Next Gen Services Interfaces Overview for Routing Devices

Published
2020-01-10

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

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

Table of Contents

4

Next Gen Services SNMP MIBS and Traps

5

Getting Started Configuration Statements

About the Documentation

IN THIS SECTION

Use this guide to get started with Next Gen Services on MX240, MX480 and MX960 routers running the MX-SPC3 services card. It provides basic overview information and procedures to configure and enable Next Gen Services, log system events, as well as, the associated statements and commands.

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 xii 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 xii 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)*

<table>
<tr><th>Convention</th><th>Description</th><th>Examples</th></tr>
<tr><td>*Italic text like this*</td><td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td><td>Configure the machine’s domain name:
[edit]
root@# **set system domain-name** *domain-name*</td></tr>
<tr><td>**Text like this**</td><td>Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.</td><td>• 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**.</td></tr>
<tr><td>< > (angle brackets)</td><td>Encloses optional keywords or variables.</td><td>**stub <default-metric *metric*>;**</td></tr>
<tr><td>| (pipe symbol)</td><td>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.</td><td>**broadcast | multicast**

(*string1* | *string2* | *string3*)</td></tr>
<tr><td># (pound sign)</td><td>Indicates a comment specified on the same line as the configuration statement to which it applies.</td><td>**rsvp { # Required for dynamic MPLS only**</td></tr>
<tr><td>[ ] (square brackets)</td><td>Encloses a variable for which you can substitute one or more values.</td><td>**community name members [*community-ids*]**</td></tr>
<tr><td>Indention and braces ({ })</td><td>Identifies a level in the configuration hierarchy.</td><td rowspan="2">[edit]
routing-options {
  static {
    route default {
      nexthop *address*;
      retain;
    }
  }
}</td></tr>
<tr><td>; (semicolon)</td><td>Identifies a leaf statement at a configuration hierarchy level.</td></tr>
</table>

GUI Conventions

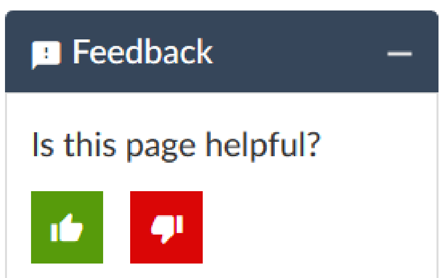
Table 2: Text and Syntax Conventions *(continued)*

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

Documentation Feedback

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

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



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

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

Creating a Service Request with JTAC

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

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

1

CHAPTER

Overview

Next Gen Services Overview

IN THIS SECTION

This topic provides an overview of Next Gen Services and includes the following subjects:

Next Gen Services Features

Next Gen Services provide capabilities for manipulating traffic before it is delivered to its destination. Next Gen Services features run on the MX Series, and are based on a different software architecture than legacy MX Series services. You can run Next Gen Services on MX240, MX480 and MX960 routers. Some Next Gen Services features use different Junos CLI statements than the equivalent legacy service.

> **NOTE:** The only services card that supports Next Gen Services services is the MX-SPC3. If you are running Next Gen Services services, the MX chassis can only use MX-SPC3 services cards. Next Gen Services use their own software architecture, which is not compatible with legacy services.

Table 3 on page 20 provides a summary of Next Gen Services.

Table 3: Next Gen Services Summary

Next Gen Services Supported by MX-SPC3 Services Card	
Carrier Grade NAT	6rd Softwires
	Deterministic NAT
	Dynamic Address-Only Source NAT
	Global System Logging
	IPv4 Connectivity Across IPv6-Only Network Using 464XLAT
	Network Address Port Translation
	Port Forwarding
	Static Source NAT
	Stateful NAT64
	Static Destination NAT
	Stateless Source Network Prefix Translation for IPv6
	Twice NAPT
	Twice Static NAT
	Class of Service
Stateful Firewall Services	
Intrusion Detection Services	
Traffic Load Balancing	
DNS Request Filtering	
Aggregated Multiservices Interfaces	
Inter-chassis High Availability	NAT, Stateful Firewall, and IDS Flows

Table 3: Next Gen Services Summary *(continued)*

Next Gen Services Supported by MX-SPC3 Services Card
See Protocols and Applications Supported by MX-SPC3 Services Card for information about the protocols and applications that the MX-SPC3 supports.

Next Gen Services Documentation

You can run Next Gen Services on the MX240, MX480, and MX960 if you have the MX-SPC3 services card installed in the router. Refer to our TechLibrary for all MX router documentation. For Next Gen Services, refer to the following documentation:

- To get started, see the *Next Gen Services Interfaces Overview for Routing Devices*, which provides a configuration overview of what you need to configure to get started with Next Gen Services. It also includes the basic configuration statements and commands you'll use to perform these steps.
- To learn about and configure Next Gen Services, see *Next Gen Services Interfaces User Guide for Routing Devices*.
- For details on installing or replacing the MX-SPC3 card, see *MX Series 5G Universal Routing Platform Interface Module Reference*.
- To monitor flows and sample traffic — See the *Monitoring, Sampling, and Collection Services Interfaces Feature Guide*, which describes how to configure traffic flow monitoring, packet flow capture, traffic sampling for accounting or discard, port mirroring to an external device, and real-time performance monitoring.
- Broadband Subscriber Services Feature Guide

Enabling Next Gen Services

To run Next Gen Services, you must enable it on the MX Series router. This enables the operating system to run it's own operating system (OS) for Next Gen Services. The Next Gen Service OS does not support running MS-MPC or MS-DPCs services in the same chassis.

There are specific steps you'll need to take if you're migrating your services from legacy services cards to the MX-SPC3. The Next Gen Services CLI differs from these legacy services. For more information, see "Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3" on page 30.

Supported Services Card

The only services card that supports Next Gen Services services is the MX-SPC3. If you are running Next Gen Services services, the MX chassis can only use MX-SPC3 services cards.

You cannot run MS-MPC, MS-MIC or MS-DPC inline services in the same chassis with the MX-SPC3.

Compatibility with Other Services Cards

The MX-SPC3 services card is compatible end-to-end with the MX Series Switch Fabrics, Routing Engines and MS-MPC line cards as described in Table 4 on page 22.

Table 4: MX-SPC3 Services Card Compatibility with MX Series Switch Fabrics, Routing Engines and MPC Line Cards

Switch Fabric	Route Engine	MPC Line Cards
SCBE	RE-S-1800X4-16G-UPG-BB RE-S-1800X4-32G-UB	MPC2E-3D MPC2-3D-NG MPC3E and MPC3E-3D-NG MPC4E-3D MPC-3D-16XGE
SCBE2	RE-S-1800X4-16G-UPG-BB RE-S-1800X4-32G-UB RE-S-X6-64G-UB	MPC2E-3D MPC2-3D-NG MPC3E and MPC3E-3D-NG MPC4E-3D MPC5E and MPC5EQ MPC7E, MPC7EQ, and MPC-3D-16XGE MPC-3D-16XGE

Configuring Interfaces for Next Gen Services

All Next Gen Services are provided by the MX-SPC3 services card. The interfaces on the MX-SPC3 services card are referred to as a virtual multi service (vms) pic and when you configure an interface for a Next Gen Service, you specify the interface as follows:

```
user@host# set services service-set service-set-name interface-service service-interface
  vms-slot-number/pic-number/0.logical-unit-number
```

Aside from the CLI differences, you need to be aware of the basic hardware differences between the MS-MPC and the MX-SPC3. The MS-MPC contains four CPU complexes whereas the MX-SPC3, while more powerful, contains two CPU complexes. Each CPU complex represents a single integrated PIC, meaning that the MS-MPC has four integrated PICs whereas the MX-SPC3 has two integrated PICs.

Because the number of PICs directly affects the number of interfaces, you might need to add logical units to each interface on the MX-SPC3 to increase the number of interfaces to four. For example, if you currently use all four interfaces on the MS-MPC and you have a service set per interface, you can create two logical units per interface on the MX-SPC3 to bring the total number of interfaces to four, and then reassociate the four service sets to these four logical interfaces.

Methods for Applying Services to Traffic

When you configure Next Gen Services, you can apply those services with either of the following methods:

- Apply the configured services to traffic that flows through a particular interface on the MX router.
- Apply the configured services to traffic that is destined for a particular next hop.

RELATED DOCUMENTATION

Enabling and Disabling Next Gen Services | 24

Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

Enabling and Disabling Next Gen Services

IN THIS SECTION

To use Next Gen Services, you must first enable it on the MX Series router. This topic describes how to enable Next Gen Services, how to disable Next Gen Services, and how to determine whether Next Gen Services is enabled or disabled on your system.

Enabling Next Gen Services on an MX Series Router

There are specific steps you'll need to take if you're migrating your services from MS-MPC cards to the MX-SPC3 services cards. The Next Gen Services CLI differs from these legacy services.

The following procedure is a general procedure for enabling and disabling Next Gen Services.

Before you do anything, you'll need to back up your configuration.

For more details on the differences between the configuration of the MX-SPC3 services card and legacy services cards, see "Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3" on page 30 and plan your migration appropriately.

You can run Next Gen Services on the MX240, MX480 and MX960 using the MX-SPC3 services card. To use Next Gen Services on the MX Series, you must first enable Next Gen Services:

1. Delete any router configuration that is for services. This includes configuration under the **[edit services]** hierarchy, configuration for services interfaces, and any configuration that refers to services interfaces.

2. Enable Next Gen Services.

```
user@host> request system enable unified-services
```

3. When the following message appears, enter **yes**.

```
Before enabling unified services, please move to baseline configuration.
Are above conditions satisfied ? [yes,no]
```

4. Reboot the MX Series chassis.

```
user@host> request system reboot
```

Disabling Next Gen Services on an MX Series Router

To disable Next Gen Services on the MX Series:

1. Delete any router configuration that is for services. This includes configuration under the **[edit services]** hierarchy, configuration for services interfaces, and any configuration that refers to services interfaces.

2. Disable Next Gen Services.

```
user@host> request system disable unified-services
```

3. When the following message appears, enter **yes**.

```
Before disabling unified services, please move to baseline configuration.
Are above conditions satisfied ? [yes,no]
```

```
Unified-Services downgrade staged. Please reboot with 'request system reboot'
command to complete the downgrade

WARNING: cli has been replaced by an updated version:
CLI release 20190829.221548_builder.r1052644 built by builder on 2019-08-29
22:27:13 UTC
Restart cli using the new version ? [yes,no] (yes)
```

4. Reboot the MX Series chassis.

```
user@host> request system reboot
```

Determining Whether Next Gen Services is Enabled on an MX Series Router

To determine whether Next Gen Services is enabled:

- Enter the following command:

```
user@host> show system unified-services status
```

  One of the following messages appears:

  - **Enabled**—Next Gen Services is enabled and ready to use.
  - **Unified Services : Upgrade staged , please reboot with 'request system reboot' to enable unified services.**—You must perform a system reboot before Next Gen Services is enabled.
  - **Disabled**—Next Gen Services is disabled.
  - **Unified Services : Upgrade staged , please reboot with 'request system reboot' to disable unified services.**—You must perform a system reboot before Next Gen Services is disabled.

RELATED DOCUMENTATION

Next Gen Services Overview | 19
Next Gen Services Feature Configuration Overview | 29
Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

2

CHAPTER

Configuration Overview

Next Gen Services Feature Configuration Overview

IN THIS SECTION

To configure services with Next Gen Services, you need to configure the following objects:

- Service rules
- Service sets
- Services interfaces

Service Rules and Rule Sets

Service rules specify a set of matching conditions and a set of actions to apply to traffic when it matches the conditions. For example, a stateful firewall rule can specify a destination address that must be matched, and take the action of dropping packets that have that destination address.

Service rule sets consist of a group of services rules that belong to the same category. For example, a stateful firewall rule set consists of stateful firewall rules.

Service Sets

A service set specifies one or more service rules or rule sets to apply to traffic. The service set also specifies a services interface, which indicates where the services processing is performed.

A service set is either an interface-style service set or a next-hop-style service set.

Interface-Style Service Set

The service set applies the service rules to all traffic that flows through a particular interface.

Next-Hop-Style Service Set

The service set applies the service rules to traffic that is destined for a particular next hop. You must redirect the next-hop traffic to the services interface that the service set uses.

Services Interfaces

A services interface indicates where a service is applied to traffic. Services interfaces are not physical links to external devices.

If a service is performed on an MX-SPC3 services card, the service interface has the format:

```
vms-slot-number/pic-number/port-number
```

If a service is performed on a line card's PFE (inline services), the service interface has the format si-*slot-number*/*pic-number*/0.

RELATED DOCUMENTATION

Next Gen Services Overview | 19
How to Configure Services Interfaces for Next Gen Services | 77
Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3

IN THIS SECTION

Overview

Next Gen Services on the MX-SPC3 require you to configure services differently from what you are accustomed to on MX series routers. These changes more closely align the way you configure services on the MX Series router with the way you configure similar services on the SRX Series services gateway. Once you are familiar with this more unified approach, you should be able to configure services on these two platforms in a more seamless fashion, ultimately resulting in less training overhead and lower risk of configuration error.

Aside from the CLI differences, you need to be aware of the basic hardware differences between the MS-MPC and the MX-SPC3. The MS-MPC contains four CPU complexes whereas the MX-SPC3, while more powerful, contains two CPU complexes. Each CPU complex represents a single integrated PIC, meaning that the MS-MPC has four integrated PICs whereas the MX-SPC3 has two integrated PICs.

Because the number of PICs directly affects the number of interfaces (Table 5 on page 31), you might need to add logical units to each interface on the MX-SPC3 to increase the number of interfaces to four. For example, if you currently use all four interfaces on the MS-MPC and you have a service set per interface, you can create two logical units per interface on the MX-SPC3 to bring the total number of interfaces to four, and then reassociate the four service sets to these four logical interfaces.

Table 5: Hardware Differences: MS-MPC versus MX-SPC3

	MS-MPC	MX-SPC3
number of CPU complexes	4	2
number of PICs per CPU complex	1	1
number of interfaces per PIC	1	1
total number of interfaces on card	4	2

NOTE: See the MX Series 5G Universal Routing Platform Interface Module Reference for more information on the MX-SPC3 hardware.

The following sections provide an overview of the basic configuration differences between services on the MS-MPC and services on the MX-SPC3. The intent of these sections is to help you get started by using basic examples to illustrate the major changes. These examples show a subset of the CLI configuration options and do not replace the more formal treatment of the subject matter found in the Next Gen Services Interfaces User Guide for Routing Devices and the Junos OS CLI Reference Guide.

The configuration examples in these sections are presented side-by-side so you can easily see the differences between the two. The examples are intended to show you how to configure existing MS-MPC features on the MX-SPC3. The examples are not intended to show you how to configure new features only found on the MX-SPC3. For legibility and ease of comparison, the order of statements presented might differ slightly from the actual order of statements displayed in the CLI.

If you have a large set of existing legacy services, we recognize that these changes might be an inconvenience to you. To help you migrate from the MS-MPC to the MX-SPC3, we suggest that you proceed as follows:

- Look through the examples in this guide to get an overall view of the changes required.
- Look through the set of configuration examples in knowledge base article KB35348.
- Look through the Next Gen Services Interfaces User Guide for Routing Devices and the Junos OS CLI Reference Guide to understand all the features, configuration options, and syntax.
- Contact JTAC for help with your migration.

You do not need to make these configuration changes if you continue to run legacy services on the MS-MPC. However, once you deploy the MX-SPC3 on a router, you must replace all MS-MPCs on that router and reconfigure your services to align with the Next Gen Services configuration paradigm.

Interfaces

The **ms** interfaces on MS-MPC cards are called **vms** interfaces on MX-SPC3 cards. There are no changes to the names of **ams** and **mams** interfaces.

In addition, a number of parameters that are configured under **services-options** on an **ms** interface are configured under **service-set-options** in a service set.

Table 6 on page 33 shows examples of these changes.

Table 6: Interfaces and Service Options

MS-MPC	MX-SPC3

[edit interfaces]
ms-5/1/0 {
<...>
}
	[edit interfaces]
	# Change interface name to vms.
	vms-5/1/0 {
	<...>
	}

[edit interfaces]
ms-5/1/0 {
services-options {
open-timeout 40;
close-timeout 40;
inactivity-tcp-timeout 10;
inactivity-asymm-tcp-timeout 10;
tcp-tickles 8;
ignore-errors tcp;
}
}
	[edit services]
	service-set sset1 {
	service-set-options {
	# Set tcp parameters under tcp-session.
	tcp-session {
	open-timeout 40;
	close-timeout 40;
	inactivity-tcp-timeout 10;
	inactivity-asymm-tcp-timeout 10;
	tcp-tickles 8;
	ignore-errors tcp;
	}
	}
	}

[edit interfaces]
ms-5/1/0 {
services-options {
inactivity-non-tcp-timeout 40;
session-timeout 10;
}
}
	[edit services]
	service-set sset1 {
	# Set non-tcp parameters directly under
	# service-set-options.
	service-set-options {
	inactivity-non-tcp-timeout 40;
	session-timeout 10;
	}
	}

[edit interfaces]
ms-5/1/0 {
services-options {
fragment-limit 32;
reassembly-timeout 3;
}
}
	These parameters are hardcoded as follows:
	• fragment-limit 62
	• reassembly-timeout 2

Table 6: Interfaces and Service Options *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>[edit interfaces]
ms-5/1/0 {
    services-options {
        session-limit {
            maximum 100;
            cpu-load-threshold 12;
            rate 10;
        }
    }
}</pre></td><td><pre>[edit services]
# Maximum number of sessions can be
# specified per service-set.
service-set sset1 {
    service-set-options {
        session-limit {
            maximum 100;
        }
    }
}

[edit interfaces]
# All session-limit parameters continue to be
# configurable per interface. If the maximum
# number of sessions is different from the associated
# service-set, the smaller number takes effect.
vms-5/1/0 {
    services-options {
        session-limit {
            maximum 100;
            cpu-load-threshold 12;
            rate 10;
        }
    }
}</pre></td></tr>
<tr><td><pre>[edit interfaces]
ms-5/1/0 {
    services-options {
        pba-interim-logging-interval 10;
    }
}</pre></td><td><pre>[edit interfaces]
# Set interim-logging-interval under the nat branch.
nat {
    source {
        pool src-pool {
            port {
                block-allocation {
                    interim-logging-interval 10;
                }
            }
        }</pre></td></tr>
</table>

Table 6: Interfaces and Service Options *(continued)*

MS-MPC	MX-SPC3

[edit interfaces]
ms-5/1/0 {
services-options {
syslog {
host {
<...>
}
}
}
}
	See **service-set syslog stream host**.

[edit interfaces]
ms-5/1/0 {
services-options {
syslog {
message-rate-limit 10;
}
}
}
	[edit services]
	service-set sset1 {
	syslog {
	event-rate 10;
	}
	}

[edit interfaces]
ms-5/1/0 {
services-options {
ignore-errors alg;
disable-global-timeout-override;
trio-flow-offload {
minimum-bytes 1000;
}
}
}
	Not supported

Service Set

Table 7 on page 36 shows minor changes in the way some **service-set** parameters are configured.

Table 7: Service Set

MS-MPC	MX-SPC3

[edit services]
service-set sset1 {
tcp-mss 1460;
service-set-options {
tcp-non-syn drop-flow-send-rst;
tcp-fast-open drop;
}
}
	[edit services]
	service-set sset1 {
	service-set-options {
	# Set tcp parameters under tcp-session.
	tcp-session {
	tcp-mss 1460;
	tcp-non-syn drop-flow-send-rst;
	tcp-fast-open drop;
	}
	}
	}

[edit services]
service-set sset1 {
replicate-services {
replication-threshold 180;
}
}
	[edit interfaces]
	# Set replication-threshold on the interface.
	vms-5/1/0 {
	redundancy-options {
	replication-threshold 180;
	}
	}

[edit services]
service-set sset1 {
syslog {
host 10.1.1.1 {
port 514;
}
}
}
	[edit services]
	service-set sset1 {
	syslog
	# Process security logs in the dataplane.
	mode stream;
	stream s1 {
	# Specify host to send security logs to.
	host {
	10.1.1.1;
	port 514;
	}
	}
	}
	}

Table 7: Service Set *(continued)*

MS-MPC	MX-SPC3

[edit services]
service-set sset1 {
  syslog {
    host local;
  }
}
	[edit services]
	service-set sset1 {
	  syslog
	    # Process security logs in the control plane,
	    # saving logs to local file specified by rtlog.
	    mode event;
	  }
	}
	rtlog {
	  traceoptions {
	    # Specify filename for logs.
	    file rtlog size 1g;
	    flag all;
	  }
	}

[edit services]
service-set sset1 {
  service-order <...>
}
	Service order is fixed.

[edit services]
service-set sset1 {
  sampling-service <...>
}
	J-Flow logging is supported inline.

[edit services]
service-set sset1 {
  tag-rule-sets <...>
  tag-rules <...>
  hcm-profile <...>
  hcm-url-rule-sets <...>
  hcm-url-rules <...>
  service-set-options {
    bypass-traffic-on-pic-failure;
  }
}
	Currently unsupported

Stateful Firewall

Rules and Policies

Stateful firewall rules for Next Gen Services on the MX-SPC3 are structured slightly differently from stateful firewall rules for services on the MS-MPC. On the MX-SPC3, you enclose the rules within a **policies** wrapper, and you define the match terms and actions for the rule in a **policy** contained within the rule.

Just like a stateful firewall service on the MS-MPC, you create a service set to associate an interface with a rule set. A rule set contains references to one or more rules. Rules are applied sequentially in the order that you list them until a match occurs and an action taken.

Each rule contains one or more pairs of match terms and actions. On the MX-SPC3, each pair of match terms and actions is called a policy. Policies are applied sequentially in the order that you specify them until a match occurs and an action taken.

Table 8 on page 38 shows the configuration differences between stateful firewall rules on the MS-MPC and the MX-SPC3. In particular, note the different definitions for the **permit**/**deny**/**reject** actions.

Table 8: Stateful Firewall Rules and Policies

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set s1 {
stateful-firewall-rule-sets
rule-set-basic-sfw;
interface-service {
service-interface ms-1/1/0;
}
}
	service-set s1 {
	stateful-firewall-rule-sets rule-set-basic-sfw;
	interface-service {
	service-interface vms-1/1/0;
	}
	}

stateful-firewall {	# Enclose stateful firewall rules within the policies wrapper. policies {

Table 8: Stateful Firewall Rules and Policies *(continued)*

MS-MPC	MX-SPC3

rule Rule1 {
match-direction input;
term ping-https-apps {
from {
source-address {
any
}
destination-address {
any
}
applications [junos-icmp-ping
junos-https];
}
then {
accept/reject/discard
skip-ids;
syslog;
}
}
term accept {
then {
accept;
}
}
} # end Rule1
	stateful-firewall-rule Rule1 {
	match-direction input;
	# Define match terms and actions in a policy.
	policy ping-https-apps {
	# Unlike the from statement, the match statement (and
	# source-address, destination-address, and application)
	# are mandatory.
	match {
	source-address any;
	destination-address any;
	application [junos-icmp-ping junos-https];
	}
	then {
	# permit = allow
	# deny = silently drop
	# reject = drop and send ICMP unreachable or TCP RST
	permit/deny/reject
	# skip-ids is not supported. One possible way of
	# achieving this same goal is to create two
	# service-sets, one with IDS and one without IDS,
	# and route your next-hop-service
	# traffic to the desired service set via the associated
	# inside or outside interface.
	log;
	}
	}
	policy accept {
	match {
	source-address any;
	destination-address any;
	application any;
	}
	then {
	permit;
	}
	}
	} # end Rule1

Table 8: Stateful Firewall Rules and Policies *(continued)*

MS-MPC	MX-SPC3

rule Rule2 {
match-direction output;
term local {
from {
source-address {
10.1.3.2/32;
}
application-sets APPL-SET1;
}
then {
accept;
}
}
} # end Rule2
	stateful-firewall-rule Rule2 {
	match-direction output;
	policy local {
	match {
	source-address 10.1.3.2/32;
	destination-address any;
	# application can refer to an application set.
	application APPL-SET1;
	}
	then {
	permit;
	}
	}
	} # end Rule2

rule-set rule-set-basic-sfw {
rule Rule1;
rule Rule2;
}
} # end stateful-firewall
	# Use the stateful-firewall-rule-set element to list the
	# firewall rules in the order that you want them applied.
	stateful-firewall-rule-set rule-set-basic-sfw {
	stateful-firewall-rule Rule1;
	stateful-firewall-rule Rule2;
	}
	} # end policies

Address Lists and Ranges

Stateful firewall rules can contain match terms that refer to address ranges and lists.

On the MS-MPC, you use **source-address-range** and **destination-address-range** elements to specify address ranges and **prefix-list** elements under **policy-options** to specify address lists. The **prefix-list** element is not for use solely for stateful firewall rules. You also use the **prefix-list** element to specify address lists for use within routing policies.

On the MX-SPC3, the **prefix-list** element is not used for stateful firewall rules. You use an **address-book** under **services** to define address lists and ranges for use within stateful firewall rules. The **prefix-list** element still exists, but is used exclusively for routing policies. You therefore need to configure both **address-book** and **prefix-list** elements if you are specifying address lists for stateful firewall rules and address lists for routing policies.

Table 9 on page 41 shows the differences between how you specify addresses for stateful firewall rules on the MS-MPC versus the MX-SPC3.

Table 9: Addresses

MS-MPC	MX-SPC3

[edit]
policy-options {
prefix-list p1 {
10.1.22.45/32;
192.168.0.11/32;
}
}
 	
[edit services]
stateful-firewall {
rule sfw-rule {
match-direction input;
term banned-addresses {
from {
source-prefix-list {
p1;
}
source-address-range {
low 10.1.22.100 high
10.1.22.109;
}
}
then {
reject;
syslog;
}
}
<...>
	[edit services]
	# Define address lists and address ranges in an address book.
	address-book {
	global {
	address-set p1 {
	address p1-a;
	address p1-b;
	}
	address p1-a 10.1.22.45/32;
	address p1-b 192.168.0.11/32;
	address p2 {
	address-range 10.1.22.100/32 {
	to {
	10.1.22.109/32;
	}
	}
	}
	}
	} # end address-book
	policies {
	stateful-firewall-rule sfw-rule {
	match-direction input;
	policy banned-addresses {
	match {
	# Refer to the addresses defined in the address book.
	source-address [p1 p2];
	destination-address any;
	application any;
	}
	then {
	deny;
	log;
	}
	<...>

Applications

The MX-SPC3 supports more built-in Junos applications than the MS-MPC. You can match on these built-in applications when you create a stateful firewall rule.

To see the complete list of built-in applications, use the **show groups junos-defaults applications** configuration mode command. For example:

```
[edit]
# show groups junos-defaults applications | match junos
application junos-ftp {
application junos-ftp-data {
application junos-tftp {
application junos-twamp {
application junos-rtsp {
application junos-netbios-session {

<...>
```

Traceoptions and Counters

Stateful firewalls for Next Gen Services on the MX-SPC3 support additional capabilities to help debug and count traffic:

- **traceoptions -** Use to trace policy-related events such as policy lookups and rules-based events. The events are captured in the specified file for viewing.
- **count -** Use to count traffic-related events such as incoming/outgoing bytes and packets. View the counters using show commands:
  - **show services policies detail -** the output includes traffic-related counters when you specify the **count** option in your policy
  - **show services policies hit-count -** the hit count is always available regardless of whether you use the **count** option in your policy or not

Table 10 on page 43 shows how to use the **traceoptions** and **count** elements:

Table 10: Traceoptions and Count

MS-MPC	MX-SPC3

Not supported	[edit services]
	policies {
	# Enable traceoptions to trace policy-related events.
	  traceoptions {
	    file policylogs size 10m files 5;
	    flag all;
	  }
	  stateful-firewall-rule Rule1 {
	    match-direction input;
	    policy my-policy {
	      match {
	        source-address any;
	        destination-address any;
	        application [junos-dns-udp junos-dns-tcp];
	      }
	      then {
	        permit
	        # Enable counting of traffic events.
	        count;
	      }
	    } # end my-policy
	  ...

Carrier Grade Network Address Translation (CGNAT)

Configuring NAT for Next Gen Services on the MX-SPC3 is different from configuring NAT on legacy services on the MS-MPC in a number of ways:

- On the MX-SPC3, you configure source NAT separately from destination NAT. You configure source NAT in the source branch of the configuration tree and you configure destination NAT in the destination branch of the configuration tree. Source NAT and destination NAT each has its own sets of address pools and rules in its respective branch of the configuration tree.
- On the MX-SPC3, if you configure both source NAT and destination NAT, destination NAT applies first, and then source NAT applies to the destination NAT translated result. In other words, you write the source NAT rule not based on the original packet, but based on the destination NAT translated result.

- On the MX-SPC3, you do not explicitly configure a **translation-type**. The type of translation is determined implicitly by your configuration.
- On the MX-SPC3, port translation is the default behavior for dynamic mappings (where different pre-NAT addresses might map to the same post-NAT address over time). If you do not explicitly include the **port** statement in a pool definition, port translation takes place with a port range [1024, 65535], and the port is selected in a round robin fashion. If you do not want port translation to take place, you must add a **port** statement with the **no-translation** option. This default does not apply to static mappings where a pre-NAT address always maps to the same post-NAT address.

Table 11 on page 44 through Table 23 on page 65 show examples of how the different translation types are configured on the MX-SPC3.

Table 11: Example: Basic-NAT44

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>[edit services]</pre></td><td><pre>[edit services]</pre></td></tr>
<tr><td><pre>service-set sset1 {
    nat-rules rule-basic-nat44;
    interface-service {
        service-interface ms-1/2/0;
    }
}</pre></td><td><pre>service-set sset1 {
    nat-rule-sets rule-basic-nat44;
    interface-service {
        service-interface vms-2/0/0;
    }
}</pre></td></tr>
<tr><td><pre>nat {</pre></td><td><pre>nat {
    source {</pre></td></tr>
<tr><td><pre>   pool src-pool {
        address 10.10.10.0/24;
    }</pre></td><td><pre>   pool src-pool {
            address {
                10.10.10.0/24;
            }
            # host-address-base indicates a type of static mapping
            # where the base address 10.45.1.0/32 maps to the
            # lowest address in the pool, namely 10.10.10.0/32,
            # and the other addresses map sequentially from there
            # e.g. 10.45.1.1 maps to 10.10.10.1, and so on.
            # Since this is a static mapping, there is no port translation
            # by default.
            # Note that host-address-base does not have to be the
            # lowest address allowed by the subsequent source rule.
            # Any packet with a source address allowed by the source rule
            # but is lower than the host-address-base is discarded.
            host-address-base 10.45.1.0/32;
        }</pre></td></tr>
</table>

Table 11: Example: Basic-NAT44 *(continued)*

MS-MPC	MX-SPC3

rule rule-basic-nat44 {
match-direction input;
term t1 {
from {
source-address {
10.45.1.0/24
}
}
then {
translated {
source-pool src-pool;
translation-type {
basic-nat44;
}
}
}
}
}
	rule-set rule-basic-nat44 {
	match-direction input;
	rule r1 {
	match {
	source-address 10.45.1.0/24;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

} # end nat	} # end source } # end nat

Table 12: Example: Basic-NAT66

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-basic-nat66;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-basic-nat66;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

pool src-pool {
address 2001:DB8:2222::0/128;
}
	pool src-pool {
	address {
	2001:DB8:2222::0/128;
	}
	}

Table 12: Example: Basic-NAT66 *(continued)*

MS-MPC	MX-SPC3

rule rule-basic-nat66 {
      match-direction input;
      term t1 {
        from {
          source-address {
            2001:DB8:1111::0/128;
          }
        }
        then {
          translated {
            source-pool src-pool;
            translation-type {
              basic-nat66;
            }
          }
        }
      }
    }
	rule-set rule-basic-nat66 {
	      match-direction input;
	      rule r1 {
	        match {
	          source-address 2001:DB8:1111::0/128;
	        }
	        then {
	          source-nat {
	            pool {
	              src-pool;
	            }
	          }
	        }
	      }
	    }

} # end nat	} # end source } # end nat

Table 13: Example: Dynamic-NAT44

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
  nat-rules rule-dynamic-nat44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
	service-set sset1 {
	  nat-rule-sets rule-dynamic-nat44;
	  interface-service {
	    service-interface vms-2/0/0;
	  }
	}

nat {	nat { source {

Table 13: Example: Dynamic-NAT44 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td>
<pre>
pool src-pool {
    address-range low 10.10.10.2 high
        10.10.10.10;
}
</pre>
</td><td>
<pre>
pool src-pool {
    address {
        10.10.10.2/32 to 10.10.10.10/32;
    }
    # Since this is implicitly a dynamic mapping,
    # there is port translation by default , so we need to
    # explictly specify that we don’t want port translation.
    port {
        no-translation;
    }
}
</pre>
</td></tr>
<tr><td>
<pre>
rule rule-dynamic-nat44 {
    match-direction input;
    term t0 {
        from {
            applications junos-icmp-all;
        }
        then {
            no-translation;
        }
    }
    term t1 {
        from {
            destination-address {
                10.99.0.2/32;
            }
            source-address-range {
                low 10.45.0.2 high 10.45.0.10;
            }
        }
        then {
            translated {
                source-pool src-pool;
                translation-type {
                    dynamic-nat44;
                }
            }
        }
    }
}
</pre>
</td><td>
<pre>
rule-set rule-dynamic-nat44 {
    match-direction input;
    rule r0 {
        match {
            source-address 0.0.0.0/32;
            application junos-icmp-all;
        }
        then {
            source-nat {
                off;
            }
        }
    }
    rule r1 {
        match {
            source-address-name addr1;
            destination-address 10.99.0.2/32;
        }
        then {
            source-nat {
                pool {
                    src-pool;
                }
            }
        }
    }
}
</pre>
</td></tr>
</table>

Table 13: Example: Dynamic-NAT44 *(continued)*

MS-MPC	MX-SPC3
} # end nat	} # end source } # end nat

	address-book {
	  global {
	    address addr1 {
	      address-range 10.45.0.2/32 {
	        to {
	          10.45.0.10/32;
	        }
	      }
	    }
	  }
	}

Table 14: Example: NAPT-44

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
  nat-rules rule-napt44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
	service-set sset1 {
	  nat-rule-sets rule-napt44;
	  interface-service {
	    service-interface vms-2/0/0;
	  }
	}

nat {	nat { source {

pool src-pool {
    address 10.10.10.0/24;
    port {
      automatic;
    }
  }
	pool src-pool {
	      address {
	        10.10.10.0/24;
	      }
	      # Since this is implicitly a dynamic mapping,
	      # and there is no explicit port statement
	      # to indicate otherwise, the default port
	      # mapping behavior takes effect.
	    }

Table 14: Example: NAPT-44 *(continued)*

MS-MPC	MX-SPC3

rule rule-napt44 {
match-direction input;
term t1 {
from {
source-address {
10.45.1.0/24
}
application-sets accept-algs;
}
then {
translated {
source-pool src-pool;
translation-type {
napt44;
}
}
}
}
}
	rule-set rule-napt44 {
	match-direction input;
	rule r1 {
	match {
	source-address 10.45.1.0/24;
	application accept-algs;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

} # end nat	} # end source } # end nat

Table 15: Example: napt-66

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-napt66;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-napt66;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

Table 15: Example: napt-66 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>
    pool src-pool {
        address 2001:DB8:2222::0/112;
        port {
            range low 20000 high 30000;
        }
    }
</pre></td><td><pre>
    pool src-pool {
        address {
            2001:DB8:2222::0/112;
        }
        port {
            range {
                20000;
                to {
                    30000;
                }
            }
        }
    }
</pre></td></tr>
<tr><td><pre>
    rule rule-napt66 {
        match-direction input;
        term t1 {
            from {
                source-address {
                    2001:DB8:1111::0/96;
                }
            }
            then {
                translated {
                    source-pool src-pool;
                    translation-type {
                        napt66;
                    }
                }
            }
        }
    }
</pre></td><td><pre>
    rule-set rule-napt66 {
        match-direction input;
        rule r1 {
            match {
                source-address 2001:DB8:1111::0/96;
            }
            then {
                source-nat {
                    pool {
                        src-pool;
                    }
                }
            }
        }
    }
</pre></td></tr>
<tr><td><pre>
} # end nat
</pre></td><td><pre>
    } # end source
} # end nat
</pre></td></tr>
</table>

Table 16: Example: Deterministic NAT-44

MS-MPC	MX-SPC3
[edit services]	[edit services]

Table 16: Example: Deterministic NAT-44 *(continued)*

MS-MPC	MX-SPC3

service-set sset1 {
  nat-rules rule-dnat-44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
	service-set sset1 {
	  nat-rule-sets rule-dnat-44;
	  interface-service {
	    service-interface vms-2/0/0;
	  }
	}

nat {	nat { destination {

pool dest-pool {
  address 10.10.10.2/32;
}
	pool dest-pool {
	  address {
	    10.10.10.2/32;
	  }
	}

rule rule-dnat-44 {
  match-direction input;
  term t1 {
    from {
      destination-address {
        10.45.0.2/32
      }
    }
    then {
      translated {
        destination-pool dest-pool;
        translation-type {
          dnat-44;
        }
      }
    }
  }
}
	rule-set rule-dnat-44 {
	  match-direction input;
	  rule r1 {
	    match {
	      destination-address 10.45.0.2/32;
	    }
	    then {
	      destination-nat {
	        pool {
	          dest-pool;
	        }
	      }
	    }
	  }
	}

} # end nat	} # end destination } # end nat

Table 17: Example: Stateful-NAT464

MS-MPC	MX-SPC3
[edit services]	[edit services]

Table 17: Example: Stateful-NAT464 *(continued)*

MS-MPC	MX-SPC3

service-set sset1 {
nat-rules rule-stateful-nat464;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-stateful-nat464-src;
	nat-rule-sets rule-stateful-nat464-dest;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

pool src-pool {
address 10.10.10.0/24;
port {
automatic;
}
}
	pool src-pool {
	address {
	10.10.10.0/24;
	}
	port {
	automatic {
	round-robin;
	}
	}
	}

Table 17: Example: Stateful-NAT464 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>
    rule rule-stateful-nat464 {
      match-direction input;
      term t1 {
        from {
          source-address {
            2001:DB8:1111::0/96;
          }
          destination-address {
            2001:DB8:2222::0/96;
          }
          applications [junos-icmp-all
            junos-icmp-ping junos-traceroute
            junos-traceroute-ttl 1];
        }
        then {
          translated {
            source-pool src-pool;
            clat-prefix 2001:DB8:1111::0/96;
            destination-prefix
              2001:DB8:2222::0/96;
            translation-type {
              stateful-nat464;
            }
          }
        }
      }
    }
</pre></td><td><pre>
    # This source rule applies after the destination rule.
      rule-set rule-stateful-nat464-src {
        match-direction input;
        rule r1 {
          match {
            source-address 2001:DB8:1111::0/96;
            # Since destination NAT happens first, the
            # destination IPv6 prefix has been stripped off,
            # resulting in an IPv4 destination address.
            destination-address 0.0.0.0/32;
            application [junos-icmp-all junos-icmp-ping
              junos-traceroute junos-traceroute-ttl 1];
          }
          then {
            source-nat {
              pool {
                src-pool;
              }
              clat-prefix 2001:DB8:1111::0/96;
            }
          }
        }
      }
</pre></td></tr>
<tr><td><pre>
  } # end nat
</pre></td><td><pre>
    } # end source
</pre></td></tr>
<tr><td></td><td><pre>
    destination {
</pre></td></tr>
</table>

Table 17: Example: Stateful-NAT464 *(continued)*

MS-MPC	MX-SPC3

	# This destination rule applies before the source rule.
	rule-set rule-stateful-nat464-dest {
	match-direction input;
	rule r1 {
	match {
	destination-address 2001:DB8:2222::0/96;
	}
	then {
	destination-nat {
	destination-prefix 2001:DB8:2222::0/96;
	}
	}
	}
	}

	} # end destination } # end nat

Table 18: Example: Stateful-NAT64

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-stateful-nat64;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-stateful-nat64-src;
	nat-rule-sets rule-stateful-nat64-dest;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

Table 18: Example: Stateful-NAT64 *(continued)*

MS-MPC	MX-SPC3

pool src-pool {
    address 10.10.10.0/24;
    port {
        automatic;
            random-allocation;
        }
    }
    mapping-timeout 500;
}
	pool src-pool {
	    address {
	        10.10.10.0/24;
	    }
	    port {
	        automatic {
	            random-allocation;
	        }
	    }
	    mapping-timeout 500;
	}

Table 18: Example: Stateful-NAT64 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td>rule rule-stateful-nat64 {
match-direction input;
term t1 {
from {
destination-address {
2001:DB8:2222::0/64;
}
}
then {
translated {
source-pool src-pool;
destination-prefix
2001:DB8:2222::0/64;
translation-type {
stateful-nat64;
}
}
}
}
term t2 {
from {
destination-address {
2001:DB8:3333::0/64;
}
}
then {
translated {
source-pool src-pool;
destination-prefix
2001:DB8:3333::0/64;
translation-type {
stateful-nat64;
}
}
}
}
}</td><td># This source rule applies after the destination rule.
rule-set rule-stateful-nat64-src {
match-direction input;
rule r1 {
match {
source-address 0::0/128;
Since destination NAT applies first, the
destination address is now IPv4.
destination-address 0.0.0.0/32;
}
then {
source-nat {
pool {
src-pool;
}
}
}
}
}</td></tr>
<tr><td>} # end nat</td><td>} # end source</td></tr>
<tr><td></td><td>destination {</td></tr>
</table>

Table 18: Example: Stateful-NAT64 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td></td><td><pre>
# This destination rule applies before the source rule.
  rule-set rule-stateful-nat64-dest {
    match-direction input;
    rule r1 {
      match {
        destination-address 2001:DB8:2222::0/64;
      }
      then {
        destination-nat {
          destination-prefix 2001:DB8:2222::0/64;
        }
      }
    }
    rule r2 {
      match {
        destination-address 2001:DB8:3333::0/64;
      }
      then {
        destination-nat {
          destination-prefix 2001:DB8:3333::0/64;
        }
      }
    }
  }
</pre></td></tr>
<tr><td></td><td><pre>
  } # end destination
} # end nat
</pre></td></tr>
</table>

Table 19: Example: Twice-Basic-NAT-44

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td>[edit services]</td><td>[edit services]</td></tr>
<tr><td><pre>
service-set sset1 {
  nat-rules rule-twice-basic-nat-44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
</pre></td><td><pre>
service-set sset1 {
  nat-rule-sets rule-twice-basic-nat-44-src;
  nat-rule-sets rule-twice-basic-nat-44-dest;
  interface-service {
    service-interface vms-2/0/0;
  }
}
</pre></td></tr>
</table>

Table 19: Example: Twice-Basic-NAT-44 *(continued)*

MS-MPC	MX-SPC3
nat {	nat { source {

pool src-pool {
address 10.98.10.0/24;
}
pool dest-pool {
address 10.99.10.0/24;
}
	pool src-pool {
	address {
	10.98.10.0/24;
	}
	# host-address-base indicates a type of static mapping where
	# the base address 10.10.10.0/32 maps to the lowest
	# address in the pool, namely 10.98.10.0/32,
	# and the other addresses map sequentially from there
	# e.g. 10.10.10.1 maps to 10.98.10.1, and so on.
	# Since this is a static mapping, there is no port translation
	# by default.
	# Note that host-address-base does not have to be the
	# lowest address allowed by the subsequent source rule.
	# Any packet with a source address allowed by the source rule
	# but is lower than the host-address-base is discarded.
	host-address-base 10.10.10.0/32;
	}

rule rule-twice-basic-nat-44 {
match-direction input;
term t1 {
from {
source-address {
10.10.10.0/24;
}
destination-address {
10.20.10.0/24;
}
}
then {
translated {
source-pool src-pool;
destination-pool dest-pool;
translation-type {
twice-basic-nat-44;
}
}
}
}
}
	# This source rule applies after the destination rule.
	rule-set rule-twice-basic-nat-44-src {
	match-direction input;
	rule r1 {
	match {
	source-address 10.10.10.0/24;
	# Since destination NAT happens first, the destination
	# address refers to the NAT'd address.
	destination-address 10.99.10.0/24;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

Table 19: Example: Twice-Basic-NAT-44 *(continued)*

MS-MPC	MX-SPC3
} # end nat	} # end source
	destination {

	pool dest-pool {
	address {
	10.99.10.0/24;
	}
	}

	# This destination rule applies before the source rule.
	rule-set rule-twice-basic-nat-44-dest {
	match-direction input;
	rule r1 {
	match {
	destination-address 10.20.10.0/24;
	}
	then {
	destination-nat {
	pool {
	dest-pool;
	}
	}
	}
	}
	}

	} # end destination } # end nat

Table 20: Example: Twice-Dynamic-NAT-44

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-twice-dynamic-nat-44;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-twice-dynamic-nat-44-src;
	nat-rule-sets rule-twice-dynamic-nat-44-dest;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

Table 20: Example: Twice-Dynamic-NAT-44 ***(continued)***

MS-MPC	MX-SPC3
nat {	nat { source {

pool src-pool {
address 10.98.10.0/24;
}
pool dest-pool {
address 10.99.10.0/24;
}
	pool src-pool {
	address {
	10.98.10.0/24;
	}
	port {
	no-translation;
	}
	}

rule rule-twice-dynamic-nat-44 {
match-direction input;
term t1 {
from {
source-address {
10.10.10.0/24;
}
destination-address {
10.20.10.0/24;
}
}
then {
translated {
source-pool src-pool;
destination-pool dest-pool;
translation-type {
twice-dynamic-nat-44;
}
}
}
}
}
	# This source rule applies after the destination rule.
	rule-set rule-twice-dynamic-nat-44-src {
	match-direction input;
	rule r1 {
	match {
	source-address 10.10.10.0/24;
	# Since destination NAT happens first, the destination
	# address refers to the NAT'd address.
	destination-address 10.99.10.0/24;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

} # end nat	} # end source
	destination {

Table 20: Example: Twice-Dynamic-NAT-44 *(continued)*

MS-MPC	MX-SPC3

	pool dest-pool {
	  # By default, address mapping in destination pools is static.
	  address {
	    10.99.10.0/24;
	  }
	}

	# This destination rule applies before the source rule.
	  rule-set rule-twice-dynamic-nat-44-dest {
	    match-direction input;
	    rule r1 {
	      match {
	        destination-address 10.20.10.0/24;
	      }
	      then {
	        destination-nat {
	          pool {
	            dest-pool;
	          }
	        }
	      }
	    }
	  }

	} # end destination } # end nat

Table 21: Example: Twice-NAPT-44

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
  nat-rules rule-twice-napt-44;
  interface-service {
    service-interface ms-1/2/0;
  }
}
	service-set sset1 {
	  nat-rule-sets rule-twice-napt-44-src;
	  nat-rule-sets rule-twice-napt-44-dest;
	  interface-service {
	    service-interface vms-2/0/0;
	  }
	}

nat {	nat { source {

Table 21: Example: Twice-NAPT-44 *(continued)*

MS-MPC	MX-SPC3

pool src-pool {
address 10.98.10.0/24;
port {
automatic;
secured-port-block-allocation block-size
256 max-blocks-per-address 1
active-block-timeout 300;
}
}
pool dest-pool {
address 10.99.10.2/32;
}
	pool src-pool {
	address {
	10.98.10.0/24;
	}
	port {
	automatic {
	round-robin;
	}
	block-allocation {
	block-size 256;
	maximum-blocks-per-host 1;
	active-block-timeout 300;
	}
	}
	}

rule rule-twice-napt-44 {
match-direction input;
term t1 {
from {
source-address {
10.10.10.0/24;
}
destination-address {
10.20.10.2/32;
}
}
then {
translated {
source-pool src-pool;
destination-pool dest-pool;
translation-type {
twice-napt-44;
}
}
}
}
}
	# This source rule applies after the destination rule.
	rule-set rule-twice-napt-44-src {
	match-direction input;
	rule r1 {
	match {
	source-address 10.10.10.0/24;
	# Since destination NAT happens first, the
	# destination address refers to the NAT'd address.
	destination-address 10.99.10.2/32;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

} # end nat	} # end source
	destination {

Table 21: Example: Twice-NAPT-44 *(continued)*

MS-MPC	MX-SPC3

	pool dest-pool {
	address {
	10.99.10.2/32;
	}
	}

	# This destination rule applies before the source rule.
	rule-set rule-twice-napt-44-dest {
	match-direction input;
	rule r1 {
	match {
	source-address 10.10.10.0/24;
	destination-address 10.20.10.2/32;
	}
	then {
	destination-nat {
	pool {
	dest-pool;
	}
	}
	}
	}
	}

	} # end destination } # end nat

Table 22: Example: Deterministic-NAPT44

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-deterministic-napt44;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-deterministic-napt44;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

Table 22: Example: Deterministic-NAPT44 *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>
pool src-pool {
    address 10.10.10.0/24;
    port {
        range low 1024 high 19999;
        deterministic-port-block-allocation block-size
            256;
    }
    mapping-timeout 120;
}
</pre></td><td><pre>
pool src-pool {
    address {
        10.10.10.0/24;
    }
    port {
        range {
            1024;
            to {
                19999;
            }
        }
        deterministic {
            block-size 256;
            # host address specifies the subnet that you
            # want to apply to this pool.
            host address 10.2.0.0/20;
        }
    }
    mapping-timeout 120;
}
</pre></td></tr>
<tr><td><pre>
rule rule-deterministic-napt44 {
    match-direction input;
    term t1 {
        from {
            source-address {
                10.2.0.0/18;
            }
        }
        then {
            translated {
                source-pool src-pool;
                translation-type {
                    deterministic-napt44;
                }
                mapping-type endpoint-independent;
            }
        }
    }
}
</pre></td><td><pre>
rule-set rule-deterministic-napt44 {
    match-direction input;
    rule r1 {
        match {
            source-address 10.2.0.0/18;
        }
        then {
            source-nat {
                pool {
                    src-pool;
                }
                mapping-type endpoint-independent;
            }
        }
    }
}
</pre></td></tr>
</table>

Table 22: Example: Deterministic-NAPT44 *(continued)*

MS-MPC	MX-SPC3
} # end nat	} # end source } # end nat

Table 23: Example: Deterministic-NAPT64

MS-MPC	MX-SPC3
[edit services]	[edit services]

service-set sset1 {
nat-rules rule-deterministic-napt64;
interface-service {
service-interface ms-1/2/0;
}
}
	service-set sset1 {
	nat-rule-sets rule-deterministic-napt64-src;
	nat-rule-sets rule-deterministic-napt64-dest;
	interface-service {
	service-interface vms-2/0/0;
	}
	}

nat {	nat { source {

pool src-pool {
address 10.98.10.0/24;
port {
automatic;
random-allocation;
}
deterministic-port-block-allocation
block-size 256;
}
}
	pool src-pool {
	address {
	10.98.10.0/24;
	}
	port {
	automatic {
	random-allocation;
	}
	deterministic {
	block-size 256;
	host address 2001:DB8:1111::1/120;
	}
	}
	}

Table 23: Example: Deterministic-NAPT64 *(continued)*

MS-MPC	MX-SPC3

rule rule-deterministic-napt64 {
match-direction input;
term t1 {
from {
source-address {
2001:DB8:1111::1/120;
}
}
then {
translated {
destination-prefix
2001:DB8:2222::/96;
source-pool src-pool;
translation-type {
deterministic-napt64;
}
}
}
}
}
	# This source rule applies after the destination rule.
	rule-set rule-deterministic-napt64-src {
	match-direction input;
	rule r1 {
	match {
	source-address 2001:DB8:1111::1/120;
	# Since destination NAT happens first, the destination
	# address refers to the NAT'd address.
	destination-address 0.0.0.0/32;
	}
	then {
	source-nat {
	pool {
	src-pool;
	}
	}
	}
	}
	}

} # end nat	} # end source
	destination {

	pool dest-pool {
	address {
	10.99.10.2/32;
	}
	}

Table 23: Example: Deterministic-NAPT64 *(continued)*

MS-MPC	MX-SPC3

	# This destination rule applies before the source rule.
	rule-set rule-destination-napt64-dest {
	match-direction input;
	rule r1 {
	match {
	destination-address 2001:DB8:2222::/96;
	}
	then {
	destination-nat {
	destination-prefix 2001:DB8:2222::/96;
	}
	}
	}
	}

	} # end destination } # end nat

Intrusion Detection System (IDS)

IDS rules for Next Gen Services on the MX-SPC3 are defined under the **screen** branch. There are minor differences in the naming of the various elements, but the main change is in the behavior for detecting packets with IPv4 options and IPv6 extensions:

- For the IDS service on the MS-MPC, the default behavior is to detect and drop packets with IPv4 options and IPv6 extensions. If you want to allow these packets, you have to allow them explicitly through configuration.
- For the IDS Next Gen Service on the MX-SPC3, the default behavior is to allow packets with IPv4 options and IPv6 extensions. If you want to detect and drop these packets, you have to disallow them explicitly through configuration.

Table 24 on page 68 shows examples of the configuration differences.

Table 24: IDS Rules

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>
[edit services]
service-set sset1 {
    ids-rules r1;
    ids-rules r2;
}
</pre></td><td><pre>
[edit services]
service-set sset1 {
    # Replace ids-rules with ids-option.
    ids-option ids1;
    ids-option ids2;
}
</pre></td></tr>
<tr><td><pre>
[edit services]
ids {
    rule r1 {
        match-direction input;
        term t1 {
            <...>
        }
    }
}
</pre></td><td><pre>
[edit services]
# Define ids rules under the screen branch.
screen {
    # Replace rule with ids-option.
    ids-option ids1 {
        match-direction input;
        # Flatten hierarchy by removing term and placing
        # contents directly under ids-option.
        <...>
    }
}
</pre></td></tr>
<tr><td><pre>
[edit services]
ids {
    rule r1 {
        match-direction input;
        term t1 {
            then {
                allow-ip-options [loose-source-route
                    route-record router-alert security
                    stream-id strict-source-route timestamp
                    ];
            }
        }
    }
}
</pre></td><td><pre>
[edit services]
screen {
    ids-option ids1 {
        match-direction input;
        # By default, all ip options are allowed.
    }
}
</pre></td></tr>
</table>

Table 24: IDS Rules *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>[edit services]
ids {
   rule r1 {
      match-direction input;
      term t1 {
         then {
            <no allow-ip-options configured>
         }
      }
   }
}</pre></td><td><pre>[edit services]
screen {
   ids-option ids1 {
      match-direction input;
      # Explicitly specify the disallowed options.
      ip {
         loose-source-route-option;
         record-route-option;
         security-option;
         stream-option;
         strict-source-route-option;
         timestamp-option;
         # router-alert option for IPv4 is not supported.
      }
   }
}</pre></td></tr>
<tr><td><pre>[edit services]
ids {
   rule r1 {
      match-direction input;
      term t1 {
         then {
            allow-ipv6-extension-header [ah dstopts
               esp fragment hop-by-hop mobility
               routing];
         }
      }
   }
}</pre></td><td><pre>[edit services]
screen {
   ids-option ids1 {
      match-direction input;
      # By default, all ipv6 extensions are allowed.
   }
}</pre></td></tr>
</table>

Table 24: IDS Rules *(continued)*

MS-MPC	MX-SPC3

[edit services]
ids {
rule r1 {
match-direction input;
term t1 {
then {
<no allow-ipv6-extension-header
configured>
}
}
}
}
	[edit services]
	screen {
	ids-option ids1 {
	match-direction input;
	ip {
	# Explicitly specify the disallowed extensions.
	ipv6-extension-header {
	AH-header;
	ESP-header;
	fragment-header;
	hop-by-hop-header;
	mobility-header;
	routing-header;
	# dstoptions is not supported.
	}
	}
	}
	}

[edit services]
ids {
rule r1 {
match-direction input;
term t1 {
then {
aggregation {
source-prefix 24;
destination-prefix 24;
source-prefix-ipv6 64;
destination-prefix-ipv6 64;
}
}
}
}
}
	[edit services]
	screen {
	ids-option ids1 {
	match-direction input;
	aggregation {
	source-prefix-mask 24;
	destination-prefix-mask 24;
	source-prefix-v6-mask 64;
	destination-prefix-v6-mask 64;
	}
	}
	}

Table 24: IDS Rules *(continued)*

MS-MPC	MX-SPC3

[edit services]
ids {
rule r1 {
match-direction input;
term t1 {
then {
icmp-fragment-check;
icmp-large-packet-check;
}
}
}
}
	[edit services]
	screen {
	ids-option ids1 {
	match-direction input;
	# Group icmp checks under icmp.
	icmp {
	fragment;
	large;
	}
	}
	}

[edit services]
ids {
rule r1 {
match-direction input;
term t1 {
then {
land-attack-check;
tcp-winnuke-check;
tcp-syn-fragment-check;
tcp-syn-defense;
}
}
}
}
	[edit services]
	screen {
	ids-option ids1 {
	match-direction input;
	# Group tcp checks under tcp.
	tcp {
	land;
	winnuke;
	syn-frag;
	# tcp-syn-defense is not supported.
	}
	}
	}

Table 24: IDS Rules *(continued)*

MS-MPC	MX-SPC3

[edit services]
ids {
rule r1 {
match-direction input;
term t1 {
then {
session-limit {
by-source {
maximum 100;
rate 10;
packets 1k;
}
by-destination {
maximum 100;
rate 10;
packets 1k;
}
}
}
}
}
}
	[edit services]
	screen {
	ids-option ids1 {
	match-direction input;
	limit-session {
	by-source {
	maximum-sessions 100;
	session-rate 10;
	packet-rate 1k;
	}
	by-destination {
	maximum-sessions 100;
	session-rate 10;
	packet-rate 1k;
	}
	}
	}
	}

Table 24: IDS Rules *(continued)*

MS-MPC	MX-SPC3

[edit services]
ids {
  rule r1 {
    match-direction input;
    term t1 {
      then {
        session-limit {
          by-source {
            by-protocol {
              tcp {
                maximum 100;
                rate 10;
                packets 1k;
              }
              udp {
                maximum 100;
                rate 10;
                packets 1k;
              }
              icmp {
                maximum 100;
                rate 10;
                packets 1k;
              }
            }
          }
        }
      }
    }
  }
}
	[edit services]
	screen {
	  ids-option ids1 {
	    match-direction input;
	    limit-session {
	      by-source {
	        by-protocol {
	          tcp {
	            maximum-sessions 100;
	            session-rate 10;
	            packet-rate 1k;
	          }
	          udp {
	            maximum-sessions 100;
	            session-rate 10;
	            packet-rate 1k;
	          }
	          icmp {
	            maximum-sessions 100;
	            session-rate 10;
	            packet-rate 1k;
	          }
	        }
	      }
	    }
	  }
	}

Table 24: IDS Rules *(continued)*

<table>
<tr><th>MS-MPC</th><th>MX-SPC3</th></tr>
<tr><td><pre>
[edit services]
ids {
    rule r1 {
        match-direction input;
        term t1 {
            then {
                session-limit {
                    by-destination {
                        by-protocol {
                            tcp {
                                maximum 100;
                                rate 10;
                                packets 1k;
                            }
                            udp {
                                maximum 100;
                                rate 10;
                                packets 1k;
                            }
                            icmp {
                                maximum 100;
                                rate 10;
                                packets 1k;
                            }
                        }
                    }
                }
            }
        }
    }
}
</pre></td><td><pre>
[edit services]
screen {
    ids-option ids1 {
        match-direction input;
        limit-session {
            by-destination {
                by-protocol {
                    tcp {
                        maximum-sessions 100;
                        session-rate 10;
                        packet-rate 1k;
                    }
                    udp {
                        maximum-sessions 100;
                        session-rate 10;
                        packet-rate 1k;
                    }
                    icmp {
                        maximum-sessions 100;
                        session-rate 10;
                        packet-rate 1k;
                    }
                }
            }
        }
    }
}
</pre></td></tr>
</table>

Migrate from the MS-MPC to the MX-SPC3

Use this procedure to configure a router to support Next Gen Services.

You typically use this procedure to migrate a router supporting legacy services on the MS-MPC to a router supporting Next Gen Services on the MX-SPC3, but this procedure applies even if the router that you are migrating from does not contain MS-MPC cards.

Because Next Gen Services configuration is not compatible with legacy service provisioning, migrating a router to support Next Gen Services on the MX-SPC3 requires you to completely deprovision and reprovision your router . Furthermore:

- You cannot install an MX-SPC3 card in a router that has MS-MPC or MS-MIC cards.
- You cannot configure Next Gen Services on a router equipped with MS-MPC or MS-MIC cards.
- You cannot configure legacy services on a router equipped with MX-SPC3 cards.

In other words, a router can run with either MS-MPC / MS-MIC cards or MX-SPC3 cards but not both at the same time.

> **NOTE:** This procedure is service affecting. You are setting the router to factory default configuration.

1. Upgrade the router to release 19.3R2.

2. Back up the current router configuration to a remote host.

3. Set the router to factory default configuration.

   a. Load the router with the factory default configuration:

   ```
   root# load factory-default
   ```

   b. Configure the management interface with the same IP address as you had before you loaded the factory default configuration:

   ```
   root# set interfaces fxp0 unit 0 family inet address <mgt-ip-address>
   ```

   c. Configure SSH so that you can continue to access the router. For example:

```
root# set system services ssh root-login allow
root# set system services ssh max-sessions-per-connection 32
root# set system root-authentication plain-text-password
New password:
Retype new password:
```

d. Commit the changes.

4. Enable Next Gen Services on the router.

   Junos OS provides a system-wide operational parameter that you enable if you want to configure Next Gen Services on a router. By default, this parameter is not enabled.

   From operational mode:

```
root> request system enable unified-services
Before enabling unified services, please move to baseline configuration.
Are above conditions satisfied ? [yes,no]
```

> **NOTE:** This setting is persistent and survives a reboot.

5. Reboot the router.

```
root> request system reboot
```

6. Replace the MS-MPC cards with MX-SPC3 cards.

7. Reprovision your router.

   As a starting point, you can restore the backup from step 2 but you might need to change this configuration to be compatible with Next Gen Services before you can commit.

SEE ALSO

Next Gen Services Overview | 19
Enabling and Disabling Next Gen Services | 24

How to Configure Services Interfaces for Next Gen Services

To configure services interfaces:

1. Configure the services interface name.

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

   Where the *interface-name* one of the following:

   - vms-*slot-number*/*pic-number*/*port-number* for an MX-SPC3 services card
   - si-*slot-number*/*pic-number*/0 for a line card PFE (inline services interface)

2. Configure the unit and family for the interface.

   - If you are using the services interface in an interface service set:

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family (inet | inet6)
```

   - If you are using the services interface in a next-hop service set, configure inside and outside interface units:

```
[edit]
user@host# set interfaces interface-name unit logical-unit-number family (inet | inet6)
user@host# set interfaces interface-name unit logical-unit-number service-domain inside
user@host# set interfaces interface-name unit logical-unit-number family (inet | inet6)
user@host# set interfaces interface-name unit logical-unit-number service-domain outside
```

   For example:

```
[edit]
user@host# set interfaces vms-1/0/0 unit 100 family inet
user@host# set interfaces vms-1/0/0 unit 100 service-domain inside
user@host# set interfaces vms-1/0/0 unit 1000 family inet
```

```
user@host# set interfaces vms-1/0/0 unit 1000 service-domain outside
```

3. When neither NAT nor the **max-sessions-per-subscriber** statement at the **[edit service-set *service-set-name* service-set-options]** hierarchy level are configured, enable the creation of subscribers if you want to track subscribers.

```
[edit interfaces interface-name services-options]
user@host# set enable-subscriber-analysis
```

4. Configure CPU resource restrictions for the services interface.

```
[edit interfaces interface-name services-options session-limit]
user@host# set cpu-load-threshold percentage
```

   When the CPU usage exceeds the 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.

5. Configure the maximum number of sessions allowed simultaneously on a services card.

```
[edit interfaces interface-name services-options session-limit]
user@host# set maximum number
```

   If you specify the maximum number of sessions to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for the maximum number of sessions.

6. Configure the maximum number of new sessions allowed per second on a services card.

```
[edit interfaces interface-name services-options session-limit]
user@host# set rate rate
```

RELATED DOCUMENTATION

Next Gen Services Overview | 19
How to Configure Next-Hop Style Service Sets for Next Gen Services | 80

How to Configure Service Set Limits for Next Gen Services | 82

Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

How to Configure Interface-Style Service Sets for Next Gen Services

To configure an interface service set:

1. Configure the service set name.

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

2. Specify the service interface that the service set uses to apply services.

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

3. Specify the service rules that the service set applies to traffic.

   For example:

   ```
   [edit services service-set ss1]
   user@host# set nat-rule-sets internal-nat
   ```

4. (Optional) Enable the service set to process unidirectional traffic.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# set enable-asymmetric-traffic-processing
   ```

5. Enable service-processing at routing engine (RE).

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

6. Apply the service set to an interface that is passing traffic. You can apply a service filter to apply the service set to only certain traffic on the interface.

```
[edit interfaces interface-name unit logical-unit-number family (inet | inet6) service]
user@host# set (input | output) service-set service-set-name <service-filter filter-name>
```

For details about configuring the service-filter, see *Guidelines for Configuring Service Filters*.

The **input** option applies the service set to the input side of the interface, and the **output** option applies the service set to the output side of the interface. If you are using a bidirectional service rule in the service set, then the same service set must be used for input and output.

RELATED DOCUMENTATION

Next Gen Services Overview | 19
How to Configure Interface-Style Service Sets for Next Gen Services | 79
How to Configure Service Set Limits for Next Gen Services | 82
Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

How to Configure Next-Hop Style Service Sets for Next Gen Services

To configure a next-hop service set:

1. Configure the service set name.

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

2. Specify the services interface inside unit and outside unit for the service set.

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

The inside-service-interface must be a service interface logical unit that is configured with **service-domain inside** The outside-service-interface must be a service interface logical unit that is configured with **service-domain outside**.

3. Specify the service rules that the service set applies to traffic.

   For example:

   ```
   [edit services service-set SS1]
   user@host# set nat-rule-sets internal-nat
   ```

4. (Optional) Enable the service set to process unidirectional traffic.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# set enable-asymmetric-traffic-processing
   ```

5. Configure a static route to force traffic to the inside or outside interface of the next-hop service set.

   For example, if you want traffic with the destination 198.51.100.33 to be processed by the service set with the inside interface vms-1/0/0.100:

   ```
   [edit routing-options]
   user@host# set static route 198.51.100.33 next-hop vms-1/0/0.100
   ```

RELATED DOCUMENTATION

Next Gen Services Overview | 19

How to Configure Interface-Style Service Sets for Next Gen Services | 79

How to Configure Service Set Limits for Next Gen Services | 82

Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

How to Configure Service Set Limits for Next Gen Services

To configure service set limits:

1. Set the maximum number of session setups allowed per second for the service set. After this setup rate is reached, any additional session setup attempts are dropped. If you do not include the **max-session-creation-rate** statement, the session setup rate is not limited.

   ```
   [edit services service-set service-set-name ]
   user@host# set max-session-setup-rate (number | numberk)
   ```

   If you use the *number*k format, 1k=1000.

2. Enable packets to bypass without creating a new session when the flow in the service set exceeds the limit that is set by the **max-flows** statement at the **[edit services service-set *service-set-name*]** hierarchy level.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# bypass-traffic-on-exceeding-flow-limits
   ```

3. To limit the session open information in you system logs, you can disable it from being collected.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# set disable-session-open-syslog
   ```

4. Configure the maximum number of sessions allowed from a single subscriber.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# set max-sessions-per-subscriber session-number
   ```

5. Specify the maximum number of sessions allowed simultaneously on the service set. If you specify the maximum number of sessions to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for the maximum number of sessions.

   ```
   [edit services service-set service-set-name service-set-options]
   user@host# set session-limit maximum number
   ```

6. Configure the session lifetime for the service set in seconds. The session is closed after this amount of time, even if traffic is running on the session.

```
[edit services service-set service-set-name service-set-options]
user@host# set session-timeout seconds
```

7. Specify the inactivity timeout period for non-TCP established sessions.

```
user@host# set inactivity-non-tcp-timeout seconds
```

8. Configure the TCP session parameters for the service-set.

   1. Set the timeout period for the Transmission Control Protocol (TCP) session tear-down.

      ```
      [edit services service-set-name services-options]
      user@host# set close-timout seconds
      ```

      The default value is 1 second. The range is 2 through 300 seconds.

   2. Configure the inactivity timeout period for asymmetric TCP established sessions

      ```
      [edit services service-set service-set-name service-set-options tcp-session]
      user@host# set inactivity-asymm-tcp-timeout seconds
      ```

   3. Configure the number of seconds that a unidirectional TCP session can be inactive before it is closed.

      ```
      [edit services service-set service-set-name service-set-options tcp-session]
      user@host# set inactivity-tcp-timeout seconds
      ```

      The default value is 30 seconds. The range is 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*

   4. Set the timeout period for Transmission Control Protocol (TCP) session establishment, for use with SYN-cookie defenses against network intrusion.

      ```
      [edit services service-set-name service-set-options ]
      user@host# set 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 Network Attack Protection With IDS Screens for Next Gen Services*.

RELATED DOCUMENTATION

Next Gen Services Overview | 19
How to Configure Interface-Style Service Sets for Next Gen Services | 79
Next Gen Services Feature Configuration Overview | 29
Configuration Differences Between Adaptive Services on the MS-MPC and Next Gen Services on the MX-SPC3 | 30

3

CHAPTER

Enabling Load Balancing and High Availability Using Services Interfaces

Understanding Aggregated Multiservices Interfaces for Next Gen Services

IN THIS SECTION

This topic provides an overview of using the Aggregated Multiservices Interfaces feature with the MX-SPC3 services card for Next Gen Services. It contains the following sections:

Aggregated Multiservices Interface

In Junos OS, you can combine multiple services interfaces to create a bundle of services interfaces that can function as a single interface. Such a bundle of interfaces is known as an *aggregated multiservices interface* (AMS), and is denoted as ams*N* in the configuration, where *N* is a unique number that identifies an AMS interface (for example, ams0). Starting in Junos OS Release 19.3R2, AMS interfaces are supported on the Next Gen Services MX-SPC3 services card.

> **NOTE:** MX240, MX480, MX960 routers support Next Gen Services using the MX-SPC3 services card. When running Next Gen Services, you cannot run other legacy MX line card services in the same chassis, for example, you cannot run the MS-MPC card inline services.

AMS configuration provides higher scalability, improved performance, and better failover and load-balancing options.

An AMS configuration enables service sets to support multiple services PICs by associating an AMS bundle with a service set. For Next Gen Services, the MX-SPC3 services card supports up to two PICs and you can have a maximum of eight MX-SPC3 services cards in your chassis. This enables a Next Gen Services AMS bundle to have up to 16 services PICs as member interfaces and you can distribute services among the member interfaces.

Member interfaces are identified as mams in the configuration. The chassisd process in routers that support AMS configuration creates a mams entry for every multiservices interface on the router.

When you configure services options at the ams interface level, the options apply to all member interfaces (mams) for the ams interface.

The options also apply to service sets configured on services interfaces corresponding to the ams interface's member interfaces. All settings are per PIC. For example, session-limit applies per member and not at an aggregate level.

> **NOTE:** You cannot configure services options at both the ams (aggregate) and member-interface level. If services options are configured on **vms-x/y/z**, they also apply to service sets on **mams-x/y/z**.
>
> When you want services options settings to apply uniformly to all members, configure services options at the ams interface level. If you need different settings for individual members, configure services options at the member interface level.

> **NOTE:** If you modify a NAT pool that is being used by a service set assigned to an AMS interface, you must deactivate and activate the service set before the NAT pool changes take effect.

Traffic distribution over the member interfaces of an AMS interface can occur in either a round-robin fashion or hash-based. You can configure the following hash key values to regulate the traffic distribution: **source-ip**, **destination-ip** , and **protocol**. For services that require traffic symmetry, you must configure symmetrical hashing. Symmetrical hashing configuration ensures that both forward and reverse traffic is routed through the same member interface.

If the service set is applied on the Gigabit Ethernet or 10-Gigabit Ethernet interface (interface-style service set) that functions as the NAT inside interface, then the hash keys used for load balancing might be configured in such a way that the ingress key is set as destination IP address and the egress key is set as source IP address. Because the source IP address undergoes NAT processing, it is not available for hashing the traffic in the reverse direction. Therefore, load balancing does not happen on the same IP address and forward and reverse traffic does not map to the same PIC. With the hash keys reversed, load balancing occurs correctly.

With next-hop services, for forward traffic, the ingress key on the inside interface load -balances traffic, and for reverse traffic, the ingress key on the outside interface load -balances traffic or per-member next hops steer reverse traffic. With interface-style services, the ingress key load-balances forward traffic and the egress key load-balances forward traffic or per-member next hops steer reverse traffic. Forward traffic is traffic entering from the inner side of a service set and reverse traffic is traffic entering from the outer side of a service set. The forward key is the hash key used for the forward direction of traffic and the reverse key is the hash key used for the reverse direction of traffic (depends on whether it relates to interface services or next-hop services style.)

With stateful firewalls, you can configure the following combinations of forward and reverse keys for load balancing. In the following combinations presented for hash keys, FOR-KEY refers to the forward key, REV-KEY denotes the reverse key, SIP signifies source IP address, DIP signifies destination IP address, and PROTO refers to protocol such as IP.

- FOR-KEY: SIP, REV-KEY: DIP
- FOR-KEY: SIP,PROTO REV-KEY: DIP, PROTO
- FOR-KEY: DIP, REV-KEY: SIP
- FOR-KEY: DIP,PROTO REV-KEY: SIP, PROTO
- FOR-KEY: SIP,DIP REV-KEY: SIP, DIP
- FOR-KEY: SIP,DIP,PROTO REV-KEY: SIP, DIP,PROTO

With static NAT configured as basic NAT44 or destination NAT44, and with stateful firewall configured or not, if the forward direction of traffic must undergo NAT processing, configure the hash keys as follows:

- FOR-KEY: DIP, REV-KEY: SIP
- FOR-KEY: DIP,PROTO REV-KEY: SIP, PROTO

If the reverse direction of traffic must undergo NAT processing, configure the hash keys as follows:

- FOR-KEY: SIP, REV-KEY: DIP
- FOR-KEY: SIP,PROTO REV-KEY: DIP, PROTO

With dynamic NAT configured, and with stateful firewall configured or not, only the forward direction traffic can undergo NAT. The forward hash key can be any combination of SIP, DIP, and protocol, and the reverse hash key is ignored.

> **NOTE:** The Junos OS AMS configuration supports IPv4 and IPv6 traffic.

IPv6 Traffic on AMS Interfaces Overview

You can use AMS interfaces for IPv6 traffic. To configure IPv6 support for an AMS interface, include the **family inet6** statement at the **[edit interfaces *ams-interface-name* unit 1]** hierarchy level. When **family inet** and **family inet6** are set for an AMS interface subunit, the **hash-keys** is configured at service-set level for interface style and at IFL level for next-hop style.

When a member interface of an AMS bundle fails, traffic destined to the failed member is redistributed among the remaining active members. The traffic (flows or sessions) traversing through the existing active members is unaffected. If M members are currently active, the expected result is that only about 1/M fraction of the traffic (flows/sessions) is impacted because that amount of traffic is shifted from the failed member to remain active members. When the failed member interface comes back online, only a fraction of the traffic is redistributed to the new member. If N members are currently active, the expected result is that only about 1/(N+1) fraction of the traffic (flows/sessions) is impacted because that amount of traffic moves to the new restored member. The 1/M and 1/(N+1) values assume that the flows are uniformly distributed among members, because a packet-hash is used to load-balance and because traffic usually contains a typical random combination of IP addresses (or any other fields that are used as load-balancing keys).

Similar to IPv4 traffic, for IPv6 packets, an AMS bundle must contain members of only one services PIC type.

The number of flows distributed, in an ideal environment, can be 1/N in a best-case scenario when the Nth member goes up or down. However, this assumption considers that the hash keys load-balance the real or dynamic traffic. For example, consider a real-world deployment where member A is serving only one flow, whereas member B is serving 10 flows. If member B goes down, then the number of flows disrupted is 10/11. The NAT pool-split behavior is designed to utilize the benefits of the rehash-minimization feature. The splitting of a NAT pool is performed for dynamic NAT scenarios (dynamic NAT, NAT64, and NAPT44).

If the original and redistributed flows are defined as follows:

- Member-original-flows—The traffic mapped to a member when all members are up.
- Member-redistributed-flows—The additional traffic mapped to a member when some other member fails. These traffic flows might need to be rebalanced when member interfaces come up and go down.

With the preceding definitions of the original and redistributed flows for member interfaces, the following observations apply:

- The member-original-flows of a member stay intact as long as that member is up. Such flows are not impacted when other members move between the up and down states.
- The member-redistributed-flows of a member can change when other members go up or down. This change of flows occurs because these additional flows need to be rebalanced among all active members. Therefore, the member-redistributed-flow can vary a lot based on other members going down or up. Although it might seem that when a member goes down, the flows on active-members are preserved, and that when a member goes up, flows on active-members are not preserved in an effective way, this behavior is only because of static or hash-based rebalancing of traffic among active members.

The rehash-minimization feature handles the operational changes in a member interface status only (such as member offline or member Junos OS reset). It does not handle changes in configuration. For example, addition or deletion, or activation and deactivation, of member interfaces at the **[edit interfaces ams*N***

load-balancing-options member-interface mams-a/b/0] hierarchy level requires the member PICs to be bounced. Twice NAT or hairpinning is not supported, similar to IPv4 support for AMS interfaces.

Member Failure Options and High Availability Settings

Because multiple service interfaces are configured as part of an AMS bundle, AMS configuration also provides for failover and high availability support. You can either configure one of the member interfaces as a backup interface that becomes active when any one of the other member interfaces goes down, or configure the AMS in such a way that when one of the member interfaces goes down, the traffic assigned to that interface is shared across the active interfaces.

The **member-failure-options** configuration statement enables you to configure how to handle traffic when a member interface fails. One option is to redistribute the traffic immediately among the other member interfaces. However, redistribution of traffic involves recalculating the hash tags, and might cause some disruption in traffic on all the member interfaces.

The other option is to configure the AMS to drop all traffic that is assigned to the failed member interface. With this you can optionally configure an interval, **rejoin-timeout**, for the AMS to wait for the failed interface to come back online after which the AMS can redistribute the traffic among other member interfaces. If the failed member interface comes back online before the configured wait time, traffic continues unaffected on all member interfaces, including the interface that has come back online and resumed the operations.

You can also control the rejoining of the failed interface when it comes back online. If you do not include the **enable-rejoin** statement in the **member-failure-options** configuration, the failed interface cannot rejoin the AMS when it comes back online. In such cases, you can manually rejoin that to the AMS by executing the **request interfaces revert *interface-name*** operational mode command.

The **rejoin-timeout** and **enable-rejoin** statements enable you to minimize traffic disruptions when member interfaces flap.

> **NOTE:** When **member-failure-options** are not configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

The **high-availability-options** configuration enables you to designate one of the member interfaces as a backup interface. The backup interface does not participate in routing operations as long as it remains a backup interface. When a member interface fails, the backup interface handles the traffic assigned to the failed interface. When the failed interface comes back online, it becomes the new backup interface.

In a many-to-one configuration (N:1), a single backup interface supports all other member interfaces in the group. If any of the member interfaces fails, the backup interface takes over. In this stateless configuration, data is not synchronized between the backup interface and the other member interfaces.

When both **member-failure-options** and **high-availability-options** are configured for an AMS, the **high-availability-options** configuration takes precedence over the **member-failure-options** configuration. If a second failure occurs before the failed interface comes back online to be the new backup, the **member-failure-options** configuration takes effect.

Warm Standby Redundancy

Starting in Junos OS Release 19.3R2, the N:1 warm standby option is supported on the MX-SPC3 if you are running Next Gen Services. Each warm standby AMS interface contains two members; one member is the service interface you want to protect, called the primary interface, and one member is the secondary (backup) interface. The primary interface is the active interface and the backup interface does not handle any traffic unless the primary interface fails.

To configure warm standby on an AMS interface, you use the **redundancy-options** statement. You cannot use the **load-balancing-options** statement in a warm standby AMS interface.

To switch from the primary interface to the secondary interface, issue the **request interface switchover ams*N*** command.

To revert to the primary interface from the secondary interface, issue the **request interface revert ams*N*** command.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, AMS interfaces are supported on the Next Gen Services MX-SPC3 services card.
19.3R2	Starting in Junos OS Release 19.3R2, the N:1 warm standby option is supported on the MX-SPC3 if you are running Next Gen Services.

Configuring Aggregated Multiservices Interfaces

The aggregated multiservices (AMS) interface configuration in Junos OS enables you to combine services interfaces from multiple PICs to create a bundle of interfaces that can function as a single interface. You identify the PIC that you want to act as the backup.

1. Create an aggregated multiservices interface and add member interfaces. Starting in Junos OS Release 19.3R2, an MX-SPC3 Next Gen Services AMS interface can have up to 16 member interfaces with a maximum of 8 MX-SPC3 services cards with up to 2 PICs on each card. Starting with Junos OS Release 16.2, an MS-MPC AMS interface can have up to 36 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface can have a maximum of 24 member interfaces.

   > **NOTE:** The member interface format is **mams-*a*/*b*/0**, where *a* is the Flexible PIC Concentrator (FPC) slot number and *b* is the PIC slot number.

   ```
   [edit interfaces]
   user@host# set interface-name load-balancing-options member-interface mams-a/b/0
   user@host# set interface-name load-balancing-options member-interface mams-a/b/0
   ```

   For example on an MS-MPC, which can have up to four PICs:

   ```
   [edit interfaces]
   user@host# set ams1 load-balancing-options member-interface mams-1/1/0
   user@host# set ams1 load-balancing-options member-interface mams-1/2/0
   ```

   For example on an MX-SPC3, which can have up to two PICs:

   ```
   [edit interfaces]
   user@host# set ams1 load-balancing-options member-interface mams-1/0/0
   user@host# set ams1 load-balancing-options member-interface mams-1/1/0
   ```

2. Configure logical units for the AMS interface.

   ```
   [edit interfaces]
   user@host# set interface-name unit logical-unit-number family family
   user@host# set interface-name unit logical-unit-number family family
   ```

   For example:

```
[edit interfaces]
user@host# set ams1 unit 1 family inet
user@host# set ams1 unit 2 family inet6
```

3. Configure member failure options.

```
[edit interfaces interface-name]
user@host# set load-balancing-options member-failure-options drop-member-traffic rejoin-timeout seconds
user@host# set load-balancing-options member-failure-options drop-member-traffic enable-rejoin
```

For example:

```
[edit interfaces ams1]
user@host# set load-balancing-options member-failure-options drop-member-traffic rejoin-timeout 1000
user@host# set load-balancing-options member-failure-options drop-member-traffic enable-rejoin
```

4. Configure the preferred backup.

```
[edit interfaces interface-name]
user@host# set load-balancing-options high-availability-options many-to-one preferred-backup
  preferred-backup
```

For example:

```
[edit interfaces ams1]
user@host# set load-balancing-options high-availability-options many-to-one preferred-backup mams-1/2/0
```

5. **NOTE:** This step is not applicable to the Next Gen Services MX-SPC3 services card in the MX240, MX480 or MX960 chassis.

If the AMS interface has more than 24 member interfaces, set the service PIC boot timeout value to 240 or 300 seconds for every services PIC on the MX Series router. We recommend that you use a value of 240.

NOTE: Starting with Junos OS Release 16.2, an AMS interface can have up to 36 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface could have a maximum of 24 member interfaces.

```
[edit interfaces interface-name multiservice-options]
user@host# set pic-boot-timeout (240 | 300);
```

For example:

```
[edit interfaces sp-1/1/0 multiservice-options]
user@host# set pic-boot-timeout 240
```

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, an MX-SPC3 Next Gen Services AMS interface can have up to 16 member interfaces with a maximum of 8 MX-SPC3 services cards with up to 2 PICs on each card.
16.2	Starting with Junos OS Release 16.2, an MS-MPC AMS interface can have up to 36 member interfaces.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces for Next Gen Services | 87

Configuring Load Balancing on AMS Infrastructure

Configuring load balancing requires an aggregated multiservices (AMS) system. AMS involves grouping several services PICs together. An AMS configuration eliminates the need for separate routers within a system. The primary benefit of having an AMS configuration is the ability to support load balancing of traffic across multiple services PICs.

AMS is supported on the MS-MPC and MS-MIC. Starting in Junos OS Release 19.3R2, AMS interfaces are also supported on the MX-SPC3 if you are running Next Gen Services.

High availability (HA) is supported on AMS infrastructure on all MX Series 5G Universal Routing Platforms. AMS has several benefits:

- Support for configuring behavior if a services PIC that is part of the AMS configuration fails
- Support for specifying hash keys for each service set in either direction
- Support for adding routes to individual PICs within the AMS system

Configuring AMS Infrastructure

AMS supports load balancing across multiple service sets. All ingress or egress traffic for a service set can be load balanced across different services PICs. To enable load balancing, you have to configure an aggregate interface with existing services interfaces.

To configure failure behavior in AMS, include the **member-failure-options** statement:

```
[edit interfaces ams1]
load-balancing-options {
  member-failure-options {
    drop-member-traffic {
      rejoin-timeout rejoin-timeout;
    }
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
}
```

If a PIC fails, you can configure the traffic to the failed PIC to be redistributed by using the **redistribute-all-traffic** statement at the **[edit interfaces *interface-name* load-balancing-options member-failure-options]** hierarchy level. If the **drop-member-traffic** statement is used, all traffic to the failed PIC is dropped. Both options are mutually exclusive.

> **NOTE:** If **member-failure-options** is not explicitly configured, the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Only mams- interfaces (services interfaces that are part of AMS) can be aggregated. After an AMS interface has been configured, you cannot configure the individual constituent mams- interfaces. A mams- interface cannot be used as an ams interface (this is not applicable to Next Gen Services MX-SPC3). AMS supports

IPv4 (**family inet**) and IPv6 (**family inet6**). You cannot configure addresses on an AMS interface. Network Address Translation (NAT) is the only application that runs on AMS infrastructure at this time.

NOTE: You cannot configure unit 0 on an AMS interface.

To support multiple applications and different types of translation, AMS infrastructure supports configuring hashing for each service set. You can configure the hash keys separately for ingress and egress. The default configuration uses source IP, destination IP, and the protocol for hashing; incoming-interface for ingress and outgoing-interface for egress are also available.

NOTE: When using AMS in a load-balanced setup for the NAT solution, the number of NAT IP addresses must be greater than or equal to the number of active mams-interfaces you have added to the AMS bundle.

Configuring High Availability

In an AMS system configured with high availability, a designated services PIC acts as a backup for other active PICs that are part of the AMS system in a many-to-one (N:1) backup configuration. In a N:1 backup configuration, one PIC is available as backup for all other active PICs. If any of the active PICs fail, the backup PIC takes over for the failed PIC. In an N:1 (stateless) backup configuration, traffic states and data structures are not synchronized between the active PICs and the backup PIC.

An AMS system also supports a one-to-one (1:1) configuration. In the case of 1:1 backup, a backup interface is paired with a single active interface. If the active interface fails, the backup interface takes over. In a 1:1 (stateful) configuration, traffic states and data structures are synchronized between the active PICs and the backup PIC. Stateful synchronization is required for high availability of IPsec connections. For IPsec connections, AMS supports 1:1 configuration only.

NOTE: AMS 1:1 high availability is not supported for Next Gen Services in this release.

High availability for load balancing is configured by adding the **high-availability-options** statement at the **[edit interfaces *interface-name* load-balancing-options]** hierarchy level.

To configure N:1 high availability, include the **high-availability-options** statement with the **many-to-one** option:

```
[edit interfaces ams1]
load-balancing-options {
    high-availability-options {
        many-to-one {
            preferred-backup preferred-backup;
        }
    }
}
```

Starting in Junos OS Release 16.1, you can configure stateful 1:1 high availability on an MS-MPC. To configure stateful 1:1 high availability, at the **[edit interfaces *interface-name* load-balancing-options]** hierarchy level, include the **high-availability-options** statement with the **one-to-one** option:

NOTE: The Next Gen Services MX-SPC3 services card does not support AMS 1:1 high availability.

```
[edit interfaces ams1]
load-balancing-options {
    high-availability-options {
        one-to-one {
            preferred-backup preferred-backup;
        }
    }
}
```

Load Balancing Network Address Translation Flows

Network Address Translation (NAT) has been programmed as a plug-in and is a function of load balancing and high availability. The plug-in runs on AMS infrastructure. All flows for translation are automatically distributed to different services PICs that are part of the AMS infrastructure. In case of failure of an active services PIC, the configured backup PIC takes over the NAT pool resources of the failed PIC. The hashing method selected depends on the type of NAT. Using NAT on AMS infrastructure has a few limitations:

- NAT flows to failed PICs cannot be restored.
- There is no support for IPv6 flows.

  IPv6 address pools are not supported with AMS, however NAT64 is supported with AMS, so that IPv6 flows enters AMS.

NAT64 is supported for Next Gen Services on the MX-SPC3 services card, there is no support of NAT66. IPv6 flows for different NAT services are supported except where the translation is required to be IPv6 to IPv6 or IPv4 to IPv6.

- Twice NAT is not supported for load balancing on MS-MPC cards.

  Twice NAT is supported for load balancing on the Next Gen Services MX-SPC3 services card.

- Deterministic NAT uses warm-standby AMS configuration and can distribute the load using multiple AMS bundles in warm-standby mode.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, AMS interfaces are also supported on the MX-SPC3 if you are running Next Gen Services.
16.1	Starting in Junos OS Release 16.1, you can configure stateful 1:1 high availability on an MS-MPC.

Configuring Warm Standby for Services Interfaces

You can configure an N:1 warm standby option for MS-MPCs, MS-MICs, and MX-SPC3s by creating multiple aggregated multiservices (AMS) interfaces, each of which contains the service interface you want to backup and the service interface that acts as the backup. The same backup service interface can be used in all these AMS interfaces. Starting in Junos OS Release 19.3R2, the N:1 warm standby option is also supported on the MX-SPC3 if you are running Next Gen Services.

To configure warm standby for services interfaces:

1. Create an AMS interface.

   ```
   [edit interfaces]
   user@host# set amsN
   ```

   The variable *N* is a unique number, such as 0 or 1.

2. Specify the primary service interface that you want to backup.

   ```
   [edit interfaces amsN]
   user@host# set redundancy-options primary mams-a/b/0
   ```

The variable *a* is the FPC slot number and *b* is the PIC slot number for the primary service interface.

3. Specify the secondary service interface, which backs up the primary interface.

```
[edit interfaces amsN]
user@host# set redundancy-options secondary mams-a/b/0
```

The variable *a* is the FPC slot number and *b* is the PIC slot number for the secondary service interface.

4. Repeat Steps 1 through 3 to create an AMS interface for each service interface that you want to backup. You can use the same secondary service interface in each AMS interface.

Release History Table

Release	Description
19.3R2	Starting in Junos OS Release 19.3R2, the N:1 warm standby option is also supported on the MX-SPC3 if you are running Next Gen Services.

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

4

CHAPTER

Next Gen Services SNMP MIBS and Traps

Next Gen Services SNMP MIBs and Traps

IN THIS SECTION

This topic describes the SNMP MIBS and traps for Next Gen Services with the MX-SPC3 services. As a reference, it also compares MX-SPC3 services card MIBS and traps with the MPC services card.

Service-Set Related SNMP MIBs

Table 25 on page 103, Table 26 on page 105, and Table 27 on page 106 describe the MIB objects in the service-set related SNMP MIB tables supported in **jnxSPMIB**. This MIB is supported for both MS-MPC services cards and MX-SPC3 services cards with the exception of the following:

- The MX-SPC3 services card supports counters, such as memory usage and cpu usage, at the per service-set and per pic level, whereas MS-MPC services cards support these counters at the service level, for example, stateful firewall (SFW) and NAT).

  The MX-SPC3 card uses the **jnxSpSvcSetTable** MIB for these counters and the MS-MPC services card uses the **jnxSpSvcSetSvcTypeTable** MIB for these counters.

- InTable 25 on page 103 the **jnxSpSvcSetTable**, the object **jnxSpSvcSetSvcType** field will show a value of “ALL” since no per service-type specific counters are supported.

Table 25: Service-Set SNMP MIB Table (jnxSpSvcSetTable)

MIB Object	jnxSpSvcSet Entry Number	Description
jnxSpSvcSetIfName	jnxSpSvcSetEntry 4	The name of the interface identifying the AS PIC. If more than one interface is associated with the AS PIC, the name associated with the lower layer interface is used.

Table 25: Service-Set SNMP MIB Table (jnxSpSvcSetTable) ***(continued)***

MIB Object	jnxSpSvcSet Entry Number	Description
jnxSpSvcSetIfIndex	jnxSpSvcSetEntry 5	An index number associated with the interface name.
jnxSpSvcSetMemoryUsage	jnxSpSvcSetEntry 6	Amount of memory used by the service set, in bytes.
jnxSpSvcSetCpuUtil	jnxSpSvcSetEntry 7	Amount of CPU processing used by the service set, expressed as a percentage of total CPU usage. J Series Services Routers do not have a dedicated CPU for services. CPU usage on these routers appears as 0.
jnxSpSvcSetSvcStyle	jnxSpSvcSetEntry 8	Type of service for the service set. Service types include: • Unknown—The service type is not known. • Interface-service—The service is interface based. • Next-hop-service—The service is next-hop based.
jnxSpSvcSetMemLimitPktDrops	jnxSpSvcSetEntry 9	Number of packets dropped because the service set exceeded its memory limits (operating in the Red zone).
jnxSpSvcSetCpuLimitPktDrops	jnxSpSvcSetEntry 10	Number of packets dropped because the service set exceeded the average CPU limits (when total CPU usage exceeds 85 percent).
jnxSpSvcSetFlowLimitPktDrops	jnxSpSvcSetEntry 11	Number of packets dropped because the service set exceeded the flow limit.
jnxSpSvcSetMemoryUsage64		Amount of memory used by the service set, in bytes.
jnxSpSvcSetMemLimitPktDrops64		Number of packets dropped because the service set exceeded its memory limits (operating in the Red zone).

Table 25: Service-Set SNMP MIB Table (jnxSpSvcSetTable) *(continued)*

MIB Object	jnxSpSvcSet Entry Number	Description
jnxSpSvcSetCpuLimitPktDrops64		Number of packets dropped because the service set exceeded the average CPU limits (when total CPU usage exceeds 85 percent).
jnxSpSvcSetFlowLimitPktDrops64		Number of packets dropped because the service set exceeded the flow limit.
jnxSpSvcSetSessCount		Number of valid sessions in the service-set.

Table 26: Service-Set Service Type SNMP MIB Table (jnxSpSvcSetSvcTypeTable)

MIB Object	(jnxSpSvcSetSvcType Entry Number	Description
jnxSpSvcSetSvcTypeIndex	jnxSpSvcSetSvcTypeEntry 1	An integer used to identify the service type.
jnxSpSvcSetSvcTypeIfName	jnxSpSvcSetSvcTypeEntry 2	The name of the interface identifying the AS PIC. If more than one interface is associated with the AS PIC, the name associated with the lower layer interface is used.
jnxSpSvcSetSvcTypeName	jnxSpSvcSetSvcTypeEntry 3	The name of the service type.
jnxSpSvcSetSvcTypeSvcSets	jnxSpSvcSetSvcTypeEntry 4	Number of service sets configured on the AS PIC that use this service type.
jnxSpSvcSetSvcTypeMemoryUsage	jnxSpSvcSetSvcTypeEntry 5	Amount of memory used by this service type, expressed in bytes.
jnxSpSvcSetSvcTypePctMemoryUsage	jnxSpSvcSetSvcTypeEntry 6	Amount of memory used by this service type, expressed as a percentage of total memory.

Table 26: Service-Set Service Type SNMP MIB Table (jnxSpSvcSetSvcTypeTable) *(continued)*

MIB Object	(jnxSpSvcSetSvcType Entry Number	Description
jnxSpSvcSetSvcTypeCpuUtil	jnxSpSvcSetSvcTypeEntry 7	Amount of CPU processing used by the service set, expressed as a percentage of total CPU usage. J Series Services Routers do not have a dedicated CPU for services. CPU usage on these routers appears as 0.

Table 27: Service-Set Interface SNMP MIB Table (jnxSpSvcSetIfTable)

MIB Object	jnxSpSvcSetIf Entry Number	Description
jnxSpSvcSetIfTableName	jnxSpSvcSetIfEntry 1	The name of the interface used to identify the AS PIC. If more than one interface is associated with the AS PIC, the name associated with the lower layer interface is used.
jnxSpSvcSetIfsvcSets	jnxSpSvcSetIfEntry 2	The number of service sets configured on the AS PIC.
jnxSpSvcSetIfMemoryUsage	jnxSpSvcSetIfEntry 3	Amount of memory used by the AS PIC, expressed in bytes.
jnxSpSvcSetIfPctMemoryUsage	jnxSpSvcSetIfEntry 4	Amount of memory used by the AS PIC, expressed as a percentage of total memory.
jnxSpSvcSetIfPolMemoryUsage	jnxSpSvcSetIfEntry 5	Amount of policy memory used by the AS PIC, expressed in bytes.
jnxSpSvcSetIfPctPolMemoryUsage	jnxSpSvcSetIfEntry 6	Amount of policy memory used by the AS PIC, expressed as a percentage of the total.

Table 27: Service-Set Interface SNMP MIB Table (jnxSpSvcSetIfTable) *(continued)*

MIB Object	jnxSpSvcSetIf Entry Number	Description
jnxSpSvcSetIfMemoryZone	jnxSpSvcSetIfEntry 7	The memory usage zone currently occupied by the AS PIC. The definitions of each zone are: • Green—All new flows are allowed. • Yellow—Unused memory is reclaimed. All new flows are allowed. • Orange—New flows are allowed only for service sets that use less than their equal share of memory. • Red—No new flows are allowed.
jnxSpSvcSetIfCpuUtil	jnxSpSvcSetIfEntry 8	Amount of CPU processing used by the AS PIC, expressed as a percentage of total CPU usage. J Series Services Routers do not have a dedicated CPU for services. CPU usage on these routers appears as 0.
jnxSpSvcSetIfMemoryUsage64		Amount of policy memory used by the AS PIC, expressed in bytes.
jnxSpSvcSetIfPolMemoryUsage64		Amount of policy memory used by the AS PIC, expressed as a percentage of the total.
jnxSpSvcSetIfNumTotalSessActive		Total number of active sessions in the PIC.
jnxSpSvcSetIfPeakTotalSessActive		Number of active sessions in the PIC at any time.
jnxSpSvcSetIfNumCreatedSessPerSec		Number of created sessions per second in the PIC
jnxSpSvcSetIfNumDeletedSessPerSec		Number of deleted sessions per second in the PIC

Table 27: Service-Set Interface SNMP MIB Table (jnxSpSvcSetIfTable) ***(continued)***

MIB Object	jnxSpSvcSetIf Entry Number	Description
jnxSpSvcSetIfNumTotalTcpSessActive jnxSpSvcSetIfNumTotalUdpSessActive jnxSpSvcSetIfNumTotalOtherSessActive		Number of active sessions (TCP, UDP and other)in the PIC
jnxSpSvcSetIfPeakTotalTcpSessActive jnxSpSvcSetIfPeakTotalUdpSessActive jnxSpSvcSetIfPeakTotalOtherSessActive		Number of active sessions (TCP, UDP, and others) in the PIC
jnxSpSvcSetIfPeakCreatedSessPerSec		Number of created sessions per sec in the PIC
jnxSpSvcSetIfPeakDeletedSessPerSec		Number of deleted sessions per sec in the PIC
jnxSpSvcSetIfNumTotalTcpIpv4SessActive jnxSpSvcSetIfNumTotalTcpIpv6SessActive jnxSpSvcSetIfNumTotalUdpIpv4SessActive jnxSpSvcSetIfNumTotalUdpIpv6SessActive jnxSpSvcSetIfNumTotalOtherIpv4SessActive jnxSpSvcSetIfNumTotalOtherIpv6SessActive		Total number of active sessions (TCP, UDP and other) for IPv4 and IPv6 in the PIC
jnxSpSvcSetIfNumTotalTcpGatedSessActive jnxSpSvcSetIfNumTotalUdpGatedSessActive		Number of TCP and UDP gated sessions in the PIC
jnxSpSvcSetIfNumTotalTcpRegSessActive jnxSpSvcSetIfNumTotalUdpRegSessActive		Number of TCP and UDP regular sessions in the PIC
jnxSpSvcSetIfNumTotalTcpTunSessActive jnxSpSvcSetIfNumTotalUdpTunSessActive		Number of TCP and UDP tunneled sessions in the PIC
jnxSpSvcSetIfSessPktRecv		Number of packets received in session handling

Table 27: Service-Set Interface SNMP MIB Table (jnxSpSvcSetIfTable) *(continued)*

MIB Object	jnxSpSvcSetIf Entry Number	Description
jnxSpSvcSetIfSessPktXmit		Number of packets transmitted as a part of session handling
jnxSpSvcSetIfSessSlowPathDiscard		Number of packets discarded in slow path
jnxSpSvcSetIfSessSlowPathForward		Number of packets forwarded in slow path
jnxSpSvcSetIfMspNumCreatedSubsPerSec		Number of subscribers created per sec
jnxSpSvcSetIfMspNumDeletedSubsPerSec		Number of Subscribers deleted per sec
jnxSpSvcSetIfMspNumTotalSubsActive		Number of active subscribers
jnxSpSvcSetIfMspPeakCreatedSubsPerSec		Peak number of created subscribers per sec in the PIC
jnxSpSvcSetIfMspPeakDeletedSubsPerSec		Peak number of deleted subscribers per sec in the PIC
jnxSpSvcSetIfMspPeakTotalSubsActive		Peak number of total active subscribers in the PIC

Summary Mapping of MX-SPC3 CLI Services Operational Commands to SNMP MIBs

Table 28 on page 110 summarizes the mapping of the MX-SPC3 services card operations commands to the respective SNMP MIB.

Table 28: Summary Mapping of MX-SPC3 CLI Services Set Command to SNMP MIBs

CLI Command	Variable Name	MIB Tables	MIB Object
show services service-sets cpu-usage	cpu-utilization-percent	jnxSpSvcSetTable	jnxSpSvcSetCpuUtil
show services service-sets memory-usage	bytes-used		jnxSpSvcSetMemoryUsage64
show services service-sets memory-usage zone	mem-zone		jnxSpSvcSetIfMemoryZone
show services service-sets statistics packet-drops	cpulimit-drops		jnxSpSvcSetCpuLimitPktDrops64
	flowlimit-drops		jnxSpSvcSetFlowLimitPktDrops64
	memlimit-drops		jnxSpSvcSetMemLimitPktDrops64
show services service-sets summary	service-set-bytes-used	jnxSpSvcSetIfTable	jnxSpSvcSetIfMemoryUsage64
	service-set-cpu-utilization		jnxSpSvcSetIfCpuUtil
	service-set-percent-bytes-used		jnxSpSvcSetIfPctMemoryUsage
	service-set-percent-policy-bytes-used		jnxSpSvcSetIfPctPolMemoryUsage
	service-set-policy-bytes-used		jnxSpSvcSetIfPolMemoryUsage64
	service-sets-configured		jnxSpSvcSetIfSvcSets
show services sessions count	sess-count	jnxSpSvcSetTable	jnxSpSvcSetSessCount

Table 28: Summary Mapping of MX-SPC3 CLI Services Set Command to SNMP MIBs *(continued)*

CLI Command	Variable Name	MIB Tables	MIB Object
show services sessions analysis	num-total-session-active	jnxSpSvcSetIfTable	jnxSpSvcSetIfNumTotalSessActive
	peak-total-session-active		jnxSpSvcSetIfPeakTotalSessActive
	num-created-session-per-sec		jnxSpSvcSetIfNumCreatedSessPerSec
	num-deleted-session-per-sec		jnxSpSvcSetIfNumDeletedSessPerSec
	num-total-tcp-session-active		jnxSpSvcSetIfNumTotalTcpSessActive
	num-total-udp-session-active		jnxSpSvcSetIfNumTotalUdpSessActive
	peak-total-tcp-session-active		jnxSpSvcSetIfPeakTotalTcpSessActive
	peak-total-udp-session-active		jnxSpSvcSetIfPeakTotalUdpSessActive
	num-total-other-session-active		jnxSpSvcSetIfNumTotalOtherSessActive
	peak-created-session-per-second		jnxSpSvcSetIfPeakCreatedSessPerSec
	peak-deleted-session-per-second		jnxSpSvcSetIfPeakDeletedSessPerSec
	peak-total-other-session-active		jnxSpSvcSetIfPeakTotalOtherSessActive
	num-total-tcp-ipv4-session-active		jnxSpSvcSetIfNumTotalTcpIpv4SessActive
	num-total-tcp-ipv6-session-active		jnxSpSvcSetIfNumTotalTcpIpv6SessActive
	num-total-udp-ipv4-session-active		jnxSpSvcSetIfNumTotalUdpIpv4SessActive
	num-total-udp-ipv6-session-active		jnxSpSvcSetIfNumTotalUdpIpv6SessActive
	num-total-tcp-gated-session-active		jnxSpSvcSetIfNumTotalTcpGatedSessActive
	num-total-udp-gated-session-active		jnxSpSvcSetIfNumTotalUdpGatedSessActive
	num-total-other-ipv4-session-active		jnxSpSvcSetIfNumTotalOtherIpv4SessActive
	num-total-other-ipv6-session-active		jnxSpSvcSetIfNumTotalOtherIpv6SessActive
	num-total-tcp-regular-session-active		jnxSpSvcSetIfNumTotalTcpRegSessActive

Table 28: Summary Mapping of MX-SPC3 CLI Services Set Command to SNMP MIBs *(continued)*

CLI Command	Variable Name	MIB Tables	MIB Object
	num-total-udp-regular-session-active	jnxSpSvcSetIfTable	jnxSpSvcSetIfNumTotalUdpRegSessActive
	num-total-tcp-tunneled-session-active		jnxSpSvcSetIfNumTotalTcpTunSessActive
	num-total-udp-tunneled-session-active		jnxSpSvcSetIfNumTotalUdpTunSessActive
	session-pkts-received		jnxSpSvcSetIfSessPktRecv
	session-pkts-transmitted		jnxSpSvcSetIfSessPktXmit
	session-slow-path-discard		jnxSpSvcSetIfSessSlowPathDiscard
	session-slow-path-forward		jnxSpSvcSetIfSessSlowPathForward
show services subscriber analysis	msp-num-created-subs-per-sec		jnxSpSvcSetIfMspNumCreatedSubsPerSec
	msp-num-deleted-subs-per-sec		jnxSpSvcSetIfMspNumDeletedSubsPerSec
	msp-num-total-subs-active		jnxSpSvcSetIfMspNumTotalSubsActive
	msp-peak-created-subs-per-second		jnxSpSvcSetIfMspPeakCreatedSubsPerSec
	msp-peak-deleted-subs-per-second		jnxSpSvcSetIfMspPeakDeletedSubsPerSec
	msp-peak-total-subs-active		jnxSpSvcSetIfMspPeakTotalSubsActive

NAT SNMP MIBs

This section describes the **jnxSrcNatStatsTable** MIB objects.

Table 29 on page 113 describes the source NAT SNMP MIB objects for the MS-MPC services card. This table exposes the source NAT translation attributes of the translated addresses.

Table 30 on page 114 describes the source NAT SNMP MIB objects for the MX-SPC3 services card. This table contains information on source IP address translation only.

Table 29: MS-MPC Services Card Source NAT SNMP MIB Table (jnxSrcNatStatsTable)

jnxSrcNatStatsTable	MIB Object	Description
	jnxNatSrcPoolName	The name of dynamic source IP address pool
	jnxNatSrcXlatedAddrType	V4 or V6. The type of dynamic source IP address allocated from the address pool used in the NAT translation
	jnxNatSrcPoolType	The source port pool type indicates whether the address translation is done with port or without the port, or if it is a static translation. Ex napt-44, nat64 etc
	jnxNatSrcNumPortAvail	The number of ports available with this pool
	jnxNatSrcNumPortInuse	The number of ports in use for this NAT address entry
	jnxNatSrcNumAddressAvail	The total number of addresses available in this pool
	jnxNatSrcNumAddressInUse	The number of addresses in use from this pool
	jnxNatSrcNumSessions	The number of sessions are in use based on this NAT address entry
jnxNatRuleTable		This table monitors NAT rule hits
	jnxNatRuleName	NAT rule name
	jnxNatRuleType	NAT types: Static Source, Static Destination, Dynamic Source and NAPT. Ex: napt44 etc
	jnxNatRuleTransHits	The number of hits on this NAT rule
jnxNatPoolTable		This table monitors NAT pool hits
	jnxNatPoolName	NAT Pool name

Table 29: MS-MPC Services Card Source NAT SNMP MIB Table (jnxSrcNatStatsTable) *(continued)*

jnxSrcNatStatsTable	MIB Object	Description
	jnxNatPoolType	NAT types: Static Source, Static Destination, Dynamic Source and NAPT. Ex: napt44 etc
	jnxNatPoolTransHits	The number of hits on this NAT Pool

Table 30: MX-SPC3 Source NAT SNMP MIB Table (jnxNatObjects)

jnxJsSrcNatStatsTable	MIB Object	Description
	jnxJsNatSrcPoolName	The name of dynamic source IP address pool
	jnxJsNatSrcXlatedAddrType	New MIB. The type of dynamic source IP address allocated from the address pool used in the NAT translation. Value is v4 or v6
	jnxJsNatSrcPoolType	withPAT or withoutPAT or static
	jnxJsNatSrcNumPortAvail	New MIB. The number of ports available with this pool
	jnxJsNatSrcNumPortInuse	The number of ports in use for this NAT address entry
	jnxJsNatSrcNumSessions	The number of sessions are in use based on this NAT address entry
	jnxJsNatSrcNumAddressAvail	New MIB. The total number of addresses available in this pool
	jnxJsNatSrcNumAddressInuse	New MIB. The number of addresses in use from this pool
jnxJsNatRuleTable		This table monitors NAT rule hits
	jnxJsNatRuleName	NAT rule name
	jnxJsNatRuleType	NAT types: Source, Destination and Static
	jnxJsNatRuleTransHits	The number of hits on this NAT rule. **Status is deprecated. New - jnxJsNatRuleHits**

Table 30: MX-SPC3 Source NAT SNMP MIB Table (jnxNatObjects) *(continued)*

jnxJsSrcNatStatsTable	MIB Object	Description
	jnxJsNatRuleHits	The number of hits on this NAT rule,
	jnxJsNatRuleNumOfSessions	The number of sessions on this NAT rule
	jnxJsNatTransType	New MIB. **Details below**
jnxJsNatPoolTable		This table monitors NAT pool hits
	jnxJsNatPoolName	NAT Pool name
	jnxJsNatPoolType	NAT types: Source, Destination and Static
	jnxJsNatPoolTransHits	The number of hits on this NAT pool. **Status is deprecated. New - jnxJsNatPoolHits**
	jnxJsNatPoolHits	The number of hits on this NAT pool to deprecate jnxJsNatRuleTransHits.

SNMP Traps

Table 31 on page 115 describes the SNMP traps supported by both the MS-MPC services card and the MX-SPC3 services card.

Table 31: SNMP Traps

Trap	Description
SPD_TRAP_OIDS(jnxSpSvcSetZoneEntered)	jnxSpSvcSetZoneEntered — Indicates that an AS PIC has entered a more severe memory usage zone from a less severe memory usage zone. The zone entered is identified by JnxSpSvcSetIfMemoryZone
SPD_TRAP_OIDS(jnxSpSvcSetZoneExited)	jnxSpSvcSetZoneExited — Indicates that an AS PIC has exited a more severe memory usage zone to a less severe memory usage zone. The zone entered is identified by JnxSpSvcSetIfMemoryZone.

Table 31: SNMP Traps *(continued)*

Trap	Description
SPD_TRAP_OIDS(jnxSpSvcSetCpuExceeded)	jnxSpSvcSetCpuExceeded — Indicates that an AS PIC has over 85% CPU usage.
SPD_TRAP_OIDS(jnxSpSvcSetCpuOk)	jnxSpSvcSetCpuOk — Indicates that an AS PIC has returned to less than 85%CPU usage.
SPD_TRAP_OIDS(jnxSpSvcSetFlowLimitUtilized)	jnxSpSvcSetFlowLimitUtilized — Indicates a service-set has reached its upper limit of flows threshold of a maximun flows allowed for a service set.

Configuring SNMP Trap Generation

This sections describes how to configure the MS-MPC service card versus the MX-SPC3 services card to generate SNMP traps.

Configuring SNMP Trap for NAT Ports in a Source NAT Pool

If the current usage is above the raise threshold or below the clear threshold, we will generate a SNMP trap.

Configuring SNMP Traps for NAT Ports in a Source NAT Pool on an MS-MPC

```
user@host# set services nat pool NAT_POOL_TEST snmp-trap-thresholds address-port low 50
user@host# set services nat pool NAT_POOL_TEST snmp-trap-thresholds address-port high 75
```

Configuring SNMP Traps for NAT Ports in a Source NAT Pool on an MX-SPC3

```
user@host# set services nat source pool NAT_POOL_TEST pool-utilization-alarm raise-threshold 50
user@host# set services nat source pool NAT_POOL_TEST pool-utilization-alarm clear-threshold 40
```

Configuring SNMP Trap for Sessions

This is infra trap which configures SNMP flow thresholds for all flows for a service set or flows for all NAT pools configured for a service set.

Configuring a Sessions SNMP Trap on an MS-MPC

```
user@host# set services service-set SS_TEST max-flows 2m
user@host# set services service-set SS_TEST snmp-trap-thresholds flow low 50
user@host# set services service-set SS_TEST snmp-trap-thresholds flow high 75
```

Configuring a Sessions SNMP Trap on an MX-SPC3

```
user@host# set services service-set ss1 service-set-options session-limit maximum 2000
user@host# set services service-set ss1 snmp-trap-thresholds session low 50
user@host# set services service-set ss1 snmp-trap-thresholds session high 60
```

Example-Configuration for MX-SPC3 NAT for Three SNMP MIB Tables

Example Configuration

`user@host>` **show services | display set**

```
Configuration
=============
show services | display set

set services service-set ss1_nh_style1 nat-rule-sets rset1
set services service-set ss1_nh_style1 nat-rule-sets rset2
set services service-set ss1_nh_style1 nat-rule-sets rset5
set services service-set ss1_nh_style1 next-hop-service inside-service-interface
vms-0/0/0.1
set services service-set ss1_nh_style1 next-hop-service outside-service-interface
 vms-0/0/0.2
set services nat source pool src_pool2_v6 address 300::0/128
set services nat source pool src_pool1 address 50.0.0.0/29
set services nat source rule-set rset1 rule nr1 match source-address 10.0.0.0/32
set services nat source rule-set rset1 rule nr1 match destination-address
20.0.0.0/32
set services nat source rule-set rset1 rule nr1 match application any
set services nat source rule-set rset1 rule nr1 then source-nat pool src_pool1
set services nat source rule-set rset1 match-direction input
set services nat source rule-set rset2 rule nr2_v6 match source-address 200::0/34
set services nat source rule-set rset2 rule nr2_v6 match destination-address
400::0/34
set services nat source rule-set rset2 rule nr2_v6 match application any
set services nat source rule-set rset2 rule nr2_v6 then source-nat pool src_pool2_v6
set services nat source rule-set rset2 match-direction input
set services nat destination pool src_pool5_dnat address 20.0.0.0/30
set services nat destination rule-set rset5 rule nr5_dnat match destination-address
 21.0.0.0/30
set services nat destination rule-set rset5 rule nr5_dnat match application any
set services nat destination rule-set rset5 rule nr5_dnat then destination-nat
pool src_pool5_dnat
set services nat destination rule-set rset5 match-direction input
set services nat traceoptions file nat-trace.txt
set services nat traceoptions flag all
```

show snmp mib walk jnxJsSrcNatStatsTable

user@host>**show snmp mib walk jnxJsSrcNatStatsTable**

```
jnxJsNatSrcPoolName.2.112.49.0.0.0.0.0.0 = p1
jnxJsNatSrcXlatedAddrType.2.112.49.0.0.0.0.0.0 = 1
jnxJsNatSrcPoolType.2.112.49.0.0.0.0.0.0 = 1
jnxJsNatSrcNumPortInuse.2.112.49.0.0.0.0.0.0 = 0
jnxJsNatSrcNumSessions.2.112.49.0.0.0.0.0.0 = 0
jnxJsNatSrcNumPortAvail.2.112.49.0.0.0.0.0.0 = 10
jnxJsNatSrcNumAddressAvail.2.112.49.0.0.0.0.0.0 = 1
jnxJsNatSrcNumAddressInuse.2.112.49.0.0.0.0.0.0 = 0
```

show snmp mib walk jnxJsNatPoolTable

user@host>**show snmp mib walk jnxJsNatPoolTable**

```
jnxJsNatPoolName.9.115.114.99.95.112.111.111.108.49.1 = src_pool1
jnxJsNatPoolName.14.115.114.99.95.112.111.111.108.53.95.100.110.97.116.2 =
src_pool5_dnat
jnxJsNatPoolType.9.115.114.99.95.112.111.111.108.49.1 = 1
jnxJsNatPoolType.14.115.114.99.95.112.111.111.108.53.95.100.110.97.116.2 = 2
jnxJsNatPoolTransHits.9.115.114.99.95.112.111.111.108.49.1 = 0
jnxJsNatPoolTransHits.14.115.114.99.95.112.111.111.108.53.95.100.110.97.116.2 = 0
jnxJsNatPoolHits.9.115.114.99.95.112.111.111.108.49.1 = 0
jnxJsNatPoolHits.14.115.114.99.95.112.111.111.108.53.95.100.110.97.116.2 = 0
jnxJsNatPoolUtil.9.115.114.99.95.112.111.111.108.49.1 = 0
jnxJsNatPoolUtil.14.115.114.99.95.112.111.111.108.53.95.100.110.97.116.2 = 0
```

show snmp mib walk jnxJsNatRuleTable

user@host>**show snmp mib walk jnxJsNatRuleTable**

```
jnxJsNatRuleName.3.110.114.49.1 = nr1
jnxJsNatRuleName.6.110.114.50.95.118.54.1 = nr2_v6
jnxJsNatRuleName.8.110.114.53.95.100.110.97.116.2 = nr5_dnat
jnxJsNatRuleType.3.110.114.49.1 = 1
jnxJsNatRuleType.6.110.114.50.95.118.54.1 = 1
jnxJsNatRuleType.8.110.114.53.95.100.110.97.116.2 = 2
jnxJsNatRuleTransHits.3.110.114.49.1 = 0
jnxJsNatRuleTransHits.6.110.114.50.95.118.54.1 = 0
jnxJsNatRuleTransHits.8.110.114.53.95.100.110.97.116.2 = 0
jnxJsNatRuleHits.3.110.114.49.1 = 0
jnxJsNatRuleHits.6.110.114.50.95.118.54.1 = 0
```

```
jnxJsNatRuleHits.8.110.114.53.95.100.110.97.116.2 = 0
jnxJsNatRuleNumOfSessions.3.110.114.49.1 = 0
jnxJsNatRuleNumOfSessions.6.110.114.50.95.118.54.1 = 0
jnxJsNatRuleNumOfSessions.8.110.114.53.95.100.110.97.116.2 = 0
jnxJsNatTransType.3.110.114.49.1 = 13
jnxJsNatTransType.6.110.114.50.95.118.54.1 = 22
jnxJsNatTransType.8.110.114.53.95.100.110.97.116.2 = 13
```

SNMP Trace Logs for Traps

This section provides some example trace logs for these SNMP traps.

CPU-Utilization Trap

```
Mar 20 15:07:52.575680 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Mar 20 15:07:52.575697 snmpd[0]  <<< V2 Trap
Mar 20 15:07:52.575714 snmpd[0]  <<<  Source:      10.48.12.170
Mar 20 15:07:52.575730 snmpd[0]  <<<  Destination: 190.1.1.1
Mar 20 15:07:52.575745 snmpd[0]  <<<  Version:     SNMPv2
Mar 20 15:07:52.575761 snmpd[0]  <<<  Community:   rtlogd_trap
Mar 20 15:07:52.575777 snmpd[0]  <<<
Mar 20 15:07:52.575807 snmpd[0]  <<<   OID  : sysUpTime.0
Mar 20 15:07:52.575824 snmpd[0]  <<<   type : TimeTicks
Mar 20 15:07:52.575841 snmpd[0]  <<<   value: (7605999) 21:07:39.99
Mar 20 15:07:52.575856 snmpd[0]  <<<
Mar 20 15:07:52.575878 snmpd[0]  <<<   OID  : snmpTrapOID.0
Mar 20 15:07:52.575894 snmpd[0]  <<<   type : Object
Mar 20 15:07:52.575915 snmpd[0]  <<<   value: jnxSpSvcSetCpuExceeded
Mar 20 15:07:52.575945 snmpd[0]  <<<
Mar 20 15:07:52.575968 snmpd[0]  <<<   OID  : jnxSpSvcSetIfCpuUtil.4294967295
Mar 20 15:07:52.575984 snmpd[0]  <<<   type : Gauge
Mar 20 15:07:52.576000 snmpd[0]  <<<   value: 45
Mar 20 15:07:52.576015 snmpd[0]  <<<
Mar 20 15:07:52.576033 snmpd[0]  <<<   OID  : jnxSpSvcSetIfTableName.4294967295
Mar 20 15:07:52.576049 snmpd[0]  <<<   type : OctetString
Mar 20 15:07:52.576066 snmpd[0]  <<<   value: "ms-2/0/0"
Mar 20 15:07:52.576085 snmpd[0]  <<<   HEX  : 6d 73 2d 32  2f 30 2f 30
Mar 20 15:07:52.576100 snmpd[0]  <<<
Mar 20 15:07:52.576118 snmpd[0]  <<<   OID  : snmpTrapEnterprise.0
Mar 20 15:07:52.576134 snmpd[0]  <<<   type : Object
Mar 20 15:07:52.576155 snmpd[0]  <<<   value: jnxProductNameMX480
Mar 20 15:07:52.576169 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Memoryzone Trap

```
Mar 21 10:53:31.550471 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Mar 21 10:53:31.550491 snmpd[0]  <<< V2 Trap
Mar 21 10:53:31.550507 snmpd[0]  <<<  Source:      10.48.12.170
Mar 21 10:53:31.550522 snmpd[0]  <<<  Destination: 190.1.1.1
Mar 21 10:53:31.550536 snmpd[0]  <<<  Version:     SNMPv2
Mar 21 10:53:31.550551 snmpd[0]  <<<  Community:   rtlogd_trap
Mar 21 10:53:31.550566 snmpd[0]  <<<
Mar 21 10:53:31.550585 snmpd[0]  <<<   OID  : sysUpTime.0
Mar 21 10:53:31.550600 snmpd[0]  <<<   type : TimeTicks
Mar 21 10:53:31.550616 snmpd[0]  <<<   value: (6076788) 16:52:47.88
Mar 21 10:53:31.550631 snmpd[0]  <<<
Mar 21 10:53:31.550649 snmpd[0]  <<<   OID  : snmpTrapOID.0
Mar 21 10:53:31.550664 snmpd[0]  <<<   type : Object
Mar 21 10:53:31.550681 snmpd[0]  <<<   value: jnxSpSvcSetZoneEntered
Mar 21 10:53:31.550695 snmpd[0]  <<<
Mar 21 10:53:31.550714 snmpd[0]  <<<   OID  : jnxSpSvcSetIfMemoryZone.4294967295
Mar 21 10:53:31.550729 snmpd[0]  <<<   type : Number
Mar 21 10:53:31.550744 snmpd[0]  <<<   value: 2
Mar 21 10:53:31.550758 snmpd[0]  <<<
Mar 21 10:53:31.550776 snmpd[0]  <<<   OID  : jnxSpSvcSetIfTableName.4294967295
Mar 21 10:53:31.550791 snmpd[0]  <<<   type : OctetString
Mar 21 10:53:31.550806 snmpd[0]  <<<   value: "ms-2/0/0"
Mar 21 10:53:31.550824 snmpd[0]  <<<   HEX  : 6d 73 2d 32  2f 30 2f 30
Mar 21 10:53:31.550838 snmpd[0]  <<<
Mar 21 10:53:31.550856 snmpd[0]  <<<   OID  : snmpTrapEnterprise.0
Mar 21 10:53:31.550871 snmpd[0]  <<<   type : Object
Mar 21 10:53:31.550888 snmpd[0]  <<<   value: jnxProductNameMX480
Mar 21 10:53:31.550901 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

Session Limit Trap

```
Mar 21 10:53:31.551133 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
Mar 21 10:53:31.551152 snmpd[0]  <<< V2 Trap
Mar 21 10:53:31.551168 snmpd[0]  <<<  Source:      10.48.12.170
Mar 21 10:53:31.551184 snmpd[0]  <<<  Destination: 190.1.1.1
Mar 21 10:53:31.551197 snmpd[0]  <<<  Version:     SNMPv2
Mar 21 10:53:31.551212 snmpd[0]  <<<  Community:   rtlogd_trap
Mar 21 10:53:31.551228 snmpd[0]  <<<
Mar 21 10:53:31.551246 snmpd[0]  <<<   OID  : sysUpTime.0
Mar 21 10:53:31.551262 snmpd[0]  <<<   type : TimeTicks
Mar 21 10:53:31.551278 snmpd[0]  <<<   value: (6076788) 16:52:47.88
```

```
Mar 21 10:53:31.551292 snmpd[0]  <<<
Mar 21 10:53:31.551311 snmpd[0]  <<<   OID  : snmpTrapOID.0
Mar 21 10:53:31.551326 snmpd[0]  <<<   type : Object
Mar 21 10:53:31.551343 snmpd[0]  <<<   value: jnxSpSvcSetFlowLimitUtilised
Mar 21 10:53:31.551358 snmpd[0]  <<<
Mar 21 10:53:31.551376 snmpd[0]  <<<   OID  : jnxSpSvcSetFlowLimitUtil.0
Mar 21 10:53:31.551391 snmpd[0]  <<<   type : Number
Mar 21 10:53:31.551406 snmpd[0]  <<<   value: 45
Mar 21 10:53:31.551421 snmpd[0]  <<<
Mar 21 10:53:31.551439 snmpd[0]  <<<   OID  : jnxSpSvcSetNameUtil.0
Mar 21 10:53:31.551454 snmpd[0]  <<<   type : OctetString
Mar 21 10:53:31.551471 snmpd[0]  <<<   HEX  : 20 bc 55 88  01
Mar 21 10:53:31.551486 snmpd[0]  <<<
Mar 21 10:53:31.551503 snmpd[0]  <<<   OID  : snmpTrapEnterprise.0
Mar 21 10:53:31.551518 snmpd[0]  <<<   type : Object
Mar 21 10:53:31.551535 snmpd[0]  <<<   value: jnxProductNameMX480
Mar 21 10:53:31.551549 snmpd[0]  <<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
```

RELATED DOCUMENTATION

SNMP MIB Explorer

Explore System Log Messages

5

CHAPTER

Getting Started Configuration Statements

bypass-traffic-on-exceeding-flow-limits

Syntax

```
bypass-traffic-on-exceeding-flow-limits;
```

Hierarchy Level

[editservices service-set *service-set-name* service-set-options]

Release Information

Statement introduced in Junos OS Release 10.1.
Statement introduced in Junos OS Release 19.3R2 on MX240, MX480 and MX960 routers using the MX-SPC3 services card..

Description

bypass-traffic-on-exceeding-flow-limitsbypass-traffic-on-exceeding-flow-limitsbypass-traffic-on-exceeding-flow-limits

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces

category (System Logging)

Syntax

category *category*, *category*....*category*;

Hierarchy Level

[edit services service-set *service-set-name* **syslog stream**]

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services on the MX-SPC3 services card.

Description

Specify the categories for which you want to collect logs.

Options

all—All events are logged

content-security—Content security events are logged

fw-auth—Fw-auth events are logged

screen —Screen events are logged

alg—ALG events are logged

nat—NAT events are logged

flow—Flow events are logged

sctp—Sctp events are logged

gtp—Gtp events are logged

ipsec—Ipsec events are logged

idp—Idp events are logged

rtlog—Rtlog events are logged

pst-ds-lite—Pst-ds-lite events are logged

appqos—Appqos events are logged

secintel—Secintel events are logged

aamw—AAMW events are logged

sfw—Stateful Firewall events are logged

session —Session open and close events are logged

session-open—Session open events are logged

session-close—Session close events are logged

urlf—DNS request filtering events are logged

ha—Stateful High-Availability open and close events are logged

ha-open—Stateful High-Availability open events are logged

ha-close—Stateful High-Availability close events are logged

pcp—PCP logs

Required Privilege Level

system—To view this statement in the configuration.

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

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

drop-member-traffic (Aggregated Multiservices)

Syntax

```
drop-member-traffic {
   rejoin-timeout rejoin-timeout;
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options member-failure-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify whether the broadband gateway should drop traffic to a services PIC when it fails.

For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration is valid only when two or more services PICs have failed.

The remaining statement is explained separately. See CLI Explorer.

Default

If this statement is not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

member-failure-options (Aggregated Multiservices) | 160

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

enable-asymmetric-traffic-processing (Service Set Next Gen Services)

Syntax

```
enable-asymmetric-traffic-processing;
```

Hierarchy Level

[edit services service-set *service-set-name* service-set-options]

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Enable the service set to handle unidirectional traffic.

Required Privilege Level

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

RELATED DOCUMENTATION

enable-rejoin (aggregated Multiservices)

Syntax

```
enable-rejoin;
```

Hierarchy Level

[edit interfaces *interface-name* load-balancing-options member-failure-options redistribute-all-traffic]

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Enable the failed member to rejoin the aggregated Multiservices (AMS) interface after the member comes back online.

For many-to-one (N:1) high availability (HA) for service applications like Network Address Translation (NAT), this configuration allows the failed members to rejoin the pool of active members automatically.

Default

If you do not configure this option, then the failed members do not automatically rejoin the **ams** interface even after coming back online.

Required Privilege Level

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

RELATED DOCUMENTATION

redistribute-all-traffic (Aggregated Multiservices) | 169

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

enable-subscriber-analysis (Services Options VMS Interfaces)

Syntax

```
enable-subscriber-analysis;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Enable the creation of subscribers if the following are not configured, but you want subscribers to be created:

- NAT
- The **max-sessions-per-subscriber** statement at the **[edit services service-set *service-set-name*]** hierarchy level

Required Privilege Level

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

RELATED DOCUMENTATION

How to Configure Services Interfaces for Next Gen Services | 77

enable-subscriber-analysis (Services Options VMS Interfaces)

Syntax

```
enable-subscriber-analysis;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Enable the creation of subscribers if the following are not configured, but you want subscribers to be created:

- NAT
- The **max-sessions-per-subscriber** statement at the **[edit services service-set *service-set-name*]** hierarchy level

Required Privilege Level

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

RELATED DOCUMENTATION

How to Configure Services Interfaces for Next Gen Services | 77

event-rate (Next Gen Services Service-Set Local System Logging)

Syntax

```
event-rate rate-per-second;
```

Hierarchy Level

```
[edit services services-set name syslog]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Rate at which log messages are sent per second to the local file.

Options

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

file (Next Gen Services Global System Logging)

Syntax

```
file <filename> <files files> <match match> <size size> <(world-readable | no-world-readable)>;
```

Hierarchy Level

```
[edit services rtlog traceoptions]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Trace file information

Options

All other options are explained separately.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

filename (Next Gen Services Global System Logging)

Syntax

```
filename;
```

Hierarchy Level

```
[edit services rtlog traceoptions file]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Name of file in which to write trace information

Options

filename—Name of file in which to write trace information

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

files (Next Gen Services Global System Logging)

Syntax

```
files files;
```

Hierarchy Level

```
[edit services rtlog traceoptions file filename]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Maximum number of trace files

Options

files—Maximum number of trace files

Default: 3

Range: 2 through 1000

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

flag (Next Gen Services Global System Logging)

Syntax

```
flag name;
```

Hierarchy Level

```
[edit services rtlog traceoptions]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

List of things to include in trace.

Options

name—

Values:

- all—Enable all interface trace flags. event —Trace interface events.
- cache—Enable interface flags for Web filtering cache maintained on the routing table.
- enhanced—Enable interface flags for processing through Enhanced Web Filtering.
- ipc—Trace interface IPC messages.
- media—Trace interface media changes.
- critical—Trace critical events.
- major—Trace major events

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

format (Next Gen Services Service-Set Remote System Logging)

Syntax

```
format format;
```

Hierarchy Level

```
edit services service-set name syslog stream stream-name
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services MX-SPC3 services card.

Description

Specify the file format for the log messages being sent to the remote server.

Options

The file format can be one of the following:

binary—Binary syslog defined by Juniper Networks. Requires Juniper Networks decoders on the server side to decode the logs.

sd-syslog—Structured syslog (defined by RFC5424)

syslog—Traditional syslog (defined by RFC5424)

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

host (Next Gen Services Service-Set Remote System Logging)

Syntax

```
host host-ip-address;
```

Hierarchy Level

```
edit services service-set name syslog stream stream-name
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Specify the IP address of syslog server to receive log messages.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

hash-keys (Interfaces)

Syntax

```
hash-keys {
    egress-key (source-ip | destination-ip);
    ingress-key (source-ip | destination-ip);
    ipv6-source-prefix-length ipv6-source-prefix-length;
}
```

Hierarchy Level

```
[edit interfaces unit unit-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
ipv6-source-prefix-length option introduced in Junos OS Release 18.2R1.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card. The **ipv6-source-prefix-length** option is not supported for Next Gen Services.

Description

Configure the hash keys used for load balancing in aggregated multiservices (AMS) for next-hop style services. The hash keys supported in the ingress and egress direction are the source IP address and destination IP address.

Hash keys are used to define the load-balancing behavior among the various members in the AMS. For example, if **hash-keys** is configured as **source-ip**, then the hashing is performed based on the source IP address of the packet, so that all packets with the same source IP address land on the same member. When you use **ingress-key** and **egress-key**, you must configure hash keys to take the traffic direction into consideration. For example, if you configure **hash-keys** as **source-ip** in the ingress direction, then you must configure **hash-keys** as **destination-ip** in the egress direction. This is required to ensure that the packets of the same flow reach the same member of the AMS group.

If you are configuring an AMS interface used in a service set for DS-Lite,

The remaining statements are explained separately. See CLI Explorer.

Options

egress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction.

egress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the egress flow direction.

ingress-key destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the ingress flow direction.

ingress-key source-ip—Use the source IP address of the flow to compute the hash used in load balancing. Configure the hash keys to be used in the ingress flow direction.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Load Balancing on AMS Infrastructure | 95

high-availability-options (Aggregated Multiservices)

Syntax

```
high-availability-options {
  (many-to-one | one-to-one) {
    preferred-backup preferred-backup;
  }
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the high availability options for the aggregated multiservices (AMS) interface. For service applications, if only the load-balancing feature is being used, then this configuration is optional.

For many-to-one (N:1) high availability support for service applications like Network Address Translation (NAT), the preferred backup services PIC, in hot standby mode, backs up one or more (N) active services PICs.

> **NOTE:** In both cases, if one of the active services PICs goes down, then the backup replaces it as the active PIC. When the failed PIC comes back up, it becomes the new backup. This is called *floating backup*.

One-to-one (1:1) high availability support associates a single backup interface with a single active interface. 1:1 configuration is supported only on the MS-MPC and MX-SPC3. In 1:1 (stateful) configurations, synchronization causes the active and back up PICs to synchronize traffic states and data structures, preventing data loss during a failover event. Stateful synchronization is required for IPsec high availability support. For IPsec connections, AMS supports 1:1 configuration only.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

load-balancing-options | 150

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

inactivity-asymm-tcp-timeout (Service Set Next Gen Services)

Syntax

```
inactivity-asymm-tcp-timeout seconds;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Configure the number of seconds that a unidirectional TCP session can be inactive before it is closed. Valid settings: 4 through 86400 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

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

inline-services (PIC level)

Syntax

```
inline-services {
   bandwidth (1g | 10g | 20g | 30g | 40g | 100g);
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Enable inline services on PICs residing on MPCs and optionally specify a bandwidth for traffic on the inline service interface.

The remaining statement is explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

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

RELATED DOCUMENTATION

Enabling Inline Service Interfaces

Configuring an L2TP LNS with Inline Service Interfaces

load-balancing-options (Aggregated Multiservices)

Syntax

```
load-balancing-options {
    high-availability-options {
        (many-to-one | one-to-one) {
            preferred-backup preferred-backup;
        }
    }
    member-failure-options {
        drop-member-traffic {
            rejoin-timeout rejoin-timeout;
        }
        redistribute-all-traffic {
            enable-rejoin;
        }
    }
    hash-keys {
        egress-key (destination-ip | source-ip);
        ingress-key (destination-ip | source-ip);
    }
    member-interface interface-name;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the high availability (HA) options for the aggregated multiservices (AMS) interface.

Many-to-one (N:1) high availability mode for service applications like Network Address Translation (NAT) is supported. In the case of N:1 high availability mode, one services PIC is the backup (in hot standby mode) for one or more (N) active services PICs. If one of the active services PICs goes down, then the backup replaces it as the active services PIC. When the failed PIC comes back online, it becomes the new backup. This is called *floating backup mode*. In an N:1 (stateless) configuration, traffic states and data structures are not synchronized between active PICs and the backup PIC.

You can also configure a one-to-one (1:1) high availability mode. In the 1:1 configuration, a single interface is configured as the backup for another single active interface. If the active interface goes down, the backup interface replaces it as the active interface. A 1:1 (stateful) configuration synchronizes traffic states and data structures between the active services PIC and the backup services PIC. This is required for IPsec connections. One-to-one high availability is supported on the MS-MPC but it is not supported for MX-SPC3 in this release.

Load-balancing might not be uniform among member interfaces in certain network deployments. The variance can be because of a misconfiguration, which causes the traffic itself not to be sufficiently randomly distributed, causing the hash keys to be ineffective (for example, the hash key is destination IP but all sessions have only source IP address). The variation can be within the expected range and the load balancing depends on the IP addresses chosen. The hash calculation performs a checksum on several bits of the IP address and not only on the last few lower significant bits of the IP address. In such a scenario, the load-balancing ratio can change, for instance, if the source IP address is changed from 20.0.0.0/24 to 20.0.1.0/24.

The distribution of traffic across member interfaces of an AMS interface is static load-balancing. Flows are load balanced based on a packet hash on parameters such as source IP or destination IP. Load-balancing effectiveness depends on the IP address or protocol diversity. For example, if the hash key is destination IP and all packets have the same destination, then all flows are directed to the same member. This is flow-level load balancing and not per packet. As a result, traffic between a pair of addresses may be 10,000 pps, whereas another pair of addresses may have 1 pps. The load of the former is not distributed among members. High availability is limited to stateless HA. When a backup interface takes over as an active interface, all flows are reestablished (for example. packets may undergo NAT processing differently after failover).

With a stateful firewall, static NAT as basic-nat44 or destination-nat44, and dynamic NAT as nat64, napt-44, dynamic-nat44, and with application layer gateways (ALGs) configured, NAT hairpinning is not supported. Input direction for rule match to be applied is supported only for dynamic NAT types (NAT64, NAT44, and dynamic-NAT44). Service-set policies need to have input or input-output direction only. Flows on all active members are reset when the number of actives changes. The resetting of flows can be avoided at the cost of failed-member's traffic loss using certain options.

The remaining statements are explained separately. See CLI Explorer.

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

local-category (Next Gen Services Service-Set Local System Logging)

Syntax

```
local-category category, category....category;
```

Hierarchy Level

```
[edit services service-set name  syslog
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Specify the category for which you want to collect local logs.

Options

all—All events are logged

content-security—Content security events are logged

fw-auth—Fw-auth events are logged

screen —Screen events are logged

alg—Alg events are logged

nat—NAT events are logged

flow—Flow events are logged

sctp—Sctp events are logged

gtp—Gtp events are logged

ipsec—Ipsec events are logged

idp—Idp events are logged

rtlog—Rtlog events are logged

pst-ds-lite—Pst-ds-lite events are logged

appqos—Appqos events are logged

secintel—Secintel events are logged

aamw—AAMW events are logged

sfw—Stateful Firewall events are logged

session —Session open and close events are logged

session-open—Session open events are logged

session-close—Session close events are logged

urlf—DNS request filtering events are logged

ha—Stateful High-Availability open and close events are logged

ha-open—Stateful High-Availability open events are logged

ha-close—Stateful High-Availability close events are logged

pcp—PCP logs

Required Privilege Level
system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

local-log-tag (Next Gen Services Service-Set System Logging)

Syntax

```
local-log-tag tag-stamp;
```

Hierarchy Level

```
[edit services service-set name  syslog
edit services service-set name syslog stream stream-name
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Each log message is stamped with this tag.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

many-to-one (Aggregated Multiservices)

Syntax

```
many-to-one {
    preferred-backup preferred-backup;
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options high-availability-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the many-to-one (N:1) preferred backup for the aggregated multiservices (AMS) interface.

> **NOTE:** The preferred backup must be one of the member interfaces (mams–) that have already been configured at the [**edit interfaces *interface-name* load-balancing-options**] hierarchy level. Even in the case of mobile control plane redundancy, which is one-to-one (1:1), the initial preferred backup is configured at this hierarchy level.

Options

preferred-backup *preferred-backup*—Use the specified interface as the preferred backup member interface.

The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

interface—To view this statement in the configuration.

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

RELATED DOCUMENTATION

high-availability-options (Aggregated Multiservices) | 146

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

match (Next Gen Services Global System Logging)

Syntax

```
match match;
```

Hierarchy Level

```
[edit services rtlog traceoptions file]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Regular expression for lines to be logged

Options

match—Regular expression for lines to be logged

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

max-session-setup-rate (Service Set)

Syntax

```
max-session-setup-rate (number | numberk);
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.1R1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Set the maximum number of session setups allowed per second for the service set. After this setup rate is reached, any additional session setup attempts are dropped. If you do not include the **max-session-setup-rate** statement, the session setup rate is not limited.

Options

max-session-setup-rate *number*—Use the specified maximum number of session setups per second.

Range: 1 through 429,496,729

Default: 0 (The session setup rate is not limited.)

***number*k**—Maximum number of sessions, expressed in thousands. Starting in Junos OS Release 18.4R1, 1k=1000. Prior to Junos OS Release 18.4R1, 1k=1024.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Set Limitations

max-sessions-per-subscriber (Service Set Next Gen Services)

Syntax

```
max-sessions-per-subscriber session-number;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Set the maximum number of sessions allowed from a single subscriber.

Options

session-number—Maximum number of sessions.

> **NOTE:** There is no default value. You must configure a value for the configuration to take effect.

Range: 1 through 32000

Required Privilege Level

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

RELATED DOCUMENTATION

maximum

Syntax

```
maximum number;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.6.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the maximum number of sessions allowed simultaneously on services cards. If you specify the maximum number of sessions to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for the maximum number of sessions.

Options

number—Maximum number of sessions.

Range: 1 through 4,294,967,295

Required Privilege Level

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

RELATED DOCUMENTATION

member-failure-options (Aggregated Multiservices)

Syntax

```
member-failure-options {
  drop-member-traffic {
    rejoin-timeout rejoin-timeout;
  }
  redistribute-all-traffic {
    enable-rejoin;
  }
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the possible behavior for the aggregated Multiservices (AMS) interface in case of failure of more than one active member.

> **NOTE:** The **drop-member-traffic** configuration and the **redistribute-all-traffic** configuration are mutually exclusive.

Table 32 on page 161 displays the behavior of the member interface after the failure of the first services PIC. Table 33 on page 161 displays the behavior of the member interface after the failure of two services PICs.

> **NOTE:** The AMS infrastructure has been designed to handle one failure automatically. However, in the unlikely event that more than one services PIC fails, the AMS infrastructure provides configuration options to minimize the impact on existing traffic flows.

Table 32: Behavior of Member Interface After One Multiservices PIC Fails

High Availability Mode	Member Interface Behavior
Many-to-one (N:1) high availability support for service applications	Automatically handled by the AMS infrastructure

Table 33: Behavior of Member Interface After Two Multiservices PICs Fail

High Availability Mode	Configuration	**rejoin-timeout**	Behavior when member rejoins before **rejoin-timeout** expires	Behavior when member rejoins after **rejoin-timeout** expires
Many-to-one (N:1) high availability support for service applications	**drop-member-traffic**	Configured	The existing traffic for the second failed member will *not* be redistributed to the other members. The first member to rejoin becomes an active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.	The existing traffic for the second failed member will *not* be redistributed to the other members. The first member will rejoin the AMS automatically. However, the other members who are rejoining will be moved to the discard state.
Many-to-one (N:1) high availability support for service applications	**redistribute-all-traffic**	Not applicable	Before rejoin, the traffic is redistributed to existing active members. After a failed member rejoins, the traffic is load-balanced afresh. This may impact existing traffic flows.	

The remaining statements are explained separately. See CLI Explorer.

Default

If **member-failure-options** are not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds.

Required Privilege Level

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

RELATED DOCUMENTATION

load-balancing-options (Aggregated Multiservices) | 150

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

member-interface (Aggregated Multiservices)

Syntax

```
member-interface interface-name;
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the member interfaces for the aggregated multiservices (AMS) interface. You can configure multiple interfaces by specifying each interface in a separate statement.

Starting with Junos OS Release 16.2, an AMS interface can have up to 32 member interfaces. In Junos OS Release 16.1 and earlier, an AMS interface can have a maximum of 24 member interfaces. If you configure more than 24 member interfaces, you must set the *pic-boot-timeout* value to 240 or 300 seconds at the **[edit interfaces *interface-name* multiservice-options]** hierarchy level for every services PIC interface on the MX Series router.

For high availability service applications like Network Address Translation (NAT) that support many-to-one (N:1) redundancy, you can specify two or more interfaces.

On an MS-MPC, you can configure one-to-one (1:1) redundancy. In a 1:1 (stateful) configuration, a single backup interface provides redundancy for a single active interface. A 1:1 configuration is required for IPsec. 1:1 redundancy is not supported on the MX-SPC3 in this release.

> **NOTE:** The member interfaces that you specify must be members of aggregated multiservices interfaces (mams-).

Options

interface-name—Name of the member interface. The member interface format is mams-*a*/*b*/0, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces for Next Gen Services | 87
Configuring Aggregated Multiservices Interfaces | 93
load-balancing-options (Aggregated Multiservices) | 150

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

rate

Syntax

```
rate new-sessions-per-second;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 9.6.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the maximum number of new sessions allowed per second on services cards.

Options

rate *new-sessions-per-second*—Specify the maximum number of new sessions allowed per second.

Range: 0, which indicates no limit, or greater.

Required Privilege Level

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

redistribute-all-traffic (Aggregated Multiservices)

Syntax

```
redistribute-all-traffic {
    enable-rejoin;
}
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options member-failure-options]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Enable the option to redistribute traffic of a failed active member to the other active members.

For many-to-one (N:1) high availability support for Network Address Translation (NAT), the traffic for the failed member is automatically redistributed to the other active members.

The remaining statement is explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

member-failure-options (Aggregated Multiservices) | 160

redundancy-options (Aggregated Multiservices)

Syntax

```
redundancy-options {
    primary mams-a/b/0;
    secondary mams-a/b/0;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 17.2 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure warm standby for an aggregated multiservices (AMS) interface. Specify a primary and a secondary (backup) member services interface for the AMS interface. The primary interface is the service interface that you want to back up, and it is the active interface unless it fails. The secondary interface is the backup interface, and does not handle any traffic unless the primary interface fails. You can use the same services interface as the backup in multiple warm standby AMS interfaces.

You cannot use both the **redundancy-options** and the **load-balancing-options** statements in the same AMS interface.

Options

primary mams-*a*/*b*/0—Name of the primary services interface, where *a* is the FPC slot number and *b* is the PIC slot number.

secondary mams-*a*/*b*/0—Name of the secondary (backup) services interface, where *a* is the FPC slot number and *b* is the PIC slot number.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Warm Standby for Services Interfaces | 99

rejoin-timeout (Aggregated Multiservices)

Syntax

```
rejoin-timeout rejoin-timeout;
```

Hierarchy Level

```
[edit interfaces interface-name load-balancing-options member-failure-options drop-member-traffic]
```

Release Information

Statement introduced in Junos OS Release 11.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Configure the time by when failed members (members in the **DISCARD** state) should rejoin the aggregated Multiservices (AMS) interface automatically. All members that do not rejoin by the configured time are moved to the **INACTIVE** state and the traffic meant for each of the members is dropped.

If multiple members fail around the same time, then they are held in the **DISCARD** state using a single timer. When the timer expires, all the failed members move to **INACTIVE** state at the same time.

Default

If you do not configure a value, the default value of 120 seconds is used.

Options

rejoin-timeout—Time, in seconds, by which a failed member must rejoin.

Default: 120 seconds

Required Privilege Level

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

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

Example: Configuring an Aggregated Multiservices Interface (AMS)

drop-member-traffic (Aggregated Multiservices) | 132

service-domain

Syntax

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

Hierarchy Level

[edit interfaces *interface-name* unit *logical-unit-number* family inet],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet]

Release Information

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

Description

Specify the service interface domain. If you specify this interface using the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level, the interface domain must match that specified with the **inside-service-interface** and **outside-service-interface** statements.

Options

inside—Interface used within the network.

outside—Interface used outside the network.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring the Address and Domain for Services Interfaces

service-interface (Services Interfaces)

Syntax

service-interface *interface-name*;

Hierarchy Level

[edit services service-set *service-set-name* interface-service]

Release Information

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

Description

Specify the name for the services interface associated with an interface-wide service set.

Options

interface-name—Identifier of the service interface.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces

Applying Services to Subscriber-Aware Traffic with a Service Set

services-options (Next Gen Services Interfaces)

Syntax

```
services-options {
enable-subscriber-analysis
  jflow-log {
    message-rate-limit messages-per-second;
  }
  session-limit {
    maximum number;
    rate new-sessions-per-second;
    cpu-load-threshold percentage;
  }
```

Hierarchy Level

```
[edit interfaces interfaces-name]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series.

Description

Define the service options to be applied on the virtual multi-service (VMS) interface.

This statement is supported only on the MX-SPC3 Services Card.

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.

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-options (Next Gen Services Services)

Syntax

```
service-set-options {
  bypass-traffic-on-exceeding-flow-limits;
  disable-session-open-syslog ;
  enable-asymmetric-traffic-processing;
  inactivity-non-tcp-timeout ;
  max-sessions-per-subscriber
  session-limit;
  session-timeout;
  tcp-session {
    inactivity-asymm-tcp-timeout;
    inactivity-tcp-timeout ;
    open-timeout ;
    tcp-fast-open ;
    tcp-mss ;
    tcp-non-syn ;
    tcp-tickles ;
  }
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Specify the service set options to apply to a service set.

disable-session-open-syslog—Disable session open information from being collected in system logs.

inactivity-non-tcp-timeout —Specify the inactivity timeout period for non-TCP established sessions.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

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

RELATED DOCUMENTATION

Configuring Service Sets to be Applied to Services Interfaces

Configuring APPID Support for Unidirectional Traffic

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

session-limit (Service Set Next Gen Services)

Syntax

```
session-limit {
    maximum number;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Specify the maximum number of sessions allowed simultaneously on the service set. If you specify the maximum number of sessions to be zero, it indicates that the configuration is not effective. You must specify a value higher than zero for the maximum number of sessions.

Options

number—Maximum number of sessions.

Range: 1 through 4,294,967,295

Required Privilege Level

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

RELATED DOCUMENTATION

session-timeout (Service Set Next Gen Services)

Syntax

```
session-timeout seconds;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series.

Description

Define session lifetime for the service set in seconds. The session is closed after this amount of time, even if traffic is running on the session.

Options

seconds—Duration of session.

Range: 4 through 86,400

Required Privilege Level

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

RELATED DOCUMENTATION

size (Next Gen Services Global System Logging)

Syntax

```
size size;
```

Hierarchy Level

```
[edit services rtlog traceoptions file]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Maximum trace file size

Options

size—Maximum trace file size

Default: 128k

Range: through

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

snmp-trap-thresholds (Next Gen Services)

Syntax

```
snmp-trap-thresholds {
    flow high percent low percent;
    nat-address-port high percent low percent;
    session high percent low percent;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series routers (MX240, MX480 and MX960) running Next Gen Services with the MX-SPC3 services card.

Description

Define snmp traps for Next Gen Services service sets.

Options

session—Specify the low and high session threshold limits for generating SNMP traps.

The default for high = 90%.

The default for low = 70%.

Required Privilege Level

system

source-address (Next Gen Services Service-Set Remote System Logging)

Syntax

```
source-address address;
```

Hierarchy Level

```
edit services service-set name syslog
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Specify the IP address of the source for Next Gen Services system log messages.

> **BEST PRACTICE:** The syslog source address can be any arbitrary IP address. It does not have to be an IP address that is assigned to the device. Rather, this IP address is used on the syslog collector to identify the syslog source. The best practice is to configure the source address as the IP address of the interface that the traffic is sent out on.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

stream | 183

stream (Next Gen Services Service-Set Remote System Logging)

Syntax

stream *stream-name* (*severity debug* | *category screen* | *format sd-syslog* | *host*);

Hierarchy Level

edit services service-set *name* **syslog**

Release Information

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the name of the stream to the remote log server.

> **NOTE:** Each remote server requires a unique stream name.

Options

severity debug—

category screen—

format sd-syslog—

host—

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

stream | 183

syslog (Next Gen Services Service-Set System Logging)

Syntax

```
syslog ;
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Configure the filename Next Gen Services system logs.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

tcp-session (Service Set Next Gen Services)

Syntax

```
tcp-session {
    inactivity-asymm-tcp-timeout;
    inactivity-tcp-timeout ;
    open-timeout ;
    tcp-fast-open ;
    tcp-mss ;
    tcp-non-syn ;
    tcp-tickles ;
}
```

Hierarchy Level

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

Release Information

Statement introduced in Junos OS Release 19.3R2 on MX Series.

Description

Configure the TCP options for the service set.

Options

close-timeout—Timeout period for TCP session tear-down (2. through 300 seconds)

ignore-errors—Ignore anomalies or errors for TCP

inactivity-asymm-tcp-timeout—

tcp-tickles—Number of TCP keep-alive packets to be sent for bidirectional TCP flows

inactivity-tcp-timeout—Inactivity timeout period for TCP established sessions

open-timeout—Timeout period for TCP session establishment (seconds)

tcp-fast-open—Tcp-fast-Open enabled packets will be handled accordingly

tcp-mss—Enable the limit on TCP Max. Seg. Size in SYN packets

tcp-non-syn—Deny session creation on receiving first non SYN packet

Required Privilege Level

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

RELATED DOCUMENTATION

tcp-tickles (Service Set Next Gen Services)

Syntax

```
tcp-tickles tcp-tickles;
```

Hierarchy Level

```
[edit service-set service-set-name service-set-optionstcp-session]
```

Release Information

Statement introduced in Junos OS Release 19.3R1 on MX Series.

Description

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

Required Privilege Level

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

RELATED DOCUMENTATION

traceoptions (Next Gen Services Global System Logging)

Syntax

```
traceoptions {
    apply-groups group-names;
    apply-groups-except group-names;
    flag name;
    file filename,
    no-remote-trace;
}
```

Hierarchy Level

```
[edit services rtlog]
```

Release Information

Support introduced in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Specify the trace information you want to include in the system log messages.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

world-readable (Next Gen Services Global System Logging)

Syntax

```
world-readable;
```

Hierarchy Level

```
[edit services rtlog traceoptions file]
```

Release Information

Statement introduced in Junos OS Release 19.3R2 for Next Gen Services.

Description

Allow any user to read the log file

Options

world-readable—Allow any user to read the log file

Required Privilege Level

system

RELATED DOCUMENTATION

Understanding System Logging for Next Gen Services

Enabling Global System Logging for Next Gen Services

Configuring System Logging to One or More Remote Servers for Next Gen Services

Configuring Local System Logging for Next Gen Services

6

CHAPTER

Operational Commands

request system disable unified-services

Syntax

```
request system disable unified-services
```

Release Information

Command introduced in Junos OS Release 19.3R1 on MX Series running Next Gen Services.

Description

Disable Next Gen Services services on the MX Series.

Before you disable Next Gen Services, delete any router configuration for services. This includes configuration under the **[edit services]** hierarchy, configuration for services interfaces, and any configuration that refers to services interfaces.

After you enter **request system enable unified-services**, reboot the chassis.

Required Privilege Level

RELATED DOCUMENTATION

Enabling and Disabling Next Gen Services | 24

List of Sample Output

request system disable unified-services on page 191

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system disable unified-services

`user@host>` **request system disable unified-services**

```
Before disabling unified services, please move to baseline configuration.
Are above conditions satisfied ? [yes,no]
```

request system enable unified-services

Syntax

```
request system enable unified-services
```

Release Information

Command introduced in Junos OS Release 19.3R1 on MX Series running Next Gen Services.

Description

Enable Next Gen Services services on the MX Series.

Before you enable Next Gen Services, delete any router configuration for services. This includes configuration under the **[edit services]** hierarchy, configuration for services interfaces, and any configuration that refers to services interfaces.

After you enter **request system enable unified-services**, reboot the chassis.

Required Privilege Level

RELATED DOCUMENTATION

Enabling and Disabling Next Gen Services | 24

List of Sample Output

request system enable unified-services on page 192

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system enable unified-services

`user@host>` **request system enable unified-services**

```
Before enabling unified services, please move to baseline configuration.
Are above conditions satisfied ? [yes,no]
```

show interfaces load-balancing (Aggregated Multiservices)

Syntax

```
show interfaces load-balancing
<detail>
<interface-name>
```

Release Information

Command introduced in Junos OS Release 11.4.

interface-name option added in Junos OS Release 16.1.

Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display information about the aggregated multiservices interface (AMS) as well as its individual member interfaces and the status of the replication state.

Options

none—Display standard information about status of all AMS interfaces.

detail—(Optional) Display detailed status of all AMS interfaces.

interface-name—(Optional) Name of the aggregated multiservices interface (**ams**). If this is omitted, then the information for all the aggregated multiservices interfaces, including those used in control plane redundancy and high availability (HA) for service applications, is displayed.

Required Privilege Level

view

RELATED DOCUMENTATION

Understanding Aggregated Multiservices Interfaces

Understanding Aggregated Multiservices Interfaces for Next Gen Services | 87

Example: Configuring an Aggregated Multiservices Interface (AMS)

List of Sample Output

show interfaces load-balancing on page 195
show interfaces load-balancing detail on page 196
show interfaces load-balancing detail (Specific Interface) on page 196

Output Fields

Table 34 on page 194 lists the output fields for the **show interfaces load-balancing** (aggregated multiservices interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 34: Aggregated Multiservices show interfaces load-balancing Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices (AMS) interface.	**detail** none
State	Status of AMS interfaces: • **Coming Up**—Interface is becoming operational. • **Members Seen**—Member interfaces (mams) are available. • **Up**—Interface is configured and operational. • **Wait for Members**—Member interfaces (mams) are not available. • **Wait Timer**—Interface is waiting for member interfaces (mams) to come online.	**detail** none
Last change	Time (in *hh:mm:ss* [*hours:minutes:seconds*] format) when the state last changed.	**detail** none
Members	Number of member interfaces (mams-).	none specified
Member count	Number of member PICs (mams) that are part of the aggregated interface.	**detail** none
HA Model	High availability (HA) model supported on the interface. • **Many-to-One**—The preferred backup Multiservices PIC, in hot standby mode, backs up one or more (N) active Multiservices PICs. • **One-to-One**—–The preferred backup Multiservices PIC, in hot standby mode, backs up only one active Multiservices PIC. NOTE: **One-to-One** is not supported on MX-SPC3 cards.	**detail** none

Table 34: Aggregated Multiservices show interfaces load-balancing Output Fields *(continued)*

Field Name	Field Description	Level of Output

Members	Information about the member interfaces:
	• **Interface**—Name of the member interface.
	• **Weight**—Not applicable for the current release.
	• **State**—State of the member interface (mams-).
	  ◦ **Active**—Member is an active member.
	  ◦ **Backup**—Member is a backup.
	  ◦ **Discard**—Member has not yet rejoined the ams interface after failure.
	  ◦ **Down**—Member has not yet powered on.
	  ◦ **Inactive**—Member has failed to rejoin the ams interface within the configured **rejoin-timeout**.
	  ◦ **Invalid**—Multiservices PIC corresponding to the member interface has been configured but is not physically present in the chassis.
		detail

Sync-state	Synchronization (sync) status of the control plane redundancy. The sync state is displayed only when the ams interface is **Up**.
	• **Interface**—Name of the member interface.
	• **Status**—Synchronization status of the member interfaces.
	  ◦ **In progress**—The active member is currently synchronizing its state information with the backup member.
	  ◦ **In sync**—The active member has finished synchronizing its state information with the backup and the backup is ready to take over if the active member fails.
	  ◦ **NA (Not applicable)**—The backup member is not yet ready to synchronize with the active (primary) member. This condition may occur if the backup is still powered off or still booting.
	  ◦ **Unknown**—The daemons are still initializing and the state information is unavailable.
		detail

Sample Output

show interfaces load-balancing

`user@host>` **show interfaces load-balancing**

```
Interface   State       Last change   Members   HA Model
ams0        Up          00:10:02      4         Many-to-One
```

show interfaces load-balancing detail

user@host> **show interfaces load-balancing detail**

```
Load-balancing interfaces detail
Interface         : ams0
  State           : Up
  Last change     : 00:10:23
  Member count    : 4
  HA Model        : Many-to-One
  Members         :
      Interface     Weight   State
      mams-4/0/0    10       Active
      mams-4/1/0    10       Active
      mams-5/0/0    10       Active
      mams-5/1/0    10       Backup
  Sync-state      :
      Interface     Status
      mams-4/0/0    Unknown
      mams-4/1/0    Unknown
      mams-5/0/0    Unknown
```

show interfaces load-balancing detail (Specific Interface)

user@host> **show interfaces load-balancing ams0 detail**

```
Load-balancing interfaces detail
Interface         : ams0
  State           : Up
  Last change     : 00:11:28
  Member count    : 4
  HA Model        : Many-to-One
  Members         :
      Interface     Weight   State
      mams-4/0/0    10       Active
      mams-4/1/0    10       Active
      mams-5/0/0    10       Active
      mams-5/1/0    10       Backup
```

```
Sync-state     :
    Interface    Status
    mams-4/0/0   Unknown
    mams-4/1/0   Unknown
    mams-5/0/0   Unknown
```

show services service-sets statistics syslog

Syntax

```
show services service-sets statistics syslog
<interface interface-name>
<service-set service-set-name>
<brief | detail>
```

Release Information

Command introduced in Junos OS Release 11.1.
Support for this command introduced in Junos OS Release 19.3R2 for Next Gen Services with the MX-SPC3 services card on MX240, MX480 and MX960 routers.

Description

Display the system log statistics with optional filtering by interface and service set name.

Options

none—Display the system log statistics for all services interfaces and all service sets.

brief—(Default) (Optional) Display abbreviated system log statistics.

detail—(Optional) Display detailed system log statistics.

interface *interface-name*—(Optional) Display the system log statistics for a specific adaptive service interface.
On M Series and T Series routers, *interface-name* can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***.

service-set *service-set-name*—(Optional) Display the system log statistics for a specific named service-set.

Required Privilege Level

view

RELATED DOCUMENTATION

clear services service-sets statistics syslog

List of Sample Output

show services service-sets statistics syslog brief on page 202
show services service-sets statistics syslog detail on page 203

Output Fields

Table 35 on page 199 lists the output fields for the **show services service-sets statistics syslog** command. Output fields are listed in the approximate order in which they appear.

Table 35: show services service-sets statistics syslog Output Fields

Field Name	Field Description	Level
Interface	Name of a services interface.	all
Rate limit	Maximum number of messages per second written to the interface's system log.	all
Sent	Number of messages sent that are not associated with a service set.	all
Dropped	Number of messages dropped that are not associated with a service set.	all
Service-set		
Service-set	Name of a service set.	all
Sent	Number of sent messages that are associated with the service set.	all
Dropped	Number of dropped messages that are associated with the service set.	all

Session open logs	The following information is displayed for system log messages for session open events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 35: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

Session close logs	The following information is displayed for system log messages for session close events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Packet logs	The following information is displayed for system log messages for packet events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Stateful firewall logs	The following information is displayed for system log messages for stateful firewall events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 35: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

ALG logs	The following information is displayed for system log messages for ALG events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

NAT logs	The following information is displayed for system log messages for NAT events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

IDS logs	The following information is displayed for system log messages for IDS events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Table 35: show services service-sets statistics syslog Output Fields *(continued)*

Field Name	Field Description	Level

Other logs	The following information is displayed for system log messages for other types of events that are logged and are associated with the service set:
	• **Sent**—Number of messages sent.
	• **Dropped**—Number of messages dropped. Counts are given for these drop reasons:
	  ◦ **low priority**—Priority of the message was too low for the message to be sent.
	  ◦ **no class set**—Specific classes of event messages were configured and this class was not selected.
	  ◦ **above rate limit**—Maximum number of system log messages per second was exceeded.
		detail

Sample Output

show services service-sets statistics syslog brief

user@host> **show services service-sets statistics syslog brief**

```
Interface: sp-1/1/0
  Rate limit: 200000
  Sent: 0
  Dropped: 0
  Service-set: sset-sfw-sp1
    Sent: 20
    Dropped: 3488
  Service-set: sset-nat-sp1
    Sent: 18
    Dropped: 91
Interface: sp-1/2/0
  Rate limit: 15000
  Sent: 0
  Dropped: 0
  Service-set: sset-sfw-sp2
    Sent: 210
    Dropped: 579
```

Sample Output

show services service-sets statistics syslog detail

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

```
Interface: ms-2/1/0
  Rate limit: 0
  Sent: 0
  Dropped: 0
  Service-set: sset1
    Sent: 0
    Dropped: 0
    Session open logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Session close logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Packet logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Stateful firewall logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    ALG logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    NAT logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    IDS logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP MAP logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
```

```
limit: 0)
    PCP protocol logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP protocol error logs:
Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    PCP debug logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
    Other logs:
      Sent: 0
      Dropped: 0 (low priority: 0, none severity: 0, no class set: 0, above rate
limit: 0)
```

For Next Gen Services MX-SPC3 Services Card

Following shows the output for the **show services service-sets statistics syslog** on the MX-SPC3 services cards **vms-x/y/z** interfaces.

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

```
show services service-sets statistics syslog
Log Module Statistics
Interface-Name- vms-2/0/0
Service-set Name- Sset1
Name                  Generated       Discarded
--------------------------------------------
UTM                   0               0
FW_AUTH               0               0
SCREEN                0               0
ALG                   0               0
NAT                   0               0
FLOW                  0               0
SCTP                  0               0
GTP                   0               0
IPSEC                 0               0
```

```
IDP                 0               0
RTLOG               0               0
PST_DS_LITE         0               0
APPQOS              0               0
SECINTEL            0               0
AAMW                0               0
OTHERS              0               0

Log stream Statistics
Interface-Name- vms-2/0/0
Service-set Name- Sset1
Name                send            Fail
--------------------------------------------
database            0               0
```

show services service-sets summary

Syntax

```
show services service-sets summary
<interface interface-name>
```

Release Information

Command introduced before Junos OS Release 7.4.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display service set summary information.

Options

none—Display service set summary information for all adaptive services interfaces.

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

On M Series and T Series routers, ***interface-name*** can be **ms-*fpc/pic/port***, **sp-*fpc/pic/port***, or **rsp*number***.

On MX Series MX240, MX480, and MX960 routers, ***interface-name*** can be **vms-*fpc/pic/port*** for the MX-SPC3 services card for Next Gen Services.

Required Privilege Level

view

List of Sample Output

show services service-sets summary on page 207
show services service-sets summary interface on page 207

Output Fields

Table 36 on page 206 lists the output fields for the **show services service-sets summary** command. Output fields are listed in the approximate order in which they appear.

Table 36: show services service-sets summary Output Fields

Field Name	Field Description
Interface	Name of an adaptive services interface
Service type	Type of adaptive service, such as stateful firewall (SFW), Network Address Translation (NAT), intrusion detection service (IDS), Layer 2 Tunneling Protocol (L2TP), Compressed Real-Time Transport Protocol (CRTP), or IP Security (IPsec)

Table 36: show services service-sets summary Output Fields *(continued)*

Field Name	Field Description
Service sets configured	Total number of service sets configured on the PIC that use internal service set IDs and do not consume external service sets, including CRTP and L2TP
Bytes used	Bytes used by a particular service or all services
Policy bytes used	Policy bytes used by a particular service or all services
CPU utilization	Percentage of the CPU resources being used

Sample Output

show services service-sets summary

`user@host>` **show services service-sets summary**

```
                 Service sets
              CPU
Interface    configured          Bytes used        Session bytes used     Policy
 bytes used      utilization
vms-3/0/0         1         3453621040 (24.93%)         0 ( 0.00%)       8161168
 ( 0.90%)        0.14 %
```

show services service-sets summary interface

`user@host>` **show services service-sets summary interface sp-1/3/0**

```
Interface: sp-1/3/0
                  Service sets                            CPU
  Service type    configured                Bytes used    utilization
  SFW/NAT/IDS               1           54 ( 0.00 %)          N/A
  L2TP                      1           58 ( 0.00 %)          N/A
  CRTP                      1           58 ( 0.00 %)          N/A
  System                    0       920831 ( 0.44 %)          N/A
  Idle                      0            0 ( 0.00 %)          N/A
  Total                     3       921001 ( 0.44 %)          N/A
```

show services sessions (Aggregated Multiservices)

Syntax

```
show services sessions
<brief | extensive | terse>
<application-protocol protocol>
<count>
<destination-port destination-port>
<destination-prefix destination-prefix>
<interface interface-name>
<limit number>
<protocol protocol>
<service-set service-set>
<source-port source-port>
<source-prefix source-prefix>
```

Release Information

Statement introduced in Junos OS Release 16.1 on MX Series.
Support added in Junos OS Release 19.3R2 for Next Gen Services on MX Series routers MX240, MX480 and MX960 with the MX-SPC3 services card.

Description

Display the session information for each service set in each member interface of the AMS interface.

Options

none—Display standard information about all sessions.

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

application-protocol—(Optional) Display information about one of the following application protocols:

- **ftp**—File Transfer Protocol
- **icmp**—Internet Control Message Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rtsp**—Real-Time Streaming Protocol
- **sqlnet**—SQL *Net
- **tcp**—Transmission Control Protocol
- **traceroute**—Traceroute
- **tftp**—Trivial File Transfer Protocol
- **udp**—User Datagram Protocol

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

destination-port *destination-port*—(Optional) Display information for a particular destination port. The range of values is from 0 through 65,535.

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

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

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

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

- ***number***—Numeric protocol value from 0 through 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP encapsulation protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

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

source-port *source-port*—(Optional) Display information for a particular source port. The range of values is from 0 through 65,535.

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

Required Privilege Level
view

List of Sample Output

Output Fields

Table 37 on page 210 lists the output fields for the **show services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 37: show services sessions Output Fields

Field Name	Field Description
Interface	Name of the member interface (**mams-**) and the aggregated multiservices interface (**ams**) to which it belongs.
Session ID	Session ID that uniquely identifies the session.
ALG	Name of the application.
Flags	Session flag for the ALG: • **0x1**—Found an existing session. • **0x2**—Reached session or flow limit. • **0x3**—No memory available for new sessions. • **0x4**—No free session ID available.
IP Action	Flag indicating whether IP action has been set for the session.
Offload	Flag indicating whether the session has been offloaded to the Packet Forwarding Engine.
Asymmetric	Flag indicating whether the session is unidirectional.
Service set	Name of a service set. Individual empty service sets are not displayed.
Sessions Count	Number of sessions.
Flow or Flow Prot	Protocol used for this session.
Source	Source prefix of the flow in the format ***source-prefix:port***. For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.

Table 37: show services sessions Output Fields *(continued)*

Field Name	Field Description
State	Status of the flow: • **Drop**—Drop all packets in the flow without response. • **Forward**—Forward the packet in the flow without looking at it. • **Reject**—Drop all packets in the flow with response. • **Watch**—Inspect packets in the flow. • **Bypass**—Bypass packets in the flow. • **Unknown**—Unknown flow status.
Packet Direction	Direction of the flow: ingress **(I)**, egress **(O)**, or unknown.
Frm count	Number of frames in the flow.

Sample Output

show services sessions brief

user@host> **show services sessions brief**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777217, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.2:63    ->     40.40.40.2:63    Forward  I           85689
UDP         40.40.40.2:63    ->   30.30.30.160:6000  Forward  O               0
```

show services sessions interface mams-5/0/0 extensive

user@host> **show services sessions interface mams-5/0/0 extensive**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.62:63      ->    30.30.30.176:6003
UDP        30.30.30.62:63    ->    40.40.40.62:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
```

```
UDP        40.40.40.62:63    ->   30.30.30.176:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.57:63      ->    30.30.30.163:6003
UDP        30.30.30.57:63    ->    40.40.40.57:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.57:63    ->   30.30.30.163:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0

[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.63:63      ->    30.30.30.165:6004
UDP        30.30.30.63:63    ->    40.40.40.63:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.63:63    ->   30.30.30.165:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.60:63      ->    30.30.30.164:6004
UDP        30.30.30.60:63    ->    40.40.40.60:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.60:63    ->   30.30.30.164:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
```

```
[...output truncated...]
mams-5/0/0 (ams0)
Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.64:63      ->    30.30.30.168:6002
UDP         30.30.30.64:63    ->    40.40.40.64:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP         40.40.40.64:63    ->   30.30.30.168:6002  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.56:63      ->    30.30.30.171:6001
UDP         30.30.30.56:63    ->    40.40.40.56:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP         40.40.40.56:63    ->   30.30.30.171:6001  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

[...output truncated...]
mams-5/1/0 (ams0)
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.61:63      ->    30.30.30.172:6004
UDP         30.30.30.61:63    ->    40.40.40.61:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP         40.40.40.61:63    ->   30.30.30.172:6004  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
```

```
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

NAT PLugin Data:
  NAT Action:   Translation Type - NAPT-44
    NAT source     30.30.30.52:63      ->    30.30.30.175:6003
UDP        30.30.30.52:63    ->    40.40.40.52:63    Forward  I            1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP        40.40.40.52:63    ->   30.30.30.175:6003  Forward  O               0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no

[...output truncated...]
```

show services sessions terse

`user@router>` **show services sessions terse**

```
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.62:63    ->    40.40.40.62:63    Forward  I            2541
UDP        40.40.40.62:63    ->   30.30.30.176:6003  Forward  O               0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.57:63    ->    40.40.40.57:63    Forward  I            2541
UDP        40.40.40.57:63    ->   30.30.30.163:6003  Forward  O               0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.50:63    ->    40.40.40.50:63    Forward  I            2541
UDP        40.40.40.50:63    ->   30.30.30.162:6003  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.48:63    ->    40.40.40.48:63    Forward  I            2541
UDP        40.40.40.48:63    ->   30.30.30.161:6003  Forward  O               0
[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.63:63    ->    40.40.40.63:63    Forward  I            2543
UDP        40.40.40.63:63    ->   30.30.30.165:6004  Forward  O               0
```

```
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.60:63    ->    40.40.40.60:63    Forward  I            2543
UDP         40.40.40.60:63    ->   30.30.30.164:6004  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.59:63    ->    40.40.40.59:63    Forward  I            2543
UDP         40.40.40.59:63    ->   30.30.30.167:6003  Forward  O               0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.58:63    ->    40.40.40.58:63    Forward  I            2543
UDP         40.40.40.58:63    ->   30.30.30.166:6003  Forward  O               0
[...output truncated...]
mams-5/0/0 (ams0)
Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.64:63    ->    40.40.40.64:63    Forward  I            2543
UDP         40.40.40.64:63    ->   30.30.30.168:6002  Forward  O               0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.56:63    ->    40.40.40.56:63    Forward  I            2543
UDP         40.40.40.56:63    ->   30.30.30.171:6001  Forward  O               0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.55:63    ->    40.40.40.55:63    Forward  I            2543
UDP         40.40.40.55:63    ->   30.30.30.170:6001  Forward  O               0
Service Set: napt_set, Session: 16777222, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.51:63    ->    40.40.40.51:63    Forward  I            2543
UDP         40.40.40.51:63    ->   30.30.30.169:6001  Forward  O               0
[...output truncated...]
mams-5/1/0 (ams0)
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.61:63    ->    40.40.40.61:63    Forward  I            2544
UDP         40.40.40.61:63    ->   30.30.30.172:6004  Forward  O               0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.52:63    ->    40.40.40.52:63    Forward  I            2545
UDP         40.40.40.52:63    ->   30.30.30.175:6003  Forward  O               0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP         30.30.30.47:63    ->    40.40.40.47:63    Forward  I            2545
UDP         40.40.40.47:63    ->   30.30.30.174:6003  Forward  O               0
```

```
Service Set: napt_set, Session: 16777230, ALG: none, Flags: 0x2000, IP Action: no,
 Offload: no, Asymmetric: no
UDP        30.30.30.46:63    ->    40.40.40.46:63    Forward  I            2545
UDP        40.40.40.46:63    ->   30.30.30.173:6003  Forward  O               0
[...output truncated...]
```

show services sessions count

user@host> **show services sessions count**

```
Interface   Service set                                                 Sessions count
mams-1/0/0  napt_set                                                                19
mams-1/0/0  ss1                                                                      0
mams-1/1/0  napt_set                                                                18
mams-1/1/0  ss1                                                                      0
mams-5/0/0  napt_set                                                                 9
mams-5/0/0  ss1                                                                      0
mams-5/1/0  napt_set                                                                17
mams-5/1/0  ss1                                                                      0
```

show services sessions service-set

Syntax

```
show services sessions service-set
```

Release Information

Command introduced in Junos OS Release 19.3R2 for Next Gen Services on MX Series.

Description

Display the open and close sessions for a service-set.

Required Privilege Level

show services sessions service-set

`user@host>` **show services sessions service-set *service-set-name***

```
Session ID: 268436944, Policy name: self-traffic-policy/1, Timeout: 554, Valid
Logical system: root-logical-system
  In: 5.5.5.1/12253 --> 70.0.0.2/514;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
Bytes: 84,
  Out: 70.0.0.2/514 --> 5.5.5.1/12253;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
 Bytes: 84,

Session ID: 268436945, Policy name: self-traffic-policy/1, Timeout: 554, Valid
Logical system: root-logical-system
  In: 5.5.5.1/12254 --> 70.0.0.2/514;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
Bytes: 84,
  Out: 70.0.0.2/514 --> 5.5.5.1/12254;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
 Bytes: 84,

Session ID: 268436946, Policy name: self-traffic-policy/1, Timeout: 596, Valid
Logical system: root-logical-system
  In: 5.5.5.1/12255 --> 70.0.0.2/514;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
Bytes: 84,
  Out: 70.0.0.2/514 --> 5.5.5.1/12255;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 1,
 Bytes: 44,

Session ID: 268436947, Policy name: self-traffic-policy/1, Timeout: 554, Valid
```

```
Logical system: root-logical-system
  In: 5.5.5.1/12256 --> 70.0.0.2/514;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
Bytes: 84,
  Out: 70.0.0.2/514 --> 5.5.5.1/12256;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
 Bytes: 84,

Session ID: 268436948, Policy name: self-traffic-policy/1, Timeout: 596, Valid
Logical system: root-logical-system
  In: 5.5.5.1/12257 --> 70.0.0.2/514;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 2,
Bytes: 84,
  Out: 70.0.0.2/514 --> 5.5.5.1/12257;tcp, Conn Tag: 0x0, If: .local..6, Pkts: 1,
 Bytes: 44,
Total sessions: 5
```

show services tcp-log

Syntax

```
show services tcp-log
```

Release Information

Command introduced in Junos OS Release 19.3R2 for Next Gen Services on MX Series.

Description

Display the specified TCP log.

Required Privilege Level

RELATED DOCUMENTATION

Sample Output

show services tcp-log

user@host> **show services tcp-log**

```
user@hst> show services tcp-log log1
Interface: vms-1/0/0

State: Reconnect-In-Progress
    5.5.5.1 -> 70.0.0.2 : 514
```

show system unified-services status

Syntax

```
show system unified-services status
```

Release Information

Command introduced in Junos OS Release 19.3R1 on MX Series.

Description

Determine whether Next Gen Services is enabled or disabled on the MX.

Required Privilege Level

List of Sample Output

show system unified-services status on page 220

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

show system unified-services status

`user@host>` **show system unified-services status**

One of the following four messages appears:

```
Enabled
```

```
Unified Services : Upgrade staged , please reboot with 'request system reboot' to
 enable unified services.
```

```
Disabled
```

```
Unified Services : Upgrade staged , please reboot with 'request system reboot' to
 disable unified services.
```