the IKE negotiation.

Options

none—(same as brief) Display information about local and remote certificates associated with all service sets.

brief | detail—(Optional) Display the specified level of output.

service-set *service-set*—(Optional) Display information about local and remote certificates associated with only the specified service set.

Required Privilege Level

view

List of Sample Output

show services ipsec-vpn certificates on page 1869
show security ipsec-vpn certificates detail on page 1870

Output Fields

Table 69 on page 1868 lists the output fields for the **show services ipsec-vpn certificates** command. Output fields are listed in the approximate order in which they appear.

Table 69: show services ipsec-vpn certificates Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the IPsec service set.	All levels
Total entries	Number of certificate cache entries.	All levels
Certificate cache entry	Identification number of the certificate cache entry.	All levels

Table 69: show services ipsec-vpn certificates Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flags	Information about the digital certificate, including whether the certificate is a root certificate and trusted.	none **brief**
Issued to	Device that was issued the digital certificate.	none **brief**
Issued by	Authority that issued the digital certificate.	none **brief**
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	All levels
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	none **brief**
Public key algorithm	Specifies the encryption algorithm used with the private key, such as **rsaEncryption (1024 bits)**.	**detail**
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show services ipsec-vpn certificates

```
user@host> show services ipsec-vpn certificates
```

```
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Flags: Non-root Trusted
    Issued to: router3.example.com, Issued by: juniper
    Alternate subject: router3.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:33:58 GMT
      Not after: 2008 Nov 22nd, 00:03:58 GMT

 Certificate cache entry: 2
    Flags: Non-root Trusted
    Issued to: router2.example.com, Issued by: juniper
    Alternate subject: router2.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:28:22 GMT
      Not after: 2008 Nov 21st, 23:58:22 GMT

  Certificate cache entry: 1
    Flags: Root Trusted
    Issued to: juniper, Issued by: juniper
    Validity:
      Not before: 2005 Oct 18th, 23:54:22 GMT
      Not after: 2025 Oct 19th, 00:24:22 GMT
```

show security ipsec-vpn certificates detail

`user@host>` **show services ipsec-vpn certificates detail**

```
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Certificate version: 3
    Serial number: 4355 94f9
    Alternate subject: router3.example.com
    Public key algorithm: rsaEncryption
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
      60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
    Distribution CRL:
      C=us, O=juniper, CN=CRL1
      http://CA-1/CRL/juniper_us_crlfile.crl
    Use for key: Digital signature

  Certificate cache entry: 2
```

```
  Certificate version: 3
  Serial number: 4355 94f8
  Alternate subject: router2.example.com
  Public key algorithm: rsaEncryption
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    30:c3:a4:04:da:33:9d:60:23:5a:48:75:48:2c:f0:c6:96:6c:31:fa (sha1)
    9a:a2:ce:ef:7e:10:80:a0:c8:4d:2f:e7:e1:d3:69:9d (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature

Certificate cache entry: 1
  Certificate version: 3
  Flags: Root
  Serial number: 4355 9235
  Public key algorithm: rsaEncryption
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
```

show services ipsec-vpn ike security-associations

Syntax

```
show services ipsec-vpn ike security-associations
<brief | detail>
<peer-address>
```

Release Information

Command introduced before Junos OS Release 7.4.
Statistics for Internet Key Exchange (IKE) security associations for each services PIC introduced in Junos OS Release 12.1.

Description

(Adaptive services interface only) Display information for Internet Key Exchange (IKE) security associations. If no security association is specified, the information for all security associations is displayed.

Options

none—(same as brief) Display standard information for all IPsec security associations.

brief | detail—(Optional) Display the specified level of output.

peer-address—(Optional) Display information about a particular security association address.

Required Privilege Level

view

List of Sample Output

show services ipsec-vpn ike security-associations on page 1875
show services ipsec-vpn ike security-associations detail on page 1876
show services ipsec-vpn ike security-associations (on ACX500 Routers) on page 1877

Output Fields

Table 70 on page 1872 lists the output fields for the **show services ipsec-vpn ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 70: show services ipsec-vpn ike security-associations Output Fields

Field Name	Field Description	Level of Output
IKE peer	Remote end of the IKE negotiation.	**detail**
Role	Part played in the IKE session. The router triggering the IKE negotiation is the initiator, and the router accepting the first IKE exchange packets is the responder.	**detail**

Table 70: show services ipsec-vpn ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote Address	Responder's address.	none specified
State	State of the IKE security association: • **Matured**—IKE security association is established. • **Not matured**—The IKE security association is in the process of negotiation.	none specified
Initiator cookie	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels
Responder cookie	The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received. Of the numerous security services available, protection against denial of service (DoS) is one of the most difficult to address. A “cookie” or anticlogging token (ACT) is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. An exchange prior to CPU-intensive public key operations can thwart some DoS attempts (such as simple flooding with invalid IP source addresses).	All levels
Exchange type	Specifies the number of messages in an IKE exchange, and the payload types that are contained in each message. Each exchange type provides a particular set of security services, such as anonymity of the participants, perfect forward secrecy of the keying material, and authentication of the participants. Junos OS supports two types of exchanges: • **Main**—The exchange is done with six messages. **Main** encrypts the payload, protecting the identity of the neighbor. • **Aggressive**—The exchange is done with three messages. **Aggressive** does not encrypt the payload, leaving the identity of the neighbor unprotected. • **IKEv2**—The exchange is negotiated using IKE version 2.	All levels
PIC	The services PIC for which the IKE security associations are displayed.	All levels

Table 70: show services ipsec-vpn ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Authentication method	Authentication method that determines which payloads are exchanged and when they are exchanged. Value can be ECDSA-signatures (256 bit key), ECDSA-signatures (384 bit key), Pre-shared-keys, or RSA-signatures. **NOTE:** In Junos FIPS mode, ECDSA is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, ECDSA is supported in Junos FIPS mode.	**detail**
Local	Prefix and port number of the local end.	**detail**
Remote	Prefix and port number of the remote end.	**detail**
Lifetime	Number of seconds remaining until the IKE security association expires.	**detail**
Algorithms	Header for the IKE algorithms output. • **Authentication**—(**detail** output only) Type of authentication algorithm used: **md5** or **sha1** • **Encryption**—(**detail** output only) Type of encryption algorithm used: **des-cbc**, **3des-cbc**, or **None**. • **Pseudo random function**—Function that generates highly unpredictable random numbers: **hmac-md5** or **hmac-sha1**.	**detail**
Traffic statistics	Number of bytes and packets received and transmitted on the IKE security association. • **Input bytes, Output bytes**—Number of bytes received and transmitted on the IKE security association. • **Input packets, Output packets**—Number of packets received and transmitted on the IKE security association.	**detail**
Flags	Notification to the key management process of the status of the IKE negotiation: • **caller notification sent**—Caller program notified about the completion of the IKE negotiation. • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.	**detail**

Table 70: show services ipsec-vpn ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
IPsec security associates	Number of IPsec security associations created and deleted with this IKE security association.	**detail**

Phase 2 negotiations in progress	Number of phase 2 negotiations in progress and status information:
	• Negotiation type—Type of phase 2 negotiation. The Junos OS currently supports **quick mode**.
	• Message ID—Unique identifier for a phase 2 negotiation.
	• Local identity—Identity of the local phase 2 negotiation. The format is ***id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*)**.
	• Remote identity—Identity of the remote phase 2 negotiation. The format is ***id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*)**
	• Flags—Notification to the key management process of the status of the IKE negotiation:
	  • **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.
		detail

Sample Output

show services ipsec-vpn ike security-associations

`user@host>` **show services ipsec-vpn ike security-associations**

```
Remote Address  State        Initiator cookie  Responder cookie  Exchange type

192.0.2.1        Matured       062d291d21275fc7  82ef00e3d1f1c981  Main

192.0.2.2        Matured       cd6d581d7bb1664d  88a707779f3ad8d1  Main
```

```
192.0.2.3         Matured       86621051e3e78360  6bc5cc83fd67baa4  IKEv2


PIC: sp-0/3/0

192.0.2.7         Matured       565e2813075e6fdb  67886757a74edcd6  IKEv2
```

show services ipsec-vpn ike security-associations detail

user@host> **show services ipsec-vpn ike security-associations detail**

```
IKE peer 198.51.100.2
      Role: Responder, State: Matured
      Initiator cookie: d91c9f20f78e1d4e, Responder cookie: 727a04ed8d5021a1
      Exchange type: IKEv2, Authentication method: Pre-shared-keys
      Local: 2013.0.113.2:500, Remote: 198.51.100:500
      Lifetime: Expires in 1357 seconds
      Algorithms:
       Authentication        : sha1
       Encryption            : 3des-cbc
       Pseudo random function: hmac-sha1
      Traffic statistics:
       Input  bytes  :               22244
       Output bytes  :               22236
       Input  packets:                 263
       Output packets:                 263
      Flags: Caller notification sent
      IPSec security associations: 0 created, 0 deleted
      Phase 2 negotiations in progress: 0

IKE peer 192.0.2.4
  Role: Initiator, State: Matured
  Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  Lifetime: Expires in 187 seconds
  Algorithms:
   Authentication        : md5
   Encryption            : 3des-cbc
   Pseudo random function: hmac-md5
  Traffic statistics:
   Input  bytes  :                1000
   Output bytes  :                1280
```

```
   Input  packets:                   5
   Output packets:                   9
  Flags: Caller notification sent
  IPsec security associations: 2 created, 0 deleted
  Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 3582889153
    Local: 192.0.2.5:500, Remote: 192.0.2.4:500
    Local identity: ipv4_subnet(tcp:80,[0..7]=10.1.1.0/24)
    Remote identity: ipv4_subnet(tcp:100,[0..7]=10.1.2.0/24)
    Flags: Caller notification sent, Waiting for done
```

show services ipsec-vpn ike security-associations (on ACX500 Routers)

user@host> **show services ipsec-vpn ike security-associations**

```
Remote Address  State         Initiator cookie  Responder cookie  Exchange type
192.168.10.130  Matured       90864887dfecb178  9a2ee2ab786f960d  Main
192.168.20.130  Matured       1dd17732a8c9b13a  b06e5072ac7362bf  Main
192.0.2.7       Matured       565e2813075e6fdb  67886757a74edcd6  IKEv2
```

show services ipsec-vpn ipsec security-associations

Syntax

```
show services ipsec-vpn ipsec security-associations
<brief | detail | extensive>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(Adaptive services interface only) Display IPsec security associations for the specified service set. If no service set is specified, the security associations for all service sets are displayed.

Options

none—Display standard information about IPsec security associations for all service sets.

brief | detail | extensive—(Optional) Display the specified level of output.

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

Required Privilege Level

view

List of Sample Output

show services ipsec-vpn ipsec security associations extensive on page 1882
show services ipsec-vpn ipsec security associations detail on page 1883
show services ipsec-vpn ipsec security associations (on ACX500 Routers) on page 1884

Output Fields

Table 71 on page 1878 lists the output fields for the **show services ipsec-vpn ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 71: show services ipsec-vpn ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec security associations are defined. If appropriate, includes the outside service interface VRF name.	All levels
Rule	Name of the rule set applied to the security association.	**detail extensive**
Term	Name of the IPsec term applied to the security association.	**detail extensive**

Table 71: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	**detail extensive**
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
IPsec inside interface	Name of the logical interface hosting the IPsec tunnels.	All levels
Tunnel MTU	MTU of the IPsec tunnel.	All levels
Total uptime	Total amount of time that an IPsec tunnel has been up across security association rekeys.	**detail**
Local identity	Protocol, address or prefix, and port number of the local entity of the IPsec association. The format is **id-type-name (proto-name:port-number,[0..*id-data-len*] = *iddata-presentation*)**. The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the ***id-data-len*** parameter can be one of the following, depending on the address configured in the IPsec rule: • For an IPv4 address, the length is 4 and the value displayed is 3. • For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. • For a range of IPv4 addresses, the length is 8 and the value displayed is 7. • For an IPv6 address prefix, the length is 16 and the value displayed is 15. • For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. • For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. The value of the ***id-data-presentation*** field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the local peer of the IPsec association, it is displayed instead of the address details.	All levels

Table 71: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote identity	Protocol, address or prefix, and port number of the remote entity of the IPsec association. The format is **id-type-name (proto-name:port-number,[0..*id-data-len*] = *iddata-presentation*)**. The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the ***id-data-len*** parameter can be one of the following, depending on the address configured in the IPsec rule: • For an IPv4 address, the length is 4 and the value displayed is 3. • For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. • For a range of IPv4 addresses, the length is 8 and the value displayed is 7. • For an IPv6 address prefix, the length is 16 and the value displayed is 15. • For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. • For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. The value of the ***id-data-presentation*** field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the remote peer of the IPsec association, it is displayed instead of the address details.	All levels
Primary remote gateway	IP address of the configured primary remote peer.	All levels
Backup remote gateway	IP address of the configured backup remote peer.	All levels
State	State of the primary or backup interface: **Active**, **Offline**, or **Standby**. Both ES PICs are initialized to **Offline**. For primary and backup peers, **State** can be **Active** or **Standby**. If both peers are in a state of **Standby**, no connection exists yet between the two peers.	All levels
Failover counter	Number of times a PIC switched between primary and backup interfaces, or the number of times the tunnel switched between the primary and remote peers since the software has been activated.	All levels
Direction	Direction of the security association: **inbound** or **outbound**.	All levels

Table 71: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index. • When the value of **Protocol** is **AH** or **ESP**, **AUX-SPI** is always **0**. • When the value of **Protocol** is **AH+ESP**, **AUX-SPI** is always a positive integer.	All levels
Mode	Mode of the security association: • **transport**—Protects single host-to-host protections. • **tunnel**—Protects connections between security gateways.	**detail extensive**
Type	Type of security association: • **manual**—Security parameters require no negotiation. They are static, and are configured by the user. • **dynamic**—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode.	**detail extensive**
State	Status of the security association: • **Installed**—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) • **Not installed**—The security association is not installed in the security association database.	**detail extensive**
Protocol	Protocol supported: • **transport** mode supports Encapsulation Security Protocol (**ESP**) or Authentication Header (**AH**). • **tunnel** mode supports **ESP** or **AH+ESP**.	All levels
Authentication	Type of authentication used: **hmac-md5-96**, **hmac-sha1-96**, or **none**.	**detail extensive**
Encryption	Type of encryption algorithm used: can be **3des-cbc**, **aes-cbc (128 bits)**, **aes-cbc (192 bits)**, **aes-cbc (256 bits)**, **aes-gcm (128 bits)**, **aes-gcm(192 bits)**, **aes-gcm (256 bits)**, **des-cbc**, or **None**. **NOTE:** In Junos FIPS mode, AES-GCM is not supported in Junos OS Release 17.3R1. Starting in Junos OS Release 17.4R1, AES-GCM is supported in Junos FIPS mode.	**detail**

Table 71: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Soft lifetime **Hard lifetime**	Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This information allows the key management system to negotiate a new SA before the hard lifetime expires. • **Expires in** *seconds* **seconds**—Number of seconds left until the security association expires. • **Expires in** *kilobytes* **kilobytes**—Number of kilobytes left until the security association expires.	**detail extensive**
Anti-replay service	State of the service that prevents packets from being replayed: **Enabled** or **Disabled**.	**detail extensive**
SA lifetime	Configured hard lifetime (total lifetime), in seconds, for the security association.	**detail**
Replay window size	Configured size, in packets, of the antireplay service window: **32** or **64**. The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is **0**, antireplay service is disabled.	**detail**
disable-natt	Configure to disable NAT-T functionality. By default the NAT-T is enabled.	All levels.
nat-keepalive	Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.	All levels.

Sample Output

show services ipsec-vpn ipsec security associations extensive

`user@host>` **show services ipsec-vpn ipsec security-associations extensive**

```
Service set: service-set-1
  Rule: _junos_, Term: term-1, Tunnel index: 1
  Local gateway: 192.0.2.2, Remote gateway: 198.51.100.4
  IPSec inside interface: sp-2/0/0.1  Local identity:
```

```
ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Primary remote gateway: 192.0.2.1, State: Standby
  Backup remote gateway: 198.51.100.4, State: Active
  Failover counter: 1

   Direction: inbound, SPI: 3743521590, AUX-SPI: 0
   Mode: tunnel, Type: dynamic, State: Installed
   Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
   Soft lifetime: Expires in 23043 seconds
   Hard lifetime: Expires in 23178 seconds
   Anti-replay service: Enabled, Replay window size: 64

   Direction: outbound, SPI: 2551045240, AUX-SPI: 0
   Mode: tunnel, Type: dynamic, State: Installed
   Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
   Soft lifetime: Expires in 23043 seconds
   Hard lifetime: Expires in 23178 seconds
   Anti-replay service: Enabled, Replay window size: 64

disable-natt: No, nat-keepalive: 10
```

show services ipsec-vpn ipsec security associations detail

user@host> **show services ipsec-vpn ipsec security-associations detail**

```
Service set: ipsec-sset-0, IKE Routing-instance: default

  Rule: ipsec-rule-0, Term: term0, Tunnel index: 1
  Local gateway: 192.0.2.1, Remote gateway: 192.0.2.2
  IPSec inside interface: ms-3/0/0.1, Tunnel MTU: 1500
  UDP encapsulate: Disabled, UDP Destination port: 0
  Local identity: ipv4_subnet(any:0,[0..7]=198.51.100.0/16)
  Remote identity: ipv4_subnet(any:0,[0..7]=203.0.113.0/16)
  NATT Detection: Not Detected, NATT keepalive interval: 0
  Total uptime:  0 days 0 hrs 1 mins 4 secs

  Direction: inbound, SPI: 4004530393, AUX-SPI: 0
  Mode: tunnel, Type: dynamic, State: Installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
  Soft lifetime: Expires in 27885 seconds
  Hard lifetime: Expires in 28736 seconds
  Anti-replay service: Enabled, Replay window size: 4096
  Copy ToS: Enabled
```

```
  Copy TTL: Disabled, TTL value: 64
  SA lifetime: 28800 seconds

  Direction: outbound, SPI: 1323638473, AUX-SPI: 0
  Mode: tunnel, Type: dynamic, State: Installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
  Soft lifetime: Expires in 27885 seconds
  Hard lifetime: Expires in 28736 seconds
  Anti-replay service: Enabled, Replay window size: 4096
  Copy ToS: Enabled
  Copy TTL: Disabled, TTL value: 64
  SA lifetime: 28800 seconds
```

show services ipsec-vpn ipsec security associations (on ACX500 Routers)

`user@host>` **show services ipsec-vpn ipsec security-associations**

```
Service set: SS_1, IKE Routing-instance: Customer-1

  Rule: rule_1, Term: 1, Tunnel index: 2
  Local gateway: 192.168.1.11, Remote gateway: 192.168.10.130
  IPSec inside interface: ms-0/2/0.8, Tunnel MTU: 1300
  UDP encapsulate: Disabled, UDP Destination port: 0
    Direction SPI         AUX-SPI     Mode       Type     Protocol
    inbound   2204677182  0           tunnel     dynamic  ESP
    outbound  3015420439  0           tunnel     dynamic  ESP

Service set: SS_2, IKE Routing-instance: Customer-1

  Rule: Customer-1_rule_1, Term: 1, Tunnel index: 1
  Local gateway: 192.168.1.12, Remote gateway: 192.168.20.130
  IPSec inside interface: ms-0/2/0.7, Tunnel MTU: 1300
  UDP encapsulate: Disabled, UDP Destination port: 0
    Direction SPI         AUX-SPI     Mode       Type     Protocol
    inbound   2093089828  0           tunnel     dynamic  ESP
    outbound  2160146627  0           tunnel     dynamic  ESP
```

show services ipsec-vpn ipsec statistics

Syntax

```
show services ipsec-vpn ipsec statistics
<brief | detail>
<remote-gw remote-peer-address>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
New fields added in Junos OS Release 10.0.

Description

(Adaptive services interface only) Display IPsec statistics for the specified service set. If no service set is specified, the statistics for all service sets are displayed.

Options

none—Display standard IPsec statistics for all service sets.

brief | detail—(Optional) Display the specified level of output.

remote-gw *remote-peer-address*—(Optional) Display IPsec statistics for an individual IPsec tunnel and an individual remote host.

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

Required Privilege Level

view

List of Sample Output

show services ipsec-vpn ipsec statistics detail on page 1887
show services ipsec-vpn ipsec statistics remote-gw on page 1888
show services ipsec-vpn ipsec statistics (on ACX500) on page 1888

Output Fields

Table 72 on page 1885 lists the output fields for the **show services ipsec-vpn ipsec statistics** command. Output fields are listed in the approximate order in which they appear.

Table 72: show services ipsec-vpn ipsec statistics Output Fields

Field Name	Field Description	Level of Output
PIC	The physical interface on which the IPsec tunnel is configured.	All levels

Table 72: show services ipsec-vpn ipsec statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec tunnel is defined.	All levels
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	All levels
ESP statistics	Encapsulation Security Payload (ESP) statistics: • **Encrypted bytes**—Total number of bytes encrypted by the local system across the IPsec tunnel. • **Decrypted bytes**—Total number of bytes decrypted by the local system across the IPsec tunnel. • **Encrypted packets**—Total number of packets encrypted by the local system across the IPsec tunnel. • **Decrypted packets**—Total number of packets decrypted by the local system across the IPsec tunnel	All levels
AH Statistics	Authentication Header statistics: • **Input bytes**—Total number of bytes received by the local system across the IPsec tunnel. • **Output bytes**—Total number of bytes transmitted by the local system across the IPsec tunnel. • **Input packets**—Total number of packets received by the local system across the IPsec tunnel. • **Output packets**—Total number of packets transmitted by the local system across the IPsec tunnel.	All levels

Table 72: show services ipsec-vpn ipsec statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Errors	• **AH authentication failures**—Number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel. • **ESP authentication failures**—Number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets. • **ESP Decryption failures**—Number of ESP decryption failures. • **Bad headers**—Number of invalid headers detected. • **Bad trailers**—Number of invalid trailers detected. • **Replay before window drops**—Number of replay errors. A replay error is generated when a duplicate packet is received within the replay window. • **Replayed pkts**—Number of packets replayed. • **IP integrity errors**—Number of IP integrity errors. • **Exceeds tunnel MTU**—Number of times the tunnel maximum transmission unit (MTU) value was exceeded. • **Rule lookup failures**—Number of rule lookup failures. • **No SA errors**—Number of errors resulting from a missing security association (SA). • **Flow errors**—Number of flow errors. • **Misc errors**—Number of miscellaneous errors.	All levels

Sample Output

show services ipsec-vpn ipsec statistics detail

`user@host>` **show services ipsec-vpn ipsec statistics**

```
PIC: sp-0/2/0, Service set: ss0

ESP Statistics:
  Encrypted bytes:               0
  Decrypted bytes:               0
  Encrypted packets:             0
  Decrypted packets:             0
AH Statistics:
  Input bytes:                 168
```

```
  Output bytes:                168
  Input packets:                 2
  Output packets:                2
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

show services ipsec-vpn ipsec statistics remote-gw

user@host> **show services ipsec-vpn ipsec statistics remote-gw 192.0.2.1**

```
PIC: sp-3/1/0, Service set: service-set-2
Local gateway: 198.51.100.1, Remote gateway: 192.0.2.1, Tunnel index: 2
ESP Statistics:
 Encrypted bytes:               0
 Decrypted bytes:               0
 Encrypted packets:             0
 Decrypted packets:             0
AH Statistics:
 Input bytes:                   0
 Output bytes:                  0
 Input packets:                 0
 Output packets:                0
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

show services ipsec-vpn ipsec statistics (on ACX500)

user@host> **show services ipsec-vpn ipsec statistics**

```
PIC: ms-0/2/0, Service set: SS_1

ESP Statistics:
  Encrypted bytes:          4121664
  Decrypted bytes:           151584
  Encrypted packets:          64162
  Decrypted packets:           1579
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 3, No SA errors: 0
  Flow errors: 0, Misc errors: 0


PIC: ms-0/2/0, Service set: SS_2

ESP Statistics:
  Encrypted bytes:              576
  Decrypted bytes:              576
  Encrypted packets:              6
  Decrypted packets:              6
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
```

```
Rule lookup failures: 0, No SA errors: 0
Flow errors: 0, Misc errors: 0
```

show services link-services cpu-usage

Syntax

```
show services link-services cpu-usage
<brief | detail>
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 8.4.

Description

(M Series and T Series routers only) Display information about Link Services IQ (LSQ) CPU usage.

Options

none—Display standard information about CPU usage for all LSQ interfaces.

brief | detail—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display information about the specified LSQ interface.

Required Privilege Level

view

List of Sample Output

show services link-services cpu-usage brief (AS PIC) on page 1893
show services link-services cpu-usage brief (MultiServices PIC) on page 1894
show services link-services cpu-usage detail (AS PIC) on page 1894
show services link-services cpu-usage detail (MultiServices PIC) on page 1895

Output Fields

Table 73 on page 1891 lists the output fields for the **show services link-services cpu-usage** command. Output fields are listed in the approximate order in which they appear.

Table 73: show services link-services cpu-usage Output Fields

Field Name	Field Description	Level of Output
Role	CPU functional category.	**brief**
1 Second Average	Percentage of usage during 1-second duration.	All levels
5 Second Average	Percentage of usage during 5-second duration.	All levels

Table 73: show services link-services cpu-usage Output Fields *(continued)*

Field Name	Field Description	Level of Output
QoS	Quality of service (QoS) CPU, which takes care of queuing and scheduling of incoming IP packets on a per-bundle basis. It schedules packets with higher QoS values first.	All levels
Sequencer	Assigns sequence numbers to outgoing MLPPP fragments and interleaves link fragmentation and interleaving (LFI) traffic.	All levels
Load Balancer	Distributes load across different fragmenter CPUs.	All levels
Fragmenter	Main LSQ CPU; fragments IP packets into MLPPP fragments and also reassembles MLPPP fragments into IP packets.	All levels
Total	Sum of all CPU functions.	**brief**
Idle	Counts idle cycles when the CPU does not have any work.	**detail**
Timer	Takes care of periodic events driven by a timer, such as timeouts.	**detail**
System	System housekeeping thread.	**detail**
Input (QoS)	Acquires and queues incoming IP frames from hardware interfaces.	**detail**
Output (QoS)	Sends scheduled frames to the next processing CPU.	**detail**
Output Frags (QoS)	Sends outstanding frames to the fragmenter CPU.	**detail**
Bypass (QoS)	Sends outstanding frames for LFI.	**detail**
Free frame (QoS)	Frees dropped frames.	**detail**
CPU*number*	Identifier number of specific CPU.	**detail**
Drop (Fragmenter)	Drops frames that have been marked by the QoS CPU.	**detail**
Frag (Fragmenter)	Fragments IP frames into MLPPP fragments.	**detail**
Reass (Fragmenter)	Reassembles MLPPP fragments into IP frames.	**detail**

Table 73: show services link-services cpu-usage Output Fields *(continued)*

Field Name	Field Description	Level of Output
Freeback (Fragmenter)	Handles freeback of credits from other CPUs (MultiServices PICs only).	**detail**
Input LFI (Sequencer)	Receives LFI traffic from QoS CPU and transmits it with strict priority over MLPPP.	**detail**
Input Frag (Sequencer)	Receives MLPPP fragments from fragmenter CPUs, assigns sequence numbers, and appends MLPPP headers.	**detail**
Output Frag (Sequencer)	Load-balances and transmits fragments across links.	**detail**
Retry (Sequencer)	Retries transmission if hardware was busy in the previous attempt.	**detail**
Input Alloc (Load Balancer)	Acquires frames from hardware interfaces and validates them.	**detail**
Input (Load Balancer)	Performs error and sanity checks and check frames for PortMapping.	**detail**
Output (Load Balancer)	Sends frame to next processing CPU.	**detail**
Freeback (Load Balancer)	Handles freeback of credits from other CPUs.	**detail**

Sample Output

show services link-services cpu-usage brief (AS PIC)

`user@host>` **show services link-services cpu-usage interface lsq-0/0/0 brief**

```
Role            1 Second Average       5 Second Average
QOS                        1.0%                    1.0%
Sequencer                 0.1%                   0.1%
Fragmenter                 0.1%                    0.1%
Total                      0.1%                    0.1%
```

show services link-services cpu-usage brief (MultiServices PIC)

user@host> **show services link-services cpu-usage interface lsq-0/0/0 brief**

```
Role           1 Second Average       5 Second Average

QoS                       0.1%                   0.1%
Fragmenter                0.1%                   0.1%
Load Balancer             0.0%                   0.0%
Total                     0.1%                   0.1%
```

show services link-services cpu-usage detail (AS PIC)

user@host> **show services link-services cpu-usage interface lsq-0/0/0 detail**

```
QoS              Idle   Timer  System  Input Output Output Bypass  Free
                                                Frags          frame

CPU0            99.1%    0.9%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
CPU1            99.8%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
1 sec ave       99.5%    0.5%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
5 sec ave       99.5%    0.5%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%

Fragmenter       Idle   Timer  System   Drop   Frag  Reass   Free
                                                      back

CPU0            96.6%    0.1%    0.0%   0.0%   0.0%   3.3%   0.0%
CPU1            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU2            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU3            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU4            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU5            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU6            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU7            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU8            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
1 sec ave       99.5%    0.1%    0.0%   0.0%   0.0%   0.4%   0.0%
5 sec ave       99.5%    0.1%    0.0%   0.0%   0.0%   0.4%   0.0%

Sequencer        Idle   System  Input  Input Output  Retry
                                 LFI    Frag   Frag

CPU0            99.9%     0.1%   0.0%   0.0%   0.0%   0.0%
CPU1           100.0%     0.0%   0.0%   0.0%   0.0%   0.0%
```

```
1 sec ave       99.9%     0.1%   0.0%   0.0%   0.0%   0.0%
5 sec ave       99.9%     0.1%   0.0%   0.0%   0.0%   0.0%
```

show services link-services cpu-usage detail (MultiServices PIC)

`user@host>` **show services link-services cpu-usage interface lsq-0/0/0 detail**

```
QoS              Idle   Timer  System  Input Output Output Bypass  Free
                                                    Frags         frame

CPU0            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
CPU1            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
CPU2            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
CPU3            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
CPU4            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
1 sec ave       99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%
5 sec ave       99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%   0.0%

Fragmenter       Idle   Timer  System   Drop   Frag  Reass   Free
                                                          back

CPU0            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU1            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU2            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU3            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU4            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU5            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU6            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU7            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU8            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU9            99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU10           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU11           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU12           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU13           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU14           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU15           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU16           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
CPU17           99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
1 sec ave       99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%
5 sec ave       99.9%    0.1%    0.0%   0.0%   0.0%   0.0%   0.0%

Load-Balancer    Idle   System  Input  Input Output   Free
                                Alloc                 back
```

```
CPU0            100.0%     0.0%   0.0%   0.0%   0.0%   0.0%
CPU1            100.0%     0.0%   0.0%   0.0%   0.0%   0.0%
1 sec ave       100.0%     0.0%   0.0%   0.0%   0.0%   0.0%
5 sec ave       100.0%     0.0%   0.0%   0.0%   0.0%   0.0%
```

show services l2tp multilink

Syntax

```
show services l2tp multilink
<brief | detail | extensive | statistics>
<bundle-id number>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Display L2TP output organized by multilink bundle.

Options

none—Same as brief.

brief | detail | extensive | statistics—(Optional) Display the specified level of output. Use the **statistics** option to display packets and bytes that have been encapsulated in the Multilink Protocol. Nonmultilink packets received on member sessions are not counted here.

bundle-id *number*—(Optional) Display L2TP multilink bundle information for only the specified bundle.

Required Privilege Level

view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**

L2TP Minimum Configuration | **1038**

clear services l2tp multilink | **1632**

List of Sample Output

show services l2tp multilink extensive on page 1903

Output Fields

Table 74 on page 1898 lists the output fields for the **show services l2tp multilink** command. Output fields are listed in the approximate order in which they appear.

Table 74: show services l2tp multilink Output Fields

Field Name	Field Description	Level of Output
Bundle ID	Bundle identifier.	All levels
Links	Number of links in the multilink bundle.	All levels
Bundle endpoint	Endpoint discriminator that represents the device transmitting the packet.	All levels
Input MRRU	Maximum packet size that the input interface can process.	detail
Output MRRU	Maximum packet size that the output interface can process.	detail
Session local ID	Identifier of the local endpoint of the L2TP session, as assigned by the L2TP network server (LNS).	detail
Session remote ID	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	detail

Table 74: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	Status of the L2TP session: • **Established**—The session is operating. • **closed**—The session is being closed. • **destroyed**—The session is being destroyed. • **clean-up**—The session is being cleaned up. • **lns-ic-accept-new**—A new session is being accepted. • **lns-ic-idle**—The session has been created and is idle. • **lns-ic-reject-new**—The new session is being rejected. • **lns-ic-wait-connect**—The session is waiting for the peer's incoming call connected (ICCN) message.	detail
Username	Name of the user logged in to the session.	detail
Mode	Mode of the interface representing the multilink bundle: **dedicated** or **shared**.	extensive
Local IP	IP address of the local endpoint of the Point-to-Point Protocol (PPP) session.	extensive
Remote IP	IP address of the remote endpoint of the PPP session.	extensive
Local name	Name of the LNS instance in which the session was created.	extensive
Remote name	Name of the LAC from which the session was created.	extensive

Table 74: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
Local MRU	Maximum receive unit (MRU) setting of the local device, in bytes.	extensive
Remote MRU	MRU setting of the remote device, in bytes.	extensive

Table 74: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
Statistics since		extensive

Table 74: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets. • **Lcp Echo Req Tx**—Number of LCP echo requests transmitted, in packets. • **Lcp Echo Req Rx**—Number of LCP echo requests received, in packets. • **Lcp Echo Rep Tx**—Number of LCP echo responses transmitted, in packets. • **Lcp Echo Rep Rx**—Number of LCP echo responses received, in packets. • **Lcp Echo Req Timeout**—Number of LCP echo requests that timed out. • **Lcp Echo Req Error**—Number of errors received for LCP echo packets. • **Lcp Echo Rep Error** —Number of errors transmitted for LCP echo packets. • **MRRU**—Maximum packet size	

Table 74: show services l2tp multilink Output Fields *(continued)*

Field Name	Field Description	Level of Output
	processed. • **TX**—Number of packets transmitted. • **RX**—Number of packets received. • **link**—Link of the multilink bundle associated with the L2TP session.	

Sample Output

show services l2tp multilink extensive

`user@host>` **show services l2tp multilink extensive**

```
Bundle ID: 1
  Links: 2, Bundle endpoint: user@example.com
  Input MRRU: 1524, Output MRRU: 1524
  Session local ID: 46122, Session remote ID: 39307
    State: Established, Username: user1@example.com, Mode: dedicated
    Local IP: 10.58.255.129:1701, Remote IP: 10.58.255.131:1701
    Local name: router3, Remote name: router4
  Session local ID:  4254, Session remote ID: 39308
    State: Established, Username: user2@example.com, Mode: dedicated
    Local IP: 10.1.255.1:1701, Remote IP: 10.1.255.2:1701
    Local name: router1, Remote name: router2
  Statistics since: Mon May 17 11:47:35 2004
                        Packets        Bytes
      Control Tx              7          196
      Control Rx              3           90
      Data Tx                 0            0
      Data Rx                 0            0
      Errors Tx               0
      Errors Rx               0
   Lcp Echo Req Tx         0
   Lcp Echo Req Rx         0
   Lcp Echo Rep Tx         0
   Lcp Echo Rep Rx         0
   Lcp Echo Req Timeout         0
```

```
Lcp Echo Req Error           0
Lcp Echo Rep Error           0
MRRU 1486 droptime 0 maxfrag 0   minfrag 32  minmru 1482 maxqlen 3000
  TX: Packets 0    Frags 0    Txseq 0x0
  RX: Packets 24   Frags 24   Rxseq 0x18   mseq 23  maxdiff 1   reass 24
     fragments copied 0
  link 0 : seq 0x17 mru 1482 encaplen 8  qlen 0   context 0xea01eb0
```

show services l2tp radius

Syntax

```
show services l2tp radius
<accounting (servers | statistics)>
<authentication (servers | statistics)>
<servers>
<statistics>
```

Release Information
Command introduced in Junos OS Release 9.0.

Description
(M7i, M10i, and M120 routers only) Display RADIUS servers and statistics information for the RADIUS servers configured on the router.

Options
You must include one of the following keywords to provide a valid completion for the command:

accounting (servers | statistics)—(Optional) Display RADIUS servers or statistical accounting information only.

authentication (servers | statistics)—(Optional) Display RADIUS servers or statistical authentication information only.

servers—(Optional) Display RADIUS authentication and accounting server information only.

statistics—(Optional) Display RADIUS authentication and accounting statistics information only.

Required Privilege Level
view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | 1037
L2TP Minimum Configuration | 1038

List of Sample Output
show services l2tp radius servers on page 1907
show services l2tp radius statistics on page 1908

Output Fields

Table 75 on page 1906 lists the output fields for the **show services l2tp radius** command. Output fields are listed in the approximate order in which they appear.

Table 75: show services l2tp radius Output Fields

Field Name	Field Description
IP Address	IP address of the server.
State	(**servers** keyword only) Present state of the server.
UDP Port	Number of the UDP port used to send authentication or accounting messages to the server.
Retry Count	(**servers** keyword only) Number of times the RADIUS client resends a packet if no ACK is received.
Timeout	(**servers** keyword only) Length of time the client waits for an ACK before retransmission.
Pending Requests	(**servers** keyword only) Number of client pending authentication or accounting requests.
Maximum Sessions	(**servers** keyword only) Maximum number of pending requests on each RADIUS client before the server moves to the next RADIUS client, which is 200 times the maximum number of clients that can be created on a server (which is 12).
Dead Time	(**servers** keyword only) Interval to wait before retrying a server after it fails to send a response to an authentication or accounting request.
Secret Type	(**servers** keyword only) Secret type configured on the RADIUS server.
Profile	(**servers** keyword only) Name of profile configured for the RADIUS server.
Access requests	(**statistics** keyword only) Number of access requests sent to the server.
Rollover requests	(**statistics** keyword only) Number of requests coming into the server as a result of the previous server timing out.
Retransmissions	(**statistics** keyword only) Number of retransmissions.
Access accepts	(**statistics** keyword only) Number of access accept messages received from the server.
Access rejects	(**statistics** keyword only) Number of access reject messages received from the server.
Access challenges	(**statistics** keyword only) Number of access challenges received from the server.

Table 75: show services l2tp radius Output Fields *(continued)*

Field Name	Field Description
Malformed responses	(**statistics** keyword only) Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).
Bad authenticators	(**statistics** keyword only) Number of responses in which the authenticator is incorrect for the matching request. This can occur if the RADIUS secrets for the client and server do not match.
Requests pending	(**statistics** keyword only) Number of requests waiting for a response.
Request timeouts	(**statistics** keyword only) Number of requests that timed out.
Unknown responses	(**statistics** keyword only) Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.
Packets dropped	(**statistics** keyword only) Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request. For example, if the router sends a request that times out, the router removes the request from the list and sends a new request. If the server is slow and sends a response to the first request after the router removes the request, the packet is dropped.

Sample Output

show services l2tp radius servers

```
user@host> show services l2tp radius servers
```

```
                    RADIUS Authentication Servers

                          UDP  Retry         Pending  Maximum  Dead   Secret
  IP Address      State   Port Count Timeout Requests Sessions Time   Type
192.0.2.1         Active   1812 2     25      0        2400     300  radius-key

198.51.100.1      Active   1812 5     35      0        2400     300  radius-key

203.0.113.1      Active   1812 2     25      0        2400     300  radius-key
172.28.30.174    Active   1812 7     75      0        2400     300  radius-key
172.28.30.175    Active   1812 7     75      0        2400     300  radius-key
172.28.30.176    Active   1812 4     55      0        2400     300  radius-key
172.31.30.176   Active   1812 3     3       0        2400     300  none-set
```

```
   172.31.130.174 Active   1812 7     75      0        2400     300  radius-key

                       RADIUS Accounting Servers

                            UDP  Retry         Pending  Maximum  Dead   Secret
     IP Address     State   Port Count Timeout Requests Sessions Time   Type
   192.0.2.1        Active   1813 2     25      0        2400     300  radius-key

   198.51.100.1     Active   1813 5     35      0        2400     300  radius-key

   203.0.113.1     Active   1813 2     25      0        2400     300  radius-key
   172.28.30.174   Active   1813 7     75      0        2400     300  radius-key
   172.28.30.175   Active   1813 7     75      0        2400     300  radius-key
   172.28.30.176   Active   1813 4     55      0        2400     300  radius-key
   172.31.30.176  Active   1813 3     3       0        2400     300  none-set
   172.31.130.174 Active   1813 7     75      0        2400     300  radius-key

                       RADIUS Accounting Servers

 Profile: user1
```

show services l2tp radius statistics

user@host> **show services l2tp radius statistics**

```
     RADIUS Authentication Statistics

Authentication statistics:
  Server 192.0.2.1, UDP port: 1812
    Access requests     : 40
    Rollover requests   : 5
    Retransmissions     : 2
    Access accepts      : 39
    Access rejects      : 1
    Access challenges   : 3
    Malformed responses : 0
    Bad authenticators  : 0
    Requests pending    : 1
    Request timeouts    : 0
    Unknown responses   : 0
    Packets dropped     : 0

     RADIUS Accounting Statistics
```

```
Accounting statistics:
 Server 172.31.130.174, UDP port: 1813
   Total requests      : 9
   Start requests      : 6
   Interim requests    : 1
   Stop requests       : 2
   Rollover requests   : 0
   Retransmissions     : 1
   Total response      : 9
   Start responses     : 6
   Interim responses   : 1
   Stop responses      : 2
   Malformed responses : 0
   Bad authenticators  : 0
   Requests pending    : 1
   Request timeouts    : 0
   Unknown responses   : 0
   Packets dropped     : 0
```

show services l2tp session

Syntax

```
show services l2tp session
<brief | detail | extensive>
<interface interface-name>
<local-gateway gateway-address>
<local-gateway-name gateway-name>
<local-session-id session-id>
<local-tunnel-id tunnel-id>
<peer-gateway gateway-address>
<peer-gateway-name gateway-name>
<statistics>
<tunnel-group group-name>
<user username>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.

Description

(M10i and M7i routers only) Display information about active L2TP sessions for LNS.

(MX Series routers only) Display information about active L2TP sessions for LAC and LNS.

Options

none—Display standard information about all active L2TP sessions.

brief | detail | extensive—(Optional) Display the specified level of output.

interface *interface-name*—(Optional) Display L2TP session information for only the specified adaptive services or inline services interface. The interface type depends on the line card as follows:

- **si-*fpc/pic/port***— MPCs on MX Series routers only. This option is not available for L2TP on M Series routers.
- **sp-*fpc/pic/port***—AS or Multiservices PICs on M7i, M10i, and M120 routers only. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—(Optional) Display L2TP session information for only the specified local gateway address.

local-gateway-name *gateway-name*—(Optional) Display L2TP session information for only the specified local gateway name.

local-session-id *session-id*—(Optional) Display L2TP session information for only the specified local session identifier.

local-tunnel-id *tunnel-id*—(Optional) Display L2TP session information for only the specified local tunnel identifier.

peer-gateway *gateway-address*—(Optional) Display L2TP session information for only the specified peer gateway address.

peer-gateway-name *gateway-name*—(Optional) Display L2TP session information for only the specified peer gateway name.

statistics—(Optional) Display the number of control packets and bytes transmitted and received for the session. You cannot include this option with any of the level options, **brief**, **detail**, or **extensive**.

tunnel-group *group-name*—(Optional) Display L2TP session information for only the specified tunnel group. To display information about L2TP CPU and memory usage, you can include the tunnel group name in the **show services service-sets memory-usage *group-name*** and **show services service-sets cpu-usage *group-name*** commands. This option is not available for L2TP LAC on MX Series routers.

user *username*—(M Series routers only) (Optional) Display L2TP session information for only the specified username.

Required Privilege Level
view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**
L2TP Minimum Configuration | **1038**
clear services l2tp session | **1634**

List of Sample Output

Output Fields

Table 76 on page 1912 lists the output fields for the **show services l2tp session** command. Output fields are listed in the approximate order in which they appear.

Table 76: show services l2tp session Output Fields

Field Name	Field Description	Level of Output
Interface	(LNS only) Name of an adaptive services interface.	All levels
Tunnel group	(LNS only) Name of a tunnel group.	All levels
Tunnel local ID	Identifier of the local endpoint of the tunnel, as assigned by the L2TP network server (LNS).	All levels
Session local ID	Identifier of the local endpoint of the L2TP session, as assigned by the LNS.	All levels
Session remote ID	Identifier of the remote endpoint of the L2TP session, as assigned by the L2TP access concentrator (LAC).	All levels
State	State of the L2TP session: • **Established**—Session is operating. This is the only state supported for the LAC. • **closed**—Session is being closed. • **destroyed**—Session is being destroyed. • **clean-up**—Session is being cleaned up. • **lns-ic-accept-new**—New session is being accepted. • **lns-ic-idle**—Session has been created and is idle. • **lns-ic-reject-new**—New session is being rejected. • **lns-ic-wait-connect**—Session is waiting for the peer's incoming call connected (ICCN) message.	All levels
Bundle ID	(LNS only) Bundle identifier. Indicates the session is part of a multilink bundle. Sessions that have a blank **Bundle** field are not participating in the Multilink Protocol. Sessions in a multilink bundle might belong to different L2TP tunnels. For L2TP output organized by bundle ID, issue the **show services l2tp multilink extensive** command.	All levels
Mode	(LNS) Mode of the interface representing the session: **shared** or **exclusive**. (LAC) Mode of the interface representing the session: **shared** or **dedicated**. Only **dedicated** is currently supported for the LAC.	**extensive**
Local IP	IP address of local endpoint of the Point-to-Point Protocol (PPP) session.	**extensive**

Table 76: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Remote IP	IP address of remote endpoint of the PPP session.	**extensive**
Username	(LNS only) Name of the user logged in to the session.	All levels
Assigned IP address	(LNS only) IP address assigned to remote client.	**extensive**
Local name	For LNS, name of the LNS instance in which the session was created. For LAC, name of the LAC.	**extensive**
Remote name	For LNS, name of the LAC from which the session was created. For LAC, name of the LAC instance.	**extensive**
Local MRU	(LNS only) Maximum receive unit (MRU) setting of the local device, in bytes.	**extensive**
Remote MRU	(LNS only) MRU setting of the remote device, in bytes.	**extensive**
Tx speed	Transmit speed of the session conveyed from the LAC to the LNS, in bits per second (bps) and the source method from which the speed is derived. Starting in Junos OS Release 14.1, either the initial (**initial**) line speed or both the initial and current (**update**) line speeds can be displayed on MX Series routers: • When connection speed updates are not enabled, then only the initial line speed is displayed. • When connection speed updates are enabled, then both the initial and the current speeds are displayed. For Junos OS Release 17.2 and Release 17.3, only the current (**update**) line speed can be displayed on MX Series routers. Starting in Junos OS Release 17.4R1, once again either the initial (**initial**) line speed or both the initial and current (**update**) line speeds can be displayed on MX Series routers. Starting in Junos OS Release 15.1, when the Tx connect speed method is set to none, the value of zero (0) is displayed.	**extensive**

Table 76: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Rx speed	Receive speed of the session conveyed from the LAC to the LNS, in bits per second (bps) and the source method from which the speed is derived. Starting in Junos OS Release 14.1, either the initial (**initial**) line speed or both the initial and current (**update**) line speeds can be displayed on MX Series routers: • When connection speed updates are not enabled, then only the initial line speed is displayed. • When connection speed updates are enabled, then both the initial and the current speeds are displayed. For Junos OS Release 17.2 and Release 17.3, only the current (**update**) line speed can be displayed on MX Series routers. Starting in Junos OS Release 17.4R1, once again either the initial (**initial**) line speed or both the initial and current (**update**) line speeds can be displayed on MX Series routers. Starting in Junos OS Release 15.1, when the Tx connect speed method is set to none, the value of zero (0) is displayed.	**extensive**
Bearer type	Type of bearer enabled: • **0**—Might indicate that the call was not received over a physical link (for example, when the LAC and PPP are located in the same subsystem). • **1**—Digital access requested. • **2**—Analog access requested. • **4**—Asynchronous Transfer Mode (ATM) bearer support.	**extensive**
Framing type	Type of framing enabled: • **1**—Synchronous framing • **2**—Asynchronous framing	**extensive**
LCP renegotiation	(LNS only) Whether Link Control Protocol (LCP) renegotiation is configured: **On** or **Off**.	**extensive**
Authentication	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).	**extensive**
Interface ID	(LNS only) Identifier used to look up the logical interface for this session.	**extensive**

Table 76: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Interface unit	Logical interface for this session.	All levels
Call serial number	Unique serial number assigned to the call.	**extensive**
Policer bandwidth	Maximum policer bandwidth configured for this session.	**extensive**
Policer burst size	Maximum policer burst size configured for this session.	**extensive**
Firewall filter	Configured firewall filter name.	**extensive**
Session encapsulation overhead	Overhead allowance configured for this session, in bytes.	**extensive**
Session cell overhead	Cell overhead activation (**On** or **Off**).	**extensive**
Create time	Date and time when the call was created.	**extensive**
Up time	Length of time elapsed since the call became active, in hours, minutes, and seconds.	**extensive**
Idle time	Length of time elapsed since the call became idle, in hours, minutes, and seconds.	**extensive**

Table 76: show services l2tp session Output Fields *(continued)*

Field Name	Field Description	Level of Output
Statistics since	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets. • **LCP echo req Tx**—Number of LCP echo requests transmitted, in packets. • **LCP echo req Rx**—Number of LCP echo requests received, in packets. • **LCP echo rep Tx**—Number of LCP echo responses transmitted, in packets. • **LCP echo rep Rx**—Number of LCP echo responses received, in packets. • **LCP echo Req timout**—Number of LCP echo requests that timed out. • **LCP echo Req error**—Number of errors received for LCP echo packets. • **LCP echo Rep error** —Number of errors transmitted for LCP echo packets.	**extensive**

Sample Output

show services l2tp session (LNS on M Series Routers)

`user@host>` **show services l2tp session**

```
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID:  8802
  Local Remote Interface State               Bundle Username
  ID    ID     unit
  37966      5         2 Established
```

show services l2tp session (LNS on MX Series Routers)

`user@host>` **show services l2tp session**

```
Tunnel local ID: 40553
  Local  Remote   State               Interface        Interface
```

```
  ID     ID                          unit              Name
  17967  1        Established        1073749824        si-5/2/0
```

show services l2tp session (LAC)

```
user@host> show services l2tp session
```

```
Tunnel local ID: 31889
  Local  Remote   State               Interface         Interface
  ID     ID                           unit              Name
   31694      1   Established               311         pp0
```

show services l2tp session detail (LAC)

```
user@host> show services l2tp session detail
```

```
Tunnel local ID: 31889
  Session local ID: 31694, Session remote ID:     1, Interface unit: 311
    State: Established, Interface: pp0, Mode: Dedicated
    Local IP: 203.0.113.2:1701, Remote IP: 203.0.113.1:1701
    Local name: ce-lac, Remote name: ce-lns
```

show services l2tp session extensive (LAC)

```
user@host> show services l2tp session extensive
```

```
Tunnel local ID: 31889
  Session local ID: 31694, Session remote ID:     1
    Interface unit: 311
    State: Established, Mode: Dedicated
    Local IP: 203.0.113.2:1701, Remote IP: 203.0.113.1:1701
    Local name: ce-lac, Remote name: ce-lns
    Tx speed: 0, Rx speed: 0
    Bearer type: 1, Framing type: 1
    LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
    Interface unit: 311, Call serial number: 0
    Policer bandwidth: 0, Policer burst size: 0
    Policer exclude bandwidth: 0, Firewall filter: 0
    Session encapsulation overhead: 0, Session cell overhead: 0
    Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
    Idle time: N/A
```

show services l2tp session extensive (LAC on MX Series Routers)

user@host> **show services l2tp session extensive**

```
Tunnel local ID: 31889
  Session local ID: 31694, Session remote ID:     1
    Interface unit: 311
    State: Established, Mode: Dedicated
    Local IP: 203.0.113.102:1701, Remote IP: 203.0.113.101:1701
    Local name: ce-lac, Remote name: ce-lns
    Tx speed: 256000, source service-profile
    Rx speed: 128000, source ancp
    Bearer type: 1, Framing type: 1
    LCP renegotiation: N/A, Authentication: None, Interface ID: N/A
    Interface unit: 311, Call serial number: 0
    Policer bandwidth: 0, Policer burst size: 0
    Policer exclude bandwidth: 0, Firewall filter: 0
    Session encapsulation overhead: 0, Session cell overhead: 0
    Create time: Tue Aug 24 14:38:23 2010, Up time: 01:06:25
    Idle time: N/A
```

show services l2tp session extensive (LNS on M Series Routers)

user@host> **show services l2tp session extensive**

```
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
  Session local ID: 56793, Session remote ID: 53304
    State: Established, Bundle ID: 5, Mode: shared
    Local IP: 203.0.113.121:1701, Remote IP: 203.0.113.202:1701
    Username: user@example.com, Assigned IP address: 203.0.113.51/32
    Local MRU: 4000, Remote MRU: 1500, Tx speed: 64000, Rx speed: 64000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_20
    Interface unit: 20, Call serial number: 4137941434
    Policer bandwidth: 64000, Policer burst size: 51200
    Firewall filter: f1
    Session encapsulation overhead: 16, Session cell overhead: On
    Create time: Tue Mar 23 14:13:15 2004, Up time: 01:16:41
    Idle time: 00:00:00
    Statistics since: Tue Mar 23 14:13:13 2004
                        Packets        Bytes
      Control Tx              4           88
      Control Rx              2           28
      Data Tx                 0            0
      Data Rx               461        29.0k
```

```
      Errors Tx              0
      Errors Rx              0

Interface: sp-1/2/0, Tunnel group: group_company_dns, Tunnel local ID: 37266
  Session local ID: 39962, Session remote ID: 53303
    State: Established, Bundle ID: 5, Mode: shared
    Local IP: 203.0.113.121:1701, Remote IP: 203.0.113.222:1701
    Username: usr1@company.example.com, Assigned IP address: 203.0.113.3/24
    Local name: router-1, Remote name: router-2
    Local MRU: 4470, Remote MRU: 4470, Tx speed: 155000000, Rx speed: 155000000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_31
    Interface unit: 31, Call serial number: 4137941433
    Policer bandwidth: 64000, Policer burst size: 51200
    Firewall filter: f1
    Create time: Tue Mar 23 14:13:17 2004, Up time: 01:16:39
    Idle time: 01:16:36
    Statistics since: Tue Mar 23 14:13:15 2004
                        Packets        Bytes
      Control Tx              6          196
      Control Rx              4          150
      Data Tx                 0            0
      Data Rx                 1           80
      Errors Tx               0
      Errors Rx               0
```

show services l2tp session extensive (LNS on MX Series Routers)

`user@host>` **show services l2tp session extensive**

```
Tunnel local ID: 40553
  Session local ID: 17967, Session remote ID: 1
    Interface unit: 1073749824
    State: Established
    Interface: si-5/2/0
    Mode: Dedicated
    Local IP: 192.0.2.2:1701, Remote IP: 192.0.2.3:1701
    Local name: lns-mx960, Remote name: testlac
    Tx speed: initial 64000, Update 256000
    Rx speed: initial 64000, Update 256000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: None
    Call serial number: 1
    Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:48
```

```
    Idle time: N/A
    Statistics since: Mon Apr 25 20:27:50 2011
                        Packets        Bytes
      Control Tx              4          219
      Control Rx              4          221
      Data Tx                 0            0
      Data Rx                10          228
      Errors Tx               0
      Errors Rx               0
```

show services l2tp session statistics (MX Series Routers)

user@host>**show services l2tp session statistics local session-id 1**

```
Tunnel local ID: 17185
Session local ID: 1, Session remote ID: 14444, Interface unit: 1073788352
State: Established
Statistics since: Mon Aug 1 13:27:47 2011
    Packets   Bytes
Data Tx   4    51
Data Rx   3    36
```

show services l2tp summary

Syntax

```
show services l2tp summary
<interface sp-fpc/pic/port>
<statistics>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support for LAC on MX Series routers introduced in Junos OS Release 10.4.
Support for LNS on MX Series routers introduced in Junos OS Release 11.4.
Support for **statistics** option introduced in Junos OS Release 13.1.

Description

(M10i and M7i routers: LNS only. MX Series routers: LAC and LNS.) Display Layer 2 Tunneling Protocol (L2TP) summary information.

Options

none—Display complete L2TP summary information. For LNS on M Series routers, display L2TP summary information for all adaptive services interfaces. For LNS on MX Series routers, display L2TP summary information for all inline services interfaces.

interface sp-*fpc/pic/port*—(Optional) Display L2TP summary information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.

statistics—(Optional) Display a summary of control packets and bytes transmitted and received.

Required Privilege Level

view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**
L2TP Minimum Configuration | **1038**

List of Sample Output

Output Fields

Table 77 on page 1922 lists the output fields for the **show services l2tp summary** command. Output fields are listed in the approximate order in which they appear.

Table 77: show services l2tp summary Output Fields

Field Name	Field Description
Administrative state	Administrative state of the tunnel is drain. In this state you cannot configure new sessions, destinations, or tunnels at the LAC or LNS.
Failover within a preference level	State of this tunnel selection method on the LAC. When enabled, tunnel selection fails over within a preference level. When disabled, tunnel selection drops to the next lower preference level. Not displayed for LNS on M Series routers.
Weighted load balancing	State of this tunnel selection method on the LAC. When enabled, the maximum session limit of a tunnel determines its weight within a preference level. Tunnel selection proceeds from greatest to least weight. When disabled, selection defaults to a round robin method. Not displayed for LNS on M Series routers.
Destination equal load balancing	State of this tunnel selection method on the LAC. When enabled, the LAC selects tunnels based on the session count for destinations and the tunnel session count. Not displayed for LNS on M Series routers.
Tunnel authentication challenge	State of tunnel authentication, indicating whether the LAC and LNS exchange an authentication challenge and response during the establishment of the tunnel. The state is **Enabled** when a secret is configured in the tunnel profile or on the RADIUS server in the Tunnel-Password attribute [69]. The state is **Disabled** when the secret is not present. Not displayed for LNS on M Series routers.
Calling number avp	When the state is **Enabled**, the LAC includes the value of the Calling Number AVP 22 in ICRQ packets sent to the LNS. When the state is **Disabled**, the attribute is not sent to the LNS. Not displayed for LNS on M Series routers.

Table 77: show services l2tp summary Output Fields *(continued)*

Field Name	Field Description
Failover Protocol	When the state is enabled, the LAC operates in the default *failover-protocol-fall-back-to-silent-failover* manner. When the state is disabled, the **disable-failover-protocol** statement has been issued and the LAC operates only in silent failover mode. Not displayed for LNS on M Series routers.
Tx connect speed method	The connection speed method configured to send the speed values in the L2TP Tx Connect Speed (AVP 24) and L2TP Rx Connect Speed (AVP 38). Possible values are: • **actual** This is the default value in Junos OS Releases 15.1, 16.1, 16.2, and 17.1. It is deprecated in Junos Releases 17.2 and higher. • **ancp** • **none** • **pppoe-ia-tag** • **service-profile** • **static** This is the default value in Junos Releases 13.3, 14.1, 14.2, 17.2 and higher. It is deprecated in Junos OS Releases 15.1, 16.1, 16.2, and 17.1.
Rx speed avp when equal	Indicates if the Rx connect speed when equal configuration is **enabled** or **disabled**.
Tunnel assignment id	Format of the tunnel name. Format of the tunnel name, based on RADIUS attributes returned from the AAA server: • **authentication-id**—Name consists of only Tunnel Assignment-Id [82]. This is the default value. • **client-server-id**—Name is a combination of Tunnel-Client-Auth-Id [90], Tunnel-Server-Endpoint [67], and Tunnel-Assignment-Id [82]. This format is available only on MX Series routers.

Table 77: show services l2tp summary Output Fields *(continued)*

Field Name	Field Description
Tunnel Tx Address Change	Action taken by LAC when it receives a request from a peer to change the destination IP address, UDP port, or both: • **accept**—Accepts change requests for the IP address or UDP port. This is the default action. • **ignore**—Ignores all change requests. • **ignore-ip-address**—Ignores change requests for the IP address but accepts them for the UDP port. • **ignore-udp-port**—Ignores change requests for the UDP port but accepts them for the IP address.
Min Retransmission Timeout for control packets	Minimum number of seconds that the local peer waits for the initial response after transmitting an L2TP control packet. If no response has been received by the time the period expires, the local peer retransmits the packet.
Min Retransmission Timeout for control packets	Minimum number of seconds that the local peer waits for the initial response after transmitting an L2TP control packet. If no response has been received by the time the period expires, the local peer retransmits the packet.
Max Retransmissions for Established Tunnel	Maximum number of times control messages are retransmitted for established tunnels.
Max Retransmissions for Not Established Tunnel	Maximum number of times control messages are retransmitted for tunnels that are not established.
Tunnel Idle Timeout	Period that a tunnel can be inactive–that is, carrying no traffic–before it times out and is torn down.
Destruct Timeout	Period that the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been destroyed.
Reassembly Service Set	Indicates active IP reassembly configured for the interface.
Destination Lockout Timeout	Timeout period for which all future destinations are locked out, meaning that they are not considered for selection when a new tunnel is created.

Table 77: show services l2tp summary Output Fields *(continued)*

Field Name	Field Description
Access Line Information	State of LAC global configuration for forwarding subscriber line information to the LNS, **Enabled** or **Disabled**. Indicates active IP reassembly configured for the interface. Starting in Junos OS Release 17.4R1, this information can also be displayed on the LNS for information it receives from the LAC.
IPv6 Services for LAC Sessions	State of LAC IPv6 service configuration for creating the IPv6 (inet6) address family for LAC subscribers, allowing the application of IPv6 firewall filters, **Enabled** or **Disabled**.
Speed Updates	State of LAC global configuration for including connection speed updates when it forwards subscriber line information to the LNS, **Enabled** or **Disabled**. Starting in Junos OS Release 17.4R1, this information can also be displayed on the LNS for updates it receives from the LAC.
Destinations	Number of L2TP destinations for the LAC. Not displayed for LNS on M Series routers.
Tunnels	Number of L2TP tunnels established on the router.
Sessions	Number of L2TP sessions established on the router.
Switched sessions	Number of L2TP tunnel-switched sessions established on the router.
Control	Count of L2TP control packets and bytes sent and received.
Data	Count of L2TP data packets and bytes sent and received.
Errors	Count of L2TP error packets and bytes sent and received.

Sample Output

show services l2tp summary (LAC on M Series routers)

```
user@host> show services l2tp summary
```

```
Administrative state is Drain
Failover within a preference level is Disabled
Weighted load balancing is Enabled
Destination equal load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Disabled
Tunnel assignment id format is authentication-id
Destinations: 1 Tunnels: 1, Sessions: 1
   Tx packets     Rx packets  Memory (bytes)
Control    260             144              11513856
Data       7.5k           16.9k             8.3k
Errors        0              0
```

show services l2tp summary (LAC on MX Series routers)

`user@host>` **show services l2tp summary**

```
Administrative state is Drain
   Failover within a preference level is Disabled
  Weighted load balancing is Disabled
  Destination equal load balancing is Enabled
  Tunnel authentication challenge is Enabled
  Calling number avp is Enabled
  Failover Protocol is Disabled
  Tx Connect speed method is static
  Rx speed avp when equal is enabled
  Tunnel Tx Address Change is Accept
  Min Retransmissions Timeout for control packets is 2 seconds
  Max Retransmissions for Established Tunnel is 7
  Max Retransmissions for Not Established Tunnel is 5
  Tunnel Idle Timeout is 60 seconds
  Destruct Timeout is 300 seconds
  Destination Lockout Timeout is 300 seconds
  Reassembly Service Set is ssnr3
  Access Line Information is Enabled, Speed Updates is Enabled
  IPv6 Services For LAC Sessions is Enabled
  Destinations: 0, Tunnels: 0, Sessions: 0, Switched sessions: 0
```

show services l2tp summary (LNS on MX Series routers)

`user@host` **show services l2tp summary**

```
 Administrative state is Drain
  Failover within a preference level is Disabled
  Weighted load balancing is Disabled
  Destination equal load balancing is Disabled
  Tunnel authentication challenge is Enabled
  Calling number avp is Enabled
  Failover Protocol is Enabled
  Tx Connect speed method is static
  reassembly Service Set is ssnr3
  Destinations: 4, Tunnels: 19, Sessions: 65, Switched sessions: 2
  Access Line Information is Enabled, Speed Updates is Enabled
```

show services l2tp summary (LNS on M Series routers)

`user@host>` **show services l2tp summary**

```
Tunnels: 2, Sessions: 2, Errors: 0
    Tx packets   Rx packets    Memory (bytes)
Control     6k           9k                688k
Data       70k          70k                3054
```

show services l2tp summary statistics (MX Series routers)

`user@host>`**show services l2tp summary statistics**

```
Administrative state is Drain
Failover within a preference level is Disabled
Weighted load balancing is Disabled
Destination equal load balancing is Disabled
Tunnel authentication challenge is Enabled
Calling number avp is Enabled
Failover Protocol is Enabled
Tx Connect speed method is advisory
Tunnel assignment id format is assignment-id
Tunnel Tx Address Change is Accept
Min Retransmissions Timeout for control packets is 4 seconds
Max Retransmissions for Established Tunnel is 7
Max Retransmissions for Not Established Tunnel is 5
Tunnel Idle Timeout is 60 seconds
Destruct Timeout is 300 seconds
Destination Lockout Timeout is 300 seconds
Destinations: 1, Tunnels: 1, Sessions: 31815, Switched sessions: 0
     Tx packets    Rx packets  Memory (bytes)
```

```
Control          90.4k           32.0k       245678080
Data             127.3k          100.8kk         0
Errors              0               0
```

show services l2tp tunnel

Syntax

```
show services l2tp tunnel
<brief | detail | extensive>
<interface sp-fpc/pic/port>
<local-gateway gateway-address>
<local-gateway-name gateway-name>
<local-tunnel-id tunnel-id>
<peer-gateway gateway-address>
<peer-gateway-name gateway-name>
<statistics>
<tunnel-group group-name>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Display information about active Layer 2 Tunneling Protocol (L2TP) tunnels for LNS.

(MX Series routers only) Display information about L2TP tunnels for LAC and LNS; the tunnels may or may not have active sessions.

Options

none—Display standard information about all active L2TP tunnels.

brief | detail | extensive—(Default) Display the specified level of output.

interface sp-*fpc/pic/port*—(Optional) Display L2TP tunnel information for only the specified adaptive services interface. This option is not available for L2TP on MX Series routers.

local-gateway *gateway-address*—(Optional) Display L2TP tunnel information for only the specified local gateway address.

local-gateway-name *gateway-name*—(Optional) Display L2TP tunnel information for only the specified local gateway name.

local-tunnel-id *tunnel-id*—(Optional) Display L2TP tunnel information for only the specified local tunnel identifier.

peer-gateway *gateway-address*—(Optional) Display L2TP tunnel information for only the specified peer gateway address.

peer-gateway-name *gateway-name*—(Optional) Display L2TP tunnel information for only the specified peer gateway name.

statistics—(Optional) Display the number of control packets and bytes transmitted and received for the tunnel. The statistics for a tunnel are retained until the tunnel is disconnected, rather than until the last session in the tunnel is cleared. Retaining the statistics enables them to increment in the event a new session subsequently uses the tunnel. You cannot include this option with any of the level options, **brief**, **detail**, or **extensive**.

tunnel-group *group-name*—(Optional) Display L2TP tunnel information for only the specified tunnel group.

Required Privilege Level
view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | **1037**
L2TP Minimum Configuration | **1038**

List of Sample Output

show services l2tp tunnel (LAC) on page 1933
show services l2tp tunnel detail (LAC) on page 1933
show services l2tp tunnel detail (LAC on MX Series Routers) on page 1933
show services l2tp tunnel detail (LNS on MX Series Routers) on page 1934
show services l2tp tunnel extensive (LAC) on page 1934
show services l2tp tunnel extensive (LNS on M Series Routers) on page 1934
show services l2tp tunnel extensive (LNS on MX Series Routers) on page 1935
show services l2tp tunnel statistics (MX Series Routers) on page 1936

Output Fields

Table 78 on page 1930 lists the output fields for the **show services l2tp tunnel** command. Output fields are listed in the approximate order in which they appear.

Table 78: show services l2tp tunnel Output Fields

Field Name	Field Description
Interface	(LNS only) Name of an adaptive services interface.
Tunnel group	(LNS only) Name of a tunnel group.

Table 78: show services l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Local ID	On the LNS, number assigned by the LNS that identifies the local endpoint of the tunnel relative to the LNS: the LNS. On the LAC, number assigned by the LAC that identifies the local endpoint of the tunnel relative to the LAC: the LAC.
Remote ID	On the LNS, number assigned by the LAC that identifies the remote endpoint of the tunnel relative to the LNS: the LAC. On the LAC, number assigned by the LNS that identifies the remote endpoint of the tunnel relative to the LAC: the LNS.
Remote IP	IP address of the peer endpoint of the tunnel.
Sessions	Number of L2TP sessions established through the tunnel.
State	State of the L2TP tunnel: • **cc_responder_accept_new**—The tunnel has received and accepted the start control connection request (SCCRQ). • **cc_responder_reject_new**—The tunnel has received and rejected the SCCRQ. • **cc_responder_idle**—The tunnel has just been created. • **cc_responder_wait_ctl_conn**—The tunnel has sent the start control connection response (SCCRP) and is waiting for the start control connection connected (SCCCN) message. • **clean-up**—The tunnel is being cleaned up. • **closed**—The tunnel is being closed. • **destroyed**—The tunnel is being destroyed. • Drain—Creation of new sessions and destinations is disabled for this tunnel. • **Established**—The tunnel is operating. This is the only state supported for the LAC. • **Terminate**—The tunnel is terminating. • **Unknown**—The tunnel is not connected to the router.
Tunnel Name	(LAC only) Name of the created tunnel. This value includes the destination name followed by the value of the RADIUS Tunnel-Assignment-ID VSA [82].
Local IP	IP address of the local endpoint of the tunnel.
Local name	Name used for local tunnel endpoint during tunnel negotiation.
Remote name	Name used for remote tunnel endpoint during tunnel negotiation.

Table 78: show services l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Effective Peer Resync Mechanism	(LAC only) Peer resynchronization mechanism (PRM) in effect for the tunnel: • Failover protocol • Silent failover—Recovery takes place in the failed endpoint only using the proprietary silent failover protocol.
Nas Port Method	NAS port method (type), which indicates whether the LAC sends Cisco NAS Port Info AVP (100) in ICRQs to the LNS: • **cisco-avp**—sends the AVP. • **none**—does not send the AVP.
Tunnel Logical System	Logical system in which the L2TP tunnel is brought up.
Tunnel Routing Instance	Routing instance in which the L2TP tunnel is brought up.
Max sessions	Maximum number of sessions that can be established on this tunnel. The displayed limit for configured sessions is set to the lowest of the following configured session values for either LAC or LNS: • Global (chassis)—**set services l2tp tunnel maximum-sessions *number*** • Tunnel profile (individual tunnel)—**set access tunnel-profile *profile-name* tunnel *tunnel-id* max-sessions *number*]** • RADIUS—Value of VSA 26–33, Tunnel-Max-Sessions For LNS only, the following configuration is also considered: • Host profile—**access profile l2tp-profile client default l2tp maximum-sessions-per-tunnel**
Window size	Number of control messages that can be sent without receipt of an acknowledgment.
Hello interval	Interval between the transmission of hello messages, in seconds.
Create time	Date and time when the tunnel was created. While the LNS and LAC are connected, this value should correspond to the when the call was created. If connection to the LAC is severed, the State changes to **Unknown** and the **Create time** value resets.
Up time	Amount of time elapsed since the tunnel became active, in hours, minutes, and seconds.
Idle time	Amount of time elapsed since the tunnel became idle, in hours, minutes, and seconds.

Table 78: show services l2tp tunnel Output Fields *(continued)*

Field Name	Field Description
Statistics since	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets.

Sample Output

show services l2tp tunnel (LAC)

```
user@host> show services l2tp tunnel
```

```
   Local ID  Remote ID  Remote IP               Sessions  State
      17185          1  203.0.113.101:1701             1  Established
```

show services l2tp tunnel detail (LAC)

```
user@host> show services l2tp tunnel detail
```

```
   Tunnel local ID: 31889, Tunnel remote ID:     1
     Remote IP: 203.0.113.101:1701
     Sessions: 1, State: Established
     Tunnel Name: 1/tunnel-to-LNS-1
     Local IP: 192.0.2.2:1701
     Local name: ce-lac, Remote name: ce-lns
     Effective Peer Resync Mechanism: silent failover
```

show services l2tp tunnel detail (LAC on MX Series Routers)

```
user@host> show services l2tp tunnel detail
```

```
Tunnel local ID: 17301, Tunnel remote ID: 1
    Remote IP: 203.0.113.101:1701
```

```
    Sessions: 1, State: Established
    Tunnel Name: 2/tunnel-to-LNS-2
    Local IP: 192.0.2.2:1701
    Local name: ce-lac, Remote name: ce-lns
    Effective Peer Resync Mechanism: silent failover
    Tunnel Logical System: default, Tunnel Routing Instance: default
```

show services l2tp tunnel detail (LNS on MX Series Routers)

user@host> **show services l2tp tunnel detail**

```
Tunnel local ID: 17301, Tunnel remote ID: 1
    Remote IP: 198.51.100.15:1701
    Sessions: 1, State: Established
    Tunnel Name: 2/2
    Local IP: 198.51.100.5:1701
    Local name: ce-bras-mx240-e, Remote name: testlac2
    Effective Peer Resync Mechanism: silent failover
    Tunnel Logical System: default, Tunnel Routing Instance: vrf1
```

show services l2tp tunnel extensive (LAC)

user@host> **show services l2tp tunnel extensive**

```
  Tunnel local ID: 17185, Tunnel remote ID:     1
    Remote IP: 203.0.113.101:1701
    Sessions: 1, State: Established
    Tunnel Name: 2/tunnel-to-LNS-2
    Local IP: 192.0.2.22:1701
    Local name: ce-lac, Remote name: ce-lns
    Effective Peer Resync Mechanism: failover protocol
    Max sessions: 32000, Window size: 4, Hello interval: 60
    Create time: Tue Nov  9 15:23:29 2010, Up time: 00:00:26
    Idle time: 00:00:00
```

show services l2tp tunnel extensive (LNS on M Series Routers)

user@host> **show services l2tp tunnel extensive**

```
Interface: sp-1/2/0, Tunnel group: group1
  Tunnel local ID: 62746, Tunnel remote ID: 16930
    Remote IP: 203.0.113.202:1701
```

```
    Sessions: 1, State: Established
    Local IP: 203.0.113.121:1701
    Local name: router-1, Remote name: router-2
    Max sessions: 50, Window size: 32, Hello interval: 60
    Create time: Tue Mar 23 14:13:15 2004, Up time: 01:14:58
    Idle time: 00:00:07
    Statistics since: Tue Mar 23 14:13:13 2004
                        Packets        Bytes
      Control Tx             80         1152
      Control Rx              3          272
      Data Tx                 0            0
      Data Rx               450        28.0k
      Errors Tx               0
      Errors Rx               0

Interface: sp-1/2/0, Tunnel group: group_company_dns
  Tunnel local ID: 37266, Tunnel remote ID: 36217
    Remote IP: 203.0.113.222:1701
    Sessions: 1, State: Established
    Local IP: 203.0.113.111:1701
    Local name: router-1, Remote name: router-2
    Max sessions: unlimited, Window size: 32, Hello interval: 60
    Create time: Tue Mar 23 14:13:15 2004, Up time: 01:14:59
    Idle time: 01:14:55
    Statistics since: Tue Mar 23 14:13:13 2004
                        Packets        Bytes
      Control Tx             81         1164
      Control Rx              3          273
      Data Tx                 0            0
      Data Rx                 1           80
      Errors Tx               0
      Errors Rx               0
```

show services l2tp tunnel extensive (LNS on MX Series Routers)

`user@host>` **show services l2tp tunnel extensive**

```
Tunnel local ID: 40553, Tunnel remote ID: 1
    Remote IP: 192.0.2.3:1701
    Sessions: 1, State: Established
    Tunnel Name: 3/1838
    Local IP: 203.0.113.2:1701
    Local name: lns-mx960, Remote name: testlac
    Effective Peer Resync Mechanism: silent failover
```

```
    Nas Port Method: none
    Tunnel Logical System: default, Tunnel Routing Instance: vrf1
    Max sessions: 60000, Window size: 4, Hello interval: 60
    Create time: Mon Apr 25 20:27:50 2011, Up time: 00:01:11
    Idle time: 00:00:00, ToS Reflect: Enabled
    Tunnel Group Name: tg1
    Statistics since: Mon Apr 25 20:27:50 2011
                        Packets        Bytes
      Control Tx              4          219
      Control Rx              4          221
      Data Tx                 0            0
      Data Rx                 6           64
      Errors Tx               0
      Errors Rx               0
```

show services l2tp tunnel statistics (MX Series Routers)

user@host>**show services l2tp tunnel statistics**

```
Tunnel local ID: 17185, Tunnel remote ID: 1
Sessions: 31.8k, State: Established
Statistics since: Mon Aug 1 13:21:38 2011
     Packets   Bytes
Control Tx     90.3k    9.0M
Control Rx     32.0k    1296.9k
Data Tx       127.3k   1591.6k
Data Rx       100.8k   1273.4k
Errors Tx      0
Errors Rx      0
```

show services l2tp user

Syntax

```
show services l2tp user
<brief | detail | extensive | statistics>
<user username>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

(M10i and M7i routers only) Display a list of active Layer 2 Tunneling Protocol (L2TP) users.

Options

none—Display all active L2TP users.

brief | detail | extensive | statistics—(Optional) Display the specified level of output. Use the **statistics** option to display L2TP user statistics.

user *username*—(Optional) Display L2TP user information for only the specified username.

Required Privilege Level

view

RELATED DOCUMENTATION

L2TP Services Configuration Overview | 1037

L2TP Minimum Configuration | 1038

List of Sample Output

show services l2tp user extensive on page 1940

Output Fields

Table 79 on page 1937 lists the output fields for the **show services l2tp user** command. Output fields are listed in the approximate order in which they appear.

Table 79: show services l2tp user Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Tunnel group	Name of a tunnel group.

Table 79: show services l2tp user Output Fields *(continued)*

Field Name	Field Description
Tunnel local ID	Local identifier of the tunnel, as assigned by the L2TP network server (LNS).
Session local ID	Local identifier of the session, as assigned by the L2TP network server (LNS).
Session remote ID	Remote identifier of the session, as assigned by the L2TP access concentrator (LAC).
State	State of the L2TP session: • **Established**—The session is operating. • **closed**—The session is being closed. • **destroyed**—The session is being destroyed. • **clean-up**—The session is being cleaned up. • **lns-ic-accept-new**—A new session is being accepted. • **lns-ic-idle**—The session has been created and is idle. • **lns-ic-reject-new**—The new session is being rejected. • **lns-ic-wait-connect**—The session is waiting for the peer's incoming call connected (ICCN) message.
Mode	Mode of the interface representing the session: **shared** or **exclusive**.
Local IP	IP address of the local endpoint of the tunnel.
Remote IP	IP address of the peer endpoint of the tunnel.
Username	Name of the user logged in to the session.
Assigned IP address	IP address assigned to remote client.
Local name	Name of the local device.
Remote name	Name of the remote device.
Local MRU	Maximum receive unit (MRU) setting of the local device, in bytes.
Remote MRU	MRU setting of the remote device, in bytes.
Tx speed	Transmit speed of the tunnel session, in bps.
Rx speed	Receive speed of the tunnel session, in bps.

Table 79: show services l2tp user Output Fields *(continued)*

Field Name	Field Description
Bearer type	Type of bearer enabled: • **0**—Might indicate that the call was not received over a physical link (for example, when the LAC and PPP are located in the same subsystem) • **1**—Digital access requested • **2**—Analog access requested • **4**—Asynchronous Transfer Mode (ATM) bearer support
Framing type	Type of framing enabled: • **1**—Synchronous framing • **2**—Asynchronous framing
LCP renegotiation	Whether Link Control Protocol (LCP) renegotiation is configured: **On** or **Off**.
Authentication	Type of authentication algorithm used: Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP).
Interface ID	Name of the logical unit.
Interface unit	Logical unit number.
Call serial number	Unique serial number assigned to the call.
Create time	Date and time when the call was created.
Up time	Amount of time elapsed since the call became active, in hours, minutes, and seconds.
Idle time	Amount of time elapsed since the call became idle, in hours, minutes, and seconds.
Statistics sine	Date and time when collection of the following statistics began: • **Control Tx**—Amount of control information transmitted, in packets and bytes. • **Control Rx**—Amount of control information received, in packets and bytes. • **Data Tx**—Amount of data transmitted, in packets and bytes. • **Data Rx**—Amount of data received, in packets and bytes. • **Errors Tx**—Number of errors transmitted, in packets. • **Errors Rx**—Number of errors received, in packets.

Sample Output

show services l2tp user extensive

user@host> **show services l2tp user extensive**

```
Interface: sp-1/2/0, Tunnel group: group1, Tunnel local ID: 62746
  Session local ID: 56793, Session remote ID: 53304
    State: Established, Mode: shared
    Local IP: 10.128.1.1:1701, Remote IP: 10.128.1.2:1701
    Username: usr1@example.com, Assigned IP address: 10.50.2.1/32
    Local name: router-1, Remote name: router-2
    Local MRU: 4000, Remote MRU: 1500, Tx speed: 64000, Rx speed: 64000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_20
    Interface unit: 20, Call serial number: 4137941434
    Create time: Tue Mar 23 14:13:15 2004, Up time: 01:16:41
    Idle time: 00:00:00
    Statistics since: Tue Mar 23 14:13:13 2004
                        Packets        Bytes
      Control Tx              4           88
      Control Rx              2           28
      Data Tx                 0            0
      Data Rx               461        29.0k
      Errors Tx               0
      Errors Rx               0
Interface: sp-1/2/0, Tunnel group: group_company_dns, Tunnel local ID: 37266
  Session local ID: 39962, Session remote ID: 53303
    State: Established, Username: usr1@company_dns.com, Mode: shared
    Local IP: 10.128.11.1:1701, Remote IP: 10.128.11.2:1701
    Username: usr1@company_dns.com, Assigned IP address: 10.48.1.1/32
    Local name: router-1, Remote name: router-2
    Local MRU: 4470, Remote MRU: 4470, Tx speed: 155000000,
                                        Rx speed: 155000000
    Bearer type: 2, Framing type: 1
    LCP renegotiation: Off, Authentication: CHAP, Interface ID: unit_31
    Interface unit: 31, Call serial number: 4137941433
    Create time: Tue Mar 23 14:13:17 2004, Up time: 01:16:39
    Idle time: 01:16:36
    Statistics since: Tue Mar 23 14:13:15 2004
                        Packets        Bytes
      Control Tx              6          196
      Control Rx              4          150
      Data Tx                 0            0
      Data Rx                 1           80
```

```
      Errors Tx              0
      Errors Rx              0
```

show services nat deterministic-nat internal-host

Syntax

```
show services nat deterministic-nat internal-host
nat-address
nat-port
```

Release Information

Command introduced in Junos OS Release 12.1.

Description

This commands prints the internal host address and algorithmically determined port ranges for the specified NAT IP address and port number. The results are calculated on the PIC and the results are sent to RE.

Options

nat-address—NAT address of the internal host.

nat-port—NAT port of the internal host.

Required Privilege Level

view

List of Sample Output

show services nat deterministic-nat internal-host on page 1943

Output Fields

Table 80 on page 1942 lists the output fields for the **nat deterministic-nat internal-host** command. Output fields are listed in the approximate order in which they appear.

Table 80: show services nat deterministic-nat internal-host Output Fields

Field Name	Field Description
Interface	Name of a service interface.
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.
Internal Host	Private IP address of a subscriber on the access network.
NAT IP address	NAT public IP address
NAT Port Start	Lowest port number in range of assigned ports.

Table 80: show services nat deterministic-nat internal-host Output Fields *(continued)*

Field Name	Field Description
NAT Port End	Highest port number in range of assigned ports.

Sample Output

show services nat deterministic-nat internal-host

`user@host>` **show services nat deterministic-nat internal-host 203.0.113.1 2000**

```
Service set: ss1
Interface: sp-2/0/0
NAT pool: pool1
Internal Host: 192.0.2.4, NAT IP Address: 203.0.113.1, NAT Port Start: 1792, NAT
Port End: 2047
```

show services nat deterministic-nat nat-port-block

Syntax

```
show services nat deterministic-nat nat-port-block
internal-host
```

Release Information

Command introduced in Junos OS Release 12.1.

Description

Display the translated NAT address and port ranges for the given internal host.

Options

internal-host—IP address of the internal host.

Required Privilege Level

view

List of Sample Output

run show services nat deterministic-nat nat-port-block on page 1945

Output Fields

Table 81 on page 1944 lists the output fields for the **show services nat deterministic-nat nat-port-block** command. Output fields are listed in the approximate order in which they appear.

Table 81: show services nat deterministic-nat nat-port-block Output Fields

Field Name	Field Description
Interface	Name of a service interface.
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.
Internal Host	Private IP address of a subscriber on the access network.
NAT IP address	NAT public IP address
NAT Port Start	Lowest port number in range of assigned ports.
NAT Port End	Highest port number in range of assigned ports.

Sample Output

run show services nat deterministic-nat nat-port-block

user@host> **show services nat deterministic-nat nat-port-block 192.0.2.1**

```
Service set: ss1
Interface: sp-2/0/0
NAT pool: pool1
Internal Host: 192.0.2.1, NAT IP Address: 203.0.113.1, NAT Port Start: 1024, NAT
Port End: 1279
```

show services nat ipv6-multicast-interfaces

Syntax

```
show services nat ipv6-multicast-interfaces
```

Release Information

Command introduced in Junos OS Release 8.5.

Description

Displays a list of interfaces enabled for IPv6 multicast.

Required Privilege Level

view

List of Sample Output

show services nat ipv6-multicast-interfaces on page 1946

Output Fields

Table 82 on page 1946 lists the output fields for the **show services nat ipv6-multicast-interfaces** command. Output fields are listed in the approximate order in which they appear.

Table 82: show services nat ipv6-multicast-interfaces Output Fields

Field Name	Field Description	Level of Output
Interface	Name of a service interface.	All levels
Admin State	Configured IPv6 multicast capability of an interface ,	All levels
Operational State	Operation IPv6 multicast status of an interface.	All levels

Sample Output

show services nat ipv6-multicast-interfaces

```
user@host> show services nat ipv6-multicast-interfaces
```

```
Interface         Admin         Operational
                  State            State
ge-5/1/9          Enabled       Enabled
ge-5/1/8          Enabled       Enabled
```

```
ge-5/1/7          Enabled       Enabled
ge-5/1/6          Enabled       Enabled
ge-5/1/5          Enabled       Enabled
ge-5/1/4          Enabled       Enabled
ge-5/1/3          Enabled       Enabled
ge-5/1/2          Enabled       Enabled
ge-5/1/1          Enabled       Enabled
ge-5/1/0          Enabled       Enabled
ge-5/0/9          Enabled       Enabled
ge-5/0/8          Enabled       Enabled
ge-5/0/7          Enabled       Enabled
ge-5/0/6          Enabled       Enabled
ge-5/0/5          Enabled       Enabled
ge-5/0/4          Enabled       Enabled
ge-5/0/3          Enabled       Enabled
ge-5/0/2          Enabled       Enabled
ge-5/0/1          Enabled       Enabled
ge-5/0/0          Enabled       Enabled
ge-1/3/9          Enabled       Enabled
ge-1/3/8          Enabled       Enabled
ge-1/3/7          Enabled       Enabled
ge-1/3/6          Enabled       Enabled
ge-1/3/5          Enabled       Enabled
ge-1/3/4          Enabled       Enabled
ge-1/3/3          Enabled       Enabled
ge-1/3/2          Enabled       Enabled
ge-1/3/1          Enabled       Enabled
ge-1/3/0          Enabled       Enabled
ge-1/2/9          Enabled       Enabled
ge-1/2/8          Enabled       Enabled
ge-1/2/7          Enabled       Enabled
ge-1/2/6          Enabled       Enabled
ge-1/2/5          Enabled       Enabled
ge-1/2/4          Enabled       Enabled
ge-1/2/3          Enabled       Enabled
ge-1/2/2          Enabled       Enabled
ge-1/2/1          Enabled       Enabled
ge-1/2/0          Enabled       Enabled
ge-1/1/9          Enabled       Enabled
ge-1/1/8          Enabled       Enabled
ge-1/1/7          Enabled       Enabled
ge-1/1/6          Enabled       Enabled
ge-1/1/5          Enabled       Enabled
ge-1/1/4          Enabled       Enabled
```

```
ge-1/1/3          Enabled       Enabled
ge-1/1/2          Enabled       Enabled
ge-1/1/1          Enabled       Enabled
ge-1/1/0          Enabled       Enabled
ge-1/0/9          Enabled       Enabled
ge-1/0/8          Enabled       Enabled
ge-1/0/7          Enabled       Enabled
ge-1/0/6          Enabled       Enabled
ge-1/0/5          Enabled       Enabled
ge-1/0/4          Enabled       Enabled
ge-1/0/3          Enabled       Enabled
ge-1/0/2          Enabled       Enabled
ge-1/0/1          Enabled       Enabled
ge-1/0/0          Enabled       Enabled
xe-0/3/0          Enabled       Enabled
xe-0/2/0          Enabled       Enabled
xe-0/1/0          Enabled       Enabled
xe-0/0/0          Enabled       Enabled
```

show services nat source mappings address-pooling-paired

Syntax

```
show services nat source mappings address-pooling-paired
```

Description

Options

address-pooling-paired—(Optional) Display only information about address-pooling paired mappings.

endpoint-independent—(Optional) Display only information about endpoint-independent mappings.

pcp—(Optional) Display only information about port control protocol mappings.

NOTE: PCP requests with the prefer-failure option request a particular external IP address and port. When the request cannot be fulfilled, the mapping is not created. In this case, the subscriber does not have a mapped IP address. Such a subscriber is counted in the summary of the number or address mappings, but is not displayed in the list of address mappings, as shown in the following examples:

```
user@host# show services nat mappings summary
```

```
Service Interface:                                  sp-2/0/0
Total number of address mappings:                          1
Total number of endpoint independent port mappings:        0
Total number of endpoint independent filters:              0
```

```
user@host# show services nat mappings address-pooling-paired
```

```
[edit]
```

This is expected behavior because unfulfilled address mappings (IP of 0.0.0.0) are not displayed in the output of the second CLI command. These address mappings will time out based on configured or default values.

Required Privilege Level

view

List of Sample Output

show services nat source mappings address-pooling-paired on page 1950

Sample Output

show services nat source mappings address-pooling-paired

`user@host>` **show services nat source mappings address-pooling-paired**

```
Interface: ms-2/0/0, Service set: ss1
Pool name: sp1
Internal address          External address     Session Count       Mapping State
1.1.1.100                     30.30.30.1           1                     Active
1.1.1.101                     30.30.30.2           1                     Active
```

show services nat source mappings address-pooling-paired private 1.1.1.100

`user@host>` **show services nat source mappings address-pooling-paired private 1.1.1.100**

```
Interface: ms-2/0/0, Service set: ss1
Pool name: sp1
Internal address          External address     Session Count       Mapping State
1.1.1.100                     30.30.30.1           1                   Active
```

show services nat source mappings address-pooling-paired public 30.30.30.2

`user@host>` **show services nat source mappings address-pooling-paired public 30.30.30.2**

```
Interface: ms-2/0/0, Service set: ss1
Pool name: sp1
Internal address          External address     Session Count       Mapping State
1.1.1.101                     30.30.30.2           1                   Active
```

show services nat source mappings address-pooling-paired pool-name sp1

```
user@host> show services nat source mappings address-pooling-paired pool-name sp1
```

```
  Interface: ms-2/0/0, Service set: ss1
Pool name: sp1
Internal address          External address     Session Count       Mapping State
1.1.1.100                     30.30.30.1             1                  Active
1.1.1.101                     30.30.30.2             1                   Active
```

show services nat mappings address-pooling-paired

```
user@host> show services nat mappings address-pooling-paired
```

```
Interface: sp-3/0/0, Service set: NAPT44-SS1
NAT pool: napt44-SS1-p1
Mapping          : 29.32.38.255    --> 192.168.75.23
Ports In Use     :     9
Session Count    :     1
Mapping State    : Active
```

show services nat mappings address-pooling-paired (mapping of active B4 for a subscriber)

```
user@host> show services nat mappings address-pooling-paired
```

```
Interface: sp-0/0/0, Service set: sset_1

NAT pool: nat_pool1

Mapping          : 2001::          --> 33.33.33.2
Ports In Use     :     1
Session Count    :     9
Mapping State    : Timeout
```

show services nat mappings endpoint-independent

```
user@host> show services nat mappings endpoint-independent
```

```
Interface: sp-3/0/0, Service set: NAPT44-SS1
NAT pool: napt44-SS1-p1
Mapping          : 29.32.38.255:10000    --> 192.168.75.23:1024
Session Count    : 1
Mapping State    : Active
```

show services nat mappings pcp

```
user@host> show services nat mappings pcp
```

```
PCP Client       : 172.16.0.1        PCP Lifetime : 45
Mapping          : 29.32.38.255:10000    --> 192.168.75.23:1024
Session Count    : 1
Mapping State    : Active
```

show services nat mappings nptv6 internal

```
user@host> show services nat mappings nptv6 internal 1111:2222:3333:aaaa:bbbb::1
```

```
 Interface       Service-set     NAT-Pool           Address Mapping
 vms-0/1/0       ss_nptv6       ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1 ->
aaaa:bbbb:cccc:dddd:bbbb::1
```

show services nat mappings nptv6 external

```
user@host> show services nat mappings nptv6 external aaaa:bbbb:cccc:dddd:bbbb::1
```

```
 Interface       Service-set     NAT-Pool              Address Mapping
 vms-0/1/0        ss_nptv6            ss_nptv6_pool   1111:2222:3333:aaaa:bbbb::1
 -> aaaa:bbbb:cccc:dddd:bbbb::1
```

show services nat pool

Syntax

```
show services nat pool
<brief | detail>
<pool-name>
pgcp <ports-per-session | remotely-controlled>
```

Release Information

Command introduced before Junos OS Release 7.4.
pgcp option added in Junos OS Release 8.5.

Description

Display information about Network Address Translation (NAT) pools.

> **NOTE:** On MS-MPCs and MS-MICs, if the line cards receive a packet immediately after the active port block timeout interval has expired, a new port block is allocated and the old port block is released thereafter (if no more ports are being used from that block). In such a scenario, you might notice that the **Max number of port blocks used** field displays a higher value than the value shown for the **Unique pool users** field in the output of the **show services nat pool detail** command. This behavior is expected with port block allocation.
>
> With MS-MPCs and MS-MICs, in the output of the **show services nat pool detail** command, the **Max ports used** and the **Ports in use** fields display values that indicate a higher number than the number of active subscribers on the member interfaces of an **ams** interface. This behavior of an increased value displayed for the number of ports allocated and maximum number of ports used is expected after you perform a Graceful Routing Engine switchover (GRES) and a restart of the MPC.
>
> With MS-MPCs and MS-MICs on MX Series routers with AMS interfaces, it is observed that the subscriber and port count details are displayed only after a long time in the output of the **show services nat pool detail** command. This behavior is expected with NAT pool counters and occurs, regardless of port block allocation being configured.

Options

none—Display standard information about all NAT pools.

brief | detail—(Optional) Display the specified level of output.

pool-name—(Optional) Display information about the specified NAT pool.

pgcp—(Optional) Display information about a NAT pool that is exclusive to the BGF.

ports-per-session—(Optional) Display the number of ports allocated per session from the NAT pool.

remotely-controlled—(Optional) Display if the NAT pool is explicitly specified by the gateway controller.

Required Privilege Level
view

List of Sample Output
show services nat pool brief on page 1957
show services nat pool detail on page 1957
show services nat pool (Secured Port Block Allocation) on page 1958
show services nat pool detail (Deterministic Port Block Allocation) on page 1958
show services nat pool (Deterministic Port Block Allocation) on page 1959
show services nat pool detail (Port Block Allocation) on page 1959

Output Fields
Table 83 on page 1954 lists the output fields for the **show services nat pool** command. Output fields are listed in the approximate order in which they appear.

Table 83: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of an adaptive services 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-nat-pt**, Y, Y, Y, Y, Y, Y, Y, Y, Y, Y, Y, Y.	All levels
Address or **Address range**	IPv4 address range of the pool.	All levels
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
Port block type	Type of port block allocation: secured or deterministic	All levels

Table 83: show services nat pool Output Fields *(continued)*

Field Name	Field Description	Level of Output
Available addresses	Number of free addresses in the NAT pool.	**detail**
Configured port range	The range of ports configured to be used for NAT pool.	**detail**
Out of port errors	Number of port allocation errors. Applicable only for dynamic NAT pools. Not displayed for static NAT pools.	**detail**
Parity port errors	Number of port allocations that failed because a port number of the desired parity was not available.	**detail**
Preserve Range errors	Number of port allocations that failed because a port in the desired range was not available.	**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**
AP-P port allocation errors	When address pooling paired (AP-P) is configured, a private IP is paired to a public IP. This is a counter of translation errors where there are free ports available in the NAT pool, but none for the NAT IP to which the private IP is paired.	**detail**
AP-P port limit allocation errors	When AP-P is configured, this is a counter of out-of-port errors that are due to a configured limit for the number of allocated ports in the **limit-ports-per-address** statement at the **[edit services nat pool *nat-pool-name*]** hierarchy level.	**detail**
Memory allocation errors	Number of memory allocation failures.	**detail**
EIF Inbound session count	Current number of EIF inbound sessions.	**detail**
EIF Inbound session Limit exceeded drops	Number of inbound connections that were dropped because the EIF limit was exceeded.	**detail**
Port block size	Number of ports in a port block.	none **brief**

Table 83: show services nat pool Output Fields *(continued)*

Field Name	Field Description	Level of Output
Max port blocks per address	Maximum number of port blocks per private address.	none **brief**
Active block timeout	Activity timeout of port block.	none **brief**
Effective port range	Effective range of port numbers.	none **brief**
Effective number of port blocks	Effective number of port blocks.	none **brief**
Effective number of ports	Effective number of ports.	none **brief**
Port block efficiency	Port block efficiency.	none **brief**
Port blocks limit exceeded errors	The total number of times when a request for more than the allowed port blocks allocated for a user arrives from a user.	All levels
Preserve range enabled	Whether the capability to preserve the privileged port range after translation is enabled. One of the following is displayed: • **Is active**—Preservation of port range is enabled. • **Not active**—Preservation of port range is not enabled.	**detail**
AP-P out of port errors	When AP-P is configured, a private IP is paired to a public IP. This is a counter of translation errors where there are free ports available in the NAT pool, but none for the NAT IP to which the private IP is paired.	**detail**
MAX number of port blocks used	The maximum number of port blocks used.	All levels
Current number of port blocks in use	Current count of the port blocks that are being used.	**detail**
Port block allocation errors	The consolidated number of port block allocation errors.	All levels

Table 83: show services nat pool Output Fields *(continued)*

Field Name	Field Description	Level of Output
Port block memory allocation errors	The number of memory allocation errors for port blocks.	All levels
DetNat subscriber exceeded port limits	The number of times a subscriber exceeded its port limits for a NAT pool that uses deterministic port block allocation.	All levels
Unique pool users	The number of different users of the NAT pools.	All levels
Current EIF Inbound flows count	Current count of EIF inbound flows, including all EIF flows per pool.	**detail**
EIF flow limit exceeded drops	Current number of flow drops due to exceeded flow limit. This number is per pool, not per EIF mapping.	**detail**

Sample Output

show services nat pool brief

```
user@host> show services nat pool brief
```

```
Interface: ms-1/0/0, Service set: s1
NAT pool          Type    Address                         Port        Ports used
dest-pool         DNAT-44 10.10.10.2-10.10.10.2
napt-pool         NAPT-44 50.50.50.1-50.50.50.254         1024-63487  0
source-dynamic-pool DYNAMIC NAT44 40.40.40.1-40.40.40.254
source-static-pool BASIC NAT44 30.30.30.1-30.30.30.254
```

show services nat pool detail

```
user@host> show services nat pool detail
```

```
Interface: ms-4/0/0, Service set: ss1
  NAT pool: srcpool, Translation type: NAPT-44
   Address range: 100.0.0.1-100.0.0.254
   Available addresses: 254
   Configured port range: 1024-65535
   Port range: 1024-65535, Ports in use: 0, Out of port errors: 0
   Parity port errors: 0, Preserve Range errors: 0
   Max ports used: 0
   AP-P port allocation errors: 0, AP-P port limit allocation errors: 0
   Memory allocation errors: 0
   EIF Inbound session count: 0
   EIF Inbound session Limit exceeded drops: 0
```

show services nat pool (Secured Port Block Allocation)

`user@host>` **show services nat pool**

```
Interface: sp-2/0/0, Service set: in
NAT pool          Type    Address                          Port        Ports used
mypool            dynamic 3.3.3.3-3.3.3.10                 512-65535   0
                          3.3.3.15-3.3.3.20
                          3.3.3.25-3.3.3.30
                          3.3.3.95-3.3.3.200
Port block size: 64, Max port blocks per address: 1, Active block timeout: 86400,
 Effective port range: 1024-65471,
Effective number of port blocks: 126882, Effective number of ports: 8120448, Port
 block efficiency: nan

Interface: sp-2/1/0, Service set: in1
NAT pool          Type    Address                          Port        Ports used
mypool1           dynamic 9.9.9.1-9.9.9.254                512-65535   0
Port block size: 64, Max port blocks per address: 1, Active block timeout: 86400,
 Effective port range: 1024-65471,
Effective number of port blocks: 255778, Effective number of ports: 16369792, Port
 block efficiency: nan
```

show services nat pool detail (Deterministic Port Block Allocation)

`user@host>` **show services nat pool detail**

```
Interface: sp-2/0/0, Service set: ss1
  NAT pool: napt_pool, Translation type: dynamic
```

```
    Address range: 5.5.5.1-5.5.5.254
    Configured port range: 1-60000, Preserve range enabled: Is active
    Port range: 2000-2002, Ports in use: 2, Out of port errors: 0, Max ports used:
 2
    AP-P out of port errors: 188
    Max number of port blocks used: 1, Current number of port blocks in use: 1,
Port block allocation errors: 0,
    Port block memory allocation errors: 0
    DetNAT subscriber exceeded port limits: 1
    Unique pool users: 1
```

show services nat pool (Deterministic Port Block Allocation)

`user@host>` **show services nat pool**

```
Interface: sp-2/0/0, Service set: ss2
NAT pool          Type    Address                          Port        Ports Used
pba               dynamic 33.33.33.1-33.33.33.128          512-65535   6604
Port block type: Deterministic port block, Port block size: 200
```

show services nat pool detail (Port Block Allocation)

`user@host>` **show services nat pool detail**

```
Interface: sp-2/0/0, Service set: s
  NAT pool: napt_pool, Translation type: dynamic
    Address range: 44.1.1.1-44.1.1.1
    Configured port range: 1-60000
    Port range: 1024-65535, Ports in use: 0, Out of port errors: 0,
    Max ports used: 0
    AP-P out-of-port errors: 0
    Current EIF Inbound flows count: 0
    EIF flow limit exceeded drops: 0
```

show services pcp statistics

Syntax

```
show services pcp statistics
```

Release Information

Command introduced in Junos OS Release 13.2
Command introduced in Junos OS Release 20.1R1 for Next Gen Services

Description

Display information PCP mappings.

Required Privilege Level

view

List of Sample Output

show services pcp statistics pcp on page 1962

Output Fields

Table 84 on page 1960 lists the output fields for the **show services pcp statistics** command. Output fields are listed in the approximate order in which they appear.

Table 84: show services pcp statistics Output Fields

Field Name	Field Description
Services PIC Name	Name of a service interface.
Protocol Statistics	Overall PCP statistics, consisting of: operational, option, and results statistics.
Operational Statistics	Operational statistics group.
Map request received	Total PCP MAP requests received from PCP clients.
Peer request received	Number of peer requests received.
Option Statistics	Number of requests using available options.
Unprocessed requests received	Number of requests received with no option specified.
Third party requests received	Number of third-party requests received.
Prefer fail option received	Number of prefer fail requests received.

Table 84: show services pcp statistics Output Fields *(continued)*

Field Name	Field Description
Filter option received	Number of filter option requests received.
Other options counters	Number of packets received with options other than **prefer-fail** and **third-party**.
Other optional received	
Results Statistics	Information about the results of PCP requests.
PCP success	Number of PCP MAP requests successfully processed by the server.
PCP unsupported version	Number of PCP packets received with version other than 1.
Not authorized	Number of unauthorized MAP delete requests.
Bad requests	Number of requests with invalid PCP packets.
Unsupported opcode	Number of packets that have an unsupported opcode.
Unsupported option	Number of packets that have an unsupported option.
Bad option	Number of packet that have a malformed option.
Network failure	Number of times a mapping could not be provided due to a network failure.
Out of resources	Number of times a mapping could not be provided because the PCP server ran out of pool resources.
Unsupported protocol	Number of requests for which the protocol was neither TCP nor UDP.
User exceeded quota	Number of requests for which the PCP client requested more than the configured number of ports.
Cannot provide external	Number of requests for which the PCP server cannot provide the external address or port requested by the client.
Address mismatch	Number of requests for which the PCP client IP address and the layer-3 source IP do not match.
Excessive number of remote peers	This counter is not currently used.

Table 84: show services pcp statistics Output Fields *(continued)*

Field Name	Field Description
Processing error	Number of requests with malformed PCP packets information, such as an invalid IP address in a **third-party** request .
Other result counters	Not currently used.

Sample Output

show services pcp statistics pcp

`user@host>` **show services pcp statistics pcp**

```
  Services PIC Name:    sp-2/1/0

Protocol Statistics:

Operational Statistics

  Map request received                                : 0
  Peer request received                               : 0
  Other operational counters                          : 0

 Option Statistics

  Unprocessed requests received                       : 0
  Third party requests received                       : 0
  Prefer fail option received                         : 0
  Filter option received                              : 0
  Other options counters                              : 0
  Option optional received                            : 0

Result Statistics

  PCP success                                         : 0
  PCP unsupported version                             : 0
  Not authorized                                      : 0
  Bad requests                                        : 0
  Unsupported opcode                                  : 0
  Unsupported option                                  : 0
  Bad option                                          : 0
```

```
Network failure                                    : 0
Out of resources                                   : 0
Unsupported protocol                               : 0
User exceeded quota                                : 0
Cannot provide external                            : 0
Address mismatch                                   : 0
Excessive number of remote peers                   : 0
Processing error                                   : 0
Other result counters                              : 0
```

show services redundancy-group

Syntax

```
show services redundancy-group
<rg-id>
<brief | extensive | terse>
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.

Description

Display redundancy group status information for all redundancy groups or a specified redundancy group.

Options

rg-id—(Optional) Name of a specific redundancy group.

brief | extensive | terse—(Optional) Display the specified level of output. When no level is specified, display terse level output.

Default: terse

Required Privilege Level

view

List of Sample Output

show services redundancy-group terse on page 1970
show services redundancy-group brief (Health Status Passed) on page 1970
show services redundancy-group brief (Health Status Failed) on page 1971
show services redundancy-group extensive on page 1972

Output Fields

Table 85 on page 1964 lists the output fields for the **show services redundancy-group** command. Output fields are listed in the approximate order in which they appear.

Table 85: show services redundancy-group Output Fields

Field Name	Field Description	Level of Output
ICCP process connection	Status of the connection between the srd and iccpd. • Connected • Not connected	all levels
Redundancy Group ID	Identifier of the redundancy group.	all levels

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
Number of peer RG connections	Total number of peers in the redundancy group.	brief, extensive
Local RG IP	IP address of the local redundancy group.	all levels
RS ID		terse
Local RS state	State of the local redundancy set. • MASTER • STANDBY • INITIALIZING • STANDBY (WARNED)	terse
Peer RS state	State of the peer redundancy set. • MASTER • STANDBY • INITIALIZING • STANDBY (WARNED)	terse
Peer RG IP	Peer redundancy group IP address.	all
Status	Status of redundancy group connection with this peer. • Connected • Not Connected	terse
Number of peer RG connections	Total number of peers in the redundancy group.	brief
Redundancy Set ID	Identifier of the redundancy set.	brief, extensive
Connection status	Status of the connection between the srd and iccpd. • Connected • Not Connected	brief, extensive

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
Redundancy Set state	State of the local redundancy set state. • INITIALIZING • MASTER • STANDBY • STANDBY (WARNED)	brief, extensive
Redundancy Set peer state	State of the peer redundancy set state. • INITIALIZING • MASTER • STANDBY • STANDBY (WARNED)	brief, extensive
Redundancy Set health status	• Passed • Failed	brief, extensive
Number of Monitored interface down	Number of monitored interfaces that are d	brief, extensive
Failed Interfaces	List of all monitored interfaces that are down.	brief, extensive
Service Set	Service set used for stateful sync.	brief, extensive
Service Interface	Service set used for	brief, extensive
Type	Type of redundancy and stateful sync for the listed service interface. • Inter-chassis • Intra-chassis	brief, extensive
Role	Role of the listed service interface. • active • backup	brief, extensive
Connection	Status of connection with peer service PIC. • Up • Down	brief, extensive

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
Synchronization	Type of synchronization. When all eligible sessions are still synchronizing, it is cold synchronization. When all current existing sessions are synchronized, it is a HOT synchronization, When long lived sessions are eligible, they are synchronized. • Hot—All current existing sessions are synced. When long-lived sessions are eligible, they are synchronized. • Cold–Eligible sessions are in the processing of synchronizing.	brief, extensive
ICCP process connection open complete count	Number of completed opens of ICCP process connections.	extensive
ICCP process connection close complete count	Number of completed closes of ICCP process connections.	
ICCP packet sent count	Number of ICCP packets sent.	extensive
ICCP packet receive count	Number of ICCP packets received.	extensive
ICCP process keepalive receive count	Number of ICCP process keepalive messages received.	extensive
ICCP process keepalive sent count	Number of ICCP process keepalive messages sent.	extensive
ICCP redundancy group add count	Number of redundancy group add messages received by srd from ICCP.	extensive
ICCP redundancy group delete count	Number of redundancy group delete messages received by srd from ICCP.	extensive
RG connection up count	Number of redundancy group connection up messages received by srd from ICCP.	extensive
RG connection down count	Number of redundancy group connection down messages received by srd from ICCP.	extensive

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
RG join count	Number of redundancy group join messages sent from srd to ICCP.	extensive
RG data receive count	Number of packets of messages received by srd from a peer.	extensive
RG data sent count	Number of packets of messages sent from srd to a peer.	extensive
RG connect message sent count	Number of connect messages sent from srd to ICCP.	extensive
RG connect message receive count	Number of connect messages received by srd from ICCP.	extensive
RG disconnect message sent count	Number of disconnect messages sent from srd to ICCP.	extensive
RG disconnect message receive count	Number of disconnect messages received by srd from ICCP.	extensive
RG ack sent count	Number of RG ack messages sent.	extensive
RG nack sent count	Number of RG nack messages sent.	extensive
RG nack receive count	Number of RG nack messages received.	extensive
Transition Events Received	Number of transition events received in each of the following categories: • Acquire mastership auto • Acquire mastership manual • Release mastership auto • Release mastership manual	extensive

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
Transition Events Ignored	Number of transition events ignored in each of the following categories: • Acquire mastership auto • Acquire mastership manual • Release mastership auto • Release mastership manual In a high-availability or redundancy pair of SDGs, in which one SDG is the master and the other is the standby, when perform a double failover of the SDGs, the second failover event is not ignored, which is the expected behavior. The event is not disregarded because it arrives as a critical redundancy-event based on the redundancy-policy. However, because the SDG is already be in Standby state, the finite state machine transitions to the Standby-Warned state until it recovers. Therefore, the event is honored and not ignored. Although there was no mastership transition, it is because of a valid reason that the SDG is already in Standby state. The redundancy-event is associated with to a mastership release policy based on the configuration and the Release mastership field under the Transition Events Ignored column displays a number that corresponds to the redundancy event. The services redundancy daemon (SRD) finite state machine quickly recovers (transitions from Standby-Warned to Standby) during restart-routing because the rpd restart-handling and recovery are fast and the following critical event is not ignored. However, disabling or deactivating the interface results in the FSM remaining in Standby-Warned until the interface is up. Any critical events during the time when the interface is down are ignored because the state is already Standby-Warned and does not transition to a different state. In summary, the following is the manner in which critical events are analyzed during state transitions: • Standby -> Standby Warned = Critical Event Not ignored [valid state transition] • Standby Warned -> Standby Warned = Critical Event Ignored [no state transition]	extensive

Table 85: show services redundancy-group Output Fields *(continued)*

Field Name	Field Description	Level of Output
Monitored Events Received	Number of monitored events received in each of the following categories: • Link-down • Routing restart/abort • Route update error • Peer mastership-acquire • Peer mastership-release	extensive
Monitored Events Ignored	Number of monitored events ignored in each of the following categories: • Link-down • Routing restart/abort • Route update error • Peer mastership-acquire • Peer mastership-release	extensive

Sample Output

show services redundancy-group terse

`user@host>` **show services redundancy-group terse**

```
ICCP process connection               : Connected

Redundancy Group ID             : 1
  Number of peer RG connections  : 1
  Local RG IP                   : 172.19.39.70
  RS ID     Local RS state     Peer RS state     Peer RG IP        Status
  1         MASTER             STANDBY           172.19.39.69      Connected
```

show services redundancy-group brief (Health Status Passed)

`user@host>` **show services redundancy-group brief**

```
ICCP process connection                 : Connected
Redundancy Group ID                     : 1
```

```
  Number of peer RG connections          : 1
  Local RG IP                            : 172.19.39.70
  Redundancy Set ID                      : 1
    Connection status                    : Connected
    Redundancy Set state                 : MASTER
    Redundancy Set peer state            : STANDBY
    Peer RG IP                           : 172.19.39.69
    Redundancy Set health status         : Passed
      Service Set : IPv6-SFW
        Service interface     Type              Role       Connection
Synchronization
        ms-1/3/0              Inter-chassis     active     Up             Hot

        ms-1/2/0              Inter-chassis     active     Up             Hot

        ms-1/1/0              Inter-chassis     active     Up             Hot

        ms-1/0/0              Inter-chassis     active     Up             Hot

      Service Set : NAPT44-SS1-SS4
        Service interface     Type              Role       Connection
Synchronization
        ms-1/3/0              Inter-chassis     active     Up             Hot

        ms-1/2/0              Inter-chassis     active     Up             Hot

        ms-1/1/0              Inter-chassis     active     Up             Hot

        ms-1/0/0              Inter-chassis     active     Up             Hot
```

show services redundancy-group brief (Health Status Failed)

`user@host>` **show services redundancy-group brief**

```
ICCP Process Connection               : Connected
Redundancy Group ID   : 1
  Number of Members   : 2
  Redundancy Set ID       : 1
    Remote IP address                          : 203.0.113.2
    Connection Status                           : Connected
    Redundancy Set State                       : STANDBY (WAIT)
    Redundancy Set Peer State                : MASTER
    Redundancy Set Health Status           : Failed
      Number of  Monitored interface down : 1            <<<<<<< Failure Reasons
```

```
      Failed Interfaces
<<<<<<<  Name of the monitored interfaces which have gone  down
        ms-2/3/0
      Service Set : ss2
        Service Interface     Type                  Role           Connection
 Synchronization
        ms-2/2/0                  Inter-chassis     backup     Up
     Hot
        ms-2/1/0                  Inter-chassis     backup     Down
  Off
        ms-2/0/0                  Inter-chassis     backup     Down
  Off
      Service Set : ss_new
        Service Interface     Type                  Role          Connection
Synchronization
        ms-2/3/0
```

show services redundancy-group extensive

user@host> **show services redundancy-group extensive**

```
ICCP process connection                        : Connected
ICCP process connection close count            : 0
ICCP process connection open complete count    : 1
ICCP packet sent count                         : 7303
ICCP packet receive count                      : 7321
ICCP process keepalive receive count           : 7253
ICCP process keepalive sent count              : 7253
ICCP redundancy group add count                : 0
ICCP redundancy group delete count             : 0
Redundancy Group ID                      : 1
  Number of peer RG connections          : 1
  Local RG IP                            : 172.19.39.70
  RG connection up count                 : 4
  RG connection down count               : 2
  RG join count                          : 4
  RG data receive count                  : 37
  RG data sent count                     : 0
  RG connect message sent count          : 4
  RG connect message receive count       : 4
  RG disconnect message sent count       : 0
  RG disconnect message receive count    : 4
  RG ack sent count                      : 4
```

```
  RG nack sent count                    : 0
  RG nack receive count                 : 4
  Redundancy Set ID                     : 1
    Connection status                   : Connected
    Redundancy Set state                : MASTER
    Redundancy Set peer state           : STANDBY
    Peer RG IP                          : 172.19.39.69
    Redundancy Set health status        : Passed
      Service Set : IPv6-SFW
        Service interface     Type              Role       Connection
Synchronization
        ms-1/3/0              Inter-chassis     active     Up             Hot

        ms-1/2/0              Inter-chassis     active     Up             Hot

        ms-1/1/0              Inter-chassis     active     Up             Hot

        ms-1/0/0              Inter-chassis     active     Up             Hot

      Service Set : NAPT44-SS1-SS4
        Service interface     Type              Role       Connection
Synchronization
        ms-1/3/0              Inter-chassis     active     Up             Hot

        ms-1/2/0              Inter-chassis     active     Up             Hot

        ms-1/1/0              Inter-chassis     active     Up             Hot

        ms-1/0/0              Inter-chassis     active     Up             Hot

    Transition events              Received         Ignored
      Acquire mastership auto      3                0
      Acquire mastership manual    0                0
      Release mastership auto      3                0
      Release mastership manual    0                0

    Monitored events               Received         Ignored
      Link-down                    145              31
      Routing restart/abort        1                0
      Route update error           0                0
      Peer mastership-acquire      3                0
      Peer mastership-release      3                0
```

show services security-intelligence category summary

Syntax

```
show services security-intelligence category summary category-name
```

Release Information

Statement introduced before Junos OS Release 18.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480, and MX960 with the MX-SPC3 services card.
Support for threat feed status (enabled, disabled, or user disabled) is added in Junos OS Release 20.1R1.

Description

Display summary for the specified Security Intelligence category.

Options

category-name—Name of the category.

Required Privilege Level

View

RELATED DOCUMENTATION

security-intelligence | 1442

List of Sample Output

show services security-intelligence category summary on page 1975

Output Fields

Table 86 on page 1974 lists the output fields for the **show services security-intelligence category summary** command. Output fields are listed in the approximate order in which they appear.

Table 86: show services security-intelligence category summary Output Fields

Field Name	Field Description
Category name	Name of the Security Intelligence category.
Status	Status of the Security Intelligence category.
Description	Description of the Security Intelligence category
Update interval	Amount of time after which Policy Enforcer sends an update for the feed.

Table 86: show services security-intelligence category summary Output Fields *(continued)*

Field Name	Field Description
TTL	Length of time (in minutes) the file remains open, receiving statistics before it is closed, transferred, and rotated. When either the time or the file size is exceeded, the file is closed and a new one is opened, whether or not a transfer site is specified.
Feed name	Information about the feed, including: • **Version** • **Object umber** • **Create time** • **Update time** • **Update status** • **Expired** • **Options** • **Status**

Sample Output

show services security-intelligence category summary

`user@host>` **show services security-intelligence category summary**

```
node1:
--------------------------------------------------------------------------

Category name     :CC
  Status          :Enable
  Description     :Command and Control data schema
  Update interval :1800s
  TTL             :3456000s
  Feed name       :cc_ip_data
    Version       :N/A
    Objects number:0
    Create time   :2018-03-16 05:57:39 PDT
    Update time   :2018-03-19 12:30:32 PDT
    Update status :N/A
    Expired       :No
    Options       :N/A
    Status        :Enabled
```

```
Feed name       :cc_ipv6_data
  Version       :20180228.1
  Objects number:1
  Create time   :2018-03-16 05:57:39 PDT
  Update time   :2018-03-16 06:19:47 PDT
  Update status :Store succeeded
  Expired       :No
  Options       :N/A
  Status        :Disabled
```

show services security-intelligence update status

Syntax

```
show services security-intelligence update status
```

Release Information

Statement introduced before Junos OS Release 18.4.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480, and MX960 with the MX-SPC3 services card.

Description

Display the status of the connection with Policy Enforcer.

Required Privilege Level

View

RELATED DOCUMENTATION

security-intelligence | 1442

List of Sample Output

show services security-intelligence update status on page 1977

Sample Output

show services security-intelligence update status

`user@host>` **show services security-intelligence update status**

```
node1:
--------------------------------------------------------------------------
Current action        :Start downloading the latest manifest.
Last update status    :Download manifest failed.
Last connection status:succeeded
Last update time      :2018-03-21 16:59:59 PDT
```

show services service-sets cpu-usage

Syntax

```
show services service-sets cpu-usage
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display service set CPU usage as a percentage. The command is supported only on Adaptive Services PICs (SP PICs).

Options

none—Display CPU usage for all adaptive services interfaces and service sets.

interface *interface-name*—(Optional) Display CPU usage for a particular interface. On M Series and T Series routers, the ***interface-name*** parameter can have the value **sp-*fpc/pic/port*** or **rsp*number***.

service-set *service-set-name*—(Optional) Display CPU usage for a particular service set. For the Layer 2 Tunneling Protocol (L2TP), you can use a tunnel group to represent a service set.

Required Privilege Level

view

List of Sample Output

show services service-sets cpu-usage on page 1979

Output Fields

Table 87 on page 1978 lists the output fields for the **show services service-sets cpu-usage** command. Output fields are listed in the approximate order in which they appear.

Table 87: show services service-sets cpu-usage Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface

Table 87: show services service-sets cpu-usage Output Fields *(continued)*

Field Name	Field Description
Service set (system category)	Name of the CPU usage category: • idp_recommended—Name of the service sets (displays all the service sets attached to the service PICs) • Idle • System • Receive • Transmit
CPU utilization %	Percentage of the CPU resources being used

Sample Output

show services service-sets cpu-usage

`user@host>` **show services service-sets cpu-usage**

```
Interface   Service set (system category)                CPU utilization %
sp-4/1/0    idp_recommended                                        18.20 %
sp-4/1/0    Idle                                                   44.69 %
sp-4/1/0    System                                                  7.01 %
sp-4/1/0    Receive                                                15.10 %
sp-4/1/0    Transmit                                               15.00 %
```

show services service-sets memory-usage

Syntax

```
show services service-sets memory-usage
<interface interface-name>
<service-set service-set-name>
<zone>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display service set memory usage.

Options

none—Display service set memory usage.

interface *interface-name*—(Optional) Display memory usage for a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port***, or **rsp*number***.

> **NOTE:** This command is not supported on Multilink Protocol–based services PICs.
>
> The interface option is not supported on Multiservice PICs.

service-set *service-set-name*—(Optional) Display memory usage for a particular service set. For Layer 2 Tunneling Protocol (L2TP), you can use a tunnel group to represent a service set.

zone—(Optional) Display the memory usage zone of the adaptive services interface or an individual service set.

Required Privilege Level

view

List of Sample Output

show services service-sets memory-usage on page 1981
show services service-sets memory-usage zone on page 1981
show services service-sets memory-usage interface on page 1981

Output Fields

Table 88 on page 1981 lists the output fields for the **show services service-sets memory-usage** command. Output fields are listed in the approximate order in which they appear.

Table 88: show services service-sets memory-usage Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service set	Name of a service set
Bytes Used	Number of bytes of memory being used
Memory zone	Memory zone in which the adaptive services interface is currently operating: • **Green**—All new flows are allowed. • **Yellow**—Unused memory is reclaimed. All new flows are allowed. • **Orange**—New flows are allowed only for service sets that are using less than their equal share of memory. • **Red**—No new flows are allowed.

Sample Output

show services service-sets memory-usage

```
user@host> show services service-sets memory-usage
```

```
Interface   Service set                                Bytes Used
ms-4/0/0    N/A                                           14817036
ms-4/1/0    N/A                                           14691700
```

show services service-sets memory-usage zone

```
user@host> show services service-sets memory-usage zone
```

```
Interface   Memory zone
```

show services service-sets memory-usage interface

```
user@host> show services service-sets memory-usage interface ms-4/1/0
```

```
Interface   Service Set                                      Bytes Used
 ms-4/1/0    N/A                                                 14691700
```

show services service-set statistics ids drops

Syntax

```
show services service-set statistics ids drops
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 17.1 on MX Series.

Description

Display statistics for packet drops resulting from header-integrity, suspicious packet pattern, and session-limit checks performed by an MS-MPC or MS-MIC.

Options

none—Display statistics for all configured service interfaces and service sets.

interface *interface-name*—(Optional) Display statistics for the specified services interface.

service-set *service-set-name* —(Optional) Display statistics for the specified service set.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | 601

List of Sample Output

show services service-set statistics ids drops on page 1990

Output Fields

Table 89 on page 1983 lists the output fields for the **show services service-set integrity-drops** command. Output fields are listed in the approximate order in which they appear.

Table 89: show services service-set statistics ids drops Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
Errors	Total errors, categorized by protocol: • **IP**—Total IP version 4 errors. • **TCP**—Total Transmission Control Protocol (TCP) errors. • **UDP**—Total User Datagram Protocol (UDP) errors. • **ICMP**—Total Internet Control Message Protocol (ICMP) errors.

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
IP Errors	

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
	Number of IPv4 errors for the following categories: • **IP packet length inconsistencies**—IP packet length did not match the Layer 2 reported length. • **Minimum IP header length check failures**—Minimum IP header length is 20 bytes. The received packet contained less than 20 bytes. • **Reassembled packet exceeds maximum IP length**—After fragment reassembly, the reassembled IP packet length exceeded 65,535. • **Illegal source address 0**—Source address is not a valid address. Invalid addresses are loopback, broadcast, multicast, and reserved addresses. Source address **0**, however, is allowed to support BOOTP and the destination address **0xffffffff**. • **Illegal destination address** —Destination address was not a valid address. The address is reserved. • **TTL zero errors**—Received packet had a time-to-live (TTL) value of 0. • **Illegal IP protocol number 0 or 255**—IP protocol is 0 or 255. • **Land attack**—IP source address is the same as the destination address. • **Non-IP packets**—Packet did not conform to the IP standard. • **IP option**—Packet had a non-allowed IP option. • **Non-IPv4 packets**—Packet was not of the IPv4 type. • **Non-IPv6 packets**—Packet was not of the IPv6 type. • **Bad checksum**—Packet had an invalid IP checksum. • **Illegal IP fragment length**—Illegal fragment length. All fragments (other than the last fragment) must have a length that is a multiple of 8 bytes. • **IP fragment overlap**—Fragments had overlapping fragment offsets. • **IP fragment limit exceeded** —Configured number of allowed fragments for a packet was exceeded. • **IP fragment reassembly timeout**—Some of the fragments for an IP packet were not received in time, and the reassembly handler dropped partial fragments. Whenever a fragment is received, it is maintained in a chain until all other fragments are received. If other fragments do not arrive

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
	within the configured value of reassembly-timeout, this packet is dropped and the value of the counter shown in this field is incremented. If other fragments arrive in time but the total number of fragments is more than the configured value of fragment-limit, all the fragments (of this packet) are dropped and the value of the counter shown in this field is incremented. • **IPv4 bad options**—Packet IP header contained IPv4 option that is not allowed. • **IPv6 bad extension headers**—Packet contained IPv6 extension header type that is not allowed. • **session-limit exceeded for source**—Number of concurrent sessions from an individual source address or subnet exceeded limit. • **session-limit exceeded for destination**—Number of concurrent sessions to an individual destination address or subnet exceeded limit. • **connections/second limit exceeded for source**—Number of connections per second for an individual source address or subnet exceeded limit. • **connections/second limit exceeded for destination**—Number of connections per second for an individual destination address or subnet exceeded limit. • **packets/second limit exceeded for source**—Number of packets per second for an individual source address or subnet exceeded limit. • **packet/second limit exceeded for destination**—Number of packets per second for an individual destination address or subnet exceeded limit. • **Unknown** —Unknown fragments.

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
TCP Errors	Number of TCP protocol errors for the following categories: • **TCP header length inconsistencies**—Minimum TCP header length is 20 bytes, and the IP packet received did not contain at least 20 bytes. • **Source or destination port number is zero**—TCP source or destination port was zero. • **Illegal sequence number, flags combination**—Packet had any type of TCP header anomaly. • **TCP winnuke**—TCP segments destined for port 139 with the urgent (URG) flag set. • **TCP SYN Fragment**—TCP SYN packet was a fragment. • **TCP connection closed due to SYN defense**—Unestablished TCP connection closed because **open-timeout** value expired. • **TCP session-limit exceeded for source**—Number of concurrent TCP sessions from an individual source address or subnet exceeded limit. • **TCP session-limit exceeded for destination**—Number of concurrent TCP sessions to an individual destination address or subnet exceeded limit. • **TCP connections/second limit exceeded for source**—Number of TCP connections per second for an individual source address or subnet exceeded limit. • **TCP connections/second limit exceeded for destination**—Number of TCP connections per second for an individual destination address or subnet exceeded limit. • **TCP packets/second limit exceeded for source**—Number of TCP packets per second for an individual source address or subnet exceeded limit. • **TCP packet/second limit exceeded for destination**—Number of TCP packets per second for an individual destination address or subnet exceeded limit.

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
UDP Errors	Number of UDP protocol errors for the following categories: • **IP data length less than minimum UDP header length (8 bytes)**—Minimum UDP header length is 8 bytes. The received IP packets contained less than 8 bytes. • **Source or destination port is zero**—UDP source or destination port was **0**. • **UDP session-limit exceeded for source**—Number of concurrent UDP sessions from an individual source address or subnet exceeded limit. • **UDP session-limit exceeded for destination**—Number of concurrent UDP sessions to an individual destination address or subnet exceeded limit. • **UDP connections/second limit exceeded for source**—Number of UDP connections per second for an individual source address or subnet exceeded limit. • **UDP connections/second limit exceeded for destination**—Number of UDP connections per second for an individual destination address or subnet exceeded limit. • **UDP packets/second limit exceeded for source**—Number of UDP packets per second for an individual source address or subnet exceeded limit. • **UDP packet/second limit exceeded for destination**—Number of UDP packets per second for an individual destination address or subnet exceeded limit.

Table 89: show services service-set statistics ids drops Output Fields *(continued)*

Field Name	Field Description
ICMP Errors	Number of ICMP protocol errors for the following categories: • **IP data length less than minimum ICMP header length (8 bytes)**—ICMP header length contained less than 8 bytes. • **ICMP error length inconsistencies**—ICMP error packet length was outside range of 48 bytes through 576 bytes. • **ICMP fragments**— ICMP packet was an IP fragment. • **ICMP session-limit exceeded for source**—Number of concurrent ICMP sessions from an individual source address or subnet exceeded limit. • **ICMP session-limit exceeded for destination**—Number of concurrent ICMP sessions to an individual destination address or subnet exceeded limit. • **ICMP connections/second limit exceeded for source**—Number of ICMP connections per second for an individual source address or subnet exceeded limit. • **ICMP connections/second limit exceeded for destination**—Number of ICMP connections per second for an individual destination address or subnet exceeded limit. • **ICMP packets/second limit exceeded for source**—Number of ICMP packets per second for an individual source address or subnet exceeded limit. • **ICMP packet/second limit exceeded for destination**—Number of ICMP packets per second for an individual destination address or subnet exceeded limit.

Sample Output

show services service-set statistics ids drops

`user@host>` **show services service-set statistics ids drops**

```
Interface: ms-1/0/0
 Service set: sset1
   Errors:
     IP: 0, TCP: 0
     UDP: 0, ICMP: 0
   IP errors:
```

```
  IP packet length inconsistencies: 0
  Illegal source address: 0
  Illegal destination address: 0
  TTL zero errors: 0, Illegal IP protocol number (0 or 255): 0
  Land attack: 0
  Non-IPv4 packets: 0
  Non-IPv6 packets: 0
  Bad checksum: 0
  Illegal IP fragment length: 0
  IP fragment overlap: 0
  IP fragment reassembly timeout: 0
  IP fragment limit exceeded: 0
  IPv4 bad options: 0
  IPv6 bad extension headers: 0
  session-limit exceeded for source: 0
  session-limit exceeded for destination: 0
  connections/second limit exceeded for source: 0
  connections/second limit exceeded for destination: 0
  packets/second limit exceeded for source: 0
  packet/second limit exceeded for destination: 0
  Unknown: 0
TCP errors:
  TCP header length inconsistencies: 0
  Source or destination port number is zero: 0
  Illegal sequence number and flags combinations: 0
  TCP winnuke: 0
  TCP SYN Fragment: 0
  TCP connection closed due to SYN defense: 0
  TCP session-limit exceeded for source: 0
  TCP session-limit exceeded for destination: 0
  TCP connections/second limit exceeded for source: 0
  TCP connections/second limit exceeded for destination: 0
  TCP packets/second limit exceeded for source: 0
  TCP packet/second limit exceeded for destination: 0
UDP errors:
  IP data length less than minimum UDP header length (8 bytes): 0
  Source or destination port number is zero: 0
  UDP session-limit exceeded for source: 0
  UDP session-limit exceeded for destination: 0
  UDP connections/second limit exceeded for source: 0
  UDP connections/second limit exceeded for destination: 0
  UDP packets/second limit exceeded for source: 0
  UDP packet/second limit exceeded for destination: 0
ICMP errors:
```

```
IP data length less than minimum ICMP header length (8 bytes): 0
ICMP error length inconsistencies: 0
ICMP fragments: 0
ICMP session-limit exceeded for source: 0
ICMP session-limit exceeded for destination: 0
ICMP connections/second limit exceeded for source: 0
ICMP connections/second limit exceeded for destination: 0
ICMP packets/second limit exceeded for source: 0
ICMP packet/second limit exceeded for destination: 0
```

show services service-sets statistics ids session-limits counters

Syntax

```
show services service-sets statistics ids session-limits counters
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 17.1 on MX Series.

Description

Display counters for session drops and packet drops resulting from session-limit checks performed by an IDS rule on an MS-MPC or MS-MIC.

Options

none—Display statistics for all configured services interfaces.

interface *interface-name*—(Optional) Display statistics for the specified services interface.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring Protection Against Network Attacks on an MS-MPC | **601**

List of Sample Output

show services service-sets statistics ids session-limits counters interface on page 1997

Output Fields

Table 90 on page 1993 lists the output fields for the **show services service-set statistics ids session-limits counters** command. Output fields are listed in the approximate order in which they appear.

Table 90: show services service-sets statistics ids session-limits counters Output Fields

Field Name	Field Description
Interface	Name of the service interface assigned to the service set.
Service set	Name of the service set to which the IDS rule is applied.

Table 90: show services service-sets statistics ids session-limits counters Output Fields *(continued)*

Field Name	Field Description
Ingress General Info	Information for IDS rules for the service set in the ingress direction. • **Match-direction**—Displays **input**. • **Rule name**—Name of the IDS rule. • **Term name**—Name of the term in the IDS rule.
Ingress TCP Counters	Session-limit TCP counters in the ingress direction for the following: • **Sessions allowed**—Number of TCP sessions allowed by the IDS rule. • **Sessions ignored**—Number of TCP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of TCP sessions dropped because the number of TCP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of TCP sessions dropped because the number of TCP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of TCP sessions dropped because suspicious TCP packets were found. • **Packets allowed**—Number of TCP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of TCP packets dropped because the number of TCP packets per second exceeded the limit.
Ingress UDP Counters	Session-limit UDP counters in the ingress direction for the following: • **Sessions allowed**—Number of UDP sessions allowed by the IDS rule. • **Sessions ignored**—Number of UDP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of UDP sessions dropped because the number of UDP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of UDP sessions dropped because the number of UDP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of UDP sessions dropped because suspicious UDP packets were found. • **Packets allowed**—Number of UDP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of UDP packets dropped because the number of TCP packets per second exceeded the limit.

Table 90: show services service-sets statistics ids session-limits counters Output Fields *(continued)*

Field Name	Field Description
Ingress ICMP Counters	Session-limit ICMP counters in the ingress direction for the following: • **Sessions allowed**—Number of ICMP sessions allowed by the IDS rule. • **Sessions ignored**—Number of ICMP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of ICMP sessions dropped because the number of ICMP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of ICMP sessions dropped because the number of ICMP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of ICMP sessions dropped because suspicious ICMP packets were found. • **Packets allowed**—Number of ICMP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of ICMP packets dropped because the number of ICMP packets per second exceeded the limit.
Ingress Other-Protocols Counters	Session-limit counters in the ingress direction for protocols other than TCP, UDP, and ICMP for the following: • **Sessions allowed**—Number of sessions allowed by the IDS rule. • **Sessions ignored**—Number of sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of sessions dropped because the number of sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of sessions dropped because the number of connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of sessions dropped because suspicious packets were found. • **Packets allowed**—Number of packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of packets dropped because the number of packets per second exceeded the limit.
Egress General Info	Information for IDS rules for the service set in the egress direction. • **Match-direction**—Displays **output**. • **Rule name**—Name of the IDS rule. • **Term name**—Name of the term in the IDS rule.

Table 90: show services service-sets statistics ids session-limits counters Output Fields *(continued)*

Field Name	Field Description
Egress TCP Counters	Session-limit TCP counters in the egress direction for the following: • **Sessions allowed**—Number of TCP sessions allowed by the IDS rule. • **Sessions ignored**—Number of TCP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of TCP sessions dropped because the number of TCP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of TCP sessions dropped because the number of TCP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of TCP sessions dropped because suspicious TCP packets were found. • **Packets allowed**—Number of TCP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of TCP packets dropped because the number of TCP packets per second exceeded the limit.
Egress UDP Counters	Session-limit UDP counters in the egress direction for the following: • **Sessions allowed**—Number of UDP sessions allowed by the IDS rule. • **Sessions ignored**—Number of UDP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of UDP sessions dropped because the number of UDP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of UDP sessions dropped because the number of UDP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of UDP sessions dropped because suspicious UDP packets were found. • **Packets allowed**—Number of UDP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of UDP packets dropped because the number of TCP packets per second exceeded the limit.

Table 90: show services service-sets statistics ids session-limits counters Output Fields *(continued)*

Field Name	Field Description
Egress ICMP Counters	Session-limit ICMP counters in the egress direction for the following: • **Sessions allowed**—Number of ICMP sessions allowed by the IDS rule. • **Sessions ignored**—Number of ICMP sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of ICMP sessions dropped because the number of ICMP sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of ICMP sessions dropped because the number of ICMP connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of ICMP sessions dropped because suspicious ICMP packets were found. • **Packets allowed**—Number of ICMP packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of ICMP packets dropped because the number of ICMP packets per second exceeded the limit.
Egress Other-Protocols Counters	Session-limit counters in the egress direction for protocols other than TCP, UDP, and ICMP for the following: • **Sessions allowed**—Number of sessions allowed by the IDS rule. • **Sessions ignored**—Number of sessions that did not undergo IDS processing because traffic matched a stateful firewall rule that included **accept skip-ids**. • **Sessions dropped due to maximum reached**—Number of sessions dropped because the number of sessions exceeded the limit. • **Sessions dropped due to high rate**—Number of sessions dropped because the number of connections per second exceeded the limit. • **Sessions dropped due to suspicious packets**—Number of sessions dropped because suspicious packets were found. • **Packets allowed**—Number of packets that the IDS rule allowed. • **Packets dropped due to high pps**—Number of packets dropped because the number of packets per second exceeded the limit.

Sample Output

show services service-sets statistics ids session-limits counters interface

`user@host>` **show services service-sets statistics ids session-limits counters interface mams-4/0/0**

```
Interface: mams-4/0/0
  Service set: ams_ss1
    Ingress General Info:
      Match-direction: input
      Rule name: ids_rule_1
      Term name: 0
    Ingress TCP Counters:
      Sessions allowed: 1000
      Sessions ignored: 0
      Sessions dropped due to maximum reached: 0
      Sessions dropped due to high rate: 0
      Sessions dropped due to suspicious packets: 0
      Packets allowed: 1000
      Packets dropped due to high pps: 0
    Ingress UDP Counters:
      Sessions allowed: 1000
      Sessions ignored: 0
      Sessions dropped due to maximum reached: 0
      Sessions dropped due to high rate: 0
      Sessions dropped due to suspicious packets: 0
      Packets allowed: 1000
      Packets dropped due to high pps: 0
    Ingress ICMP Counters:
      Sessions allowed: 100
      Sessions ignored: 0
      Sessions dropped due to maximum reached: 50
      Sessions dropped due to high rate: 0
      Sessions dropped due to suspicious packets: 0
      Packets allowed: 100
      Packets dropped due to high pps: 0
    Ingress Other-Protocols Counters:
      Sessions allowed: 0
      Sessions ignored: 0
      Sessions dropped due to maximum reached: 0
      Sessions dropped due to high rate: 0
      Sessions dropped due to suspicious packets: 0
      Packets allowed: 0
      Packets dropped due to high pps: 0
    Egress General Info:
      Match-direction: output
    Egress TCP Counters:
      Sessions allowed: 0
      Sessions ignored: 0
      Sessions dropped due to maximum reached: 0
```

```
    Sessions dropped due to high rate: 0
    Sessions dropped due to suspicious packets: 0
    Packets allowed: 0
    Packets dropped due to high pps: 0
  Egress UDP Counters:
    Sessions allowed: 0
    Sessions ignored: 0
    Sessions dropped due to maximum reached: 0
    Sessions dropped due to high rate: 0
    Sessions dropped due to suspicious packets: 0
    Packets allowed: 0
    Packets dropped due to high pps: 0
  Egress ICMP Counters:
    Sessions allowed: 0
    Sessions ignored: 0
    Sessions dropped due to maximum reached: 0
    Sessions dropped due to high rate: 0
    Sessions dropped due to suspicious packets: 0
    Packets allowed: 1
    Packets dropped due to high pps: 0
  Egress Other-Protocols Counters:
    Sessions allowed: 0
    Sessions ignored: 0
    Sessions dropped due to maximum reached: 0
    Sessions dropped due to high rate: 0
    Sessions dropped due to suspicious packets: 0
    Packets allowed: 0
    Packets dropped due to high pps: 0
```

show services service-sets statistics integrity-drops

Syntax

```
show services service-sets statistics integrity-drops
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 13.1

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display integrity-drops statistics for one adaptive services interface, for all adaptive services interfaces, or for one service-set. You can configure use the output of this command to verify the packet header for anomalies in IP, TCP, UDP, and IGMP information and to examine any anomalies and errors.

Options

none—Display integrity-drops statistics for all configured adaptive service interfaces/ service-set.

service-set *service-set-name* —(Optional) Display integrity-drops statistics for the specified service-set

interface *interface-name*—(Optional) Display integrity-drops statistics for the specified adaptive services interface.

Required Privilege Level

view

RELATED DOCUMENTATION

clear services service-sets statistics integrity-drops | 1662

List of Sample Output

show services service-sets statistics integrity-drops on page 2005

Output Fields

Table 89 on page 1983 lists the output fields for the **show services service-sets integrity-drops** command. Output fields are listed in the approximate order in which they appear.

Table 91: show services service-sets integrity-drops Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
Errors	Total errors, categorized by protocol: • **IP**—Total IP version 4 errors. • **TCP**—Total Transmission Control Protocol (TCP) errors. • **UDP**—Total User Datagram Protocol (UDP) errors. • **ICMP**—Total Internet Control Message Protocol (ICMP) errors.

Table 91: show services service-sets integrity-drops Output Fields *(continued)*

Field Name	Field Description
IP Errors	

Table 91: show services service-sets integrity-drops Output Fields *(continued)*

Field Name	Field Description
	IPv4 errors: • **IP packet length inconsistencies**—IP packet length does not match the Layer 2 reported length. • **Minimum IP header length check failures**—Minimum IP header length is 20 bytes. The received packet contains less than 20 bytes. • **Reassembled packet exceeds maximum IP length**—After fragment reassembly, the reassembled IP packet length exceeds 65,535. • **Illegal source address 0**—Source address is not a valid address. Invalid addresses are, loopback, broadcast, multicast, and reserved addresses. Source address **0**, however, is allowed to support BOOTP and the destination address **0xffffffff**. • **Illegal destination address** —Destination address is not a valid address. The address is reserved. • **TTL zero errors**—Received packet had a time-to-live (TTL) value of 0. • **Illegal IP protocol number 0 or 255**—IP protocol is 0 or 255. • **Land attack**—IP source address is the same as the destination address. • **Non-IP packets**—Packet did not conform to the IP standard. • **IP option**—Packet dropped because of a nonallowed IP option. • **Non-IPv4 packets**—Packet was not of the IPv4 type. • **Non-IPv6 packets**—Packet was not of the IPv6 type. • **Bad checksum**—Packet had an invalid IP checksum. • **Illegal IP fragment length**—Illegal fragment length. All fragments (other than the last fragment) must have a length that is a multiple of 8 bytes. • **IP fragment overlap**—Fragments have overlapping fragment offsets. • **IP fragment limit exceeded:** —Fragments dropped because the configured number of allowed fragments for a packet was exceeded. • **IP fragment reassembly timeout**—Some of the fragments for an IP packet were not received in time, and the reassembly handler dropped partial fragments. Whenever a

Table 91: show services service-sets integrity-drops Output Fields *(continued)*

Field Name	Field Description
	fragment is received, it is maintained in a chain until all other fragments are received. If other fragments do not arrive within the configured value of reassembly-timeout, this packet is dropped and the value of the counter shown in this field is incremented. If other fragments arrive in time but the total number of fragments is more than the configured value of fragment-limit, all the fragments (of this packet) are dropped and the value of the counter shown in this field is incremented. • **Unknown:** —Unknown fragments.
TCP Errors	TCP protocol errors: • **TCP header length inconsistencies**—Minimum TCP header length is 20 bytes, and the IP packet received does not contain at least 20 bytes. • **Source or destination port number is zero**—TCP source or destination port is zero. • **Illegal sequence number, flags combination**—Dropped because of TCP errors, such as an illegal sequence number, which causes an illogical combination of flags to be set.
UDP Errors	UDP protocol errors: • **IP data length less than minimum UDP header length (8 bytes)**—Minimum UDP header length is 8 bytes. The received IP packets contain less than 8 bytes. • **Source or destination port is zero**—UDP source or destination port is **0**.
ICMP Errors	ICMP protocol errors: • **IP data length less than minimum ICMP header length (8 bytes)**—ICMP header length is 8 bytes. This counter is incremented when received IP packets contain less than 8 bytes. • **ICMP error length inconsistencies**—Minimum length of an ICMP error packet is 48 bytes, and the maximum length is 576 bytes. This counter is incremented when the received ICMP error falls outside this range.

Sample Output

show services service-sets statistics integrity-drops

user@host> **show services service-sets statistics integrity-drops**

```
Interface: ms-1/0/0
 Service set: sset1
   Errors:
     IP: 0, TCP: 0
     UDP: 0, ICMP: 0
   IP errors:
     IP packet length inconsistencies: 0
     Illegal source address: 0
     Illegal destination address: 0
     TTL zero errors: 0, Illegal IP protocol number (0 or 255): 0
     Land attack: 0
     Non-IPv4 packets: 0
     Non-IPv6 packets: 0
     Bad checksum: 0
     Illegal IP fragment length: 0
     IP fragment overlap: 0
     IP fragment limit exceeded: 0
     IP fragment reassembly timeout: 0
     Unknown: 0
   TCP errors:
     TCP header length inconsistencies: 0
     Source or destination port number is zero: 0
     Illegal sequence number and flags combinations: 0
   UDP errors:
     IP data length less than minimum UDP header length (8 bytes): 0
     Source or destination port number is zero: 0
   ICMP errors:
     IP data length less than minimum ICMP header length (8 bytes): 0
     ICMP error length inconsistencies: 0
```

show services service-sets statistics packet-drops

Syntax

```
show services service-sets statistics packet-drops
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display the number of dropped packets for service sets exceeding CPU limits or memory limits.

Options

none—Display the number of dropped service sets packets for all adaptive services interfaces.

interface *interface-name*—(Optional) Display the number of dropped service sets packets for a particular interface. On M Series and T Series routers, *interface-name* can be *ms-fpc/pic/port*, *sp-fpc/pic/port*, or *rspnumber*.

Required Privilege Level

view

RELATED DOCUMENTATION

clear services flow-collector statistics

List of Sample Output

show services service-sets statistics packet-drops on page 2007

Output Fields

Table 89 on page 1983 lists the output fields for the **show services service-sets packet-drops** command. Output fields are listed in the approximate order in which they appear.

Table 92: show services service-sets packet-drops Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.

Table 92: show services service-sets packet-drops Output Fields *(continued)*

Field Name	Field Description
CPU limit Drops	Number of packets dropped because the service set exceeded the average CPU limit.
Memory limit Drops	Number of packets dropped because the service set exceeded the memory limit.
Flow limit Drops	Number of packets dropped because the service set exceeded the flow limit.

Sample Output

show services service-sets statistics packet-drops

`user@host>` **show services service-sets statistics packet-drops**

```
Interface: vms-1/0/0
  Service set: ss1
    CPU limit drops: 0
    Memory limit drops: 0
    Flow limit drops: 0
```

show services service-sets statistics syslog

Syntax

```
show services service-sets statistics syslog
<interface interface-name>
<service-set service-set-name>
<brief | detail>
```

Release Information

Command introduced in Junos OS Release 11.1.
Support for this command introduced in Junos OS Release 19.3R2 for Next Gen Services with the MX-SPC3 services card on MX240, MX480 and MX960 routers.

Description

Display the system log statistics with optional filtering by interface and service set name.

Options

none—Display the system log statistics for all services interfaces and all service sets.

brief—(Default) (Optional) Display abbreviated system log statistics.

detail—(Optional) Display detailed system log statistics.

interface *interface-name*—(Optional) Display the system log statistics for a specific adaptive service interface.
On M Series and T Series routers, *interface-name* can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***.

service-set *service-set-name*—(Optional) Display the system log statistics for a specific named service-set.

Required Privilege Level

view

RELATED DOCUMENTATION

clear services service-sets statistics syslog | **1665**

List of Sample Output

show services service-sets statistics syslog brief on page 2012
show services service-sets statistics syslog detail on page 2013

Output Fields

Table 93 on page 2009 lists the output fields for the **show services service-sets statistics syslog** command. Output fields are listed in the approximate order in which they appear.

Table 93: show services service-sets statistics syslog Output Fields

Field Name	Field Description	Level
Interface	Name of a services interface.	all
Rate limit	Maximum number of messages per second written to the interface's system log.	all
Sent	Number of messages sent that are not associated with a service set.	all
Dropped	Number of messages dropped that are not associated with a service set.	all
Service-set		
Service-set	Name of a service set.	all
Sent	Number of sent messages that are associated with the service set.	all
Dropped	Number of dropped messages that are associated with the service set.	all

Session open logs	The following information is displayed for system log messages for session open events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 93: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

Session close logs	The following information is displayed for system log messages for session close events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Packet logs	The following information is displayed for system log messages for packet events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Stateful firewall logs	The following information is displayed for system log messages for stateful firewall events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 93: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

ALG logs	The following information is displayed for system log messages for ALG events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

NAT logs	The following information is displayed for system log messages for NAT events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

IDS logs	The following information is displayed for system log messages for IDS events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 93: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

Other logs	The following information is displayed for system log messages for other types of events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Sample Output

show services service-sets statistics syslog brief

`user@host>` **show services service-sets statistics syslog brief**

```
Interface: sp-1/1/0
  Rate limit: 200000
  Sent: 0
  Dropped: 0
  Service-set: sset-sfw-sp1
    Sent: 20
    Dropped: 3488
  Service-set: sset-nat-sp1
    Sent: 18
    Dropped: 91
Interface: sp-1/2/0
  Rate limit: 15000
  Sent: 0
  Dropped: 0
  Service-set: sset-sfw-sp2
    Sent: 210
    Dropped: 579
```

Sample Output

show services service-sets statistics syslog detail

user@host> **show services service-sets statistics syslog detail**

```
Interface: ms-2/1/0
  Rate limit: 0
  Sent: 0
  Dropped: 0
  Service-set: sset1
    Sent: 0
    Dropped: 0
    Session open logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Session close logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Packet logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Stateful firewall logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    ALG logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    NAT logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    IDS logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP MAP logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
```

```
limit: 0)
    PCP protocol logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP protocol error logs:
Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP debug logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Other logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
```

For Next Gen Services MX-SPC3 Services Card

Following shows the output for the **show services service-sets statistics syslog** on the MX-SPC3 services cards **vms-x/y/z** interfaces.

`user@host>` **show services service-sets statistics syslog**

```
show services service-sets statistics syslog
Log Module Statistics
Interface-Name- vms-2/0/0
Service-set Name- Sset1
Name               Generated       Discarded
-----------------------------------------
UTM                0               0
FW_AUTH            0               0
SCREEN             0               0
ALG                0               0
NAT                0               0
FLOW               0               0
SCTP               0               0
GTP                0               0
IPSEC              0               0
```

```
IDP                0              0
RTLOG              0              0
PST_DS_LITE        0              0
APPQOS             0              0
SECINTEL           0              0
AAMW               0              0
OTHERS             0              0

Log stream Statistics
Interface-Name- vms-2/0/0
Service-set Name- Sset1
Name               send           Fail
-------------------------------------------
database           0              0
```

show services service-sets statistics tcp

Syntax

```
show services service-sets statistics tcp
<interface interface-name>
<service-set service-set-name>
```

Release Information

Command introduced in Junos OS Release 17.2.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display TCP-related statistics.

Options

interface *interface-name*—Name of adaptive services interface.

service-set *service-set-name*—Name of service set.

Required Privilege Level

view

RELATED DOCUMENTATION

Configuring TFO | 62

List of Sample Output

show services service-sets statistics tcp on page 2016

Output Fields

Sample Output

show services service-sets statistics tcp

`user@host>` **show services service-sets statistics tcp**

```
Interface:vms-0/2/0
  Service set: ss1_interface_style1
```

```
TCP open/close statistics:
  TCP first packet non-syn: 1
  TCP first packet reset: 0
  TCP first packet FIN: 0
  TCP non syn discard: 0
  TCP extension alloc fail: 0
  TFO SYN with cookie request: 0
  TFO SYN with cookie: 0
  TFO SYN ACK with cookie: 0
  TFO packets forwarded: 0
  TFO packets dropped: 0
  TFO packets stripped: 0
  TCP invalid syn ack: 0
  TCP invalid ack window check: 0
  TCP invalid syn transmit: 0
  TCP invalid reset in listen: 0
  TCP invalid reset in syn received: 0
  TCP invalid reset in syn sent: 0
  TCP invalid flags handshake: 0
TCP MSS statistics:
  TCP SYN MSS Received: 0
  TCP SYN MSS Modified: 0
```

show services service-sets statistics tcp-mss

Syntax

```
show services service-sets statistics tcp-mss
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 9.5.

Description

(M Series and T Series routers only) Display TCP maximum segment size (MSS) statistics for service sets.

Options

none—Display service set TCP MSS information for all adaptive services interfaces.

interface *interface-name*—(Optional) Display TCP MSS statistics for a particular interface. The ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp *number***.

Required Privilege Level

view

List of Sample Output

show services service-sets statistics tcp-mss on page 2019

Output Fields

Table 94 on page 2018 lists the output fields for the **show services service-sets statistics tcp-mss** command. Output fields are listed in the approximate order in which they appear.

Table 94: show services service-sets statistics tcp-mss Output Fields

Field Name	Field Description
Interface	Name of the adaptive services interface.
Service Set	Name of the configured service set.
SYN Received	Number of TCP SYN packets received.
SYN Modified	Number of TCP SYN packets with the MSS value modified to match the MSS value specified in the TCP MSS configuration.

Sample Output

show services service-sets statistics tcp-mss

```
user@host> show services service-sets statistics tcp-mss
```

```
Interface   Service Set                     SYN Received  SYN Modified
sp-1/2/0    asq_ipsec_svc_0                          500           220
```

show services service-sets summary

Syntax

```
show services service-sets summary
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display service set summary information.

Options

none—Display service set summary information for all adaptive services interfaces.

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

On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***.

On MX Series MX240, MX480, and MX960 routers, ***interface-name*** can be **vms-*fpc/pic/port*** for the MX-SPC3 services card for Next Gen Services.

Required Privilege Level

view

List of Sample Output

show services service-sets summary on page 2021
show services service-sets summary interface on page 2021

Output Fields

Table 95 on page 2020 lists the output fields for the **show services service-sets summary** command. Output fields are listed in the approximate order in which they appear.

Table 95: show services service-sets summary Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service type	Type of adaptive service, such as stateful firewall (SFW), Network Address Translation (NAT), intrusion detection service (IDS), Layer 2 Tunneling Protocol (L2TP), Compressed Real-Time Transport Protocol (CRTP), or IP Security (IPsec)

Table 95: show services service-sets summary Output Fields *(continued)*

Field Name	Field Description
Service sets configured	Total number of service sets configured on the PIC that use internal service set IDs and do not consume external service sets, including CRTP and L2TP
Bytes used	Bytes used by a particular service or all services
Policy bytes used	Policy bytes used by a particular service or all services
CPU utilization	Percentage of the CPU resources being used

Sample Output

show services service-sets summary

`user@host>` **show services service-sets summary**

```
                Service sets
              CPU
Interface    configured            Bytes used       Session bytes used     Policy
 bytes used      utilization
vms-3/0/0         1          3453621040 (24.93%)         0 ( 0.00%)      8161168
 ( 0.90%)        0.14 %
```

show services service-sets summary interface

`user@host>` **show services service-sets summary interface sp-1/3/0**

```
Interface: sp-1/3/0
                 Service sets                          CPU
  Service type   configured              Bytes used   utilization
  SFW/NAT/IDS               1           54 ( 0.00 %)       N/A
  L2TP                      1           58 ( 0.00 %)       N/A
  CRTP                      1           58 ( 0.00 %)       N/A
  System                    0       920831 ( 0.44 %)       N/A
  Idle                      0            0 ( 0.00 %)       N/A
  Total                     3       921001 ( 0.44 %)       N/A
```

show services sessions

Syntax

```
show services sessions
<brief | extensive | 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>
<utilization>
```

Release Information

Command introduced in Junos OS Release 10.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display session information.

> **NOTE:** On MX Series routers (with interchassis redundancy configured), the idle timeout for every flow is displayed in the **show services session extensive** and **show services flows extensive** commands.

Options

none—Display standard information about all sessions.

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

application-protocol *protocol*—(Optional) Display information about one of the following application protocols:

- **bootp**—Bootstrap protocols
- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols

- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **exec**—Remote Execution Protocol
- **ftp**—File Transfer Protocol
- **h323**—H.323
- **icmp**—ICMP
- **icmpv6**—ICMPv6
- **iiop**—Internet Inter-ORB Protocol
- **ike-esp-nat**—IKE ALG
- **ip**—IP
- **login**—LOGIN
- **netbios**—NETBIOS
- **netshow**—NETSHOW
- **pptp**—Point-to-Point Tunneling Protocol
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **rsh**—Remote Shell
- **sip**—Session Initiation Protocol
- **shell**—Shell
- **snmp**—SNMP
- **sql**—SQLNet
- **talk**—Talk Program
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

NOTE: You can use the **none** option with the **show services sessions count application-protocol** command to display information about sessions other than ALG sessions.

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

destination-port *destination-port*—(Optional) Display information for the specified destination port. The range of values is from 0 to 65,535.

destination-prefix *destination-prefix*—(Optional) Display information for the specified destination prefix.

interface *interface-name*—(Optional) Display information about the specified interface. On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port*** or **rsp*number***. 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
- **icmp6**—Internet Control Message Protocol version 6
- **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 Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Display information for the specified service set.

source-port *source-port*—(Optional) Display information for the specified source port. The range of values is from 0 to 65,535.

source-prefix *source-prefix*—(Optional) Display information for the specified source prefix.

utilization—(Optional) Display statistical details about session utilization.

Required Privilege Level
view

List of Sample Output
show services sessions on page 2026
show services sessions brief on page 2027
show services sessions extensive on page 2027
show services sessions terse on page 2027
show services sessions application-protocol on page 2027
show services sessions count on page 2031
show services sessions destination-port on page 2031
show services sessions destination-prefix on page 2031
show services sessions interface on page 2032
show services sessions protocol on page 2032
show services sessions service-set on page 2032
show services sessions source-port on page 2032
show services sessions source-prefix on page 2032

Output Fields
Table 96 on page 2025 lists the output fields for the **show services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 96: show services sessions Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	**application-protocol**
Session	Session ID that uniquely identifies the session.	All levels
ALG	Name of the application.	**terse**

Table 96: show services sessions Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flags	Session flag for the ALG: • **0x1**—Found an existing session. • **0x2**—Reached session or flow limit. • **0x3**—No memory available for new sessions. • **0x4**—No free session ID available. • **0x0000**—No session ID found.	All levels
IP Action	Flag indicating whether IP action has been set for the session.	All levels
Offload	Flag indicating whether the session has been offloaded to the Packet Forwarding Engine.	All levels
Asymmetric	Flag indicating whether the session is uni-directional.	**terse** **application-protocol**
Service set	Name of a service set. Individual empty service sets are not displayed.	**count**
Sessions Count	Number of sessions.	**count**

Sample Output

show services sessions

`user@host>` **show services sessions**

```
ms-2/0/0
Session: 293, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:43677 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        192.0.2.1:43677 Forward  O        1
Session: 53, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:37494 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:37494 Forward  O        1
Session: 66, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:48161 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:48161 Forward  O        1
Session: 17, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:38908 ->    10.20.20.1:53    Forward  I        1
```

```
UDP    10.20.20.1:53    ->        10.11.11.11:38908 Forward  O        1
Session: 42, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     10.10.10.2:58189 ->    10.20.20.1:53    Forward  I        1
UDP    10.20.20.1:53    ->        10.11.11.11:58189 Forward  O        1
```

show services sessions brief

The output for the **show services flows brief** command is identical to that for the **show services sessions** command. For sample output, see show services sessions on page 2026.

show services sessions extensive

`user@host>` **show services sessions extensive**

```
ms-0/1/0
Session: 2, ALG: 0, Flags: 0x0080, IP Action: no, Offload: no
NAT PLugin Data:
  NAT Action:   Translation Type - DYNAMIC NAT44
    NAT source         192.0.21.2         ->    10.10.10.127
TCP            192.0.2.2:52145 ->        198.51.100.2:23    Forward  I
   22
  Byte count: 1483
  Flow role: Unknown, Timeout: 0
TCP            198.51.100.2:23    ->   10.10.10.127:52145 Forward  O
 18
  Byte count: 2712
  Flow role: Unknown, Timeout: 0
```

show services sessions terse

`user@router>` **show services sessions terse**

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              31
```

show services sessions application-protocol

This command has the same output for the rpc, dce-rpc, rpc-portmap and dce-rpc-portmap ALGs.

`user@router>` **show services sessions application-protocol dce-rpc**

```
Interface name: ms-1/1/0
Session: 8, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:1019  ->192.168.203.194:2049  Forward  I              4
UDP    192.168.203.194:2049  ->192.168.203.198:1019  Forward  O              4
Session: 7, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:954   ->192.168.203.194:613   Forward  I              1
UDP    192.168.203.194:613   ->192.168.203.198:954   Forward  O              1
Session: 6, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:53836 ->192.168.203.194:613   Forward  I              1
UDP    192.168.203.194:613   ->192.168.203.198:53836 Forward  O              1
Session: 5, ALG: portmapper, Flags: 0x1000, IP Action: no, Offload: no
UDP    192.168.203.198:59813 ->192.168.203.194:111   Forward  I              1
UDP    192.168.203.194:111   ->192.168.203.198:59813 Forward  O              1
Session: 4, ALG: portmapper, Flags: 0x1800, IP Action: no, Offload: no
UDP    192.168.203.198:36595 ->192.168.203.194:2049  Forward  I              1
UDP    192.168.203.194:2049  ->192.168.203.198:36595 Forward  O              1
Session: 3, ALG: portmapper, Flags: 0x1000, IP Action: no, Offload: no
UDP    192.168.203.198:56050 ->192.168.203.194:111   Forward  I              1
UDP    192.168.203.194:111   ->192.168.203.198:56050 Forward  O              1
```

user@router> **show services sessions application-protocol dns**

```
Interface name: ms-2/0/0
Session: 293, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     198.51.100.2:43677 ->    203.0.113.10:53    Forward  I        1
UDP    203.0.113.10:53    ->        192.0.2.1:43677 Forward  O        1
Session: 53, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     198.51.100.2:37494 ->    203.0.113.10:53    Forward  I        1
UDP    203.0.113.10:53    ->        192.0.2.1:37494 Forward  O        1
Session: 66, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     198.51.100.2:48161 ->    203.0.113.10:53    Forward  I        1
UDP    203.0.113.10:53    ->        192.0.2.1:48161 Forward  O        1
Session: 17, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     198.51.100.2:38908 ->    203.0.113.10:53    Forward  I        1
UDP    203.0.113.10:53    ->        192.0.2.1:38908 Forward  O        1
Session: 42, ALG: 16, Flags: 0x0040, IP Action: no, Offload: no
UDP     198.51.100.2:58189 ->    203.0.113.10:53    Forward  I        1
UDP    203.0.113.10:53    ->        192.0.2.1:58189 Forward  O        1
```

user@router> **show services sessions application-protocol ftp**

```
Interface name: ms-4/1/0
Session: 1, ALG: 1, Flags: 0x0040, IP Action: no, Offload: no
```

```
TCP       192.0.2.129:32843 ->       198.51.100.129:21    Forward  I       26
TCP       198.51.100.129:21    ->        192.0.2.0:32843 Forward  O       30
```

user@router> **show services sessions application-protocol ike-esp-nat**

```
Service Set: ss_ipv4, Session: 33554435, ALG: ike-esp-nat, Flags: 0x0800, IP Action:
 no, Offload: no, Asymmetric: no
ESP 198.51.100.2:4689  ->        203.0.113.1:62108 Forward O 2199
ESP 192.0.2.2:62108  ->       198.51.100.2:4689 Forward I 0
Service Set: ss_ipv4, Session: 33554434, ALG: ike-esp-nat, Flags: 0x0800, IP Action:
 no, Offload: no, Asymmetric: no
ESP 192.0.2.2:44179  ->       198.51.100.2:43809 Forward I 2199
ESP 198.51.100.2:43809  ->       203.0.113.1:44179 Forward O 0
Service Set: ss_ipv4, Session: 33554433, ALG: ike-esp-nat, Flags: 0x0000, IP Action:
 no, Offload: no, Asymmetric: no
UDP 192.0.2.2:500  ->         198.51.100.2:500 Forward I 8
UDP 198.51.100.2:500  ->         203.0.113.1:57730 Forward O
```

user@router> **show services sessions application-protocol pptp**

```
Interface name: ms-2/0/0
Session: 3, ALG: pptp, Flags: 0x2800, IP Action: no, Offload: no, Asymmetric: no
GRE        203.0.113.138:0     ->    203.0.113.138:0     Forward  O
21
GRE        192.0.2.794:0     ->    203.0.113.138:0:65000 Forward  I
 0
Session: 2, ALG: pptp, Flags: 0x2800, IP Action: no, Offload: no, Asymmetric: no
GRE        192.0.2.794:0     ->    203.0.113.138:0:49913 Forward  I
88
GRE        203.0.113.138:0:49913 ->    192.0.2.794:65001 Forward  O
 0
Session: 1, ALG: pptp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP        192.0.2.794:1511  ->    203.0.113.138:0:1723  Forward  I
13
TCP        203.0.113.138:0:1723  ->    192.0.2.794:1511  Forward  O
12
```

user@router> **show services sessions application-protocol rtsp**

```
Interface name: ms-0/1/0
Session: 13, ALG: rtsp, Flags: 0x0800, IP Action: no, Offload: no
UDP        203.0.113.66:5004  ->        198.51.100.66:3989  Forward  O      152
```

```
UDP        198.51.100.66:3989  ->        192.0.2.161:5004  Forward  I        0
Session: 9, ALG: rtsp, Flags: 0x0800, IP Action: no, Offload: no
UDP        203.0.113.66:5004  ->        198.51.100.66:3986  Forward  O        3
UDP        198.51.100.66:3986  ->        192.0.2.161:5004  Forward  I        0
```

user@router> **show services sessions application-protocol rsh**

```
Interface name: ms-2/0/0
Session: 3, ALG: 2, Flags: 0x0840, IP Action: no, Offload: no
TCP    203.0.113.10:1023  ->     198.51.100.2:1020  Forward  O        4
TCP     198.51.100.2:1020  ->    203.0.113.10:1023  Forward  I        3
Session: 1, ALG: 2, Flags: 0x0040, IP Action: no, Offload: no
TCP     198.51.100.2:1021  ->    203.0.113.10:514   Forward  I     1331
TCP    203.0.113.10:514   ->     198.51.100.2:1021  Forward  O     2485
```

user@router> **show services sessions application-protocol sip**

```
Interface name: ms-2/0/0
Session: 4, ALG: sip, Flags: 0x0800, IP Action: no, Offload: no
UDP           198.51.100.130:6000  ->       192.0.2.129:12682 Forward  I
    246
UDP           192.0.2.129:12682 ->       198.51.100.162:6000  Forward  O
      0
Session: 1, ALG: sip, Flags: 0x0000, IP Action: no, Offload: no
UDP           198.51.100.130:5060  ->       192.0.2.130:5060  Forward  I
     10
UDP           192.0.2.130:5060  ->       198.51.100.162:5060  Forward  O
      9
```

user@router> **show services sessions application-protocol sql**

```
Interface name: ms-2/0/0
Session: 3934, ALG: sqlnet, Flags: 0x0800, IP Action: no, Offload: no
TCP     198.51.100.2:39754 ->    203.0.113.138:0:1408  Forward  I       26
TCP    203.0.113.138:0:1408  ->        192.0.2.1:39754 Forward  O       23
```

user@router> **show services sessions application-protocol talk**

```
Interface name: ms-0/2/0
Session: 4, ALG: 65, Flags: 0x0800, IP Action: no, Offload: no
TCP            203.0.113.162:36888 ->        192.0.2.2:33294 Forward  O
```

```
     4
TCP            192.0.2.1:33294 ->        203.0.113.162:36888 Forward  I
     3
Session: 7, ALG: 65, Flags: 0x0800, IP Action: no, Offload: no
UDP            203.0.113.162:1165  ->        192.0.2.2:518   Forward  O
     1
UDP            192.0.2.2:518   ->        203.0.113.162:1165  Forward  I
     1
Session: 8, ALG: 65, Flags: 0x0000, IP Action: no, Offload: no
UDP            192.0.2.2:1509  ->        203.0.113.162:518   Forward  I
     3
UDP            203.0.113.162:518   ->        192.0.2.2:1509  Forward  O
     3
Session: 6, ALG: 0, Flags: 0x0000, IP Action: no, Offload: no
UDP            192.0.2.1:123   ->        192.0.2.2:123   Forward  O
 4
```

show services sessions count

`user@host>` **show services sessions count**

```
Interface   Service set                                          Sessions count
ms-1/1/0    ss                                                              2
```

show services sessions destination-port

`user@router>` **show services sessions destination-port 21**

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              25
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              24
```

show services sessions destination-prefix

`user@router>` **show services sessions destination-prefix 10.1.1.2**

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I              25
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O              24
```

show services sessions interface

```
user@router> show services sessions interface ms-1/1/0
```

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             30
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             29
```

show services sessions protocol

```
user@router> show services sessions protocol tcp
```

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             30
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             29
```

show services sessions service-set

```
user@router> show services sessions service-set sample
```

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             31
```

show services sessions source-port

```
user@router> show services sessions source-port 21
```

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             31
```

show services sessions source-prefix

```
user@router> show services sessions source-prefix 10.2.2.2
```

```
ms-1/1/0
Session: 1, ALG: ftp, Flags: 0x2000, IP Action: no, Offload: no, Asymmetric: no
```

```
TCP           10.2.2.2:52138 ->       10.1.1.2:21    Forward  I             33
TCP           10.1.1.2:21    ->       10.2.2.2:52138 Forward  O             31
```

show services sessions (Aggregated Multiservices)

Syntax

```
show services sessions
<brief | extensive | 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

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display the session information for each service set in each member interface of the AMS interface.

Options

none—Display standard information about all sessions.

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

application-protocol—(Optional) Display information about one of the following application protocols:

- **ftp**—File Transfer Protocol
- **icmp**—Internet Control Message Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rtsp**—Real-Time Streaming Protocol
- **sqlnet**—SQL *Net
- **tcp**—Transmission Control Protocol
- **traceroute**—Traceroute
- **tftp**—Trivial File Transfer Protocol
- **udp**—User Datagram Protocol

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 through 65,535.

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 through 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
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP encapsulation protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission 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 through 65,535.

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

Required Privilege Level
view

List of Sample Output

show services sessions brief on page 2037
show services sessions interface mams-5/0/0 extensive on page 2037
show services sessions terse on page 2040
show services sessions count on page 2042

Output Fields

Table 96 on page 2025 lists the output fields for the **show services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 97: show services sessions Output Fields

Field Name	Field Description
Interface	Name of the member interface (**mams-**) and the aggregated multiservices interface (**ams**) to which it belongs.
Session ID	Session ID that uniquely identifies the session.
ALG	Name of the application.
Flags	Session flag for the ALG: • **0x1**—Found an existing session. • **0x2**—Reached session or flow limit. • **0x3**—No memory available for new sessions. • **0x4**—No free session ID available.
IP Action	Flag indicating whether IP action has been set for the session.
Offload	Flag indicating whether the session has been offloaded to the Packet Forwarding Engine.
Asymmetric	Flag indicating whether the session is unidirectional.
Service set	Name of a service set. Individual empty service sets are not displayed.
Sessions Count	Number of sessions.
Flow or Flow Prot	Protocol used for this session.
Source	Source prefix of the flow in the format ***source-prefix:port***. For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.

Table 97: show services sessions Output Fields *(continued)*

Field Name	Field Description
State	Status of the flow: • **Drop**—Drop all packets in the flow without response. • **Forward**—Forward the packet in the flow without looking at it. • **Reject**—Drop all packets in the flow with response. • **Watch**—Inspect packets in the flow. • **Bypass**—Bypass packets in the flow. • **Unknown**—Unknown flow status.
Packet Direction	Direction of the flow: ingress **(I)**, egress **(O)**, or unknown.
Frm count	Number of frames in the flow.

Sample Output

show services sessions brief

`user@host>` **show services sessions brief**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777217, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.2:63    ->     40.40.40.2:63    Forward  I           85689
UDP         40.40.40.2:63    ->   30.30.30.160:6000  Forward  O               0
```

show services sessions interface mams-5/0/0 extensive

`user@host>` **show services sessions interface mams-5/0/0 extensive**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.62:63      ->    30.30.30.176:6003
UDP        30.30.30.62:63    ->    40.40.40.62:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
```

```
UDP        40.40.40.62:63    ->   30.30.30.176:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.57:63      ->    30.30.30.163:6003
UDP        30.30.30.57:63    ->    40.40.40.57:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.57:63    ->   30.30.30.163:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0

[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.63:63      ->    30.30.30.165:6004
UDP        30.30.30.63:63    ->    40.40.40.63:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.63:63    ->   30.30.30.165:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.60:63      ->    30.30.30.164:6004
UDP        30.30.30.60:63    ->    40.40.40.60:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.60:63    ->   30.30.30.164:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
```

```
[...output truncated...]
mams-5/0/0 (ams0)
Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.64:63      ->    30.30.30.168:6002
UDP        30.30.30.64:63    ->    40.40.40.64:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.64:63    ->   30.30.30.168:6002  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.56:63      ->    30.30.30.171:6001
UDP        30.30.30.56:63    ->    40.40.40.56:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.56:63    ->   30.30.30.171:6001  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

[...output truncated...]
mams-5/1/0 (ams0)
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.61:63      ->    30.30.30.172:6004
UDP        30.30.30.61:63    ->    40.40.40.61:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.61:63    ->   30.30.30.172:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
```

```
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.52:63      ->    30.30.30.175:6003
UDP        30.30.30.52:63    ->    40.40.40.52:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.52:63    ->   30.30.30.175:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

[...output truncated...]
```

show services sessions terse

`user@router>` **show services sessions terse**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.62:63    ->    40.40.40.62:63    Forward  I            2541
UDP        40.40.40.62:63    ->   30.30.30.176:6003  Forward  O               0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.57:63    ->    40.40.40.57:63    Forward  I            2541
UDP        40.40.40.57:63    ->   30.30.30.163:6003  Forward  O               0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.50:63    ->    40.40.40.50:63    Forward  I            2541
UDP        40.40.40.50:63    ->   30.30.30.162:6003  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.48:63    ->    40.40.40.48:63    Forward  I            2541
UDP        40.40.40.48:63    ->   30.30.30.161:6003  Forward  O               0
[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.63:63    ->    40.40.40.63:63    Forward  I            2543
UDP        40.40.40.63:63    ->   30.30.30.165:6004  Forward  O               0
```

```
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.60:63    ->    40.40.40.60:63    Forward  I            2543
UDP        40.40.40.60:63    ->   30.30.30.164:6004  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.59:63    ->    40.40.40.59:63    Forward  I            2543
UDP        40.40.40.59:63    ->   30.30.30.167:6003  Forward  O               0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.58:63    ->    40.40.40.58:63    Forward  I            2543
UDP        40.40.40.58:63    ->   30.30.30.166:6003  Forward  O               0
[...output truncated...]
mams-5/0/0 (ams0)
Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.64:63    ->    40.40.40.64:63    Forward  I            2543
UDP        40.40.40.64:63    ->   30.30.30.168:6002  Forward  O               0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.56:63    ->    40.40.40.56:63    Forward  I            2543
UDP        40.40.40.56:63    ->   30.30.30.171:6001  Forward  O               0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.55:63    ->    40.40.40.55:63    Forward  I            2543
UDP        40.40.40.55:63    ->   30.30.30.170:6001  Forward  O               0
Service Set: napt_set, Session: 16777222, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.51:63    ->    40.40.40.51:63    Forward  I            2543
UDP        40.40.40.51:63    ->   30.30.30.169:6001  Forward  O               0
[...output truncated...]
mams-5/1/0 (ams0)
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.61:63    ->    40.40.40.61:63    Forward  I            2544
UDP        40.40.40.61:63    ->   30.30.30.172:6004  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.52:63    ->    40.40.40.52:63    Forward  I            2545
UDP        40.40.40.52:63    ->   30.30.30.175:6003  Forward  O               0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.47:63    ->    40.40.40.47:63    Forward  I            2545
UDP        40.40.40.47:63    ->   30.30.30.174:6003  Forward  O               0
```

```
Service Set: napt_set, Session: 16777230, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.46:63    ->    40.40.40.46:63    Forward  I            2545
UDP        40.40.40.46:63    ->   30.30.30.173:6003  Forward  O               0
[...output truncated...]
```

show services sessions count

user@host> **show services sessions count**

```
Interface   Service set                                        Sessions count
mams-1/0/0  napt_set                                                    19
mams-1/0/0  ss1                                                          0
mams-1/1/0  napt_set                                                    18
mams-1/1/0  ss1                                                          0
mams-5/0/0  napt_set                                                     9
mams-5/0/0  ss1                                                          0
mams-5/1/0  napt_set                                                    17
mams-5/1/0  ss1                                                          0
```

show services sessions analysis

Syntax

```
show services sessions analysis
<interface interface-name>
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series MS-MPC.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display session statistics.

Options

none—Display standard information about all session statistics.

interface *interface-name*—(Optional) Display information about the specified interface.

Required Privilege Level

view

List of Sample Output

show services sessions analysis interface on page 2045

Output Fields

Table 98 on page 2043 lists the output fields for the **show services sessions analysis** command. Output fields are listed in the approximate order in which they appear.

Table 98: show services sessions analysis Output Fields

Field Name	Field Description
Services PIC Name	FPC and PIC slots for the services PIC on which the sessions are running.
Session Analysis Statistics:	
Total Sessions Active	Total active sessions in the MS-PIC including TCP, UDP, ICMP and Softwires.
Total TCP Sessions Active	Total active TCP sessions in the MS-PIC.

Table 98: show services sessions analysis Output Fields *(continued)*

Field Name	Field Description
Total UDP Sessions Active	Total active UDP session in the MS-PIC.
Total Other Sessions Active	Total other active sessions in the MS-PIC including ICMP and softwires.
Total Predicted Sessions Active	Predicted sessions are created only by the ALG traffic using the L3/L4 information available.
Created Sessions per Second	Session setup rate at the time of running the command.
Deleted Sessions per Second	Session deletion rate at the time of running the command.
Peak Total Sessions Active	Highest number of active sessions since the last PIC restart or since the last time session statistics are flushed.
Peak Total TCP Sessions Active	Highest number of active TCP sessions since the last PIC restart or since the last time session stats are flushed.
Peak Total UDP Sessions Active	Highest number of active UDP sessions since the last PIC restart or since the last time session statistics are flushed.
Peak Total Other Sessions Active	Highest number of other active sessions since the last PIC restart or since the last time session statistics are flushed.
Peak Created Sessions per Second	Maximum session setup rate observed since the last PIC restart or since the last time session statistics are flushed.
Peak Deleted Sessions per Second	Maximum session deletion rate observed since the last PIC restart or from the last time session statistics are flushed.
Packets received	Total number of packets received by the MS-PIC.
Packets transmitted	Total number of packets transmitted by the MS-PIC.
Slow path forward	Number of packets forwarded in the slow path (that is, after the successful rule match and session creation).
Slow path discard	Number of packets discarded before the session creation.

Table 98: show services sessions analysis Output Fields *(continued)*

Field Name	Field Description
Session Rate Data: Number of Samples	Number of samples used to calculate the session rate since the last PIC restart or since the last time session statistics are flushed.
Session Rate Distribution(sec)	
Session Operation :Creation	Number of sampling intervals during which a number of sessions in the indicated range were created during the current sampling period.
Session Operation :Deletion	Number of sampling intervals during which a number of sessions in the indicated range were deleted during the current sampling period.
Session Lifetime Distribution(sec):	Number of TCP, UDP, and HTTP sessions whose length was in the indicated range in seconds.

Sample Output

show services sessions analysis interface

`user@host>` **show services sessions analysis interface ms-5/1/0**

```
    Services PIC Name:    ms-5/1/0

Session Analysis Statistics:

  Total sessions Active                  :0
  Total TCP Sessions Active              :0
      Tcp sessions from gate             :0
      Tunneled TCP sessions              :0
      Regular TCP sessions               :0
      IPv4 active Session                :0
      IPv6 active Session                :0
  Total UDP sessions Active              :0
      UDP sessions from gate             :0
      Tunneled UDP sessions              :0
      Regular UDP sessions               :0
      IPv4 active Session                :0
      IPv6 active Session                :0
  Total Other sessions Active            :0
      IPv4 active Session                :0
```

```
      IPv6 active Session                :0
  Created sessions per Second            :0
  Deleted sessions per Second            :0
  Peak Total sessions Active             :0
  Peak Total TCP sessions Active         :0
  Peak Total UDP sessions Active         :0
  Peak Total Other sessions Active       :0
  Peak Created Sessions per Second       :0
  Peak Deleted Sessions per Second       :0
  Packets received                       :0
  Packets transmitted                    :0
  Slow path forward                      :0
  Slow path discard                      :0
Session Rate Data:
  Number of Samples: 3518

 Session Rate Distribution(sec)

 Session Operation :Creation

    400000+            :0
    350001  - 400000   :0
    300001  - 350000   :0
    250001  - 300000   :0
    200001  - 250000   :0
    150001  - 200000   :0
     50001  - 150000   :0
     40001  -  50000   :0
     30001  -  40000   :0
     20001  -  30000   :0
     10001  -  20000   :0
      1001  -  10000   :0
         1  -   1000   :0
                0   :3518


 Session Operation :Deletion

    400000+            :0
    350001  - 400000   :0
    300001  - 350000   :0
    250001  - 300000   :0
    200001  - 250000   :0
    150001  - 200000   :0
```

```
     50001  - 150000   :0
     40001  -  50000   :0
     30001  -  40000   :0
     20001  -  30000   :0
     10001  -  20000   :0
      1001  -  10000   :0
         1  -   1000   :0
                   0   :3518


Session Lifetime Distribution(sec):

                TCP                UDP              HTTP
  240+          :0                 0                0
  120 - 240     :0                 0                0
   60 - 120     :0                 0                0
   30 - 60      :0                 0                0
   15 - 30      :0                 0                0
    5 - 15      :0                 0                0
    1 - 5       :0                 0                0
    0 - 1       :0                 0                0
```

show services sessions tcp-log

Syntax

```
show services sessions tcp-log interface interface-name
```

Release Information

Command introduced in Junos OS Release 19.1 for MX Series.

Description

Display information about the tcp log session details.

Required Privilege Level

view

Output Fields

Table 99 on page 2048 lists the output fields for the **show services sessions tcp-log interface *interface-name*** command. Output fields are listed in the approximate order in which they appear.

Table 99: show services sessions tcp-log interface Output Fields

Field Name	Field Description
Service-set	Name of a service set.
TCP	TCP log session details.

Sample Output

`user@router>` **show services sessions tcp-log interface *interface-name***

```
Service Set: junos-tcplog, Session: 33554434, ALG: None, Flags: 0x200000, IP Action:
 no, Offload: no, Asymmetric: no
TCP          18.1.1.1        ->       22.1.1.2        Forward  I              6
TCP          22.1.1.2        ->       18.1.1.1        Forward  O             6
```

show services softwire

Syntax

```
show services softwire
```

Release Information

Command introduced in Junos OS Release 10.4.
count option added in Junos OS Release 11.2.
Support added for Next Gen Services in Junos OS Release 20.2 on the MX-SPC3 security services card.

Description

Display information about softwire services. Information is displayed on both 6rd and DS-Lite services.

Options

count ***interface-name***—(Optional) Display the current softwire counts for a service set for both DS-Lite and 6rd.

count — (Optional) Display the number of created softwires.

Required Privilege Level

view

List of Sample Output

show services softwire on page 2050
show services softwire count (sp- interfaces) on page 2050
show services softwires count (vms- interfaces on page 2050

Output Fields

Table 100 on page 2049 lists the output fields for the **command-name** command. Output fields are listed in the approximate order in which they appear.

Table 100: show-services-softwire Output Fields

Field Name	Field Description	Level of Output
Interface	Interface for which information is displayed.	All levels
Service Set	Service set containing the softwire rules for the interface.	All levels
Softwire	Name of the softwire concentrator.	All levels
Direction	Direction of the flow.	All levels
Flow count	Number of flows.	All levels

Sample Output

show services softwire

```
user@host> show services softwire
```

```
Interface: sp-3/0/0, Service set: v6rd-dom1-dom3-service-set
Softwire                                    Direction     Flow count
10.10.10.2      ->     192.0.2.1               I                 13
```

show services softwire count (sp- interfaces)

```
user@host> show services softwire count
```

```
Interface   Service set      DS-Lite        6RD
sp-0/0/0    dslite-svc-set1     2            0
```

show services softwires count (vms- interfaces

```
user@host> show services softwire count
```

```
Interface   Service set    DS-Lite       6RD       MAPE
vms-2/0/0    vms-sset10       1          0
```

show services softwire flows

Syntax

```
show services softwire flows
(<interface interface-name> <service-set service-set-name>|
count <interface interface-name> <service-set service-set-name>|
ds-lite <B4 b4-address> <AFTR aftr-address>|
v6rd <initiator initiator-ip-address><concentrator concentrator-ip-address>)
```

Release Information

Command introduced in Junos OS Release 10.2.
Support added for Next Gen Services in Junos OS Release 20.2

Description

Display statistics information about the softwire flows.

> **NOTE:** Starting with Junos OS Release 14.1R4, the IPv6 prefix length associated with a subscriber's basic broadband bridging device that is subject to a limited number of sessions (**dslite-ipv6-prefix-length** attribute) is taken into account while the session count is calculated and displayed in the output of the show services softwire flows command. Until Junos OS Release 14.1R3, only IPv4 flows were counted and IPv6 flows were not considered for the statistics about softwire flows

Options

interface *interface-name*—(Optional) Display statistics information about the specified interface only.

service-set *service-set-name*—(Optional) Display statistics information about the specified service set only.

count <interface *interface-name*> <service-set *service-set-name*>|—(Optional) Display flow count information only, with optional filtering by interface and service set.

ds-lite <B4 *b4-address*> <AFTR *aftr-address*>|—(Optional) Display DS-Lite flow information, with optional filtering by B4 (softwire initiator) and AFTR (softwire concentrator).

v6rd <initiator *initiator-ip-address*><concentrator *concentrator-ip-address*>)—(Optional) Display v6rd flow information, with optional filtering by the softwire initiator and softwire concentrator.

Required Privilege Level

view

List of Sample Output

show services softwire flows on page 2053
show services softwire flows count on page 2053
show services softwire flows ds-lite B4 on page 2053
show services softwire flows ds-lite AFTR on page 2054
services softwire flows ds-lite AFTR and B4 on page 2054
show services softwires softwire-types map-e on page 2054

Output Fields

Table 101 on page 2052 lists the output fields for the **show services softwire flows** command. Output fields are listed in the approximate order in which they appear.

Table 101: show services softwire flows Output Fields

Field Name	Field Description
Interface	Name of the interface.
Service set	Name of the service set.
Flow	Description of flow, including protocol input and output interface addresses.
State	Flow state. Value is: • **Forward**
Dir	Flow direction. Values are: • **I**—inbound • **O**—outbound
Frm count	Number of frames transferred.
NAT dest	NAT translation of the decapsulated address.
Softwire	For outbound flows, the address of the local softwire initiator (B4 for DS-Lite) is shown first, followed by the address of the softwire concentrator (AFTR for DS-Lite). For inbound flows, the address of the software concentrator is shown first, followed by the address of the softwire initiator.

Sample Output

show services softwire flows

user@host> **show services softwire flows**

```
Interface: sp-0/0/0, Service set: dslite-svc-set1
Flow                                              State       Dir       Frm count
TCP      200.200.200.2:80    ->     33.33.33.1:1066  Forward  O         2005418
    NAT dest        33.33.33.1:1066    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::2
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         2007168
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1066
    Softwire           2001::2         ->         1001::1
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         2635998
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1065
    Softwire           2001::3         ->         1001::1
DS-LITE         2001::2      ->        1001::1       Forward  I         2008157
TCP      200.200.200.2:80    ->     33.33.33.1:1065  Forward  O         2637909
    NAT dest        33.33.33.1:1065    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::3
DS-LITE         2001::3      ->        1001::1       Forward  I         2640499
```

show services softwire flows count

user@host> **show services softwire flows count**

```
Interface   Service set                                          Flow count
sp-0/0/0    dslite-svc-set1                                      6
```

show services softwire flows ds-lite B4

user@host> **show services softwire flows ds-lite B4 2001::2**

```
Interface: sp-0/0/0, Service set: dslite-svc-set1
Flow                                              State       Dir       Frm count
TCP      200.200.200.2:80    ->     33.33.33.1:1066  Forward  O         2884037
    NAT dest        33.33.33.1:1066    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::2
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         2885884
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1066
    Softwire           2001::2         ->         1001::1
DS-LITE         2001::2      ->        1001::1       Forward  I         2886821
```

show services softwire flows ds-lite AFTR

user@host> **show services softwire flows ds-lite AFTR 1001::1**

```
Interface: sp-0/0/0, Service set: dslite-svc-set1
Flow                                              State       Dir       Frm count
TCP      200.200.200.2:80    ->     33.33.33.1:1066  Forward  O         3359356
    NAT dest        33.33.33.1:1066    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::2
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         3361235
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1066
    Softwire           2001::2         ->         1001::1
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         4479810
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1065
    Softwire           2001::3         ->         1001::1
DS-LITE         2001::2      ->        1001::1       Forward  I         3362168
TCP      200.200.200.2:80    ->     33.33.33.1:1065  Forward  O         4481520
    NAT dest        33.33.33.1:1065    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::3
DS-LITE         2001::3      ->        1001::1       Forward  I         4484094
```

services softwire flows ds-lite AFTR and B4

user@host> **show services softwire flows ds-lite AFTR 1001::1 B4 2001::2**

```
Interface: sp-0/0/0, Service set: dslite-svc-set1
Flow                                              State       Dir       Frm count
TCP      200.200.200.2:80    ->     33.33.33.1:1066  Forward  O         3931026
    NAT dest        33.33.33.1:1066    ->       20.20.1.2:1025
    Softwire           1001::1         ->         2001::2
TCP          20.20.1.2:1025  ->  200.200.200.2:80    Forward  I         3932792
    NAT source       20.20.1.2:1025    ->      33.33.33.1:1066
    Softwire           2001::2         ->         1001::1
DS-LITE         2001::2      ->        1001::1       Forward  I         3933782
```

show services softwires softwire-types map-e

user@host> **show services softwires softwire-types map-e mape-tun1**

```
br-address 2001:db8:ffff::1/128; //Mandatory
rule r1 {
    ipv4-prefix 192.0.2.0/24; //Mandatory
    ipv6-prefix 2001:db8:0000::/40; //Mandatory
    ea-bits-length 16; //Mandatory
```

```
    psid-offset 4; //Mandatory
    psid-len 8;
}
version 3;
```

show services softwire statistics

Syntax

```
show services softwire statistics
<ds-lite>
<ds-lite>
<inferface interface-name>
<v6rd>
```

Release Information

Command introduced in Junos OS Release 10.4.
Support for Next Gen Services with the MX-SPC3 security services card added in Junos OS Release 20.2.

Description

Display information about softwire services.

Options

ds-lite—(Optional) Display only DS-Lite.

interface *interface-name* —(Optional) Name of the interface servicing the softwire. When you omit this option, data for all interfaces are shown.

v6rd—(Optional) Display only 6rd statistics.

Required Privilege Level

view

List of Sample Output

show services softwire statistics (sp- interfaces) on page 2060
show services softwire statistics ds-lite (sp- interfaces) on page 2062
show services softwire statistics (vms- interfaces) on page 2064
show services softwire statistics ds-lite (vms- interfaces) on page 2065

Output Fields

Table 102 on page 2056 lists the output fields for the **command-name** command. Output fields are listed in the approximate order in which they appear.

Table 102: command-name Output Fields

Field Name	Field Description	Level of Output
Service PIC Name	Name of service PIC for which statistics are shown.	**statistics**

Table 102: command-name Output Fields *(continued)*

Field Name	Field Description	Level of Output
Softwires Created	Number of softwires created.	**statistics**
Softwires Created for EIF/HP	Number of softwires created for endpoint-independent filtering (EIF) or hairpinning (HP).	**statistics** for **ds-lite** only
Softwires Deleted	Number of softwires deleted.	**statistics**
Softwires Flows Created	Number of flows created.	**statistics**
Softwires Flows Deleted	Number of flows deleted.	**statistics**
Slow Path Packets Processed	Number of packets processed as initial packets in a softwire session. These packets require a rule lookup and setting up of flows; this processing of an initial packet in a flow is called *the slow path*.	**statistics**
Slow Path Packets Processed for EIF/HP	Number of slow path EIF/HP packets processed.	**statistics** for **ds-lite** only
Fast Path Packets Processed	Number of packets processed that are not *slow path*.	**statistics**
Fast Path Encapsulated	Number of packets encapsulated in the fast path.	**statistics**
Softwire EIF Accept	Number of packets that matched an EIF entry that initiated the creation of a DS-Lite tunnel. The EIF entry was previously triggered by a DS-Lite packet.	**statistics** for **ds-lite** only
Rule Match Succeeded	Number of packets that matched a softwire rule.	**statistics**
Rule Match Failed	Number of packets that did not match any softwire rule.	**statistics**

Table 102: command-name Output Fields *(continued)*

Field Name	Field Description	Level of Output
IPv6 Packets Fragmented	Number of packets fragmented by the services PIC.	**statistics** for **ds-lite** only
IPv4 Client Fragments	Number of IPv4 fragments received from the client end over the softwire tunnel destined to the server.	**statistics** for **ds-lite** only
IPv4 Server First Fragments	Number of IPv4 first fragments received from the server destined to go over the softwire tunnel to the client.	**statistics** for **ds-lite** only
IPv4 Server More Fragments	Number of IPv4 other fragments (excluding first and last fragment) received from the server destined to go over the softwire tunnel to the client.	**statistics** for **ds-lite** only
IPv4 Server Last Fragments	Number of IPv4 last fragments received from the server destined to go over the softwire tunnel to the client.	**statistics** for **ds-lite** only
ICMPv4 Packets sent	Number of ICMPv4 packets sent to the softwire concentrator.	**statistics**
ICMPv4 Error Packets sent	Number of ICMPv4 error packets sent to the softwire concentrator.	**statistics**
ICMPv6 Packets sent	Number of ICMPv6 packets sent to the softwire concentrator.	**statistics**
Dropped ICMPv6 packets destined to AFTR	Number of ICMPv6 packets dropped instead of sending to the softwire concentrator.	**statistics**
Softwire Creation Failed	Number of softwire creation failures.	**statistics** for **ds-lite** and **6rd**
Softwire Creation Failed for EIF/HP	Number of softwire creation failures for EIF/HP.	**statistics** for **ds-lite** only
Flow Creation Failed	Number of flow creation failures.	**statistics**
Flow Creation Failed for EIF/HP	Number of flow creation failures for EIF/HP.	**statistics** for **ds-lite** only

Table 102: command-name Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flow Creation Failed - Retry	Number of flow creations retried after failure.	**statistics**
Slow Path Failed	Number of failures detected in the slow path.	**statistics**
Slow Path Failed - Retry	Number of times processing of a packet was reprocessed in the slow path.	**statistics**
Packet not IPv4-in-IPv6	Number of IPv4 packets not encapsulated in IPv6.	**statistics** for **ds-lite** only
IPv6 Fragmentation Error	Number of IPv6 packets with fragmentation errors.	**statistics**
Slow Path Failed-IPv6 Next Header Offset	Number of IPv6 header errors detected in slow path processing.	**statistics** for **ds-lite** only
Decapsulated Packet not IPv4	Number of packets without IPv4 inner header.	**statistics** for **ds-lite** only
Decap Failed - IPv6 Next Header Offset	Decapsulation failure due to an unexpected inner header.	**statistics** for **ds-lite** only
Decap Failed - IPv4 L3 Integrity	Decapsulation failure due to incorrect Layer 3 data, such as not an IP packet, bad source or destination address, checksum error, or protocol error.	**statistics** for **ds-lite** only
Decap Failed - IPv4 L4 Integrity	Decapsulation failure due to incorrect Layer 4 data, such as errors in TCP, UDP, or TCP headers.	**statistics** for **ds-lite** only
No Softwire ID	Number of times a softwire ID was not found.	**statistics**
No Flow Extension	Number of times flow extensions were not found.	**statistics**
ICMPv4 Dropped Packets	Number of ICMPv4 packets dropped.	**statistics**

Table 102: command-name Output Fields *(continued)*

Field Name	Field Description	Level of Output
Packet not IPv6-in-IPv4	Number of IPv6 packets not encapsulated in IPv4.	**statistics** for **v6rd** only
Decapsulated Packet not IPv6	Number of packets without an IPv6 inner header.	**statistics** for **v6rd** only
Encapsulation Failed - No packet memory	Failed to encapsulate IPv6 packets in IPv4 due to low memory.	**statistics** for **v6rd** only
Flow limit exceeded	Flow not created because configured maximum flows per softwire is exceeded.	**statistics**
Session limit exceeded	Flow not created because configured maximum DS-Lite softwire sessions per IPv6 prefix is exceeded.	**statistics** for ds-lite only

Sample Output

show services softwire statistics (sp- interfaces)

```
user@host> show services softwire statistics
```

```
DS-Lite Statistics:


  Service PIC Name:                            :sp-0/0/0

  Statistics
  ----------

    Softwires Created                          :0
    Softwires Created for EIF/HP               :0
    Softwires Deleted                          :0
    Softwires Flows Created                    :0
    Softwires Flows Deleted                    :0
    Slow Path Packets Processed                :0
    SLow Path Packets Processed for EIF/HP     :0
    Fast Path Packets Processed                :0
    Fast Path Packets Encapsulated             :0
```

```
    Softwire EIF Accept                          :0
    Rule Match Succeeded                         :0
    Rule Match Failed                            :0
    IPv6 Packets Fragmented                      :0
    IPv4 Client Fragments                        :0
    IPv4 Server First Fragments                  :0
    IPv4 Server More Fragments                   :0
    IPv4 Server Last Fragments                   :0
    ICMPv4 Packets sent                          :0
    ICMPv4 Error Packets sent                    :0
    ICMPv6 Packets sent                          :0
    Dropped ICMPv6 packets destined to AFTR      :0

  Transient Errors
  ----------------

    Flow Creation Failed - Retry                 :0
    FLow Creation Failed - Retry for EIF/HP      :0
    Slow Path Failed - Retry                     :0

  Errors
  ------

    Softwire Creation Failed                             :0
    Softwire Creation Failed for EIF/HP                  :0
    Flow Creation Failed                                 :0
    FLow Creation Failed For EIF/HP                      :0
    Slow Path Failed                                     :0
    Packet not IPv4-in-IPv6                              :0
    IPv6 Fragmentation Error                             :0
    Softwire Creation Failed - IPv6 Next Header Offset   :0
    Decapsulated Packet not IPv4                         :0
    Decap Failed - IPv6 Next Header Offset               :0
    Decap Failed - IPv4 L3 Integrity                     :0
    Decap Failed - IPv4 L4 Integrity                     :0
    No Softwire ID                                       :0
    No Flow Extension                                    :0
    Flow Limit Exceeded                                  :0

6rd Statistics:



 Service PIC Name                                :sp-0/0/0
```

```
  Statistics
  ----------

    Softwires Created                          :0
    Softwires Deleted                          :0
    Softwires Flows Created                    :0
    Softwires Flows Deleted                    :0
    Slow Path Packets Processed                :0
    Fast Path Packets Processed                :0
    Fast Path Packets Encapsulated             :0
    Rule Match Failed                          :0
    Rule Match Succeeded                       :0

  Transient Errors
  ----------------

    Flow Creation Failed - Retry               :0
    Slow Path Failed - Retry                   :0

  Errors
  ------

    Softwire Creation Failed                   :0
    Flow Creation Failed                       :0
    Slow Path Failed                           :0
    Packet not IPv6-in-IPv4                    :0
    Slow Path Failed - IPv6 Next Header Offset :0
    Decapsulated Packet not IPv6               :0
    Encapsulation Failed - No packet memory    :0
    No Softwire ID                             :0
    No Flow Extension                          :0
    ICMPv4 Dropped Packets                     :0
```

show services softwire statistics ds-lite (sp- interfaces)

`user@host>` **show services softwire statistics ds-lite**

```
DS-Lite Statistics:


  Service PIC Name:                            :sp-0/0/0

  Statistics
```

```
----------

  Softwires Created                           :0
  Softwires Created for EIF/HP                :0
  Softwires Deleted                           :0
  Softwires Flows Created                     :0
  Softwires Flows Deleted                     :0
  Slow Path Packets Processed                 :0
  SLow Path Packets Processed for EIF/HP      :0
  Fast Path Packets Processed                 :0
  Fast Path Packets Encapsulated              :0
  Softwire EIF Accept                         :0
  Rule Match Succeeded                        :0
  Rule Match Failed                           :0
  IPv6 Packets Fragmented                     :0
  IPv4 Client Fragments                       :0
  IPv4 Server First Fragments                 :0
  IPv4 Server More Fragments                  :0
  IPv4 Server Last Fragments                  :0
  ICMPv4 Packets sent                         :0
  ICMPv4 Error Packets sent                   :0
  ICMPv6 Packets sent                         :0
  Dropped ICMPv6 packets destined to AFTR     :0

Transient Errors
----------------

  Flow Creation Failed - Retry                :0
  FLow Creation Failed - Retry for EIF/HP     :0
  Slow Path Failed - Retry                    :0

Errors
------

  Softwire Creation Failed                          :0
  Softwire Creation Failed for EIF/HP               :0
  Flow Creation Failed                              :0
  FLow Creation Failed For EIF/HP                   :0
  Slow Path Failed                                  :0
  Packet not IPv4-in-IPv6                           :0
  IPv6 Fragmentation Error                          :0
  Softwire Creation Failed - IPv6 Next Header Offset  :0
  Decapsulated Packet not IPv4                      :0
  Decap Failed - IPv6 Next Header Offset            :0
```

```
    Decap Failed - IPv4 L3 Integrity                    :0
    Decap Failed - IPv4 L4 Integrity                    :0
    No Softwire ID                                      :0
    No Flow Extension                                   :0
    Flow Limit Exceeded                                 :0
    Session Limit Exceeded                              :0
```

Sample Output

show services softwire statistics (vms- interfaces)

`user@host>` **show services softwire statistics**

```
vms-2/0/0
    Total Session Interest events       :3
    Total Session Destroy events                            :2
    Total Session Public Request events                     :0
    Total Session Accepts                                   :1
    Total Session Discards                                  :0
    Total Session Ignores                                   :0
    Total Session extension alloc failures                  :0
    Total Session extension set failures                    :0
Softwire statistics
    Total Softwire sessions created                         :1
    Total Softwire sessions deleted                         :2
    Total Softwire sessions created for reverse packets     :1
    Total Softwire session create failed for reverse pkts   :0
    Total Softwire rule match success                       :1
    Total Softwire rule match failed                        :0
    Softwire session limit exceeded                         :0
Softwire packet statistics
    Total Packets processed                                 :1
    Total packets encapsulated                              :1
    Total packets decapsulated                              :1
    Encapsulation errors                                    :0
    Decapsulation errors                                    :0
    Encapsulated pkts re-inject failures                    :0
    Decapsulated pkts re-inject failures                    :0
    DS-Lite ICMPv4 Echo replies sent                        :0
    DS-Lite ICMPv4 TTL exceeded messages sent               :0
    ICMPv6 ECHO request messages received destined to AFTR  :0
    ICMPv6 ECHO reply messages sent from AFTR               :0
```

```
    ICMPv6 ECHO requests to AFTR process failures          :0
    V6 untunnelled packets destined to AFTR dropped        :1
    Softwire policy add errors                             :0
    Softwire policy delete errors                          :0
    Softwire policy memory alloc failures                  :0
    Softwire Untunnelled packets ignored                   :0
Softwire Misc errors
    DS-Lite ICMPv4 TTL exceed message process errors       :0
```

show services softwire statistics ds-lite (vms- interfaces)

`user@host>` **show services softwire statistics ds-lite interface vms-2/0/0**

```
vms-2/0/0
    Total Session Interest events       :3
    Total Session Destroy events                           :2
    Total Session Public Request events                    :0
    Total Session Accepts                                  :1
    Total Session Discards                                 :0
    Total Session Ignores                                  :0
    Total Session extension alloc failures                 :0
    Total Session extension set failures                   :0
Softwire statistics
    Total Softwire sessions created                        :1
    Total Softwire sessions deleted                        :2
    Total Softwire sessions created for reverse packets    :1
    Total Softwire session create failed for reverse pkts  :0
    Total Softwire rule match success                      :1
    Total Softwire rule match failed                       :0
    Softwire session limit exceeded                        :0
Softwire packet statistics
    Total Packets processed                                :1
    Total packets encapsulated                             :1
    Total packets decapsulated                             :1
    Encapsulation errors                                   :0
    Decapsulation errors                                   :0
    Encapsulated pkts re-inject failures                   :0
    Decapsulated pkts re-inject failures                   :0
    DS-Lite ICMPv4 Echo replies sent                       :0
    DS-Lite ICMPv4 TTL exceeded messages sent              :0
    ICMPv6 ECHO request messages received destined to AFTR :0
    ICMPv6 ECHO reply messages sent from AFTR              :0
    ICMPv6 ECHO requests to AFTR process failures          :0
    V6 untunnelled packets destined to AFTR dropped        :1
```

```
    Softwire policy add errors                              :0
    Softwire policy delete errors                           :0
    Softwire policy memory alloc failures                   :0
    Softwire Untunnelled packets ignored                    :0
Softwire Misc errors
    DS-Lite ICMPv4 TTL exceed message process errors        :0
```

show services stateful-firewall conversations

Syntax

```
show services stateful-firewall conversations
<brief | extensive | terse>
<application-protocol protocol>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<limit number>
<pgcp>
<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.

Description

Display information about stateful firewall conversations.

Options

none—Display standard information about all stateful firewall conversations.

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

application-protocol *protocol*—(Optional) Display information about one of the following application protocols:

- **bootp**—Bootstrap protocol
- **dce-rpc**—Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—Domain Name System protocol
- **exec**—Exec
- **ftp**—File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol

- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

destination-port *destination-port*—(Optional) Display information for a particular destination port. The range of values is 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, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

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

pgcp —(Optional) Display information about stateful firewall conversations for Packet Gateway Control Protocol (PGCP) flows.

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 the specific service set.

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

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

Required Privilege Level
view

List of Sample Output
show services stateful-firewall conversations on page 2071
show services stateful-firewall conversations destination-port on page 2071

Output Fields
Table 103 on page 2069 lists the output fields for the **show services stateful-firewall conversations** command. Output fields are listed in the approximate order in which they appear.

Table 103: show services stateful-firewall conversations Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set. Individual empty service sets are not displayed, but if no service set has any flows, a flow table header is printed for each service set.
Conversation	Information about a group of related flows. • **ALG Protocol**—Application-level gateway protocol. • **Number of initiators**—Number of flows that initiated a session. • **Number of responders**—Number of flows that responded in a session.

Table 103: show services stateful-firewall conversations Output Fields *(continued)*

Field Name	Field Description
Flow or Flow Prot	Protocol used for this flow.
Source	Source prefix of the flow, in the format ***source-prefix-port***.
Destination	Destination prefix of the flow.
State	Status of the flow: • **Drop**—Drop all packets in the flow without response. • **Forward**—Forward the packet in the flow without looking at it. • **Reject**—Drop all packets in the flow with response. • **Watch**—Inspect packets in the flow.
Dir	Direction of the flow: input (**I**) or output (**O**).
Source NAT	Original and translated source IPv4 or IPv6 addresses are displayed if Network Address Translation (NAT) is configured on this particular flow or conversation.
Frm Count	Number of frames in the flow.
Destin NAT	Original and translated destination IPv4 or IPv6 addresses are displayed if NAT is configured on this particular flow or conversation.
Byte count	Number of bytes forwarded in the flow.
TCP established	Whether a TCP connection was established: **Yes** or **No**.
TCP window size	Negotiated TCP connection window size, in bytes.
TCP acknowledge	TCP acknowledgment sequence number.
TCP tickle	Whether TCP inquiry mode is on (**enabled** or **disabled**) and the time remaining to send the next inquiry, in seconds.
Master flow	Flow that initiated the conversation.
TImeout	Lifetime of the flow, in seconds.

Sample Output

show services stateful-firewall conversations

user@host> **show services stateful-firewall conversations**

```
Interface: sp-1/3/0, Service set: green
Conversation: ALG Protocol: any, Number of initiators: 1,
Number of responders: 1

Flow
Prot     Source                 Dest               State      Dir   Frm count
TCP      10.58.255.50:33005->   10.58.255.178:23   Forward    I      13
  Source NAT     10.58.255.50:33005->    10.59.16.100:4000
  Destin NAT     10.58.255.178:23  ->         0.0.0.0:4000
Byte count:          918
TCP established, TCP window size: 65535, TCP acknowledge: 2502627025
TCP tickle enabled, 0 seconds,
Master flow, Timeout: 30 seconds
TCP     10.58.255.178:23   ->    10.59.16.100:4000 Forward    O        8
```

show services stateful-firewall conversations destination-port

user@host> **show services stateful-firewall conversations destination-port 21**

```
Interface: sp-0/3/0, Service set: svc_set_trust

Interface: sp-0/3/0, Service set: svc_set_untrust
Conversation: ALG protocol: ftp
  Number of initiators: 1, Number of responders: 1
Flow                                                State    Dir       Frm count
TCP         10.50.10.2:2143  ->     10.50.20.2:21    Watch    O               0
TCP         10.50.20.2:21    ->     10.50.10.2:2143  Watch    I               0
TCP         10.50.20.2:21    ->     10.50.10.2:2143  Watch    I               0
```

show services stateful-firewall flow-analysis

Syntax

```
show services stateful-firewall flow-analysis
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 10.4R1.

Description

Display stateful firewall flow statistics.

Options

none—Display standard information about all stateful firewall flow statistics.

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level

view

List of Sample Output

show services stateful-firewall flow-analysis on page 2074
show services stateful-firewall flow-analysis interface sp-3/0/0 on page 2075

Output Fields

Table 98 on page 2043 lists the output fields for the **show services stateful-firewall flow-analysis** command. Output fields are listed in the approximate order in which they appear.

Table 104: show services stateful-firewall flow-analysis Output Fields

Field Name	Field Description
Total Flows Active	Total active flows in the MS-PIC including TCP, UDP, ICMP and Softwires.
Total TCP Flows Active	Total active TCP flows in the MS-PIC.
Total UDP Flows Active	Total active UDP flows in the MS-PIC.
Total Other Flows Active	Total other active flows in the MS-PIC including ICMP and softwires.
Total Predicted Flows Active	Predicted flows are created only by the ALG traffic using the L3/L4 information available.

Table 104: show services stateful-firewall flow-analysis Output Fields *(continued)*

Field Name	Field Description
Created Flows per Second	Flow setup rate at the time of running the command.
Deleted Flows per Second	Flow deletion rate at the time of running the command.
Peak Total Flows Active	The highest number of active flows since the last PIC restart or since the last time flow statistics are flushed.
Peak Total TCP Flows Active	The highest number of active TCP flows since the last PIC restart or since the last time flow stats are flushed.
Peak Total UDP Flows Active	The highest number of active UDP flows since the last PIC restart or since the last time flow statistics are flushed.
Peak Total Other Flows Active	The highest number of other active flows since the last PIC restart or since the last time flow statistics are flushed.
Peak Created Flows per Second	The maximum flow setup rate observed since the last PIC restart or since the last time flow statistics are flushed.
Peak Deleted Flows per Second	The maximum flow deletion rate observed since the last PIC restart or from the last time flow statistics are flushed.
Average HTTP Flow Lifetime(ms)	Average HTTP Flow Lifetime in millisecond.
Packets received	The total number of packets received by the MS-PIC.
Packets transmitted	The total number of packets transmitted by the MS-PIC.
Slow path forward	The number of packets forwarded in the slow path (i.e. after the successful rule match and flow creation).
Slow path discard	The number of packets discarded before the flow creation.
Flow Rate Data: Number of Samples	The number of samples used to calculate the flow rate, since the last PIC restart or since the last time flow statistics are flushed.

Table 104: show services stateful-firewall flow-analysis Output Fields *(continued)*

Field Name	Field Description
Flow Rate Distribution(sec) Flow Operation :Creation Flow Operation :Deletion	Histogram of the samples used for flow rate calculation.
Flow Lifetime Distribution(sec):	Histogram of the samples used to calculate the flow life time in sec.

Sample Output

show services stateful-firewall flow-analysis

`user@host>` **show services stateful-firewall flow-analysis**

```
Services PIC Name: sp-3/0/0
 Flow Analysis Statistics:
      Total Flows Active               :40
      Total TCP Flows Active           :0
      Total UDP Flows Active           :40
      Total Other Flows Active         :0
      Total Predicted Flows Active     :0
      Created Flows per Second         :0
      Deleted Flows per Second         :0
      Peak Total Flows Active          :40
      Peak Total TCP Flows Active      :0
      Peak Total UDP Flows Active      :40
      Peak Total Other Flows Active    :0
      Peak Created Flows per Second    :20
      Peak Deleted Flows per Second    :20
      Average HTTP Flow Lifetime(ms)   :0
      Packets received                 :48682539117
      Packets transmitted              :48682502703
      Slow path forward                :6550
      Slow path discard                :0
 Flow Rate Data:
      Number of Samples: 19720
 Flow Rate Distribution(sec)
 Flow Operation :Creation
```

```
     300000+            :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :19720
Flow Operation :Deletion
     300000+            :0
     250000  - 300000   :0
     200000  - 250000   :0
     160000  - 200000   :0
     150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :19720
Flow Lifetime Distribution(sec):
               TCP                UDP              HTTP
 240+         :0                 0                0
 120 - 240    :0                 0
  60 - 120    :0                 0
  30 - 60     :0                 0
  15 - 30     :0                 6530
   5 - 15     :0                 0
   1 - 5      :0                 0
   0 - 1      :0                 6530
```

Sample Output

show services stateful-firewall flow-analysis interface sp-3/0/0

`user@host>` **show services stateful-firewall flow-analysis interface sp-3/0/0**

```
Services PIC Name: sp-3/0/0
 Flow Analysis Statistics:
      Total Flows Active               :40
      Total TCP Flows Active           :0
      Total UDP Flows Active           :40
      Total Other Flows Active         :0
      Total Predicted Flows Active     :0
      Created Flows per Second         :0
      Deleted Flows per Second         :0
      Peak Total Flows Active          :40
      Peak Total TCP Flows Active      :0
      Peak Total UDP Flows Active      :40
      Peak Total Other Flows Active    :0
      Peak Created Flows per Second    :20
      Peak Deleted Flows per Second    :20
      Average HTTP Flow Lifetime(ms)   :0
      Packets received                 :54696856768
      Packets transmitted              :54696815873
      Slow path forward                :7350
      Slow path discard                :0
 Flow Rate Data:
      Number of Samples: 22139
 Flow Rate Distribution(sec)
 Flow Operation :Creation
      300000+            :0
      250000  - 300000   :0
      200000  - 250000   :0
      160000  - 200000   :0
      150000  - 160000   :0
      50000  - 150000   :0
      40000  -  50000   :0
      30000  -  40000   :0
      20000  -  30000   :0
      10000  -  20000   :0
      1000  -  10000   :0
      0  -   1000   :22139
 Flow Operation :Deletion
      300000+            :0
      250000  - 300000   :0
      200000  - 250000   :0
      160000  - 200000   :0
      150000  - 160000   :0
      50000  - 150000   :0
      40000  -  50000   :0
```

```
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
     1000  -  10000   :0
     0  -   1000   :22139
Flow Lifetime Distribution(sec):
               TCP                UDP              HTTP
 240+          :0                 0                0
 120 - 240     :0                 0
  60 - 120     :0                 0
  30 - 60      :0                 0
  15 - 30      :0                 7330
   5 - 15      :0                 0
   1 - 5       :0                 0
   0 - 1       :0                 7330
```

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 softwire processing, the type of softwire 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
- **iiop**—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**.

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 | **1671**

List of Sample Output
show services stateful-firewall flows on page 2081
show services stateful-firewall flows (For Softwire Flows) on page 2082
show services stateful-firewall flows brief on page 2082
show services stateful-firewall flows extensive on page 2083
show services stateful-firewall flows count on page 2083
show services stateful-firewall flows destination port on page 2083

show services stateful-firewall flows source port on page 2083
show services stateful-firewall flows (Twice NAT) on page 2084

Output Fields

Table 105 on page 2081 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 105: show services stateful-firewall flows Output Fields

Field Name	Field Description
Interface	Name of the interface.
Service set	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.
Flow Count	Number of flows in a session.
Flow or Flow Prot	Protocol used for this flow.
Source	Source prefix of the flow in the format ***source-prefix:port***. 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: • **Drop**—Drop all packets in the flow without response. • **Forward**—Forward the packet in the flow without looking at it. • **Reject**—Drop all packets in the flow with response. • **Watch**—Inspect packets in the flow.
Dir	Direction of the flow: input **(I)** or output **(O)**. For any configured stateful firewall rule, the reverse flow is dynamically created, so you will see an input and an output flow.
Frm count	Number of frames in the flow. If this value is zero, then that flow does not yet exist.

Sample Output

show services stateful-firewall flows

On the MX Series router, both input (I) and output (O) flow entries appear, even if traffic only flows in one direction. This applies to both NAT and non-NAT cases.

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    O
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 Softwire Flows)

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

user@host> **show services stateful-firewall flows**

```
Interface: sp-0/1/0, Service set: dslite-svc-set2
Flow                                                State    Dir       Frm count
TCP      200.200.200.2:80    ->     44.44.44.1:1025  Forward  O          219942
    NAT dest        44.44.44.1:1025    ->       20.20.1.4:1025
    Softwire           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
    Softwire           2001::2         ->         1001::1
TCP      200.200.200.2:80    ->     44.44.44.1:1024  Forward  O          219140
    NAT dest        44.44.44.1:1024    ->       20.20.1.2:1025
    Softwire           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  O          218906
    NAT dest        44.44.44.1:1026    ->       20.20.1.3:1025
    Softwire           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
    Softwire           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
    Softwire           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                                                    State     Dir       Frm
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    O
  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@host> 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                                                 State    Dir       Frm count
TCP         10.50.10.2:2143  ->     10.50.20.2:21    Watch    O               0
```

show services stateful-firewall flows source port

```
user@host> 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                                                State    Dir       Frm count
TCP         10.50.10.2:2143  ->     10.50.20.2:21    Watch    O               0
```

show services stateful-firewall flows (Twice NAT)

`user@host>` **show services stateful-firewall flows**

```
Flow                                                State    Dir       Frm count
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    O             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
```

show services stateful-firewall sip-call

Syntax

```
show services stateful-firewall sip-call
<brief | extensive | terse>
<application-protocol protocol>
<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 in Junos OS Release 7.4.

Description

Display stateful firewall Session Initiation Protocol (SIP) call information.

Options

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

brief—(Optional) Display brief SIP call information.

extensive—(Optional) Display detailed SIP call information.

terse—(Optional) Display terse SIP call information.

application-protocol—(Optional) Display information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol

- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

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 adaptive services interface. On M Series and T Series routers, ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

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

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

- **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
- **ipv6**—IPv6 within IP

- **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 sip-call | **1674**

List of Sample Output
show services stateful-firewall sip-call extensive on page 2088

Output Fields
Table 106 on page 2087 lists the output fields for the **show services stateful-firewall sip-call** command. Output fields are listed in the approximate order in which they appear.

Table 106: show services stateful-firewall sip-call Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
From	Initiator address.
To	Responder address.
Call ID	SIP call identification string.

Table 106: show services stateful-firewall sip-call Output Fields *(continued)*

Field Name	Field Description
Number of initiator flows	Number of **control**, **contact**, or **media** initiator flows.
Number of responder flows	Number of **control**, **contact**, or **media** responder flows.
protocol	Protocol used for this flow.
source-prefix	Source prefix of the flow in the format ***source-prefix* : *port***.
destination-prefix	Destination prefix of the flow.
state	Status of the flow: • **Drop**—Drop all packets in the flow without a response. • **Forward**—Forward the packet in the flow without examining it. • **Reject**—Drop all packets in the flow with a response. • **Unknown**—Unknown status. • **Watch**—Inspect packets in the flow.
direction	Direction of the flow: input (**I**), output (**O**), or unknown (**U**).
frame-count	Number of frames in the flow.
Byte count	Number of bytes forwarded in the flow.
Flow role	Role of the flow that is under evaluation: **Initiator**, **Master**, **Responder**, or **Unknown**.
Timeout	Lifetime of the flow, in seconds.

Sample Output

show services stateful-firewall sip-call extensive

`user@host>` **show services stateful-firewall sip-call extensive**

```
Interface: sp-0/3/0, Service set: test_sip_777
```

```
From: : 6507771234@10.200.100.1:0;000ff73ac89900021bb231dc-3ef68435
To: : 4085551234@10.200.100.1:0;0011bb65c2a30007777bd0fc-5748b749
Call ID: : 000ff73a-c8990004-0741adac-3e027c7e@10.20.70.2
Number of control initiator flows: : 1, Number of control responder flows:
: 1
UDP         10.20.70.2:50354 ->   10.200.100.1:5060  Watch    I
2
  Byte count: 1112
  Flow role: Master, Timeout: 30
UDP       10.200.100.1:5060  ->  10.20.170.111:50354 Watch    O
0
  Byte count: 0
  Flow role: Responder, Timeout: 30
UDP           0.0.0.0:0     ->  10.20.170.111:5060  Watch    O
7
  Byte count: 2749
  Flow role: Responder, Timeout: 30
Number of contact initiator flows: 1, Number of contact responder flows: 1
UDP           0.0.0.0:0     ->   10.20.140.11:5060  Watch    I
1
  Byte count: 409
  Flow role: Master, Timeout: 30
UDP       10.20.140.11:31864 ->  10.20.170.111:18808 Forward  O
622
  Byte count: 124400
  Flow role: Master, Timeout: 30
UDP           0.0.0.0:0     ->  10.20.170.111:18809 Forward  O
0
  Byte count: 0
  Flow role: Initiator, Timeout: 30
Number of media initiator flows: 4, Number of media responder flows: 0
UDP         10.20.70.2:18808 ->   10.20.140.11:31864 Forward  I
628
  Byte count: 125600
  Flow role: Initiator, Timeout: 30
UDP           0.0.0.0:0     ->   10.20.140.11:31865 Forward  I
0
  Byte count: 0
  Flow role: Initiator, Timeout: 30
0             0.0.0.0:0     ->        0.0.0.0:0     Unknown  U
0
  Byte count: 0
  Flow role: Unknown, Timeout: 0
```

```
0               0.0.0.0:0     ->        0.0.0.0:0     Unknown  U
Interface: sp-0/3/0, Service set: test_sip_888
```

show services stateful-firewall sip-register

Syntax

```
show services stateful-firewall sip-register
<brief | extensive | terse>
<application-protocol protocol>
<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 in Junos OS Release 7.4.

Description

Display stateful firewall Session Initiation Protocol (SIP) register information.

Options

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

brief—(Optional) Display brief SIP register information.

extensive—(Optional) Display detailed SIP register information.

terse—(Optional) Display terse SIP register information.

application-protocol—(Optional) Display information about one of the following application protocols:

- **bootp**—(SIP only) Bootstrap protocol
- **dce-rpc**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols
- **dce-rpc-portmap**—(SIP only) Distributed Computing Environment-Remote Procedure Call protocols portmap service
- **dns**—(SIP only) Domain Name System protocol
- **exec**—(SIP only) Exec
- **ftp**—(SIP only) File Transfer Protocol
- **h323**—H.323 standards
- **icmp**—Internet Control Message Protocol

- **iiop**—Internet Inter-ORB Protocol
- **login**—Login
- **netbios**—NetBIOS
- **netshow**—NetShow
- **realaudio**—RealAudio
- **rpc**—Remote Procedure Call protocol
- **rpc-portmap**—Remote Procedure Call protocol portmap service
- **rtsp**—Real-Time Streaming Protocol
- **shell**—Shell
- **sip**—Session Initiation Protocol
- **snmp**—Simple Network Management Protocol
- **sqlnet**—SQLNet
- **tftp**—Trivial File Transfer Protocol
- **traceroute**—Traceroute
- **winframe**—WinFrame

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

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

interface *interface-name*—(Optional) Display information about a particular interface. On M Series and T Series routers, the ***interface-name*** can be **sp-*fpc/pic/port*** or **rsp*number***.

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

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

- **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
- **ipv6**—IPv6 within IP

- **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 sip-register | **1677**

List of Sample Output
show services stateful-firewall sip-register extensive on page 2094

Output Fields
Table 107 on page 2093 lists the output fields for the **show services stateful-firewall sip-register** command. Output fields are listed in the approximate order in which they appear.

Table 107: show services stateful-firewall sip-register Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
SIP Register	Register information header.
Protocol	Protocol used for this flow.
Registered IP	Register IP address.

Table 107: show services stateful-firewall sip-register Output Fields *(continued)*

Field Name	Field Description
Port	Register port number.
Expiration timeout	Configured lifetime, in seconds.
Timeout remaining	Lifetime remaining, in seconds.
From	Initiator address.
To	Responder address.
Call ID	SIP call identification string.

Sample Output

show services stateful-firewall sip-register extensive

`user@host>` **show services stateful-firewall sip-register extensive**

```
Interface: sp-0/3/0, Service set: test_sip_777

SIP Register: Protocol: UDP, Registered IP: 10.20.170.111, Port: 5060, Acked
    Expiration timeout: 36000, Timeout remaining: 35544
    From: : 6507771234@10.200.100.1:0;
    To: : 6507771234@10.200.100.1:0;
    Call ID: : 000ff73a-c8990002-23b1d942-2ba1f91f@10.20.70.2

Interface: sp-0/3/0, Service set: test_sip_888

SIP Register: Protocol: UDP, Registered IP: 10.20.170.112, Port: 5060, Acked
    Expiration timeout: 36000, Timeout remaining: 35549
    From: : 8881234@10.200.100.1:0;
    To: : 8881234@10.200.100.1:0;
    Call ID: : 00112096-81fc0002-23b38905-7cb41f62@10.20.71.2
```

show services stateful-firewall statistics

Syntax

```
show services stateful-firewall statistics
<application-protocol protocol>
<brief | detail | extensive | summary>
<interface interface-name>
<service-set service-set>
```

Release Information

Command introduced before Junos OS Release 7.4.

Description

Display stateful firewall statistics.

Options

none—Display standard information about all stateful firewall statistics.

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

interface *interface-name*—(Optional) Display information about a particular interface. On M Series and T Series routers, the ***interface-name*** can be **ms-*fpc*/*pic*/*port*** or **rsp*number***.

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

Required Privilege Level

view

RELATED DOCUMENTATION

clear services stateful-firewall statistics | **1680**

List of Sample Output

show services stateful-firewall statistics extensive on page 2103

Output Fields

Table 108 on page 2096 lists the output fields for the **show services stateful-firewall statistics** command. Output fields are listed in the approximate order in which they appear.

Table 108: show services stateful-firewall statistics Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of a service set.
New flows	Rule match counters for new flows: • **Rule Accepts**—New flows accepted. • **Rule Discards**—New flows discarded. • **Rule Rejects**—New flows rejected.
Existing flow types packet counters	Rule match counters for existing flows: • **Accepts**—Match existing forward or watch flow. • **Drop**—Match existing discard flow. • **Rejects**—Match existing reject flow.
Hairpinning Counters	Hairpinning counters: • **Slow Path Hairpinned Packets**—Slow path packets that were hairpinned back to the internal network. • **Fast Path Hairpinned Packets**—Fast path packets that were hairpinned back to the internal network.
Drops	Drop counters: • **IP option**—Packets dropped in IP options processing. • **TCP SYN defense**—Packets dropped by SYN defender. • **NAT ports exhausted**—Hide mode. The router has no available Network Address Translation (NAT) ports for a given address or pool. • **Sessions dropped due to subscriber flow limit**—Sessions dropped because the subscriber's flow limit was exceeded.
Errors	Total errors, categorized by protocol: • **IP**—Total IP version 4 errors. • **TCP**—Total Transmission Control Protocol (TCP) errors. • **UDP**—Total User Datagram Protocol (UDP) errors. • **ICMP**—Total Internet Control Message Protocol (ICMP) errors. • **Non-IP packets**—Total non-IPv4 errors. • **ALG**—Total application-level gateway (ALG) errors

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
IP Errors	IPv4 errors: • **IP packet length inconsistencies**—IP packet length does not match the Layer 2 reported length. • **Minimum IP header length check failures**—Minimum IP header length is 20 bytes. The received packet contains less than 20 bytes. • **Reassembled packet exceeds maximum IP length**—After fragment reassembly, the reassembled IP packet length exceeds 65,535. • **Illegal source address 0**—Source address is not a valid address. Invalid addresses are, loopback, broadcast, multicast, and reserved addresses. Source address **0**, however, is allowed to support BOOTP and the destination address **0xffffffff**. • **Illegal destination address 0**—Destination address is not a valid address. The address is reserved. • **TTL zero errors**—Received packet had a time-to-live (TTL) value of 0. • **Illegal IP protocol number (0 or 255)**—IP protocol is 0 or 255. • **Land attack**—IP source address is the same as the destination address. • **Non-IPv4 packets**—Packet was not IPv4. (Only IPv4 is supported.) • **Bad checksum**—Packet had an invalid IP checksum. • **Illegal IP fragment length**—Illegal fragment length. All fragments (other than the last fragment) must have a length that is a multiple of 8 bytes. • **IP fragment overlap**—Fragments have overlapping fragment offsets. • **IP fragment reassembly timeout**—Some of the fragments for an IP packet were not received in time, and the reassembly handler dropped partial fragments. • **IP fragment limit exceeded: 0**—Fragments that exceeded the limit. • **Unknown: 0**—Unknown fragments.

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
TCP Errors	

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
	TCP protocol errors: • **TCP header length inconsistencies**—Minimum TCP header length is 20 bytes, and the IP packet received does not contain at least 20 bytes. • **Source or destination port number is zero**—TCP source or destination port is zero. • **Illegal sequence number and flags combinations** — Dropped because of TCP errors, such as an illegal sequence number, which causes an illogical combination of flags to be set. • **SYN attack (multiple SYN messages seen for the same flow)**—Multiple SYN packets received for the same flow are treated as a SYN attack. The packets might be retransmitted SYN packets and therefore valid, but a large number is cause for concern. • **First packet not a SYN message**—First packets for a connection are not SYN packets. These packets might originate from previous connections or from someone performing an ACK/FIN scan. • **TCP port scan (TCP handshake, RST seen from server for SYN)**—In the case of a SYN defender, if an RST (reset) packet is received instead of a SYN/ACK message, someone is probably trying to scan the server. This behavior can result in false alarms if the RST packet is not combined with an intrusion detection service (IDS). • **Bad SYN cookie response**—SYN cookie generates a SYN/ACK message for all incoming SYN packets. If the ACK received for the SYN/ACK message does not match, this counter is incremented. • **TCP reconstructor sequence number error**—This counter is incremented in the following cases: The TCP seqno is 0 and all the TCP flags are also 0. The TCP seqno is 0 and FIN/PSH/URG TCP flags are set. • **TCP reconstructor retransmissions**—This counter is incremented for the retransmitted packets during connection 3-way handshake. • **TCP partially opened connection timeout (SYN)**—This counter is incremented when the SYN Defender is enabled and the 3-way handshake is not completed within the SYN DEFENDER TIMEOUT. The connection will be closed and resources will be released by sending RST to the responder. • **TCP partially opened connection timeout (SYN-ACK)**—This counter is incremented when the SYN Defender is enabled and the 3-way handshake is not completed within the SYN DEFENDER TIMEOUT. The connection will be closed and resources will be released by sending RST to the responder.

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
	• **TCP partially closed connection reuse**—Not supported. • **TCP 3-way error - client sent SYN+ACK**—A SYN/ACK should be sent by the server on receiving a SYN. This counter is incremented when the first message received from the initiator is SYN+ACK. • **TCP 3-way error - server sent ACK**—ACK should be sent by the client on receiving a SYN/ACK from the server. This counter is incremented when the ACK is received from the Server instead of from the Client. • **TCP 3-way error - SYN seq number retransmission mismatch**—This counter is incremented when the SYN is received again with a different sequence number from the first SYN sequence number. • **TCP 3-way error - RST seq number mismatch**—A reset could be received from either side. The server could send a RST on receiving a SYN or the client could send a RST on receiving SYN/ACK. This counter is incremented when the RST is received either from the client or server with a non-matching sequence number. • **TCP 3-way error - FIN received**—This counter is incremented when the FIN is received during the 3-way handshake. • **TCP 3-way error - invalid flags (PSH, URG, ECE, CWR)**—This counter is incremented when any of the PSH, URG, ECE, or CWR flags were received during the 3-way handshake. • **TCP 3-way error - SYN recvd but no client flows**—This counter is incremented when SYN is received but not from the connection initiator. The counter is not incremented in the case of simultaneous open, when the SYN is received in both the directions. • **TCP 3-way error - first packet SYN+ACK**—The first packet received was SYN+ACK instead of SYN. • **TCP 3-way error - first packet FIN+ACK**—The first packet received was FIN+ACK instead of SYN. • **TCP 3-way error - first packet FIN**—The first packet received was FIN instead of SYN. • **TCP 3-way error - first packet RST**—The first packet received was RST instead of SYN. • **TCP 3-way error - first packet ACK**—The first packet received was ACK instead of SYN. • **TCP 3-way error - first packet invalid flags (PSH, URG, ECE, CWR)**—The first packet received had invalid flags. • **TCP Close error - no final ACK**—This counter is incremented when ACK is not received after the FINs are received from both directions.

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
	• **TCP Resumed Flow**—Plain ACKs create flows if rule match permits, and these are classified as TCP Resumed Flows. This counter is incremented in the case of a TCP Resumed Flow.
UDP Errors	UDP protocol errors: • **IP data length less than minimum UDP header length (8 bytes)**—Minimum UDP header length is 8 bytes. The received IP packets contain less than 8 bytes. • **Source or destination port is zero**—UDP source or destination port is **0**. • **UDP port scan (ICMP error seen for UDP flow)**—ICMP error is received for a UDP flow. This could be a genuine UDP flow, but it is counted as an error.
ICMP Errors	ICMP protocol errors: • **IP data length less than minimum ICMP header length (8 bytes)**—ICMP header length is 8 bytes. This counter is incremented when received IP packets contain less than 8 bytes. • **ICMP error length inconsistencies**—Minimum length of an ICMP error packet is 48 bytes, and the maximum length is 576 bytes. This counter is incremented when the received ICMP error falls outside this range. • **Duplicate ping sequence number**—Received ping packet has a duplicate sequence number. • **Mismatched ping sequence number**—Received ping packet has a mismatched sequence number. • **No matching flow**—No matching existing flow was found for the ICMP error.

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
ALG errors	Accumulation of all the application-level gateway protocol (ALG) drops counted separately in the ALG context: • **BOOTP**—Bootstrap protocol errors • **DCE-RPC**—Distributed Computing Environment-Remote Procedure Call protocols errors • **DCE-RPC portmap**—Distributed Computing Environment-Remote Procedure Call protocols portmap service errors • **DNS**—Domain Name System protocol errors • **Exec**—Exec errors • **FTP**—File Transfer Protocol errors • **H323**—H.323 standards errors • **ICMP**—Internet Control Message Protocol errors • **IIOP**—Internet Inter-ORB Protocol errors • **Login**—Login errors • **NetBIOS**—NetBIOS errors • **Netshow**—NetShow errors • **Real Audio**—RealAudio errors • **RPC**—Remote Procedure Call protocol errors • **RPC portmap**—Remote Procedure Call protocol portmap service errors • **RTSP**—Real-Time Streaming Protocol errors • **Shell**—Shell errors • **SIP**—Session Initiation Protocol errors • **SNMP**—Simple Network Management Protocol errors • **SQLNet**—SQLNet errors • **TFTP**—Trivial File Transfer Protocol errors • **Traceroute**—Traceroute errors

Table 108: show services stateful-firewall statistics Output Fields *(continued)*

Field Name	Field Description
Drop Flows	• **Maximum Ingress Drop flows allowed**--Maximum number of ingress flow drops allowed. • **Maximum Egress Drop flows allowed**--Maximum number of egress flow drops allowed. • **Current Ingress Drop flows**--Current number of ingress flow drops. • **Current Egress Drop flows**--Current number of egress flow drops. • **Ingress Drop Flow limit drops count**--Number of ingress flow drops due to maximum number of ingress flow drops being exceeded. • **Egress Drop Flow limit drops count**--Number of egress flow drops due to maximum number of egress flow drops being exceeded.

Sample Output

show services stateful-firewall statistics extensive

`user@host>` **show services stateful-firewall statistics extensive**

```
Interface: ms-1/3/0
  Service set: interface-svc-set
    New flows:
      Rule Accepts: 907, Rule Discards: 0, Rule Rejects: 0
    Existing flow types packet counters:
      Accepts: 3535, Drop: 0, Rejects: 0
    Haripinning counters:
      Slow Path Hairpinned Packets: 0, Fast Path Hairpinned Packets: 0
    Drops:
      IP option: 0, TCP SYN defense: 0
      NAT ports exhausted: 0, Sessions dropped due to subscriber flow limit: 0
    Errors:
      IP: 0, TCP: 0
      UDP: 0, ICMP: 0
      Non-IP packets: 0, ALG: 0
    IP errors:
      IP packet length inconsistencies: 0
      Minimum IP header length check failures: 0
      Reassembled packet exceeds maximum IP length: 0
      Illegal source address: 0
      Illegal destination address: 0
```

```
  TTL zero errors: 0, Illegal IP protocol number (0 or 255): 0
  Land attack: 0
  Non-IPv4 packets: 0, Bad checksum: 0
  Illegal IP fragment length: 0
  IP fragment overlap: 0
  IP fragment reassembly timeout: 0
  IP fragment limit exceeded:0
  Unknown: 0
TCP errors:
  TCP header length inconsistencies: 0
  Source or destination port number is zero: 0
  Illegal sequence number and flags combination: 0
  SYN attack (multiple SYN messages seen for the same flow): 0
  First packet not a SYN message: 0
  TCP port scan (TCP handshake, RST seen from server for SYN): 0
  Bad SYN cookie response: 0
  TCP reconstructor sequence number error: 0
  TCP reconstructor retransmissions: 0
  TCP partially opened connection timeout (SYN): 0
  TCP partially opened connection timeout (SYN-ACK): 0
  TCP partially closed connection reuse: 0
  TCP 3-way error - client sent SYN+ACK: 0
  TCP 3-way error - server sent ACK: 0
  TCP 3-way error - SYN seq number retransmission mismatch: 0
  TCP 3-way error - RST seq number mismatch: 0
  TCP 3-way error - FIN received: 0
  TCP 3-way error - invalid flags (PSH, URG, ECE, CWR): 0
  TCP 3-way error - SYN recvd but no client flows: 0
  TCP 3-way error - first packet SYN+ACK: 0
  TCP 3-way error - first packet FIN+ACK: 0
  TCP 3-way error - first packet FIN: 0
  TCP 3-way error - first packet RST: 0
  TCP 3-way error - first packet ACK: 0
  TCP 3-way error - first packet invalid flags (PSH, URG, ECE, CWR): 0
  TCP Close error - no final ACK: 0
  TCP Resumed Flow: 0
UDP errors:
  IP data length less than minimum UDP header length (8 bytes): 0
  Source or destination port is zero: 0
  UDP port scan (ICMP error seen for UDP flow): 0
ICMP errors:
  IP data length less than minimum ICMP header length (8 bytes): 0
  ICMP error length inconsistencies: 0
  Duplicate ping sequence number: 0
```

```
      Mismatched ping  sequence number: 0
      No matching flow: 0
    ALG errors:
      BOOTP: 0, DCE-RPC: 0, DCE-RPC portmap: 0
      DNS: 0, Exec: 0, FTP: 0
      H323: 0, ICMP: 0, IIOP: 0
      Login: 0, NetBIOS: 0, Netshow: 0
      Real Audio: 0, RPC: 0, RPC portmap: 0
      RTSP: 0, Shell: 0, SIP: 0
      SNMP: 0, SQLNet: 0, TFTP: 0
      Traceroute: 0
    Drop Flows:
      Maximum Ingress Drop flows allowed: 20
      Maximum Egress Drop flows allowed: 20
      Current Ingress Drop flows: 0
      Current Egress Drop flows: 0
      Ingress Drop Flow limit drops count: 0
      Egress Drop Flow limit drops count: 0
```

```
**If max-drop-flows is not configured, the following is shown**
    Drop Flows:
      Maximum Ingress Drop flows allowed: Default
      Maximum Egress Drop flows allowed: Default
```

show services stateful-firewall statistics application-protocol sip

Syntax

```
show services stateful-firewall application-protocol sip
```

Release Information

Command introduced in Junos OS Release 7.4.

Description

Display stateful firewall Session Initiation Protocol (SIP) statistics.

Options

This command has no options.

Required Privilege Level

view

List of Sample Output

show services stateful-firewall statistics application-protocol-sip on page 2108

Output Fields

Table 109 on page 2106 lists the output fields for the **show services stateful-firewall statistics application-protocol-sip** command. Output fields are listed in the approximate order in which they appear.

Table 109: show services stateful-firewall statistics application-protocol-sip Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface.
Service set	Name of the service set flow.
ALG	Name of the application-layer gateway.
Active SIP call count	Number of active SIP calls.
Active SIP registration count	Number of active SIP registrations.
REGISTER	Number of new, invalid, and retransmitted register requests sent to the SIP registrar.
INVITE	Number of new, invalid, and retransmitted invite messages sent by user agent clients.
ReINVITE	Number of new, invalid, and retransmitted reinvite messages sent by user agent clients.

Table 109: show services stateful-firewall statistics application-protocol-sip Output Fields *(continued)*

Field Name	Field Description
ACK	Number of new, invalid, and retransmitted ACK messages received (in response to a SIP Call Invite message).
BYE	Number of new, invalid, and retransmitted requests to terminate SIP dialogues.
CANCEL	Number of new, invalid, and retransmitted SIP request cancellations.
SUBSCRIBE	Number of new, invalid, and retransmitted SIP requests to subscribe for event notifications.
NOTIFY	Number of new, invalid, and retransmitted event notifications in SIP dialogues.
OPTIONS	Number of new, invalid, and retransmitted requests to query SIP capabilities.
INFO	Number of new, invalid, and retransmitted requests carrying application-level information.
UPDATE	Number of new, invalid, and retransmitted SIP dialogue updates.
REFER	Number of new, invalid, and retransmitted requests to the recipient to contact a third party.
Provisional responses	Number of new, invalid, and retransmitted responses from the user agent server to indicate the progress of a SIP transaction.
OK responses to INVITEs	OK responses sent from the user agent clients to user agent servers in response to Invite messages. The server can then return an ACK message.
OK responses to non-INVITES	OK responses to SIP messages other than an Invite message.
Redirection responses	Responses from the user agent server to a user agent client requesting the client to contact a different SIP uniform resource identifier (URI).
Request failure responses	Responses that indicate a definite failure from a particular server. The client must not retry the same request without modification after receiving this response.
Server failure responses	Responses that indicate a server failure.
Global failure responses	Responses that indicate a server has definitive information about a particular user, not just the particular instance indicated in the Request URI.
Invalid responses	Responses that are invalid.

Table 109: show services stateful-firewall statistics application-protocol-sip Output Fields *(continued)*

Field Name	Field Description
Response (all) retransmits	Retransmissions of all responses.
Parser	Syntax errors, content errors, and unknown methods counted by the message parser.

Sample Output

show services stateful-firewall statistics application-protocol-sip

`user@host>` **show services stateful-firewall statistics application-protocol sip**

```
Interface: sp-0/3/0
  Service set: test_sip_777, ALG: SIP
  Active SIP call count: 0, Active SIP registration count: 1
                   New      Invalid    Retransmit
    REGISTER         2
    INVITE           1                        0
    ReINVITE         1
    ACK              1           0            0
    BYE              0           0
    CANCEL           0           0
    SUBSCRIBE        0           0
    NOTIFY           0           0
    OPTIONS          0           0
    INFO             0           0
    UPDATE           0           0
    REFER            0           0
    Provisional responses (18x): 1, OK responses to INVITEs: 2
    OK responses to non-INVITEs: 2, Redirection (3xx) responses: 0
    Request failure (4xx) responses: 0, Server failure (5xx) responses: 0
    Global failure (6xx) responses: 0, Invalid responses: 0
    Response (all) retransmits: 0
    Parser:
      Syntax errors: 0, Content errors: 0, Unknown methods: 0
  Service set: test_sip_888, ALG: SIP
  Active SIP call count: 0, Active SIP registration count: 1
                   New      Invalid    Retransmit
    REGISTER         2
    INVITE           0                        0
```

```
ReINVITE          0
ACK               0            0             0
BYE               0            0
CANCEL            0            0
SUBSCRIBE         0            0
NOTIFY            0            0
OPTIONS           0            0
INFO              0            0
UPDATE            0            0
REFER             0            0
Provisional responses (18x): 0, OK responses to INVITEs: 0
OK responses to non-INVITEs: 2, Redirection (3xx) responses: 0
Request failure (4xx) responses: 0, Server failure (5xx) responses: 0
Global failure (6xx) responses: 0, Invalid responses: 0
Response (all) retransmits: 0
Parser:
  Syntax errors: 0, Content errors: 0, Unknown methods: 0
```

show services stateful-firewall subscriber-analysis

Syntax

```
show services stateful-firewall subscriber analysis
<interface interface-name>
```

Release Information

Command introduced in Junos OS Release 11.4.

Description

Display information about the number of active subscribers on the service physical interface card (PIC).

Options

none—Display standard information about all active subscribers on the PIC.

interface *interface-name*—(Optional) Display information about a particular interface.

Required Privilege Level

view

List of Sample Output

show services stateful-firewall subscriber analysis on page 2111
show services stateful-firewall subscriber-analysis on page 2112

Output Fields

Table 110 on page 2110 lists the output fields for the **show services stateful-firewall subscriber analysis** command. Output fields are listed in the approximate order in which they appear.

Table 110: show services stateful-firewall subscriber-analysis Output Fields

Field Name	Field Description
Services PIC Name	Name of an adaptive services interface.
Total Subscribers Active	Total number of subscribers currently active on the service PIC.
Created Subscribers per Second	Rate at which subscribers are currently being created on the service PIC.
Deleted Subscribers per Second	Rate at which subscribers are currently being deleted on the service PIC.
Peak Total Subscribers Active	Highest number of subscribers that were active during the lifetime of the service PIC.

Table 110: show services stateful-firewall subscriber-analysis Output Fields *(continued)*

Field Name	Field Description
Peak Created Subscribers per Second	Highest rate at which subscribers were being created during the lifetime of the service PIC.
Peak Deleted Subscribers per Second	Highest rate at which subscribers were being deleted during the lifetime of the service PIC.
Number of Samples	The current sampling period lifetime.
Subscriber Operation: Creation	Number of sampling intervals during which a number of subscribers in the indicated range were created during the current sampling period.
Subscriber Operation: Deletion	Number of sampling intervals during which a number of subscribers in the indicated range were deleted during the current sampling period.

Sample Output

show services stateful-firewall subscriber analysis

`user@host>` **show services stateful-firewall subscriber analysis**

```
  Services PIC Name:    sp-2/0/0
Subscriber Analysis Statistics:
  Total Subscribers Active              :100000
  Created Subscribers per Second        :0
  Deleted Subscribers per Second        :0
  Peak Total Subscribers Active         :100000
  Peak Created Subscribers per Second   :2389
  Peak Deleted Subscribers per Second   :0

Subscriber Rate Data:
  Number of Samples: 55

Subscriber Rate Distribution(sec)
Subscriber Operation :Creation

    300000+           :0
    250000  - 300000  :0
    200000  - 250000  :0
    160000  - 200000  :0
```

```
    150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
     10000  -  20000   :0
      1000  -  10000   :42
         0  -   1000   :1
Subscriber Operation :Deletion
    300000+            :0
    250000  - 300000   :0
    200000  - 250000   :0
    160000  - 200000   :0
    150000  - 160000   :0
     50000  - 150000   :0
     40000  -  50000   :0
     30000  -  40000   :0
     20000  -  30000   :0
```

show services stateful-firewall subscriber-analysis

`user@host>` **show services stateful-firewall subscriber analysis**

```
  Services PIC Name:    sp-2/0/0

Subscriber Analysis Statistics:

  Total Subscribers Active               :23547
  Created Subscribers per Second         :2389
  Deleted Subscribers per Second         :0
  Peak Total Subscribers Active          :23547
  Peak Created Subscribers per Second    :2389
  Peak Deleted Subscribers per Second    :0

Subscriber Rate Data:
  Number of Samples: 16

 Subscriber Rate Distribution(sec)

 Subscriber Operation :Creation

    300000+            :0
    250000  - 300000   :0
    200000  - 250000   :0
```

```
   160000  - 200000   :0
   150000  - 160000   :0
    50000  - 150000   :0
    40000  -  50000   :0
    30000  -  40000   :0
    20000  -  30000   :0
    10000  -  20000   :0
     1000  -  10000   :9
        0  -   1000   :1


Subscriber Operation :Deletion

   300000+            :0
   250000  - 300000   :0
   200000  - 250000   :0
   160000  - 200000   :0
   150000  - 160000   :0
    50000  - 150000   :0
    40000  -  50000   :0
    30000  -  40000   :0
    20000  -  30000   :0
    10000  -  20000   :0
     1000  -  10000   :0
        0  -   1000   :0
```

show services subscriber analysis

Syntax

```
show services subscriber analysis
<interface interface-name>
```

Release Information

Statement introduced in Junos OS Release 17.1 on MX Series MS-MPC.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display information about the number of active subscribers on the services PIC.

Options

none—Display standard information about all active subscribers on the PIC.

interface *interface-name*—(Optional) Display information about the specified interface.

Required Privilege Level

view

List of Sample Output

show services subscriber analysis interface on page 2115

Output Fields

Table 110 on page 2110 lists the output fields for the **show services subscriber analysis** command. Output fields are listed in the approximate order in which they appear.

Table 111: show services subscriber analysis Output Fields

Field Name	Field Description
Services PIC Name	Name of an adaptive services interface.
Subscriber Analysis Statistics:	
Total Subscribers Active	Total number of subscribers currently active on the service PIC.
Created Subscribers per Second	Rate at which subscribers are currently being created on the service PIC.
Deleted Subscribers per Second	Rate at which subscribers are currently being deleted on the service PIC.

Table 111: show services subscriber analysis Output Fields *(continued)*

Field Name	Field Description
Peak Total Subscribers Active	Highest number of subscribers that were active during the lifetime of the service PIC.
Peak Created Subscribers per Second	Highest rate at which subscribers were being created during the lifetime of the service PIC.
Peak Deleted Subscribers per Second	Highest rate at which subscribers were being deleted during the lifetime of the service PIC.
Number of Samples	Number of samples during the current sampling period lifetime.
Subscriber Rate Distribution(sec)	
Subscriber Operation: Creation	Number of sampling intervals during which a number of subscribers in the indicated range were created during the current sampling period.
Subscriber Operation: Deletion	Number of sampling intervals during which a number of subscribers in the indicated range were deleted during the current sampling period.

Sample Output

show services subscriber analysis interface

`user@host>` **show services subscriber analysis interface ms-5/1/0**

```
Services PIC Name:    ms-5/1/0

Subscriber Analysis Statistics:

  Total Subscribers Active              :0
  Created Subscribers per Second        :0
  Deleted Subscribers per Second        :0
  Peak Total Subscribers Active         :0
  Peak Created Subscribers per Second   :0
  Peak Deleted Subscribers per Second   :0

Subscriber Rate Data:
  Number of Samples: 3916
```

```
Subscriber Rate Distribution(sec)

Subscriber Operation :Creation

   400000+            :0
   350001  - 400000   :0
   300001  - 350000   :0
   250001  - 300000   :0
   200001  - 250000   :0
   160001  - 200000   :0
   150001  - 160000   :0
    50001  - 150000   :0
    40001  -  50000   :0
    30001  -  40000   :0
    20001  -  30000   :0
    10001  -  20000   :0
     1001  -  10000   :0
        1  -   1000   :0
                  0   :3916


Subscriber Operation :Deletion

   400000+            :0
   350001  - 400000   :0
   300001  - 350000   :0
   250001  - 300000   :0
   200001  - 250000   :0
   160001  - 200000   :0
   150001  - 160000   :0
    50001  - 150000   :0
    40001  -  50000   :0
    30001  -  40000   :0
    20001  -  30000   :0
    10001  -  20000   :0
     1001  -  10000   :0
        1  -   1000   :0
                  0   :3916
```

show services tcp-log connections

Syntax

```
show services tcp-log connections interface interface-name
```

Release Information

Command introduced in Junos OS Release 19.1 for MX Series.

Description

Display the TCP connection status for the specified interface.

Required Privilege Level

view

Output Fields

Table 112 on page 2117 lists the output fields for the **show services sessions tcp-log connections interface *interface-name*** command. Output fields are listed in the approximate order in which they appear.

Table 112: show services sessions tcp-log connections interface Output Fields

Field Name	Field Description
Session Id	TCP connection status including the state, source IP address, destination IP address, and destination port.

Sample Output

```
user@router>show services tcp-log connections interface interface-name
```

```
user@router>show services tcp-log connections interface interface-name
```

```
Session Id: 1744830467 State: Established
    1.1.1.1 -> 40.0.0.2 : 10214
```

show services traffic-load-balance statistics

Syntax

```
show services traffic-load-balance statistics
<extensive>
<group group-name>
<instance instance-name>
<num-instances number>
<real-service real-service-name>
<summary>
<virtual-service virtual-service-name>
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
num-instances option added in Junos OS Release 16.1R6 and 18.2R1 on MX Series.
Support added in Junos OS 19.3R2 for Next Gen Services with the MX-SPC3 services card.

Description

The basic form of the command displays the list of real servers associated with this group and traffic statistics, including packet count and byte count

Options

none—Display information about the load-balancing statistics in brief.

extensive—(Optional) Display extensive information about the traffic load-balancing statistics.

group *group-name*—(Optional) Display load-balancing statistics for a specified group of load-balancer servers.

instance *instance-name*—(Optional) Display load-balancing statistics for a specific traffic load balancer (TLB) instance.

num-instances *number*—(Optional) Display load-balancing statistics for a specified number of TLB instances.

real-service *real-service-name*—(Optional) Display load-balancing statistics for a specified load balancer serve.

summary—(Optional) Display summary information about the traffic load-balancing statistics.

virtual-service *virtual-service-name*—(Optional) Display load-balancing statistics for a specified TLB virtual service.

Required Privilege Level

view

List of Sample Output

show services traffic-load-balance statistics on page 2126
show services traffic-load-balance statistics extensive on page 2127
show services traffic-load-balance statistics summary on page 2131

Output Fields

Table 113 on page 2119 lists the output fields for the **show services traffic-load-balance statistics** command. Output fields are listed in the approximate order in which they appear.

Table 113: show services traffic-load-balance statistics Output Fields

Field Name	Field Description	Level of Output
Traffic load balance instance name	Name of the traffic load balancer (TLB) instance that contains the load-distribution-related configuration settings.	All levels
Multi services interface name	Name of the services interface used for the TLB instance to provide one-to-one redundancy for server health monitoring. For MS-MPC services card, this is the name of the aggregated multiservices (AMS) interface or “ms-slot/pic/port”. For Next Gen Services and the MX-SPC3 services card, this is the name of the VMS interface or “vms-slot/pic/port”.	All levels
Interface state	Inter-process communications (IPC) status between the TLB daemon (traffic-dird) and the health checking daemon (net-monitord). • **DOWN** • **UP**	All levels
Interface type	Logical interface type.	All levels
Route hold timer	Time that the programmed VIP routes are kept intact after connectivity between traffic-dird and net-monitord daemons is lost. If connectivity is not reestablished within this time, all the VIP routes are withdrawn.	All levels
Traffic load balance virtual svc name	Name of the virtual service for the TLB instance. The virtual service provides an address that is associated with the group of servers to which traffic is directed.	none **extensive**
Virtual service	Name of the virtual service for the TLB instance. The virtual service provides an address that is associated with the group of servers to which traffic is directed.	**summary**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Routing instance name	Name of the routing instance used for the virtual service.	none **extensive**
IP address	IP address of the virtual service.	none **extensive**
Address	IP address of the virtual service.	**summary**
Sts	Operational state of the virtual service.	**summary**
Packet Sent	Number of packets originating from the clients that the TLB instance virtual service processes for load balancing to next-hop servers.	**summary**
Byte Sent	Number of bytes originating from the clients that the TLB instance virtual service processes for load balancing to next-hop servers.	**summary**
Packet Recv	Number of packets returning from the next-hop servers that the TLB instance virtual service processes and forwards to the clients.	**summary**
Byte Recv	Number of bytes returning from the next-hop servers that the TLB instance virtual service processes and forwards to the clients.	**summary**
Virtual service mode	Virtual service processing mode. • **layer-2-direct-server-return**—Virtual service is in transparent mode with Layer 2 direct server return (DSR) • **direct-server-return**—Virtual service is in transparent mode with Layer 3 direct server return (DSR) • **translated**—Virtual service is in translated mode.	none **extensive**
Traffic load balance group name	Server group name used for the virtual service.	none **extensive**
Health check interface subunit	Number of the subunit of the multiservice interface used for health checking.	none **extensive**
Traffic load balance group down count	Number of times the status of the TLB server group was down.	**extensive**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Protocol	Virtual service protocol, either tcp or udp. In translated mode, packets destined to the virtual service IP address+port number+protocol are load balanced and then replaced by the real service IP address and server listening port number.	none **extensive**
Port Number	Virtual service port number. In translated mode, packets destined to the virtual service IP address+port number+protocol are load balanced and then replaced by the real service IP address and server listening port number.	none **extensive**
Server Listening Port Number	Real service port number that replaces the virtual service port number. In translated mode, packets destined to the virtual service IP address+port number+protocol are load balanced and then replaced by the real service IP address and server listening port number.	none **extensive**
Demux Nexthop index	Index number of the demultiplexing next hop for the virtual service. Index number is unique for a VIP, routing-instance, and protocol combination. The demultiplexing next hop is responsible for port-based demultiplexing of traffic to the load-balancing next hop for session distribution.	none **extensive**
DFW client-id	Client connection identifier assigned to the TLB daemon (traffic-dird) by the firewall daemon (dfwd) when the daemons are successfully connected.	**extensive**
Traffic load balance group warmup time	Time, in seconds, that passes after the traffic-dird daemon comes up until the traffic-dird programs the distribution table on the Packet Forwarding Engine.	**extensive**
Traffic load balance group auto-rejoin	Indicates whether the option that allows a server to rejoin the group automatically when it comes up is enabled or not.	**extensive**
Route metric	Routing metric assigned to the virtual service. A lower metric makes a route more preferred.	**extensive**
Virtual service down count	Number of times the status of the virtual service was down.	**extensive**
Traffic load balance hash method	Hash key parameter used for load balancing. Hash keys supported in the ingress direction are protocol, source IP address, and destination IP address.	**extensive**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Nexthop index	Index number of the next-hop for the virtual service. A group of servers function as a pool for next-hop session distribution.	none **extensive**
Up time	Period of time for which the virtual service is up, in the format *number-of-days hh:mm:ss*.	none **extensive**
Real Server Up count	Starting in Junos OS Release 16.1R6 and 18.2R1, number of real servers that are up for the specified virtual service or server group.	none
Real Server Down count	Starting in Junos OS Release 16.1R6 and 18.2R1, number of real servers that are down for the specified virtual service or server group.	none
Total packet sent count	Number of packets originating from the clients that the TLB instance virtual service processes for load balancing to next-hop servers.	none **extensive**
Total byte sent count	Number of bytes originating from the clients that the TLB instance virtual service processes for load balancing to next-hop servers.	none **extensive**
Total packet received count	Number of packets returning from the next-hop servers that the TLB instance virtual service processes and forwards to the clients.	none **extensive**
Total byte received count	Number of bytes returning from the next-hop servers that the TLB instance virtual service processes and forwards to the clients.	none **extensive**
Network monitoring profile count	Number of network monitoring profiles that are used to monitor the health of servers used in TLB session distribution.	**extensive**
Active real service count	Number of real services that are functional and active.	**extensive**
Total real service count	Total number of real services in different states.	**extensive**
Network monitoring profile index	Unique index number associated with the network monitoring profile. Network monitoring profiles are used to monitor the health of servers used in TLB session distribution.	**extensive**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Network monitoring profile name	Name configured for the network monitoring profile.	**extensive**
Probe type	Probe type used to examine the health of servers. TLB supports ICMP, TCP, and HTTP health check probes to monitor the health of servers in a group.	**extensive**
Probe interval	Frequency, in number of seconds, at which health check probes are sent.	**extensive**
Probe failure retry count	Number of failure retries, after which the real service is tagged as down.	**extensive**
Probe recovery retry count	Number of successful retries after which the real service is tagged as up.	**extensive**
Real service	Name of the TLB server (also referred to as real service). The name is the identifier for a server to which sessions can be distributed using the server distribution table in conjunction with the session distribution API.	none
Address	IP address of the configured real service.	none
Sts	Operational state of the TLB server.	none
Packet Sent	Number of packets originating from the clients that the TLB instance virtual service sends to the real service.	none
Byte Sent	Number of bytes originating from the clients that the TLB instance virtual service sends to the real service next-hop server.	none
Packet Recv	Number of packets returning from the real service next-hop server that the TLB instance virtual service processes and forwards to the clients.	none
Byte Recv	Number of bytes returning from the real service next-hop server that the TLB instance virtual service processes and forwards to the clients.	none
Traffic load balance real svc name	Name of the real service used for traffic load-balancing.	**extensive**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Routing instance name	Name of the routing instance on which the real service is configured.	**extensive**
IP address	IP address of the configured real service.	**extensive**
Traffic load balance group name	Name of the server group for real service.	**extensive**
Admin state	Administrative state of the real service, such as **Up** or **Down**.	**extensive**
Oper state	Operational state of the real service, such as **Up** or **Down**.	**extensive**
Network monitoring probe up count	Number of probes for which the status of the server whose health is checked is observed to be up. If a server group is configured for dual health check, a real service is declared to be UP only if both health-check probes are simultaneously UP; otherwise a real service declared to be DOWN.	**extensive**
Network monitoring probe down count	Number of probes for which the status of the server whose health is checked is observed to be down.	**extensive**
Total rejoin event count	Number of events that caused a server that was previously down and later operational to rejoin a group of real services for load-balancing.	**extensive**
Total up event count	Number of TLB events that identified a virtual service or real service to be up.	**extensive**
Total down event count	Number of TLB events that identified a virtual service or real service to be down.	**extensive**
Real Service packet sent count	Number of packets originating from the clients that the TLB instance virtual service sends to the real service.	**extensive**
Real Service byte sent count	Number of bytes originating from the clients that the TLB instance virtual service sends to the real service next-hop server.	**extensive**

Table 113: show services traffic-load-balance statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
Real Service packet received count	Number of packets returning from the real service next-hop server that the TLB instance virtual service processes and forwards to the clients.	**extensive**
Real Service byte received count	Number of bytes returning from the real service next-hop server that the TLB instance virtual service processes and forwards to the clients.	**extensive**
Total probe sent	Number of health-monitoring probes sent from the TLB health check daemon.	**extensive**
Total probe success	Number of health-monitoring probes sent from the TLB health check daemon that were successful.	**extensive**
Total probe fail	Number of health-monitoring probes attempted to be sent from the TLB health check daemon that failed.	**extensive**
Total probe sent fail	Number of health-monitoring probes attempted to be sent from the TLB health check daemon that were unsuccessfully initiated.	**extensive**
Probe state	Status of the health-check probe, such as **Up** or **Down**.	**extensive**
Probe sent	Number of health-check probe requests transmitted from the TLB health check daemon.	**extensive**
Probe success	Number of successful health-check probe requests transmitted from the TLB health check daemon.	**extensive**
Probe fail	Number of failed health-check probe requests transmitted from the TLB health check daemon.	**extensive**
Probe sent failed	Number of times the TLB health check daemon was unable to initiate transmission of a extensive health-check probe.	**extensive**
Probe consecutive success	Number of health-check probe requests transmitted from the TLB health check daemon that were consecutively successful.	**extensive**
Probe consecutive fail	Number of health-check probe requests transmitted from the TLB health check daemon that failed for two successive times.	**extensive**

Sample Output

show services traffic-load-balance statistics

`user@host>` **show services traffic-load-balance statistics**

```
Traffic load balance instance name    :  lb1
Multi services interface name         :  ms-3/0/0
Interface state                       :  UP
Interface type                        :  Multi services
Route hold timer                      :  180
Active real service count             :  0
Total real service count              : 100
Traffic load balance virtual svc name :  v1
IP address                            :  0.0.0.0
Virtual service mode                  :  Layer-2 based Direct Server Return mode
Routing instance name                 :  internal-client-vrf
Traffic load balance group name       :  g1
Health check interface subunit        :  40
Demux Nexthop index                   :  N/A
Nexthop index                         :  840
Up time                               :  2d 19:09
Real Server Up count                  :  1
Real Server Down count                :  1
Total packet sent count               :  0
Total byte sent count                 :  0
Real service   Address       Sts  Packet Sent Byte Sent Packet Recv Byte Recv
r11            203.0.113.11    UP   0           0         0           0
r10            203.0.113.10    UP   0           0         0           0


Traffic load balance virtual svc name :  v2
IP address                            :  192.0.2.11
Virtual service mode                  :  Translate mode
Routing instance name                 :  msp-tproxy-forwarding1
Traffic load balance group name       :  g2
Health check interface subunit        :  50
Protocol                              :  tcp
Port number                           :  8080
Server Listening Port Number          :  8084
Demux Nexthop index                   :  536
Nexthop index                         :  539
Up time                               :  2d 19:06
Total packet sent count               :  0
Total byte sent count                 :  0
```

```
Total packet received count           :  0
Total byte received count             :  0
Real service     Address      Sts  Packet Sent  Byte Sent  Packet Recv  Byte Recv
r12              203.0.113.12   UP   0            0          0            0

r13              203.0.113.13   UP   0            0          0            0
```

show services traffic-load-balance statistics extensive

user@host> **show services traffic-load-balance statistics extensive**

```
Traffic Load Balance General Information
    DFW client-id                     :  39

Traffic load balance instance name    :  lb1
Multi services interface name         :  ms-3/0/0
Interface state                       :  UP
Interface type                        :  Multi services
Route hold timer                      :  180
Active real service count             :  0
Total real service count              : 100
Traffic load balance virtual svc name :  v1
IP address                            :  0.0.0.0
Virtual service mode                  :  Layer-2 based Direct Server Return mode
Routing instance name                 :  internal-client-vrf
Traffic load balance group name       :  g1
Traffic load balance group warmup time:  15
Traffic load balance group auto-rejoin:  TRUE
Health check interface subunit        :  40
Traffic load balance group down count :  1
Route metric                          :  1
Virtual service down count            :  1
Traffic load balance hash method      :  source
Network monitoring profile count      :  1
Active real service count             :  2
Total real service count              :  2
Demux Nexthop index                   :  N/A
Nexthop index                         :  840
Up time                               :  2d 19:09
Total packet sent count               :  0
Total byte sent count                 :  0
Total packet received count           :  0
Total byte received count             :  0
```

```
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe interval                        :  5
Probe failure retry count             :  5
Probe recovery retry count            :  3

Traffic load balance real svc name    :  r11
Routing instance name                 :  server-vrf10
IP address                            :  203.0.113.11
Traffic load balance group name       :  g1
Admin state                           :  UP
Oper state                            :  UP
Network monitoring probe up count     :  1
Network monitoring probe down count   :  0
Total rejoin event count              :  0
Total up event count                  :  1
Total down event count                :  0
Real Service packet sent count                :  0
Real Service byte sent count                  :  0
Total probe sent                      :  47939
Total probe success                   :  47918
Total probe fail                      :  21
Total probe sent failed               :  0
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe state                           :  UP
Probe sent                            :  47939
Probe success                         :  47918
Probe fail                            :  21
Probe sent failed                     :  0
Probe consecutive success             :  10090
Probe consecutive fail                :  0

Traffic load balance real svc name    :  r10
Routing instance name                 :  server-vrf10
IP address                            :  203.0.113.10
Traffic load balance group name       :  g1
Admin state                           :  UP
Oper state                            :  UP
Network monitoring probe up count     :  1
Network monitoring probe down count   :  0
Total rejoin event count              :  0
```

```
Total up event count                  :  1
Total down event count                :  0
Real Service packet sent count                :  0
Real Service byte sent count                  :  0
Total probe sent                      :  47939
Total probe success                   :  47917
Total probe fail                      :  22
Total probe sent failed               :  0
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe state                           :  UP
Probe sent                            :  47939
Probe success                         :  47917
Probe fail                            :  22
Probe sent failed                     :  0
Probe consecutive success             :  10090
Probe consecutive fail                :  0

Traffic load balance virtual svc name :  v2
IP address                            :  192.0.2.11
Virtual service mode                  :  Translate mode
Routing instance name                 :  msp-tproxy-forwarding1
Traffic load balance group name       :  g2
Traffic load balance group warmup time:  15
Traffic load balance group auto-rejoin:  TRUE
Health check interface subunit        :  50
Traffic load balance group down count :  1
Protocol                              :  tcp
Port number                           :  8080
Server Listening Port Number          :  8084
Route metric                          :  1
Virtual service down count            :  1
Traffic load balance hash method      :  source-destination
Network monitoring profile count      :  1
Active real service count             :  2
Total real service count              :  2
Demux Nexthop index                   :  536
Nexthop index                         :  539
Up time                               :  2d 19:07
Total packet sent count               :  0
Total byte sent count                 :  0
Total packet received count           :  0
Total byte received count             :  0
```

```
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe interval                        :  5
Probe failure retry count             :  5
Probe recovery retry count            :  3

Traffic load balance real svc name    :  r12
Routing instance name                 :  server-vrf10
IP address                            :  203.0.113.12
Traffic load balance group name       :  g2
Admin state                           :  UP
Oper state                            :  UP
Network monitoring probe up count     :  1
Network monitoring probe down count   :  0
Total rejoin event count              :  0
Total up event count                  :  1
Total down event count                :  0
Real Service packet sent count        :  0
Real Service byte sent count          :  0
Real Service packet received count    :  0
Real Service byte received count      :  0
Total probe sent                      :  47939
Total probe success                   :  47916
Total probe fail                      :  23
Total probe sent failed               :  0
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe state                           :  UP
Probe sent                            :  47939
Probe success                         :  47916
Probe fail                            :  23
Probe sent failed                     :  0
Probe consecutive success             :  10089
Probe consecutive fail                :  0

Traffic load balance real svc name    :  r13
Routing instance name                 :  server-vrf10
IP address                            :  203.0.113.13
Traffic load balance group name       :  g2
Admin state                           :  UP
Oper state                            :  UP
Network monitoring probe up count     :  1
```

```
Network monitoring probe down count   :  0
Total rejoin event count              :  0
Total up event count                  :  1
Total down event count                :  0
Real Service packet sent count               :  0
Real Service byte sent count                 :  0
Real Service packet received count           :  0
Real Service byte received count             :  0
Total probe sent                      :  47939
Total probe success                   :  47910
Total probe fail                      :  29
Total probe sent failed               :  0
Network monitoring profile index      :  1
Network monitoring profile name       :  prof1
Probe type                            :  ICMP
Probe state                           :  UP
Probe sent                            :  47939
Probe success                         :  47910
Probe fail                            :  29
Probe sent failed                     :  0
Probe consecutive success             :  6283
Probe consecutive fail                :  0
```

show services traffic-load-balance statistics summary

`user@host>` **show services traffic-load-balance statistics summary**

```
Traffic load balance instance name    :  tlb_sdg
Multi services interface name         :  ms-8/3/0
Interface state                       :  UP
Interface type                        :  Multi services
Route hold timer                      :  180
Active real service count             :  0
Total real service count              : 100
Virtual service     Address       Sts Packet Sent Byte Sent   Packet Recv Byte
Recv
DNS-VIP1-TCP       198.51.100.1   Up  13182260    709736171   11951566    732469940

DNS-VIP1-UDP       198.51.100.1   Up  2683203     163675383   2683101     262943898

HTTP-80-ADDRESS-VIP 203.0.113.156  Up  363080548   25152313876 282072340
280409712450
HTTP-8080-ADDR-VIP  203.0.113.157  Up  363198700   25318638843 282030640
280388777065
```

```
Secure-Ent-443-VIP  203.0.113.158  Up  30561467    3012763619  28007583
3992807922
Simple-Ent-80-VIP   203.0.113.159  Up  155857682   11558785554 89649255
79217609518

Traffic load balance instance name    :  tlb_sdg_v6
Multi services interface name         :  ms-8/3/0
Interface state                       :  UP
Interface type                        :  Multi services
Route hold timer                      :  180
Virtual service  Address           Sts Packet Sent Byte Sent   Packet Recv Byte
Recv
DNS-VIP1-TCP-V6  2001:db8:a::300     Up  25118146    1829085032  24172053
2088425092
DNS-VIP1-UDP-V6  2001:db8:a::300     Up  1318497     108116747   1319249
386274267
HTTP-80-ADDR-VIP-V6 2001:db8:a::100  Up  368696950   33051271152 282178604
287789935055
HTTP-8080-ADD-VIP-V6 2001:db8:a::100 Up  368797597   33217998028 281989122
287768684085
Sec-Ent-443-VIP-V6 2001:db8:a::200   Up  0662649     3622545250  28080924
4531356641
```

show services url-filter dns-resolution profile

Syntax

```
show services url-filter dns-resolution profile profile-name <template template-name>
<fpc-slot fpc-slot pic-slot pic-slot>
```

Release Information

Command introduced in Junos OS Release 17.2.

Description

Display URL filter domain name system (DNS) resolution information.

URL filtering resolves the blocklisted domains. The total number of domains are divided into chunks of 50 domains per chunk. The **filter term** in the command output is the name of a chunk.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **show services url-filter dns-resolution profile** command is deprecated and has been replaced by the **show services web-filter dns-resolution profile** command.

Options

fpc-slot *fpc-slot* pic-slot *pic-slot*—(Optional) Specify the FPC and PIC for which you want URL filter information displayed.

profile *profile-name*—Specify the profile for which you want URL filter information displayed.

template *template-name*—(Optional) Specify the template for which you want URL filter information displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

- show services url-filter dns-resolution-statistics profile template | 2137
- show services url-filter statistics profile template | 2143
- Configuring URL Filtering | 55

List of Sample Output

show services url-filter dns-resolution profile on page 2134

Output Fields

Table 114 on page 2134 lists the output fields for the **show services url-filter dns-resolution profile** command. Output fields are listed in the approximate order in which they appear.

Table 114: show services url-filter dns-resolution profile Output Fields

Field Name	Field Description
Profile	Name of profile.
Template	Name of template.
Filter Term	Name of the domains chunk. All domains are divided into chunks of 50 domains per chunk.
IPv4 Address Count	The number of IPv4 addresses resolved for all domains under the filter term.
IPv6 Address Count	The number of IPv6 addresses resolved for all domains under the filter term.
Domain Name	Name of domain.
IPv4 Records	Listing of IPv4 addresses.
IPv6 Records	Listing of IPv6 addresses.

Sample Output

show services url-filter dns-resolution profile

`user@host>` **show services url-filter dns-resolution profile p1**

```
URL filtering DNS resolution:
Profile: p1
Template: t1

 1). Filter Term: URLF_t1_0004

      IPv4 Address Count: 20
      IPv6 Address Count: 20

    1 ). Domain Name: www.facebook.com
```

```
        IPv4 Records:
           31.13.77.36
           31.13.76.68

        IPv6 Records:
           2a03:2880:f122:83:face:b00c:0:25de
           2a03:2880:f111:83:face:b00c:0:25de

2 ). Domain Name: www.youtube.com

        IPv4 Records:
           216.58.193.78
           216.58.194.206

        IPv6 Records:
           2607:f8b0:400a:800::200e
           2607:f8b0:4005:809::200e

3 ). Domain Name: www.netflix.com

        IPv4 Records:
           50.112.200.248
           52.10.96.2
           52.25.242.211
           52.39.87.182
           52.38.44.92
           52.36.125.176
           52.40.2.42
           52.42.184.64
           52.5.80.199
           52.206.203.18
           52.5.231.14
           52.21.94.89
           52.71.118.87
           52.201.133.109
           52.71.122.233
           52.203.136.33

        IPv6 Records:
           2620:108:700f::342a:b840
           2620:108:700f::3644:fc64
           2620:108:700f::3459:2ce1
           2620:108:700f::3459:c025
```

```
2620:108:700f::3459:f556
2620:108:700f::3459:c5c5
2620:108:700f::3644:c2a0
2620:108:700f::342a:df11
2406:da00:ff00::3404:d29c
2406:da00:ff00::3415:a86e
2406:da00:ff00::3415:fda4
2406:da00:ff00::3414:91d2
2406:da00:ff00::3403:73dd
2406:da00:ff00::22c7:d016
2406:da00:ff00::3400:290b
2406:da00:ff00::3213:c65f
```

show services url-filter dns-resolution-statistics profile template

Syntax

```
show services url-filter dns-resolution-statistics profile profile-name template template-name
(extensive | summary)
```

Release Information

Command introduced in Junos Os Release 17.2.

Description

Display URL filter domain name system (DNS) resolution statistics.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **show services url-filter dns-resolution-statistics profile template** command is deprecated and has been replaced by the **show services web-filter dns-resolution-statistics profile template** command.

Options

(extensive | summary)—Specify the level of detail of information you want displayed.

profile *profile-name*—Specify the profile for which you want URL filter information displayed.

template *template-name*—Specify the template for which you want URL filter information displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

- show services url-filter dns-resolution profile | 2133
- show services url-filter statistics profile template | 2143
- Configuring URL Filtering | 55

List of Sample Output

show services url-filter dns-resolution-statistics profile template summary on page 2139
show services url-filter dns-resolution-statistics profile template extensive on page 2140

Output Fields

Table 115 on page 2138 lists the output fields for the **show services url-filter dns-resolution-statistics profile template** command. Output fields are listed in the approximate order in which they appear.

Table 115: show services url-filter dns-resolution-statistics profile template Output Fields

Field Name	Field Description	Level of Detail
Profile	Name of profile.	all
Template	Name of template.	all
DNS start time	Start time of the DNS resolution.	**summary**
Next DNS start time	Start time of the next DNS resolution.	**summary**
Number of resolved A addresses	Number of resolved IPv4 addresses.	**summary**
Number of resolved AAAA addresses	Number of resolved IPv6 addresses.	**summary**
Number of unresolved A addresses	Number of unresolved IPv4 addresses.	**summary**
Number of unresolved AAAA addresses	Number of unresolved IPv6 addresses.	**summary**
Number of resolved A domains	Number of resolved IPv4 domains.	**summary**
Number of resolved AAAA domains	Number of resolved IPv6 domains.	**summary**
Number of unresolved A domains	Number of unresolved IPv4 domains.	**summary**
Number of unresolved AAAA domains	Number of unresolved IPv6 domains.	**summary**
Number of requests sent	Number of DNS requests sent.	**summary**
Number of responses received	Number of DNS responses received.	**summary**
Domain Name	Name of domain.	**extensive**

Table 115: show services url-filter dns-resolution-statistics profile template Output Fields *(continued)*

Field Name	Field Description	Level of Detail
IPv4 Address information	IPv4 address information includes the following fields: • **DNS server IP**—IPv4 address of DNS server. • **Req Sent**—Number of DNS requests sent. • **Resp Received**—Number of DNS responses received. • **DNS retries**—Number of times no DNS response was received and so retried.	**extensive**
IPv6 Address information	IPv6 address information includes the following fields: • **DNS server IP**—IPv6 address of DNS server. • **Req Sent**—Number of DNS requests sent. • **Resp Received**—Number of DNS responses received. • **DNS retries**—Number of times no DNS response was received and so retried.	**extensive**

Sample Output

show services url-filter dns-resolution-statistics profile template summary

`user@host>` **show services url-filter dns-resolution-statistics profile1 template t1 summary**

```
URL filtering DNS resolution statistics:
Profile: p1
Template: t1

     DNS start time                     : May 01 16:40:24 PDT
     Next DNS start time                : May 01 17:40:24 PDT
     Number of resolved A domains       : 114
```

```
     Number of resolved AAAA domains     : 114
     Number of unresolved A domains      : 0
     Number of unresolved AAAA domains   : 0
     Number of requests sent             : 246
     Number of responses received        : 228
```

show services url-filter dns-resolution-statistics profile template extensive

`user@host>` **show services url-filter dns-resolution-statistics profile p1 template t1 extensive**

```
URL filtering DNS resolution statistics:
Profile: p1
Template: t1

     1) Domain Name:    www.facebook.com

         IPv4 Address information:
              DNS server IP     8.8.8.8
              Req Sent          20
              Resp Received     20
              DNS retries       0

         IPv4 Address information:
              DNS server IP     172.29.131.60
              Req Sent          21
              Resp Received     20
              DNS retries       0

         IPv6 Address information:
              DNS server IP     8.8.8.8
              Req Sent          25
              Resp Received     20
              DNS retries       0

         IPv6 Address information:
              DNS server IP     172.29.131.60
              Req Sent          24
              Resp Received     20
              DNS retries       0
     2) Domain Name:    www.youtube.com

         IPv4 Address information:
              DNS server IP     8.8.8.8
              Req Sent          21
```

```
            Resp Received     20
            DNS retries       0

        IPv4 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0
    3) Domain Name:    www.netflix.com

        IPv4 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv4 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
```

```
                Resp Received     20
                DNS retries       0
```

show services url-filter statistics profile template

Syntax

```
show services url-filter statistics profile profile-name template template-name
<fpc-slot fpc-slot pic-slot pic-slot>
```

Release Information

Command introduced in Junos Os Release 17.2.

Description

Display URL filter statistics.

> **NOTE:** Starting in Junos OS Release 18.3R1, the **show services url-filter statistics profile template** command is deprecated and has been replaced by the **show services web-filter statistics profile** command.

Required Privilege Level

view

RELATED DOCUMENTATION

- show services url-filter dns-resolution profile | 2133
- show services url-filter dns-resolution-statistics profile template | 2137
- Configuring URL Filtering | 55

List of Sample Output

show services url-filter statistics profile template on page 2144

Output Fields

Table 116 on page 2143 lists the output fields for the **show services url-filter statistics profile template** command. Output fields are listed in the approximate order in which they appear.

Table 116: show services url-filter statistics profile template Output Fields

Field Name	Field Description
Accept	Action counters for accepted packets.
Custom page	Action counters for custom page sent to recipient.

Table 116: show services url-filter statistics profile template Output Fields *(continued)*

Field Name	Field Description
Http scode	Action counters for HTTP status code response.
Redirect url	Action counters for redirect URL response.
TCP reset	Action counters for TCP reset. Connection is closed.
Bypass session count	Number of sessions not blocked by URL filtering because the match criteria was not met.
IPV4 Disable IP Blocking	Action counters for IPv4 packets that were accepted because filtering is disabled for HTTP traffic that contains an embedded IP address belonging to a blocklisted domain name in the URL filter database.
IPV6 Disable IP Blocking	Action counters for IPv6 packets that were accepted because filtering is disabled for HTTP traffic that contains an embedded IP address belonging to a blocklisted domain name in the URL filter database.
session count	The session of activity that a user with a unique IP address spends on a website during a specified period of time. A session, in this case, would be the packets going to the service PIC from the Packet Forwarding Engine and then back to the service PIC.
uplink packet count	Number of packets going from the Packet Forwarding Engine to the service PIC.
uplink bytes	Number of bytes passing uplink.
downlink packet count	Number of packets going from the service PIC to the service Packet Forwarding Engine.
downlink bytes	Number of bytes passing downlink.

Sample Output

show services url-filter statistics profile template

`user@host>` **show services url-filter statistics profile p1 template t1**

```
URL filtering action counters:
```

```
Accept session count                : 0
Accept uplink packet count          : 0
Accept uplink bytes                 : 0
Accept downlink packet count        : 0
Accept downlink bytes               : 0

Custom page session count           : 0
Custom page uplink packet count     : 0
Custom page uplink bytes            : 0
Custom page downlink packet count   : 0
Custom page downlink bytes          : 0

Http scode session count            : 0
Http scode uplink packet count      : 0
Http scode uplink bytes             : 0
Http scode dowlink packet count     : 0
Http scode downlink bytes           : 0

Redirect url session count          : 0
Redirect url uplink packet count    : 0
Redirect url uplink bytes           : 0
Redirect url downlink packet count  : 0
Redirect url downlink bytes         : 0

Tcp reset session count             : 0
Tcp reset uplink packet count       : 0
Tcp reset uplink bytes              : 0
Tcp reset downlink packet count     : 0
Tcp reset downlink bytes            : 0

Bypass session count                : 0

IPV4 Disable IP Blocking Sessions          : 0
IPV4 Disable IP Blocking uplink packets    : 0
IPV4 Disable IP Blocking uplink bytes      : 0
IPV4 Disable IP Blocking downlink packets  : 0
IPV4 Disable IP Blocking downlink bytes    : 0

IPV6 Disable IP Blocking Sessions          : 0
IPV6 Disable IP Blocking uplink packets    : 0
IPV6 Disable IP Blocking uplink bytes      : 0
IPV6 Disable IP Blocking downlink packets  : 0
```

```
IPV6 Disable IP Blocking downlink bytes    : 0
```

show services web-filter dns-resolution profile

Syntax

```
show services web-filter dns-resolution profile profile-name <template template-name>
<fpc-slot fpc-slot pic-slot pic-slot>
```

Release Information

Command introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display URL filter domain name system (DNS) resolution information.

URL filtering resolves the disallowed domains. The total number of domains are divided into chunks of 50 domains per chunk. The **filter term** in the command output is the name of a chunk.

Options

fpc-slot *fpc-slot* pic-slot *pic-slot*—(Optional) Specify the FPC and PIC for which you want URL filter information displayed.

profile *profile-name*—Specify the profile for which you want URL filter information displayed.

template *template-name*—(Optional) Specify the template for which you want URL filter information displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

- show services web-filter dns-resolution-statistics profile template | 2151
- show services web-filter statistics profile | 2160
- Configuring URL Filtering | 55

List of Sample Output

show services web-filter dns-resolution profile on page 2148

Output Fields

Table 117 on page 2148 lists the output fields for the **show services web-filter dns-resolution profile** command. Output fields are listed in the approximate order in which they appear.

Table 117: show services web-filter dns-resolution profile Output Fields

Field Name	Field Description
Profile	Name of profile.
Template	Name of template.
Filter Term	Name of the domains chunk. All domains are divided into chunks of 50 domains per chunk.
IPv4 Address Count	The number of IPv4 addresses resolved for all domains under the filter term.
IPv6 Address Count	The number of IPv6 addresses resolved for all domains under the filter term.
Domain Name	Name of domain.
IPv4 Records	Listing of IPv4 addresses.
IPv6 Records	Listing of IPv6 addresses.

Sample Output

show services web-filter dns-resolution profile

`user@host>` **show services web-filter dns-resolution profile p1**

```
URL filtering DNS resolution:
Profile: p1
Template: t1

 1). Filter Term: URLF_t1_0004

      IPv4 Address Count: 20
      IPv6 Address Count: 20

    1 ). Domain Name: www.example.com

          IPv4 Records:
             31.13.77.36
             31.13.76.68
```

```
        IPv6 Records:
           2a03:2880:f122:83:face:b00c:0:25de
           2a03:2880:f111:83:face:b00c:0:25de

2 ). Domain Name: www.youtube.com

        IPv4 Records:
           216.58.193.78
           216.58.194.206

        IPv6 Records:
           2607:f8b0:400a:800::200e
           2607:f8b0:4005:809::200e

3 ). Domain Name: www.netflix.com

        IPv4 Records:
           50.112.200.248
           52.10.96.2
           52.25.242.211
           52.39.87.182
           52.38.44.92
           52.36.125.176
           52.40.2.42
           52.42.184.64
           52.5.80.199
           52.206.203.18
           52.5.231.14
           52.21.94.89
           52.71.118.87
           52.201.133.109
           52.71.122.233
           52.203.136.33

        IPv6 Records:
           2620:108:700f::342a:b840
           2620:108:700f::3644:fc64
           2620:108:700f::3459:2ce1
           2620:108:700f::3459:c025
           2620:108:700f::3459:f556
           2620:108:700f::3459:c5c5
           2620:108:700f::3644:c2a0
           2620:108:700f::342a:df11
```

```
2406:da00:ff00::3404:d29c
2406:da00:ff00::3415:a86e
2406:da00:ff00::3415:fda4
2406:da00:ff00::3414:91d2
2406:da00:ff00::3403:73dd
2406:da00:ff00::22c7:d016
2406:da00:ff00::3400:290b
2406:da00:ff00::3213:c65f
```

show services web-filter dns-resolution-statistics profile template

Syntax

```
show services web-filter dns-resolution-statistics profile profile-name template template-name
(extensive | summary)
```

Release Information

Command introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display URL filter domain name system (DNS) resolution statistics.

Options

(extensive | summary)—Specify the level of detail of information you want displayed.

profile *profile-name*—Specify the profile for which you want URL filter information displayed.

template *template-name*—Specify the template for which you want URL filter information displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

- show services web-filter dns-resolution profile | **2147**
- show services web-filter statistics profile | **2160**
- Configuring URL Filtering | **55**

List of Sample Output

show services web-filter dns-resolution-statistics profile template summary on page 2153
show services web-filter dns-resolution-statistics profile template extensive on page 2154

Output Fields

Table 118 on page 2152 lists the output fields for the **show services web-filter dns-resolution-statistics profile template** command. Output fields are listed in the approximate order in which they appear.

Table 118: show services web-filter dns-resolution-statistics profile template Output Fields

Field Name	Field Description	Level of Detail
Profile	Name of profile.	all
Template	Name of template.	all
DNS start time	Start time of the DNS resolution.	**summary**
Next DNS start time	Start time of the next DNS resolution.	**summary**
Number of resolved A addresses	Number of resolved IPv4 addresses.	**summary**
Number of resolved AAAA addresses	Number of resolved IPv6 addresses.	**summary**
Number of unresolved A addresses	Number of unresolved IPv4 addresses.	**summary**
Number of unresolved AAAA addresses	Number of unresolved IPv6 addresses.	**summary**
Number of resolved A domains	Number of resolved IPv4 domains.	**summary**
Number of resolved AAAA domains	Number of resolved IPv6 domains.	**summary**
Number of unresolved A domains	Number of unresolved IPv4 domains.	**summary**
Number of unresolved AAAA domains	Number of unresolved IPv6 domains.	**summary**
Number of requests sent	Number of DNS requests sent.	**summary**
Number of responses received	Number of DNS responses received.	**summary**
Domain Name	Name of domain.	**extensive**

Table 118: show services web-filter dns-resolution-statistics profile template Output Fields *(continued)*

Field Name	Field Description	Level of Detail
IPv4 Address information	IPv4 address information includes the following fields: • **DNS server IP**—IPv4 address of DNS server. • **Req Sent**—Number of DNS requests sent. • **Resp Received**—Number of DNS responses received. • **DNS retries**—Number of times no DNS response was received and so retried.	**extensive**
IPv6 Address information	IPv6 address information includes the following fields: • **DNS server IP**—IPv6 address of DNS server. • **Req Sent**—Number of DNS requests sent. • **Resp Received**—Number of DNS responses received. • **DNS retries**—Number of times no DNS response was received and so retried.	**extensive**

Sample Output

show services web-filter dns-resolution-statistics profile template summary

`user@host>` **show services web-filter dns-resolution-statistics profile1 template t1 summary**

```
URL filtering DNS resolution statistics:
Profile: p1
Template: t1

     DNS start time                     : May 01 16:40:24 PDT
     Next DNS start time                : May 01 17:40:24 PDT
     Number of resolved A domains       : 114
```

```
     Number of resolved AAAA domains     : 114
     Number of unresolved A domains      : 0
     Number of unresolved AAAA domains   : 0
     Number of requests sent             : 246
     Number of responses received        : 228
```

show services web-filter dns-resolution-statistics profile template extensive

user@host> **show services web-filter dns-resolution-statistics profile p1 template t1 extensive**

```
URL filtering DNS resolution statistics:
Profile: p1
Template: t1

     1) Domain Name:    www.facebook.com

         IPv4 Address information:
              DNS server IP     8.8.8.8
              Req Sent          20
              Resp Received     20
              DNS retries       0

         IPv4 Address information:
              DNS server IP     172.29.131.60
              Req Sent          21
              Resp Received     20
              DNS retries       0

         IPv6 Address information:
              DNS server IP     8.8.8.8
              Req Sent          25
              Resp Received     20
              DNS retries       0

         IPv6 Address information:
              DNS server IP     172.29.131.60
              Req Sent          24
              Resp Received     20
              DNS retries       0
     2) Domain Name:    www.youtube.com

         IPv4 Address information:
              DNS server IP     8.8.8.8
              Req Sent          21
```

```
            Resp Received     20
            DNS retries       0

        IPv4 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0
    3) Domain Name:    www.netflix.com

        IPv4 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv4 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     8.8.8.8
            Req Sent          21
            Resp Received     20
            DNS retries       0

        IPv6 Address information:
            DNS server IP     172.29.131.60
            Req Sent          21
```

```
                Resp Received     20
                DNS retries       0
```

show services web-filter secintel-policy status

Syntax

```
show services web-filter secintel-policy status
profile profile-name
template template-name
```

Release Information

Statement introduced before Junos OS Release 18.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480, and MX960 with the MX-SPC3 services card.

Description

Display the IPv4 and IPv6 count per threat level received from the C&C feed from Policy Enforcer. It also displays the count of the number of terms used in the implicit filter per threat level.

Options

profile-name—Name of the profile

template-name—Name of the template

Required Privilege Level

view

RELATED DOCUMENTATION

security-intelligence | 1442

List of Sample Output

show services web-filter secintel-policy status on page 2157

Sample Output

show services web-filter secintel-policy status

`user@host>` **show services web-filter secintel-policy status profile**

```
URL Filtering SecIntel Policy Status:
Profile     : Profile1
```

```
C&C DB File : /var/db/url-filterd/urlf_si_cc_db.txt
Policy State: Ready
DB File Change Time : Tue Nov 27 11:01:10 2018
DB File Load Time   : Tue Nov 27 11:01:38 2018
C&C Prefix Count    : IPv4: 11093      IPv6: 5
Filters:
Threat level   Action       v4 Term Count    IPv4        v6 Term Count   IPv6

1              ACCEPT       23            1129        1               2
2              ACCEPT       11            1444        0               0
3              ACCEPT       6             996         0               0
4              ACCEPT       7             564         0               0
5              ACCEPT       7             451         0               0
6              ACCEPT       4             126         0               0
7              LOG          5             175         0               0
8              DROP AND LOG 4             396         1               1
9              ACCEPT       2             164         0               0
10             ACCEPT       33            5601        1               2
```

Sample Output

`user@host>` **show services web-filter secintel-policy-status profile Profile1 url-filter-template template200**

```
Template    : template200
       C&C DB File : /var/db/url-filterd/urlf_si_ip_white_list_db.txt
       Policy State: NA
       DB File Change Time : NA
       DB File Load Time   : NA
       C&C Prefix Count    : IPv4: 0          IPv6: 0

       C&C DB File : /var/db/url-filterd/urlf_si_ip_black_list_db.txt
       Policy State: NA
       DB File Change Time : NA
       DB File Load Time   : NA
       C&C Prefix Count    : IPv4: 0          IPv6: 0

       C&C DB File : /var/db/url-filterd/urlf_si_ip_custom_db.txt
       Policy State: Ready
```

```
       DB File Change Time : Tue Feb 04 15:22:20 2020
       DB File Load Time   : Tue Feb 04 15:24:29 2020
       C&C Prefix Count    : IPv4: 16         IPv6: 0
       Filters:
       Threat level   Action              v4 Term Count    IPv4        v6 Term
Count   IPv6

       0              ACCEPT AND SAMPLE       0             0             0
      0
       255            DROP AND SAMPLE         0             0             0
      0
       1              DROP AND SAMPLE         1             11            0
      0
       2              ACCEPT                  0             0             0
      0
       3              DROP AND SAMPLE         1             1             0
      0
       4              DROP AND SAMPLE         1             1             0
      0
       5              ACCEPT                  0             0             0
      0
       6              ACCEPT                  1             1             0
      0
       7              ACCEPT                  1             1             0
      0
       8              DROP AND SAMPLE         0             0             0
      0
       9              ACCEPT                  1             1             0
      0
       10             DROP AND SAMPLE         0             0             0
      0
```

show services web-filter statistics profile

Syntax

```
show services web-filter statistics profile profile-name
<dns-filter-template template-name>
<dns-filter-term term-name>
<fpc-slot fpc-slot pic-slot pic-slot>
<url-filter-template template-name>
```

Release Information

Command introduced in Junos OS Release 18.3R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display statistics for DNS request filtering and URL filtering for the specified filter profile.

Options

dns-filter-template *template-name*—(Optional) Display statistics for the specified DNS filter template.

dns-filter-term *term-name*—(Optional) Display statistics for the specified term in the DNS filter template.

fpc-slot *fpc-slot* pic-slot *pic-slot*—(Optional) Display statistics for the specified services PIC.

profile *profile-name*—Display statistics for the specified filter profile.

url-filter-template *template-name*—(Optional) Display statistics for the specified URL filter template.

Required Privilege Level

view

RELATED DOCUMENTATION

DNS Request Filtering for Disallowed Website Domains | 43
Configuring URL Filtering | 55

List of Sample Output

show services web-filter statistics profile dns-filter-template on page 2162
show services web-filter statistics profile on page 2163

Output Fields

Table 119 on page 2161 lists the output fields for the **show services web-filter statistics profile** command. Output fields are listed in the approximate order in which they appear.

Table 119: show services web-filter statistics profile Output Fields

Field Name	Field Description
UDP Counters	Number of UDP DNS requests, responses, and log only responses for DNS request filtering for queries of types A, AAAA, MX, CNAME, SRV, TXT, and MISC.
TCP Counters	Number of TCP DNS requests, responses, and log only responses for DNS request filtering for queries of types A, AAAA, MX, CNAME, SRV, TXT, and MISC.
Accept	Action counters for accepted packets for URL filtering.
Custom page	Action counters for custom page sent to recipient for URL filtering.
Http scode	Action counters for HTTP status code response for URL filtering.
Redirect url	Action counters for redirect URL response for URL filtering.
TCP reset	Action counters for TCP reset for URL filtering. Connection is closed.
Bypass session count	Number of sessions not blocked by URL filtering because the match criteria was not met for URL filtering.
IPV4 Disable IP Blocking	Action counters for IPv4 packets that were accepted because filtering is disabled for HTTP traffic that contains an embedded IP address belonging to a disallowed domain name in the URL filter database.
IPV6 Disable IP Blocking	Action counters for IPv6 packets that were accepted because filtering is disabled for HTTP traffic that contains an embedded IP address belonging to a disallowed domain name in the URL filter database.
session count	The session of activity that a user with a unique IP address spends on a website during a specified period of time for URL filtering. A session, in this case, would be the packets going to the service PIC from the Packet Forwarding Engine and then back to the service PIC.
uplink packet count	Number of packets going from the Packet Forwarding Engine to the service PIC for URL filtering.
uplink bytes	Number of bytes passing uplink for URL filtering.
downlink packet count	Number of packets going from the service PIC to the service Packet Forwarding Engine for URL filtering.
downlink bytes	Number of bytes passing downlink for URL filtering.

Table 119: show services web-filter statistics profile Output Fields *(continued)*

Field Name	Field Description
UDP DNS	Number of UDP DNS requests, responses, and log only responses for DNS request filtering for queries of types A, AAAA, MX, CNAME, SRV, TXT, and MISC.
TCP DNS	Number of TCP DNS requests, responses, and log only responses for DNS request filtering for queries of types A, AAAA, MX, CNAME, SRV, TXT, and MISC.

Sample Output

show services web-filter statistics profile dns-filter-template

`user@host>` **show services web-filter statistics profile pdns dns-filter-template tdns**

```
Query   Requests        Responses       Log
Type                                    only

UDP Counters:

 A      0               0               0
 AAAA   0               0               0
 MX     0               0               0
 CNAME  0               0               0
 SRV    0               0               0
 TXT    0               0               0
 MISC   0               0               0

TCP Counters:

 A      0               0               0
 AAAA   0               0               0
 MX     0               0               0
 CNAME  0               0               0
 SRV    0               0               0
 TXT    0               0               0
 MISC   0               0               0
```

Sample Output

show services web-filter statistics profile

`user@host>` **show services web-filter statistics profile Profile1**

```
URL filtering action counters:


    Accept session count                : 0
    Accept uplink packet count          : 0
    Accept uplink bytes                 : 0
    Accept downlink packet count        : 0
    Accept downlink bytes               : 0

    Custom page session count           : 0
    Custom page uplink packet count     : 0
    Custom page uplink bytes            : 0
    Custom page downlink packet count   : 0
    Custom page downlink bytes          : 0

    Http scode session count            : 0
    Http scode uplink packet count      : 0
    Http scode uplink bytes             : 0
    Http scode dowlink packet count     : 0
    Http scode downlink bytes           : 0

    Redirect url session count          : 0
    Redirect url uplink packet count    : 0
    Redirect url uplink bytes           : 0
    Redirect url downlink packet count  : 0
    Redirect url downlink bytes         : 0

    Tcp reset session count             : 0
    Tcp reset uplink packet count       : 0
    Tcp reset uplink bytes              : 0
    Tcp reset downlink packet count     : 0
    Tcp reset downlink bytes            : 0

    Bypass session count                : 0

    IPV4 Disable IP Blocking Sessions          : 0
    IPV4 Disable IP Blocking uplink packets    : 0
    IPV4 Disable IP Blocking uplink bytes      : 0
    IPV4 Disable IP Blocking downlink packets  : 0
```

```
IPV4 Disable IP Blocking downlink bytes    : 0
IPV6 Disable IP Blocking Sessions          : 0
IPV6 Disable IP Blocking uplink packets    : 0
IPV6 Disable IP Blocking uplink bytes      : 0
IPV6 Disable IP Blocking downlink packets  : 0
IPV6 Disable IP Blocking downlink bytes    : 0

DNS filtering counters:

UDP DNS A req count                        : 0
UDP DNS A resp count                       : 0
UDP DNS A log only count                   : 0
UDP DNS AAAA req count                     : 0
UDP DNS AAAA resp count                    : 0
UDP DNS AAAA log only count                : 0
UDP DNS MX req count                       : 0
UDP DNS MX resp count                      : 0
UDP DNS MX log only count                  : 0
UDP DNS CNAME req count                    : 0
UDP DNS CNAME resp count                   : 0
UDP DNS CNAME log only count               : 0
UDP DNS SRV req count                      : 0
UDP DNS SRV resp count                     : 0
UDP DNS SRV log only count                 : 0
UDP DNS TXT req count                      : 0
UDP DNS TXT resp count                     : 0
UDP DNS TXT log only count                 : 0
UDP DNS ANY req count                      : 0
UDP DNS ANY resp count                     : 0
UDP DNS ANY log only count                 : 0
UDP DNS MISC req count                     : 0
UDP DNS MISC log only count                : 0
TCP DNS A req count                        : 0
TCP DNS A resp count                       : 0
TCP DNS A log only count                   : 0
TCP DNS AAAA req count                     : 0
TCP DNS AAAA resp count                    : 0
TCP DNS AAAA log only count                : 0
TCP DNS MX req count                       : 0
TCP DNS MX resp count                      : 0
TCP DNS MX log only count                  : 0
TCP DNS CNAME req count                    : 0
TCP DNS CNAME resp count                   : 0
TCP DNS CNAME log only count               : 0
```

```
TCP DNS SRV req count                    : 0
TCP DNS SRV resp count                   : 0
TCP DNS SRV log only count               : 0
TCP DNS TXT req count                    : 0
TCP DNS TXT resp count                   : 0
TCP DNS TXT log only count               : 0
TCP DNS ANY req count                    : 0
TCP DNS ANY resp count                   : 0
TCP DNS ANY log only count               : 0
TCP DNS MISC req count                   : 0
TCP DNS MISC log only count              : 0
```