Interface Properties

Published: 2013-08-29

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

Interface Properties

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- M Series
- T Series
- MX Series

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 the *CLI User Guide*.

Documentation Conventions

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

Table 1: Notice Icons

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

Table 2 on page ix 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`

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

Convention	Description	Examples
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*
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)	Enclose 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)	Enclose a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identify 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		
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, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Services Interface

Services Interface Naming Overview

Each interface has an interface name, which specifies the media type, the slot the FPC is located in, the location on the FPC that the PIC is installed in, and the PIC port. The interface name uniquely identifies an individual network connector in the system. You use the interface name when configuring interfaces and when enabling various functions and properties, such as routing protocols, on individual interfaces. The system uses the interface name when displaying information about the interface, for example, in the **show interfaces** command.

The interface name is represented by a physical part, a logical part, and a channel part in the following format:

physical<:channel>.logical

The channel part of the name is optional for all interfaces except channelized DS3, E1, OC12, and STM1 interfaces.

The physical part of an interface name identifies the physical device, which corresponds to a single physical network connector. This part of the interface name has the following format:

type-fpc/pic/port

type is the media type, which identifies the network device. For service interfaces, it can be one of the following:

- **ams**—Aggregated multiservices (AMS) interface. An AMS interface is a bundle of services interfaces that can function as a single interface. An AMS interface is denoted as **amsN** in the configuration, where **N** is a unique number that identifies an AMS interface (for example, **ams0**). The member interfaces in an AMS interface are identified in the configuration with an **mams-** prefix (for example, **mams-1/2/0**).
- **cp**—Flow collector interface.
- **es**—Encryption interface.
- **gr**—Generic routing encapsulation tunnel interface.

- **gre**—This interface is internally generated and not configurable.
- **ip**—IP-over-IP encapsulation tunnel interface.
- **ipip**—This interface is internally generated and not configurable.
- **ls**—Link services interface.
- **lsq**—Link services intelligent queuing (IQ) interface; also used for voice services.
- **mams**—Member interface in an AMS interface.
- **ml**—Multilink interface.
- **mo**—Monitoring services interface. The logical interface **mo-*fpc/pic/port***.16383 is an internally generated, nonconfigurable interface for router control traffic.
- **ms**—Multiservices interfaces on multiservices modular interfaces card (MS-MIC) and multiservices modular port concentrators (MS-MPC).
- **mt**—Multicast tunnel interface. This interface is automatically generated, but you can configure properties on it if needed.
- **mtun**—This interface is internally generated and not configurable.
- **rlsq**—Redundancy LSQ interface.
- **rsp**—Redundancy adaptive services interface.
- **si**—Services inline interface, configured on MX3D Series routers only.
- **sp**—Adaptive services interface. The logical interface **sp-*fpc/pic/port***.16383 is an internally generated, nonconfigurable interface for router control traffic.
- **tap**—This interface is internally generated and not configurable.
- **vp**—Voice over IP (VoIP) interface, configured on J Series Services Routers only.
- **vt**—Virtual loopback tunnel interface.

Related Documentation

- *Services PIC Types*
- *Understanding Aggregated Multiservices Interfaces*
- Examples: Configuring Services Interfaces on page 19

PART 2

Configuration

CHAPTER 2

Configuration Tasks

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.

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*.

Related Documentation

- Configuring Default Timeout Settings for Services Interfaces on page 8
- Configuring System Logging for Services Interfaces on page 9
- Examples: Configuring Services Interfaces on page 19
- *Example: Configuring an Aggregated Multiservices Interface (AMS)*

Configuring Default Timeout Settings for Services Interfaces

You can specify global default settings for certain timers that apply for the entire interface. There are three statements of this type:

- **inactivity-timeout**—Sets the inactivity timeout period for established flows, after which they are no longer valid.
- **open-timeout**—Sets the timeout period for Transmission Control Protocol (TCP) session establishment, for use with SYN-cookie defenses against network intrusion.
- **close-timout**—Sets the timeout period for Transmission Control Protocol (TCP) session tear-down.

To configure a setting for the inactivity timeout period, include the **inactivity-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
inactivity-timeout seconds;
```

The default value is 30 seconds. The range of possible values is from 4 through 86,400 seconds. Any value you configure in the application protocol definition overrides the value specified here; for more information, see *Configuring Application Protocol Properties*.

To configure a setting for the TCP session establishment timeout period, include the **open-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
open-timeout seconds;
```

The default value is 30 seconds. The range of possible values is from 4 through 224 seconds. Any value you configure in the intrusion detection service (IDS) definition overrides the value specified here; for more information, see *Intrusion Detection Properties*.

To configure a setting for the TCP session teardown timeout period, include the **close-timeout** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

```
[edit interfaces interface-name services-options]
close-timeout seconds;
```

The default value is 1 second. The range of possible values is from 2 through 300 seconds.

Use of Keep-Alive Messages for Greater Control of TCP Inactivity Timeouts

Keep-alive messages are generated automatically to prevent TCP inactivity timeouts. The default number of keep-alive messages is 4. However, you can configure the number of keep-alive messages by entering the **tcp-tickles** statement at the **[edit interaces *interface-name* service-options]** hierarchy level.

When timeout is generated for a bidirectional TCP flow, keep-alive packets are sent to reset the timer. If number of consecutive keep-alive packets sent in a flow reaches the default or configured limit, the conversation is deleted. There are several possible scenarios, depending on the setting of the **inactivity-timer** and the default or configured maximum number of keep-alive messages.

- If the configured value of keep-alive messages is zero and **inactivity-timeout** is NOT configured (in which case the default timeout value of 30 is used), no keep-alive packets are sent. The conversation is deleted when any flow in the conversation is idle for more than 30 seconds.
- If the configured value of keep-alive messages is zero and the **inactivity-timeout** is configured, no keep-alive packets are sent, and the conversation is deleted when any flow in the conversation is idle for more than the configured timeout value.
- If the default or configured maximum number of keep-alive messages is some positive integer, and any of the flows in a conversation is idle for more than the default or configured value for **inactivity-timeout** keep-alive packets are sent. If hosts do not respond to the configured number of consecutive keep-alive packets, the conversation is deleted. The interval between keep-alive packets will be 1 second. However, if the host sends back an ACK packet, the corresponding flow becomes active, and keep-alive packets are not sent until the flow becomes idle again.

Related Documentation

- *Services PIC Types*
- Configuring the Address and Domain for Services Interfaces on page 7
- Configuring System Logging for Services Interfaces on page 9
- Applying Filters and Services to Interfaces on page 12
- Examples: Configuring Services Interfaces on page 19

Configuring System Logging for Services Interfaces

You specify properties that control how system log messages are generated for the interface as a whole. If you configure different values for the same properties at the **[edit services service-set *service-set-name*]** hierarchy level, the service-set values override the values configured for the interface. For more information on configuring service-set properties, see *Configuring System Logging for Service Sets*.

To configure interface-wide default system logging values, include the **syslog** statement at the **[edit interfaces *interface-name* services-options]** hierarchy level:

[edit interfaces *interface-name* services-options]

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

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.

Table 3 on page 10 lists the severity levels that you can specify in configuration statements at the **[edit interfaces *interface-name* services-options syslog host *hostname*]** hierarchy level. The levels from **emergency** through **info** are in order from highest severity (greatest effect on functioning) to lowest.

Table 3: 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 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 interface. To debug a configuration or log Network Address Translation (NAT) functionality, set the level to **info**.

For more information about system log messages, see the *Junos OS System Log Messages Reference*.

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

```
[edit interfaces interface-name services-options]
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 interfaces *interface-name* services-options syslog host *hostname*]** hierarchy level:

```
[edit interfaces interface-name services-options]
log-prefix prefix-value;
```

Related Documentation

- *Services PIC Types*
- Configuring the Address and Domain for Services Interfaces on page 7
- Configuring Default Timeout Settings for Services Interfaces on page 8
- Applying Filters and Services to Interfaces on page 12
- Examples: Configuring Services Interfaces on page 19

Enabling Fragmentation on GRE Tunnels

To enable fragmentation of IPv4 packets in generic routing encapsulation (GRE) tunnels, include the **clear-dont-fragment-bit** statement and a maximum transmission unit (MTU) setting for the tunnel as part of an existing GRE configuration at the **[edit interfaces]** hierarchy level:

```
[edit interfaces]
gr-fpc/pic/port {
  unit logical-unit-number {
    clear-dont-fragment-bit;
    ...
    family inet {
      mtu 1000;
      ...
    }
  }
}
```

This statement clears the Don't Fragment (DF) bit in the packet header, regardless of the packet size. If the packet size exceeds the tunnel MTU value, the packet is fragmented before encapsulation. The maximum MTU size configurable on the AS or Multiservices PIC is 9192 bytes.

NOTE: The **clear-dont-fragment-bit** statement is supported only on MX Series routers and all M Series routers except the M320 router.

Fragmentation is enabled only on IPv4 packets being encapsulated in IPv4-based GRE tunnels.

NOTE: This configuration is supported only on GRE tunnels on AS or Multiservices interfaces. If you commit **gre-fragmentation** as the encapsulation type on a standard Tunnel PIC interface, the following console log message appears when the PIC comes online:

gr-*fpc/pic/port*: does not support this encapsulation

The Packet Forwarding Engine updates the IP identification field in the outer IP header of GRE-encapsulated packets, so that reassembly of the packets is possible after fragmentation. The previous CLI constraint check that required you to configure either the **clear-dont-fragment-bit** statement or a tunnel key with the **allow-fragmentation** statement is no longer enforced.

Related Documentation

- *Configuring Unicast Tunnels*

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*.

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 Policy Feature Guide for Routing Devices*.

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 19.

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 Policy Feature Guide for Routing Devices*.

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 PIC Types*
- *Configuring Service Sets to be Applied to Services Interfaces*
- Examples: Configuring Services Interfaces on page 19

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 *Junos OS Operational Mode Commands*.
- The driver watchdog timer expires.
- The **request interface switchover** command is issued. For more information, see the *Junos OS Operational Mode Commands*.

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.

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;
}
```

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*.

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 *Clearing Security Associations*.

- 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.

Related Documentation

- *Services PIC Types*
- Examples: Configuring Services Interfaces on page 19
- *Example: Configuring an Aggregated Multiservices Interface (AMS)*

Flow Offloading

The Junos OS enables you to configure flow offloading for PICS on MX Series routers using Modular Port Concentrator (MPCs) with Modular Interface Cards (MICs). Flows are offloaded to Fast Update Filters (FUFs) on the Packet Forwarding Engine. Offloading produces the greatest benefits when applied to long-lasting or high-bandwidth flows

The maximum number of active offloads is 200,000 per PIC. When offloaded flows are deleted, more flows can be offloaded.

To configure flow offloading:

- At the **[edit interfaces *interface-name* services-options]** hierarchy level, enter the **trio-flow-offload minimum-bytes *minimum-bytes*** statement.

  ```
  user@host# edit services interface-name
  [edit services interface-name services-options]
  user@host# set trio-flow-offload minimum-bytes minimum- bytes
  ```

  In the following example, flows are offloaded when they consist of no less than 1024 bytes:

  ```
  user@host# edit services ms-0/1/0
  [edit services ms-0/1/0 services-options]
  user@host# set trio-flow-offload minimum-bytes 1024
  ```

Related Documentation

- trio-flow-offload on page 37

CHAPTER 3

Example

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 PIC Types*
- Configuring the Address and Domain for Services Interfaces on page 7
- Configuring Default Timeout Settings for Services Interfaces on page 8
- Configuring System Logging for Services Interfaces on page 9
- Applying Filters and Services to Interfaces on page 12
- *Example: Configuring an Aggregated Multiservices Interface (AMS)*

CHAPTER 4

Configuration Statements

address (Interfaces)

Syntax

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

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family (Interfaces) *family*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family (Interfaces) *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 Address and Domain for Services Interfaces on page 7
- *Junos OS Network Interfaces Library for Routing Devices*

clear-dont-fragment-bit

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.

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.

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 on page 11

close-timeout

Syntax close-timeout *seconds*;

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure the timeout period for Transmission Control Protocol (TCP) session tear-down.

Options **seconds**—Timeout period.
Default: 1 second
Range: 2 through 300 seconds

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

Related Documentation
- Configuring Default Timeout Settings for Services Interfaces on page 8

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*
- *Configuring Dynamic Endpoints for IPsec Tunnels*
- *Configuring Options for the LNS Inline Services Logical Interface*

facility-override

Syntax facility-override *facility-name*;

Hierarchy Level [edit interfaces *interface-name* services-options 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 for Services Interfaces on page 9

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.

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 on page 7
- *Junos OS Network Interfaces Library for Routing Devices*

host (Interfaces)

Syntax

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

Hierarchy Level [edit interfaces *interface-name* services-options 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.

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 on page 12

inactivity-timeout

Syntax inactivity-timeout *seconds*;

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the inactivity timeout period for established flows. The timeout value configured in the application protocol definition overrides this value.

Options ***seconds***—Timeout period.

Default: 30 seconds

Range: 4 through 86,400 seconds

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

Related Documentation

- Configuring Default Timeout Settings for Services Interfaces on page 8

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.

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 on page 12

interfaces

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*

log-prefix (Interfaces)

Syntax log-prefix *prefix-value*;

Hierarchy Level [edit interfaces *interface-name* services-options 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
- *Junos OS Services Interfaces Library for Routing Devices*
- Configuring System Logging for Services Interfaces on page 9

open-timeout

Syntax open-timeout *seconds*;

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a timeout period for Transmission Control Protocol (TCP) session establishment.

Options ***seconds***—Timeout period.
Default: 30 seconds
Range: 4 through 224 seconds

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

Related Documentation
- Configuring Default Timeout Settings for Services Interfaces on page 8

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.

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 on page 12

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 on page 12

primary (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 on page 14

redundancy-options

Syntax
```
redundancy-options {
  primary sp-fpc/pic/port;
  secondary sp-fpc/pic/port;
}
```

Hierarchy Level [edit interfaces (rsp0 | rsp1)]

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.

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 on page 14

secondary (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 on page 14

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.

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 on page 12

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.

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 on page 7

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.

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 on page 12
- *Junos OS Services Interfaces Library for Routing Devices*

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.

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***—Identifies the service set.

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 on page 12

services (Interfaces)

Syntax services *severity-level*;

Hierarchy Level [edit interfaces *interface-name* services-options syslog host *hostname*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the system logging severity level.

Options ***severity-level***—Assigns a severity level to the facility. Valid entries include:

- **alert**—Conditions that should be corrected immediately.
- **any**—Matches any level.
- **critical**—Critical conditions.
- **emergency**—Panic conditions.
- **error**—Error conditions.
- **info**—Informational messages.
- **notice**—Conditions that require special handling.
- **warning**—Warning 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 on page 9

services-options

Syntax

```
services-options {
  cgn-pic;
  close-timeout
  fragment-limit
  disable-global-timeout-override;
  ignore-errors <alg> <tcp>;
  inactivity-non-tcp-timeout seconds;
  inactivity-tcp-timeout seconds;
  inactivity-timeout seconds;
  open-timeout seconds;
  reassembly-timeout
  session-limit {
    maximum number;
    rate new-sessions-per-second;
    cpu-load-threshold percentage;
  }
  session-timeout seconds;
  syslog {
    host hostname {
      facility-override facility-name;
      log-prefix prefix-value;
      port port-number;
      services severity-level;
    }
    message-rate-limit messages-per-second;
  }
  tcp-tickles tcp-tickles;
  trio-flow-offload minimum-bytes minimum-bytes;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the service options to be applied on an interface.

Options 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

- *Interface Properties*.

syslog (Interfaces)

Syntax

```
syslog {
  host hostname {
    services severity-level;
    facility-override facility-name;
    log-prefix prefix-value;
    port port-number;
  }
  message-rate-limit messages-per-second;
}
```

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced before Junos OS Release 7.4.

Description 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 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 Services Interfaces on page 9

tcp-tickles

Syntax tcp-tickles *tcp-tickles*;

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced in Junos OS Release 11.4.

Description Define the maximum number of keep-alive messages sent before a TCP session is allowed to timeout.

Options ***tcp-tickles***—Number of keep-alive messages.

Range: 0 through 30

Default: 4

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

Related Documentation

- Configuring Default Timeout Settings for Services Interfaces on page 8

trio-flow-offload

Syntax trio-flow-offload minimum-bytes *minimum-bytes*;

Hierarchy Level [edit interfaces *interface-name* services-options]

Release Information Statement introduced in Junos OS Release 12.1.

Description Enable any plug-in or daemon on a PIC to generate a flow offload request to of-load flows to the Packet Forwarding Engine. This command is available on MX Series routers with Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs).

Options ***minimum-bytes***—The minimum number of bytes that trigger offloading. When this option is omitted, offloading is triggered when both the forward and reverse flows of the session have begun, meaning that at least one packet has flowed in each direction.

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

Related Documentation

- Flow Offloading on page 17

unit

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.

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.

PART 3

Administration

CHAPTER 5

Adaptive Services Interface Operational Mode Commands

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 42
request interface switchover on page 42

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
```


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***. On J Series routers, the interface type is **sp-*pim*/0/*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 48
show interfaces brief (Adaptive Services) on page 48
show interfaces detail (Adaptive Services) on page 48
show interfaces extensive (Adaptive Services) on page 49

Output Fields

Table 4 on page 43 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 4: Adaptive Services and Redundant Adaptive Services show interfaces 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

Table 4: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Type	Encapsulation being used on the interface.	All levels
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	MTU size on the physical interface.	All levels
Clocking	Reference clock source: can be **Internal** or **External**.	All levels
Speed	Speed at which the interface is running.	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
Link type	Physical interface link type: **Full-Duplex** or **Half-Duplex**.	**detail extensive** none
Link flags	Information about the link. Possible values are described in the "Link Flags" section under *Common Output Fields Description*.	**detail extensive** none
Physical info	Information about the physical interface.	**detail extensive**
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	**detail extensive**
Current address	Configured MAC address.	**detail extensive** none
Hardware address	MAC address of the hardware.	**detail extensive** none
Alternate link address	Backup address of the link.	**detail extensive** none
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	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	**detail extensive**

Table 4: Adaptive Services and Redundant Adaptive Services show interfaces 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. • **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.	**detail extensive**
Input errors	Input errors on the interface. The following paragraphs explain the counters whose meaning might not be 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 the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • **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 because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • **Resource errors**—Sum of transmit drops.	**extensive**
Output errors	Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious: • **Carrier transitions**—Number of times the interface has gone from **down** to **up**. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC is malfunctioning. • **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 the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • **MTU errors**—Number of packets larger than the MTU threshold. • **Resource errors**—Sum of transmit drops.	**extensive**
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	SNMP interface index number.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

Table 4: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
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 on the logical interface.	All levels
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified
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.	**detail extensive**
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	**detail extensive**
Transit statistics	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes generally less than 1 second for the counter to stabilize.	**detail extensive**
protocol-family	Protocol family configured on the logical interface. If the protocol is **inet**, the IP address of the interface is also displayed.	**brief**
Protocol	Protocol family configured on the logical interface, such as **iso**, **inet6**, **mpls**.	**detail extensive** none
MTU	MTU size on the logical interface.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**
Route table	Routing table in which the logical interface address is located. For example, **0** refers to the routing table 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 address flags. 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

Table 4: Adaptive Services and Redundant Adaptive Services show interfaces Output Fields *(continued)*

Field Name	Field Description	Level of Output
Broadcast	Broadcast address.	**detail extensive** none
Generation	Unique number for use by Juniper Networks technical support only.	**detail extensive**

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 (Redundant Adaptive Services)

Syntax
show interfaces rsp*number*
<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 51

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 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 adaptive services and link services intelligent queuing (IQ) interfaces and aggregated Ethernet interfaces redundancy.

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 54
show interfaces redundancy (Aggregated Ethernet) on page 54
show interfaces redundancy detail on page 54

Output Fields Table 5 on page 53 lists the output fields for the **show interfaces redundancy** command. Output fields are listed in the approximate order in which they appear.

Table 5: show interfaces redundancy Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the redundant adaptive services, link services IQ interfaces, or aggregated Ethernet 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

Table 5: show interfaces redundancy Output Fields *(continued)*

Field Name	Field Description	Level of Output
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
```

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 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
```

PART 4

Index

Index