JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Services Interfaces Overview for Routing Devices

Published
2020-06-16

junos

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

Junos® OS Services Interfaces Overview 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

About the Documentation

IN THIS SECTION

Use this guide to learn what a service interface is, what service interface cards are available, and how to configure a service interface.

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 x 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 x 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		

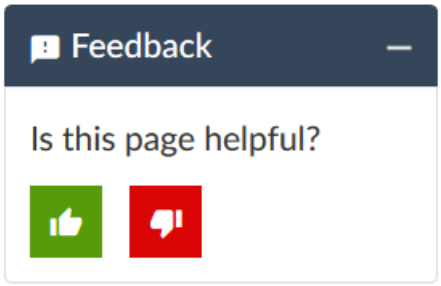
Table 2: Text and Syntax Conventions *(continued)*

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/.

CHAPTER 1

Overview

Understanding Services PICs

IN THIS SECTION

Interfaces used in router networks can be broadly classified into two:

- Networking interfaces, such as Ethernet and SONET interfaces, that primarily provide traffic connectivity. For more information on these interfaces, see the *Interfaces Fundamentals for Routing Devices* guide.
- Services interfaces, such as Adaptive Services interfaces and Multiservices interfaces, that provide specific capabilities for manipulating traffic before it is delivered to its destination.

Services interfaces enable you to add services to your network incrementally. Junos OS supports the following services interfaces:

Adaptive Services and Multiservices PICs

Adaptive Services [AS] PICs and Multiservices PICs enable you to perform multiple services on the same PIC by configuring a set of services and applications. The AS and Multiservices PICs offer a range of services that you can configure in one or more service sets. The following are some of the services you can configure on Adaptive services or multiservices interfaces:

- Class-of-service
- Intrusion detection service (IDS)
- IP Security (IPsec)
- Layer 2 tunneling protocols
- Monitoring services
- Network Address Translation (NAT)

- Stateful firewalls
- Voice services

For more information about these services, see *Adaptive Services Overview*.

> **NOTE:** On Juniper Networks MX Series 5G Universal Routing Platforms, the Multiservices DPC provides essentially the same capabilities as the Multiservices PIC. The interfaces on both platforms are configured in the same way.

Encryption Services (ES) PIC

ES PIC provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates. For more information about encryption interfaces, see *Configuring Encryption Interfaces*.

Multilink Services and Link Services PICs

Multilink Services and Link Services PICs enable you to split, recombine, and sequence datagrams across multiple logical data links. The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the members. The Junos OS supports two services PICs based on the Multilink Protocol: the Multilink Services PIC and the Link Services PIC.

For more information about multilink and link services interfaces, see *Link and Multilink Services Interfaces User Guide for Routing Devices*.

Monitoring Services PICs

Monitoring Services PICs enable you to monitor traffic flow and export the monitored traffic. Monitoring traffic allows you to perform the following tasks:

- Gather and export detailed information about IPv4 traffic flows between source and destination nodes in your network.
- Sample all incoming IPv4 traffic on the monitoring interface and present the data in cflowd record format.
- Perform discard accounting on an incoming traffic flow.
- Encrypt or tunnel outgoing cflowd records, intercepted IPv4 traffic, or both.
- Direct filtered traffic to different packet analyzers and present the data in its original format.

For more information about flow monitoring interfaces, see *Monitoring, Sampling, and Collection Services Interfaces User Guide*.

Tunnel Services PIC

Tunnel Services PIC provides a private, secure path through an otherwise public network by encapsulating arbitrary packets inside a transport protocol. Tunnels connect discontinuous subnetworks and enable encryption interfaces, virtual private networks (VPNs), and MPLS.

For more information about tunnel interfaces, see *Tunnel Services Overview*.

Multiservices MIC and Multiservices MPC

The Multiservices Modular Interfaces Card (MS-MIC) and the Multiservices Modular PIC Concentrator (MS-MPC), introduced in Junos OS Release 13.2, provide improved scaling and high performance. The MS-MIC and MS-MPC have enhanced memory (16 GB for MS-MIC, 32 GB per NPU of MS-MPC) and processing capabilities.

The services interfaces on MS-MPC and MS-MIC are identified in the configuration with an **ms-** prefix (for example, **ms-1/2/1**).

The following services packages come preinstalled and preconfigured on MS-MICs and MS-MPCs in Junos OS Release 13.2:

- Junos Traffic Vision (formerly referred to as Jflow/Flow Monitoring)
- Junos Address Aware (formerly referred to as NAT features)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as the Stateful Firewall feature)

For information about MS-MIC and MS-MPC, see "Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview" on page 18.

RELATED DOCUMENTATION

Supported Platforms | 20

Packet Flow Through the Adaptive Services or Multiservices PIC

Enabling Service Packages | 24

Services Configuration Procedure | 30

Services Interface Naming Overview | 23

Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview

Juniper Networks supports the Multiservices Modular Interfaces Card (MS-MIC) and the Multiservices Modular PIC Concentrator (MS-MPC) that provide improved scaling and high performance. The MS-MIC and MS-MPC have enhanced memory (16 GB for MS-MIC, 32 GB per NPU of MS-MPC) and processing capabilities.

The services interfaces on MS-MPC and MS-MIC are identified in the configuration with an **ms-** prefix (for example, **ms-1/2/1**). The following services packages come preinstalled and preconfigured on MS-MICs and MS-MPCs:

- Junos Traffic Vision (formerly referred to as Jflow)
- Junos Address Aware (formerly referred to as NAT features)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as the Stateful Firewall feature)
- Junos Services Crypto Base PIC Package
- Junos Services Application Level Gateways

NOTE: You can check the default packages on an MS-MIC or MS-MPC by executing the **show extension-provider system packages interface ms-*interace*** operational mode command.

The MS-MPC on your MX Series router supports a maximum of two million active routes only. If the number of active routes exceeds this threshold, the heap memory used by the Packet Forwarding Engine is exhausted. As a result, the MS-MPC becomes unresponsive.

The MS-MIC supports the following Layer 3 services such as stateful firewall, NAT, IPsec, active flow monitoring, RPM, and graceful Routing Engine switchover (GRES). For more information on the supported features, see *Protocols and Applications Supported by the MS-MIC and MS-MPC*.

The MS-MIC and MS-MPC also support the captive portal content delivery (HTTP redirect) service package when configured for installation using the **set chassis** operational mode command.

NOTE:

- Starting with Junos OS Release 14.2, the MX104 router supports two MS-MICs. Also, graceful Routing Engine switchover (GRES) is not supported for MS-MIC on the MX104 router.
- Starting from Junos OS Release 18.1R1, Junos Node Slicing supports assignment of MS-MICs and MS-MPCs to guest network functions (GNFs), or partitions created on a router by using Junos Node Slicing.
- Starting with Junos OS Release 19.2R1, the MX2020 router supports 15 MS-MPC cards.

Table 3 on page 19 lists the platforms on which the MS-MIC and MS-MPC are supported.

Table 3: MX Series Routers That Support MS-MIC and MS-MPC

	MX5	MX10	MX40	MX80	MX104	MX240	MX480	MX960	MX2010	MX2020
MS-MIC	Yes	Yes	Yes	Yes	Yes **NOTE:** MX104 is first supported in Junos OS Release 13.3R2.	Yes	Yes	Yes	Yes **NOTE:** Only Junos Traffic Visi supported.	Yes
MS-MPC	No	No	No	No	No	Yes	Yes	Yes	Yes **NOTE:** MX2010 is first supported in Junos OS Release 14.1.	Yes **NOTE:** MX is first sup in Junos O Release 14

You can install an MS-MIC on one of the following line cards:

- MPC-Type1
- MPC-Type2
- MPC-Type3

Release History Table

Release	Description
19.2R1	Starting with Junos OS Release 19.2R1, the MX2020 router supports 15 MS-MPC cards.
18.1R1	Starting from Junos OS Release 18.1R1, Junos Node Slicing supports assignment of MS-MICs and MS-MPCs to guest network functions (GNFs), or partitions created on a router by using Junos Node Slicing.
14.2	Starting with Junos OS Release 14.2, the MX104 router supports two MS-MICs.
14.1	MX2010 is first supported in Junos OS Release 14.1.
14.1	MX2020 is first supported in Junos OS Release 14.1.
13.3R2	MX104 is first supported in Junos OS Release 13.3R2.

RELATED DOCUMENTATION

- *Multiservices MIC*
- Understanding Services PICs | **15**
- *Example: Configuring Junos VPN Site Secure on MS-MIC and MS-MPC*
- *Example: Configuring Flow Monitoring on an MX Series Router with MS-MIC and MS-MPC*
- *Protocols and Applications Supported by the MS-MIC and MS-MPC*
- *Services Interfaces Overview for Routing Devices*

Supported Platforms

For information about which platforms support Adaptive Services and MultiServices PICs and their features, see "Enabling Service Packages" on page 24.

For information about PIC support on a specific Juniper Networks M Series Multiservice Edge Router or T Series Core Router, see the appropriate *PIC Guide* for the platform.

For information about MS-MIC, MS-MPC, and MS-DPC support on a specific MX Series router, see the *MX Series 5G Universal Routing Platform Interface Module Reference*.

For information about services supported on Juniper Networks SRX Series Services Gateways, see Feature Explorer.

RELATED DOCUMENTATION

Understanding Services PICs | 15

Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview | 18

2

CHAPTER

Configuration Overview

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.
- **vt**—Virtual loopback tunnel interface.

RELATED DOCUMENTATION

Understanding Services PICs | 15

Understanding Aggregated Multiservices Interfaces

Examples: Configuring Services Interfaces

Enabling Service Packages

For AS PICs, Multiservices PICs, Multiservices DPCs, and the internal Adaptive Services Module (ASM) in the M7i router, there are two service packages: Layer 2 and Layer 3. Both service packages are supported on all adaptive services interfaces, but you can enable only one service package per PIC, with the exception of a combined package supported on the ASM. On a single router, you can enable both service packages by installing two or more PICs on the platform.

NOTE: Graceful Routing Engine switchover (GRES) is automatically enabled on all services PICs and DPCs except the ES PIC. It is supported on all M Series, MX Series, and T Series routers except for TX Matrix routers. Layer 3 services should retain state after switchover, but Layer 2 services will restart. For IPsec services, Internet Key Exchange (IKE) negotiations are not stored and must be restarted after switchover. For more information about GRES, see the *High Availability User Guide*.

You enable service packages per PIC, not per port. For example, if you configure the Layer 2 service package, the entire PIC uses the configured package. To enable a 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** or **layer-3**:

```
[edit chassis fpc slot-number pic pic-number adaptive-services]
service-package (layer-2 | layer-3);
```

To determine which package an AS PIC supports, issue the **show chassis hardware** command: if the PIC supports the Layer 2 package, it is listed as **Link Services II**, and if it supports the Layer 3 package, it is listed as **Adaptive Services II**. To determine which package a Multiservices PIC supports, issue the **show chassis pic fpc-slot *slot-number* pic-slot *slot-number*** command. The **Package** field displays the value **Layer-2** or **Layer-3**.

NOTE: The ASM has a default option (**layer-2-3**) that combines the features available in the Layer 2 and Layer 3 service packages.

After you commit a change in the service package, the PIC is taken offline and then brought back online immediately. You do not need to manually take the PIC offline and online.

NOTE: Changing the service package causes all state information associated with the previous service package to be lost. You should change the service package only when there is no active traffic going to the PIC.

The services supported in each package differ by PIC and platform type. Table 4 on page 26 lists the services supported within each service package for each PIC and platform.

On the AS and Multiservices PICs, link services support includes Junos OS CoS components, LFI (FRF.12), MLFR end-to-end (FRF.15), MLFR UNI NNI (FRF.16), MLPPP (RFC 1990), and multiclass MLPPP. For more

information, see "Layer 2 Service Package Capabilities and Interfaces" on page 28 and *Layer 2 Service Package Capabilities and Interfaces*.

> **NOTE:** The AS PIC II for Layer 2 Service is dedicated to supporting the Layer 2 service package only.

Table 4: AS and Multiservices PIC Services by Service Package, PIC, and Platform

Services	ASM	AS/AS2 PICs and Multiservices PICs	AS/AS2 and Multiservices PICs	AS2 and Multiservices PICs	AS2 and Multiservices PICs
Layer 2 Service Package (Only)	**M7i**	**M7i, M10i, and M20**	**M40e and M120**	**M320, T320, and T640**	**TX Matrix**
Link Services:					
• Link services	Yes	Yes	Yes	Yes	No
• Multiclass MLPPP	Yes	Yes	Yes	Yes	No
Voice Services:					
• CRTP and LFI	Yes	Yes	Yes	Yes	No
• CRTP and MLPPP	Yes	Yes	Yes	Yes	No
• CRTP over PPP (without MLPPP)	Yes	Yes	Yes	Yes	No
Layer 3 Service Package (Only)	**M7i**	**M7i, M10i, and M20**	**M40e and M120**	**M320, T320, and T640**	**TX Matrix**
Security Services:					
• CoS	Yes	Yes	Yes	Yes	No
• Intrusion detection system (IDS)	Yes	Yes	Yes	Yes	No
• IPsec	Yes	Yes	Yes	Yes	No

Table 4: AS and Multiservices PIC Services by Service Package, PIC, and Platform *(continued)*

Services	ASM	AS/AS2 PICs and Multiservices PICs	AS/AS2 and Multiservices PICs	AS2 and Multiservices PICs	AS2 and Multiservices PICs
• NAT	Yes	Yes	Yes	Yes	No
• Stateful firewall	Yes	Yes	Yes	Yes	No
Accounting Services:					
• Active monitoring	Yes	Yes	Yes	Yes	Yes
• Dynamic flow capture (Multiservices 400 PIC only)	No	No	No	Yes	No
• Flow-tap	Yes	Yes	Yes (M40e only)	Yes	No
• Passive monitoring (Multiservices 400 PIC only)	No	Yes	Yes (M40e only)	Yes	No
• Port mirroring	Yes	Yes	Yes	Yes	Yes
LNS Services:					
• L2TP LNS	Yes	Yes (M7i and M10i only)	Yes (M120 only)	No	No
Voice Services:					
• BGF	Yes	Yes	Yes	Yes	No
Layer 2 and Layer 3 Service Package (Common Features)	**M7i**	**M7i, M10i, and M20**	**M40e and M120**	**M320, T320, and T640**	**TX Matrix**
RPM Services:					
• RPM probe timestamping	Yes	Yes	Yes	Yes	No
Tunnel Services:					

Table 4: AS and Multiservices PIC Services by Service Package, PIC, and Platform *(continued)*

Services	ASM	AS/AS2 PICs and Multiservices PICs	AS/AS2 and Multiservices PICs	AS2 and Multiservices PICs	AS2 and Multiservices PICs
• GRE (**gr-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes
• GRE fragmentation (**clear-dont-fragment-bit**)	Yes	Yes	Yes	No	No
• GRE key	Yes	Yes	Yes	Yes	No
• IP-IP tunnels (**ip-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes
• Logical tunnels (**lt-*fpc*/*pic*/*port***)	No	No	No	No	No
• Multicast tunnels (**mt-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes
• PIM de-encapsulation (**pd-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes
• PIM encapsulation (**pe-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes
• Virtual tunnels (**vt-*fpc*/*pic*/*port***)	Yes	Yes	Yes	Yes	Yes

Layer 2 Service Package Capabilities and Interfaces

When you enable the Layer 2 service package, you can configure link services. On the AS and Multiservices PICs and the ASM, link services include support for the following:

- Junos CoS components—*Layer 2 Service Package Capabilities and Interfaces* 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)*.
- 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 MLPPP links.
- 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 (RFC 1990)
- MLFR end-to-end (FRF.15)

For the LSQ interface on the AS and Multiservices PICs, 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, 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 and Multiservices PICs 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 4 on page 26.

Interface type **lsq-*fpc/pic/port*** is the physical link services IQ (**lsq**) interface. 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*]** option. For more information, see *Layer 2 Service Package Capabilities and Interfaces* and *Link and Multilink 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.

RELATED DOCUMENTATION

Understanding Services PICs | **15**

Adaptive Services Overview

Supported Platforms | **20**

Packet Flow Through the Adaptive Services or Multiservices PIC

Services Configuration Procedure | **30**

Services Configuration Procedure

You follow these general steps to configure services:

1. Define application objects by configuring statements at the **[edit applications]** hierarchy level.

2. Define service rules by configuring statements at the **[edit services (ids | ipsec-vpn | nat | stateful-firewall) rule]** hierarchy level.

3. Group the service rules by configuring the **rule-set** statement at the **[edit services (ids | ipsec-vpn | nat | stateful-firewall)]** hierarchy level.

4. Group service rule sets under a service-set definition by configuring the **service-set** statement at the **[edit services]** hierarchy level.

5. Apply the service set on an interface by including the **service-set** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet service (input | output)]** hierarchy level. Alternatively, you can configure logical interfaces as a next-hop destination by including the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level.

   NOTE: You can configure IDS, NAT, and stateful firewall service rules within the same service set. You must configure IPsec services in a separate service set, although you can apply both service sets to the same PIC.

RELATED DOCUMENTATION

Understanding Services PICs | 15

Enabling Service Packages | 24

Supported Platforms | 20

Example: Service Interfaces Configuration

The following configuration includes all the items necessary to configure services on an interface:

```
[edit]
interfaces {
    fe-0/1/0 {
        unit 0 {
            family inet {
                service {
                    input {
                        service-set Firewall-Set;
                    }
                    output {
                        service-set Firewall-Set;
                    }
                }
                address 10.1.3.2/24;
            }
        }
    }
    fe-0/1/1 {
        unit 0 {
            family inet {
                filter {
                    input Sample;
                }
                address 172.16.1.2/24;
            }
        }
    }
    sp-1/0/0 {
        unit 0 {
            family inet {
                address 172.16.1.3/24 {
                }
            }
        }
    }
}
forwarding-options {
    sampling {
        input {
            family inet {
                rate 1;
            }
        }
        output {
```

```
            cflowd 10.1.3.1 {
                port 2055;
                version 5;
            }
            flow-inactive-timeout 15;
            flow-active-timeout 60;
            interface sp-1/0/0 {
                engine-id 1;
                engine-type 136;
                source-address 10.1.3.2;
            }
        }
    }
}
firewall {
    filter Sample {
        term Sample {
            then {
                count Sample;
                sample;
                accept;
            }
        }
    }
}
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;
            }
        }
    }
}
ids {
    rule Attacks {
        match-direction output;
        term Match {
            from {
                application-sets Applications;
            }
            then {
                logging {
                    syslog;
                }
            }
        }
    }
}
nat {
    pool public {
        address-range low 172.16.2.1 high 172.16.2.32;
        port automatic;
    }
    rule Private-Public {
        match-direction input;
        term Translate {
            then {
                translated {
                    source-pool public;
                    translation-type source napt-44;
                }
            }
        }
    }
```

```
    }
    service-set Firewall-Set {
        stateful-firewall-rules Rule1;
        stateful-firewall-rules Rule2;
        nat-rules Private-Public;
        ids-rules Attacks;
        interface-service {
            service-interface sp-1/0/0;
        }
    }
}
applications {
    application ICMP {
        application-protocol icmp;
    }
    application FTP {
        application-protocol ftp;
        destination-port ftp;
    }
    application-set Applications {
        application ICMP;
        application FTP;
    }
}
```

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 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 5 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 *Configuring IDS Rules on an MS-DPC*.

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

Understanding Services PICs | 15

Configuring the Address and Domain for Services Interfaces

Configuring System Logging for Services Interfaces | 36

Applying Filters and Services to Interfaces

Examples: Configuring Services Interfaces

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*.

> **NOTE:** Starting with Junos OS Release 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.

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.

Starting with 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 for ms interface under **[edit interfaces *interface-name* services-options]** hierarchy.

Table 5 on page 37 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 5: 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 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 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;
```

Release History Table

Release	Description
14.2R5	Starting with Junos OS Release 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.

RELATED DOCUMENTATION

Understanding Services PICs | 15

Configuring the Address and Domain for Services Interfaces

Configuring Default Timeout Settings for Services Interfaces | 34

Applying Filters and Services to Interfaces

Examples: Configuring Services Interfaces

Configuring the TLS Syslog Protocol on MS-MPC and MS-MIC

IN THIS SECTION

Transport Layer Security (TLS) Overview

IN THIS SECTION

Starting with Junos OS Release 19.1R1, you can configure Transport Layer Security (TLS) for syslog messages generated by the services that run on the MS-MPC or MS-MIC service cards in an MX router. The services may be one of the following:

- Junos Address Aware (formerly referred to as NAT feaures)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as Stateful Firewall features)

Transport Layer Security (TLS) is an application-level protocol that provides encryption technology for the Internet. TLS relies on certificates and private-public key exchange pairs for this level of security. It is the most widely used security protocol for the applications that require data to be securely exchanged over a network, such as file transfers, VPN connections, instant messaging, and voice over IP (VoIP).

TLS protocol is used for certificate exchange, mutual authentication, and negotiating ciphers to secure the stream from potential tampering and eavesdropping. TLS is sometimes called as Secure Sockets Layer (SSL). TLS and SSL are not interoperable, though TLS currently provides some backward compatibility.

Benefits of TLS

TLS ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity.

Three Essential Services of TLS

The TLS protocol is designed to provide three essential services to the applications running above it: encryption, authentication, and data integrity.

- Encryption—In order to establish a cryptographically secure data channel, the server and the client must agree on which cipher suites are used and the keys used to encrypt the data. The TLS protocol specifies a well-defined handshake sequence to perform this exchange. TLS uses public key cryptography, which allows the client and server to negotiate a shared secret key without having to establish any prior knowledge of each other, and to do so over an unencrypted channel.
- Authentication—As part of the TLS handshake, the protocol allows both server and the client to authenticate their identity. Implicit trust between the client and the server (because the client accepts the certificate generated by the server) is an important aspect of TLS. It is extremely important that server authentication is not compromised; however, in reality, self- signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.
- Integrity—With encryption and authentication in place, the TLS protocol does message framing mechanism and signs each message with a Message Authentication Code (MAC). The MAC algorithm does the effective checksum, and the keys are negotiated between the client and the server.

TLS Handshake

Each TLS session begins with a handshake during which the client and server agree on the specific security key and the encryption algorithms to use for that session. At this time, the client also authenticates the server. Optionally, the server can authenticate the client. Once the handshake is complete, transfer of encrypted data can begin.

Encrypting Syslog Traffic with TLS

TLS protocol ensures the syslog messages are securely sent and received over the network. TLS uses certificates to authenticate and encrypt the communication. The client authenticates the server by requesting

its certificate and public key. Optionally, the server can also request a certificate from the client, thus mutual authentication is also possible.

A certificate on the server that identifies the server and the certificate of certificate authority (CA) issued by the server must be available with the client for TLS to encrypt syslog traffic.

For mutual authentication of client and the server, a certificate with the client that identifies the client and the certificate of CA issued by client must be available on the server. Mutual authentication ensures that the syslog server accepts log messages only from authorized clients.

TLS is used as a secure transport to counter all the primary threats to syslog listed below:

- Confidentiality to counter disclosure of the message contents.
- Integrity-checking to counter modifications to a message on a hop-by-hop basis.
- Server or mutual authentication to counter masquerade.

TLS Versions

Following are the versions of TLS:

- TLS version 1.0—Provides secure communication over networks by providing privacy and data integrity between communicating applications
- TLS version 1.1—This enhanced version of TLS provides protection against cipher-block chaining (CBC) attacks.
- TLS version 1.2 — This enhanced version of TLS provides improved flexibility for negotiation of cryptographic algorithms.

TLS Transport Protocol for Syslog Messages Configuration Overview

Starting with Junos OS Release 19.1R1, you can configure an MX series router to use Transport Layer Security (TLS) for syslog messages generated by services that run on the MS-MPC or MS-MIC service cards in an MX series router.

The following services packages are preinstalled and preconfigured on MS-MICs and MS-MPCs:

- Junos Traffic Vision (formerly referred to as Jflow)
- Junos Address Aware (formerly referred to as NAT features)
- Junos VPN Site Secure (formerly referred to as IPsec features)
- Junos Network Secure (formerly referred to as the Stateful Firewall feature)

- Junos Services Crypto Base PIC Package
- Junos Services Application Level Gateways

You can configure a maximum of four syslog servers for each set of services and send encrypted data to the servers.

Syslog messages are sent over a dedicated connection created for a given set of unique configuration parameters:

- Source IP address
- Destination IP address (TCP/TLS server)
- Port
- SSL profile name (For TLS connection)

> **NOTE:** If the ssl-profile is not configured under the tcp-log hierarchy, then it is a non-TLS TCP transport.

> **NOTE:** If there are multiple service sets that have the TCP/TLS logging configuration with the same parameters as mentioned above, the logs generated from the sessions from all those service sets share the same connection.
>
> This feature supports both IPv4 and IPv6.

> **NOTE:** The configured TCP/TLS connection remains up until the configuration is present even if there are no logging events.
>
> TCP/TLS sylog configuration support is provided for secure and reliable logging only on the data plane.
>
> For Aggregated Multi Service (AMS) with multiple active members, each member creates a separate TCP/TLS connection and syslogs generated by each member PIC are sent via their unique connections.

Configuring TCP/TLS for Syslog Messages

You can use the TCP/TLS transport protocols to send syslog messages in a reliable and secure manner to external syslog servers.

To configure the TCP/TLS protocols for syslog messages:

1. Configure the SSL initiation profile.

   NOTE: Configuration of SSL initiation profile is optional if you are not using the TLS/TCP option for syslog messages.

   ```
   [edit services]
   user@router# set ssl initiation profile ssl-init-profile protocol-version all;
   user@router# set ssl initiation profile ssl-init-profile preferred-ciphers strong;
   ```

   protocol-version—Default is set to *all*. When set to *all* SSL version 3 and TLSL version 1 is handled. Default is recommended.

   preferred-ciphers—*strong*—ciphers with key strength >= 168-bits. Use of strong ciphers is recommended.

   See *initiation (Services)* for configuring all the parameters of the initiation statement.

2. Configure the TCP log parameters.

   ```
   [edit services service-set]
   user@router# set ss1 syslog host server -ip  tcp-log source-address ip-address
   ```

   source-address—Source address for tcp logging.

3. Configure SSL profile for TCP logging.

   ```
   [edit services service-set]
   user@router# set ss1 syslog host server -ip tcp-log ssl-profile ssl-profile-name
   ```

   ssl-profile—SSL profile name for tcp logging

   See *profile (SSL Initiation)* for configuring all the options for ssl-profile.

4. [Optional] Configure routing instance name for tcp logging.

```
[edit services service-set]
user@router# set ss1 syslog host server -ip tcp-log vrf-name vrf-name
```

vrf-name—Routing instance name for tcp logging.

5. Commit the configuration.

```
user@router# commit
```

After the commit, the configuration creates a new TCP connection with TLS connection if the SSL profile is configured.

6. Verify the configuration by using the **show services tcp-log connections** command:

```
user@router>show services tcp-log connections
```

```
Interface: ms-2/0/0
Session Id: 1744830467 State: Established
    1.1.1.1 -> 40.0.0.2 : 10214
```

TCP/TLS syslog connection is established with MS-MPC's services L4 data sessions infrastructure and the session's status can be tracked with following command:

```
user@router>show services sessions tcp-log
```

```
ms-2/0/0
Service Set: System, Session: 1744830467, ALG: none, Flags: 0x200000000, IP
Action: no, Offload: no, Asymmetric: no
TCP             1.1.1.1:5229   ->        40.0.0.2:10214  Forward  O
    0
TCP            40.0.0.2:10214  ->         1.1.1.1:5229   Forward  I
15401
```

NOTE: The session-id in both the commands should match as highlighted in **bold** above.

3

CHAPTER

Configuration Statements

adaptive-services

Syntax

```
adaptive-services {
    service-package {
        extension-provider {
            control-cores control-number;
            data-cores data-number;
            data-flow-affinity {
                hash-key (layer-3 | layer-4);
            }
            forwarding-db-size size;
            object-cache-size size;
            package package-name;
            policy-db-size size;
            syslog {
                facility {
                    severity;
                    destination destination;
                }
            }
            wired-max-processes num-procs;
            wired-process-mem-size mem-size;
        }
        layer-2;
        layer-3;
    }
}
```

Hierarchy Level

```
[edit chassis fpc slot-number pic pic-number]
```

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Enable a service package on 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

- Enabling Service Packages | **24**
- Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview | **18**
- *Configuring MS-MPC-Based or MX-SPC3-Based Static HTTP Redirect Services*
- *Configuring MS-MPC-Based or MX-SPC3-Based Converged HTTP Redirect Services*

address

Syntax

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

Hierarchy Level

```
[edit interfaces interface-name unit (Interfaces)  logical-unit-number family (Interfaces) family],
[edit logical-systems logical-system-name interfaces interface-name unit (Interfaces)  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*
>
> *Junos OS Network Interfaces Library for Routing Devices*

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*
- *Configuring Application Sets*
- *Configuring Application Properties*
- *Examples: Configuring Application Protocols*
- *Verifying the Output of ALG Sessions*

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*

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

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

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

close-timeout

Syntax

close-timeout *seconds*;

Hierarchy Level

[edit interfaces *interface-name* services-options]
[edit services service-set *service-set-name* service-set-options tcp-session

Release Information

Statement introduced in Junos OS Release 12.3.
Support for Next Gen Services added in Junos OS Release 19.3R2 on MX Series MX240, MX480 and MX960 using MX-SPC3 services card.

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 | 34

cpu-load-threshold

Syntax

```
cpu-load-threshold percentage;
```

Hierarchy Level

```
[edit interfaces interface-name services-options session-limit]
```

Release Information

Statement introduced in Release 13.2.
Support added in Junos OS Release 19.3R2for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Regulate the usage of CPU resources on services cards. When the CPU usage exceeds the configured value (percentage of the total available CPU resources), the system reduces the rate of new sessions so that the existing sessions are not affected by low CPU availability. The CPU utilization is constantly monitored, and if the CPU usage remains above the configured **cpu-load-threshold** value for a continuous period of 5 seconds, Junos OS reduces the session rate value configured at **edit interfaces *interface-name* services-options session-limit rate** by 10%. This is repeated until the CPU utilization comes down to the configured limit.

Options

percentage—Percentage of total available CPU resources.

Required Privilege Level

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

RELATED DOCUMENTATION

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 | 36

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.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.

Description

Specify the hostname for the system logging utility.

Starting with 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 for ms interface under **[edit interfaces *interface-name* services-options]** hierarchy.

Options

hostname—Name of the system logging utility host machine. This can be the local Routing Engine or an external server address.

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

Applying Filters and Services to Interfaces

inactivity-timeout

Syntax

```
inactivity-timeout seconds;
```

Hierarchy Level

```
[edit interfaces interface-name services-options]
[edit services service-set-name service-set-options]
```

Release Information

Statement introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for MX-SPC3 services card on MX240, MX480 and MX960 routers.

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 | 34

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 | 36

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

open-timeout

Syntax

```
open-timeout seconds;
```

Hierarchy Level

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

```
[edit services service-set service-set-name service-set-options tcp-session]
```

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

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

Options

seconds—Timeout period.

Default: 5 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 | 34

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 | 36

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

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*

services (CoS)

Syntax

```
services cos { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced in Junos OS Release 8.1.

Description
Define the service rules to be applied to traffic.

Options
cos—Identifies the class-of-service set of rules statements.

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

services (IDS)

Syntax

```
services ids { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define the service rules to be applied to traffic.

Options
ids—Identifies the IDS set of rules statements.

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

services (IPsec VPN)

Syntax

```
services ipsec-vpn { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define the service rules to be applied to traffic.

Options
ipsec-vpn—Identifies the IPsec set of rules statements.

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

services (Hierarchy)

Syntax

```
services { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define the service rules to be applied to traffic.

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

RELATED DOCUMENTATION

- *Understanding Service Sets*

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.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.

Description
Specify the system logging severity level.

Starting with 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 for ms interface under **[edit interfaces *interface-name* services-options]** hierarchy.

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

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.

services (L2TP)

Syntax

```
services l2tp { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.

Description
Define the service properties to be applied to traffic.

Options
l2tp—Identifies the L2TP set of services statements.

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

RELATED DOCUMENTATION

- *L2TP Services Configuration Overview*

services (L2TP System Logging)

Syntax

```
services severity-level;
```

Hierarchy Level

```
[edit services l2tp tunnel-group group-name 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 of L2TP Tunnel Activity

services (Stateful Firewall)

Syntax

```
services stateful-firewall { ... }
```

Hierarchy Level

```
[edit]
```

Release Information
Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 10.4.

Description
Define the service rules to be applied to traffic.

Options
stateful-firewall—Identifies the stateful firewall set of rules statements.

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

RELATED DOCUMENTATION

> *Junos Network Secure Overview*.

services (System Logging)

Syntax

```
services severity-level;
```

Hierarchy Level

```
[edit services service-set service-set-name syslog host hostname]
```

Release Information
Statement introduced before Junos OS Release 7.4.
You can configure multiple system log hosts from Junos OS Release 17.4R1 onwards.

Description
Specify the severity level for system logging messages.

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.

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

- **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

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;
    pba-interim-logging-interval seconds;
    reassembly-timeout
    session-limit {
        maximum number;
        rate new-sessions-per-second;
        cpu-load-threshold percentage;
    }
    session-timeout seconds;
    jflow-log {
        message-rate-limit messages-per-second;
    }
    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.

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 Default Timeout Settings for Services Interfaces | 34.

Configuring System Logging for Services Interfaces | 36

service-package

Syntax

```
service-package {
    extension-provider {
        control-cores control-number;
        data-cores data-number;
        data-flow-affinity {
            hash-key (layer-3 | layer-4);
        }
        forwarding-db-size size;
        object-cache-size size;
        package package-name;
        policy-db-size size;
        syslog {
            facility {
                severity;
                destination destination;
            }
        }
        wired-max-processes num-procs;
        wired-process-mem-size mem-size;
    }
    layer-2;
    layer-3;
}
```

Hierarchy Level

[edit chassis fpc *slot-number* pic *pic-number* **adaptive-services**]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced on MX Series 5G Universal Routing Platforms with MS-DPCs in Junos OS Release 9.6.

Description

For adaptive services and multi-services interfaces, enable a service package on the specified Physical Interface Card (PIC).

Options

layer-2—Enable a Layer 2 service package on the specified PIC.

layer-3—Enable a Layer 3 service package on the specified PIC.

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

Enabling Service Packages | 24

Configuring MS-MPC-Based or MX-SPC3-Based Static HTTP Redirect Services

Configuring MS-MPC-Based or MX-SPC3-Based Converged HTTP Redirect Services

session-limit

Syntax

```
session-limit {
    maximum number;
    rate new-sessions-per-second;
    cpu-load-threshold percentage;
}
```

Hierarchy Level

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

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

Restrict the maximum number of sessions and the session rate on services cards.

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

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.

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 | 36

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 | 34

tcp-log

Syntax

```
set services service-set ss1 syslog host server-IP tcp-log
```

Hierarchy Level

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

Description

Configure TCP/TLS for logging syslog events and notifications.

Required Privilege Level

services—To view this statement in the configuration.
services-control—To add this statement to the configuration.